Department of Defense
Risk Management Guide
for Defense Acquisition Programs

7th Edition (Interim Release)

December 2014

Office of the Deputy Assistant Secretary of Defense for
Systems Engineering

Washington, D.C.

Department of Defense Risk Management Guide for Defense Acquisition Programs, 7th Edition (Interim Release)

Citation:

Department of Defense Risk Management Guide for Defense Acquisition Programs, 7th ed. 2014. (Interim Release). Washington, D.C.: Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030

Email: osd.atl.asd-re.se@mail.mil
Website: www.acq.osd.mil/se

Contents

FIGURES

TABLES

Preface

In his September 24, 2013, white paper, "Better Buying Power 3.0," the Department of Defense (DoD) Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) emphasized his priority to improve leaders' ability to understand and mitigate technical risk. He stated, "Most of product development revolves around understanding and managing risk. Risk management is an endeavor that begins with requirements formulation and assessment, includes the planning and conducting a risk reduction phase if needed, and strongly influences the structure of the development and test program. All this is necessary to minimize the likelihood of program disruption and to maximize the probability of fielding the desired product within reasonable time and cost. Effective risk management is proactive; it goes well beyond merely identifying and tracking risk." This revised edition of the *Department of Defense Risk Management Guide for Defense Acquisition Programs* reflects revisions to emphasize risk management as a proactive tool to assist programs to better understand and mitigate risk throughout the acquisition lifecycle.

This guide is one of several policy and guidance documents the Department is updating to address the USD(AT&L) Better Buying Power initiatives. The documents contain a common thread in emphasizing risk. Although a Risk Management Plan (RMP) is not mandatory, Program Managers (PM) are responsible for managing risk in accordance with the mandatory requirements contained in the DoD Instruction (DoDI) 5000.02, "Operation of the Defense Acquisition System," and are required to outline their risk management strategy in accordance with the Systems Engineering Plan (SEP) Outline (2011). DoDI 5000.02 requires PMs to identify top program risks and associated risk mitigation plans in the program acquisition strategy and to present that status at all relevant decision points and milestones. Acquisition professionals may debate the best approach for managing risk, but they agree that effective qualitative and quantitative risk, issue, and opportunity management are critical to a program's success.

This guide asserts that risk management should be forward-looking, structured, continuous, and informative. The risk, issue, and opportunity management approach presented should be tailored to the scope and complexity of each program's individual needs.

This guide is organized as follows:

Chapter 1: Introduces the scope and changes in this revised edition of the DoD risk management guide.

Chapter 2: Discusses how to document the program's risk management approach in the SEP, the Systems Engineering Management Plan (SEMP), the Acquisition Strategy, and the Risk Management Plan (RMP). Specifically, it discusses the organization and techniques for establishing an effective and systemic risk management approach before implementing a risk management process. **Risk planning** is the process to develop and document the approach that lays out the methods and responsibilities for executing risk management to include selecting the appropriate risk management tools.

Chapter 3: Provides step-by-step guidance for developing a **risk management process.** It discusses the four steps in the risk management process: identification, analysis, mitigation, and monitoring of risks.

Chapter 4: Discusses proactive risk management through integrating with other program management tools such as the Work Breakdown Structure (WBS), Integrated Master Schedule (IMS), Integrated Master Plan (IMP); and techniques such as Schedule Risk Assessments (SRA) and Cost Risk Assessment Techniques.

Chapter 5: Seeks to define the **issue management process** as a distinct and important management process. An issue is an event or situation with negative consequences that has already occurred. Because issues have negative impacts on the program, they are often inappropriately managed as risks.

Chapter 6: Discusses the application of opportunity management including the similarities and differences to risk management. The **opportunity management process** is examined for undertaking potential enhancements to a program so the PM and functional leads can identify and implement initiatives to yield improvements in the program's cost, schedule, and/or performance baseline. Opportunity management enables achieving "should" versus "will" costs discussed in Better Buying Power 2.0 (USD(AT&L) 2012).

Chapter 7: Highlights considerations to manage risks related to internal and external interfaces with **interdependent programs.** It discusses the different priorities of interdependent programs and techniques to manage and control cross-program risks.

Most sections contain a text box with expectations that warrant "foot-stomping," or emphasizing, to improve the planning and execution of risk management processes and techniques.

1 INTRODUCTION

1.1 Purpose

This guide seeks to inform Department of Defense (DoD) stakeholders regarding the effective use of the DoD risk management process to pinpoint and avoid potential program risk. It promotes the DoD process to identify, analyze, mitigate, and monitor risks, issues, and opportunities. Proactively addressing not only risks but also issues and opportunities can help programs achieve cost, schedule, and performance objectives at every stage of the life cycle.

For the purposes of understanding this guide, the terms risk, issue, and opportunity are defined as:

Risk: Risks are future uncertainties relating to achieving program technical performance goals within defined cost and schedule constraints. Defined by (1) the probability of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur

Issue: Issues are current problems (realized risks) that should be addressed with action plans, resourced and resolved

Opportunity: Opportunities are events that may or may not occur that have the potential for improving the program in terms of cost, schedule, and performance. PMs should use opportunity management to identify, analyze, plan, implement, and track initiatives that can yield improvements in the program's cost, schedule, and/or performance baseline by reallocating program resources. Defined by (1) a likelihood of the future event occurring and (2) a benefit associated with the future event.

Figure 1-1 displays the technical, programmatic, and business events that can lead to opportunities, risks, or issues that have cost, schedule, or performance consequences.

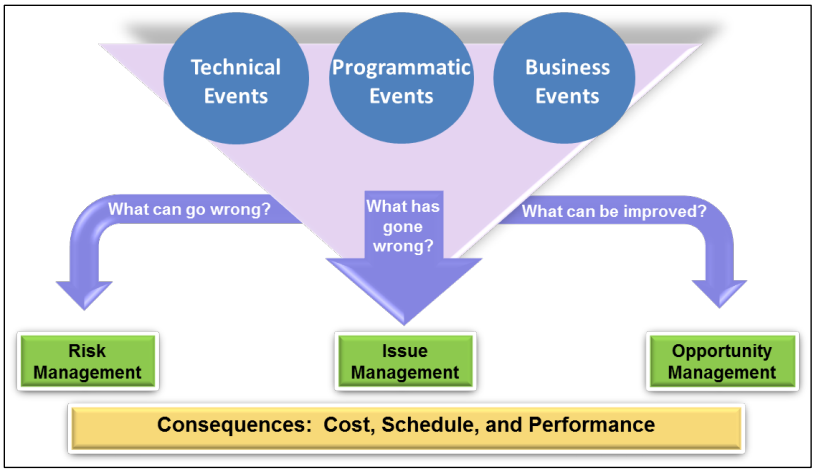


Figure 1-1. Overview

The DoD risk management process is fundamental to acquisition program success. The PM is responsible for implementing effective risk management in accordance with DoDI 5000.02, Enclosures 2 and 3. This guide will assist DoD and contractor PM's, Chief or Lead Systems

Engineers, program offices, Integrated Product Teams (IPT), working groups, and others involved in implementing risk management starting with a program's inception and continuing through disposal. PMs are encouraged to apply the fundamentals presented here to improve the management of their program.

This guide should be used in conjunction with related directives, public law (Title 10 and the Weapon Systems Acquisition Reform Act of 2009), DoDI 5000.02 ("Operation of the Defense Acquisition System"), Defense Acquisition Guidebook (DAG) Chapter 4 (Systems Engineering), Military Department guidance, instructions, policy memoranda, and regulations issued to implement risk management in DoD acquisition programs.

1.2 Scope

This guide provides a basic understanding of risk management concepts as well as methods of implementation, so programs can select the appropriate mitigation for their situation. The practice of risk management draws from many management disciplines, including but not limited to program management, systems engineering, earned value management, production planning, quality assurance, logistics, and requirements definition. The risk management approach and process should be tailored to fit the regulatory, statutory, and program requirements depending on where a program is in the life cycle.

DoD clearly distinguishes mandatory policy from recommended guidance. This document serves solely as guidance for risk management approaches for DoD acquisition programs. The management concepts presented encourage the use of risk-based management practices along with a detailed process for risk, issue, and opportunity management. This guide does not attempt to address the requirements to prevent and manage environment, safety, and occupational health (ESOH) hazards. The reader should refer to MIL-STD-882E, Standard Practice for System Safety, for guidance regarding ESOH hazards.

This revision emphasizes areas that have emerged during Office of the Secretary of Defense (OSD) program reviews as potential areas for improvement across the range of DoD programs:

- Quantitative risk management
- Integration of risk management with other program management tools
- Issue management
- Opportunity management
- Managing risks with external programs
- Risks and proactive control activities throughout the acquisition life cycle phase

1.3 Risk Management Overview

Risk is the combination of (1) the probability of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur. The undesired event may

be programmatic or technical, and either internal or external to the program. Although a future event may include positive opportunities, risk is considered to be the potential for a negative future event.

Risk management should be fully integrated with the systems engineering and program management process and should be applied beginning with the Analysis of Alternatives (AoA). Properly implemented and resourced, risk management enhances program management effectiveness and equips PMs with the tools needed to reduce life cycle costs (LCC) and increase the program's likelihood of success. Without effective risk management planning and implementation, the program office could find itself conducting high-stakes crisis management.

Through the risk management process, a program assesses the likelihood or probability of a future event and evaluates the consequences or severity of the event should it occur. The program identifies the origin of the risks in order to mitigate them before they become issues. Successful risk management requires early planning, resourcing, and aggressive implementation. Through risk management, program teams identify risk events that could prevent the program from achieving objectives. The program is able to make decisions with a full awareness of the likelihood and consequence of the risks involved.

The DoDI 5000.02 and Better Buying Power 2.0 both emphasize risk management. The objective is to provide a repeatable process throughout all acquisition phases. It is essential that programs define, implement, and document an appropriate risk management approach that is organized, comprehensive, and iterative by addressing the following questions:

1. Risk Identification: What can go wrong?
2. Risk Analysis: What is the likelihood and consequence of the risk?
3. Risk Mitigation: Should the risk be accepted, avoided, transferred, or controlled?
4. Risk Monitoring: How has the risk changed?

Figure 1-2 illustrates the risk management process.

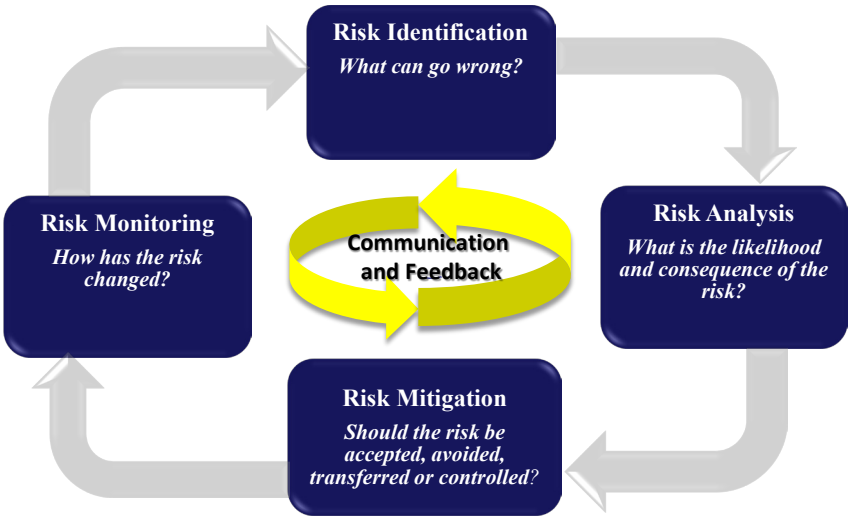


Figure 1-2. Risk Management Process

2 ESTABLISHING AN EFFECTIVE RISK MANAGEMENT APPROACH

2.1 Risk Management Planning

The first step in developing a risk management process is planning, during which a program selects the best overall approach (organization, tools, methods) for that program. If program-related activities begin in the Materiel Solution Analysis (MSA) phase, risk planning should begin with the AoA, during which stakeholders assess the technology maturity, integration, manufacturing feasibility, and schedule risks associated with each proposed materiel solution.

Effective risk management requires an efficient process for identifying risk early, analyzing the risk event likelihood and consequence, mitigating risk, and monitoring risk status. Acquisition programs may vary in complexity, from the simple procurement of existing systems to development of state-of-the-art advanced technology systems; however, effective risk management approaches have consistent characteristics and follow common guidelines regardless of program size. Progression through the risk management process should be similar among programs, but the level of detail and insight will depend on the program phase. At any point of the risk management process, the risks should be traceable to the technical requirements and overall program objectives.

The PM should begin planning and establishing the risk management process as soon as practical after establishment of the program office. As illustrated in Figure 2-1, the risk management process is closely linked with a program's cost, schedule, and performance metrics. The risk management process should remain an integral part of the program management process rather than a separate, isolated activity and should be implemented throughout the program's life. Issues and opportunities should be an element of the PM process but are managed differently than risks.

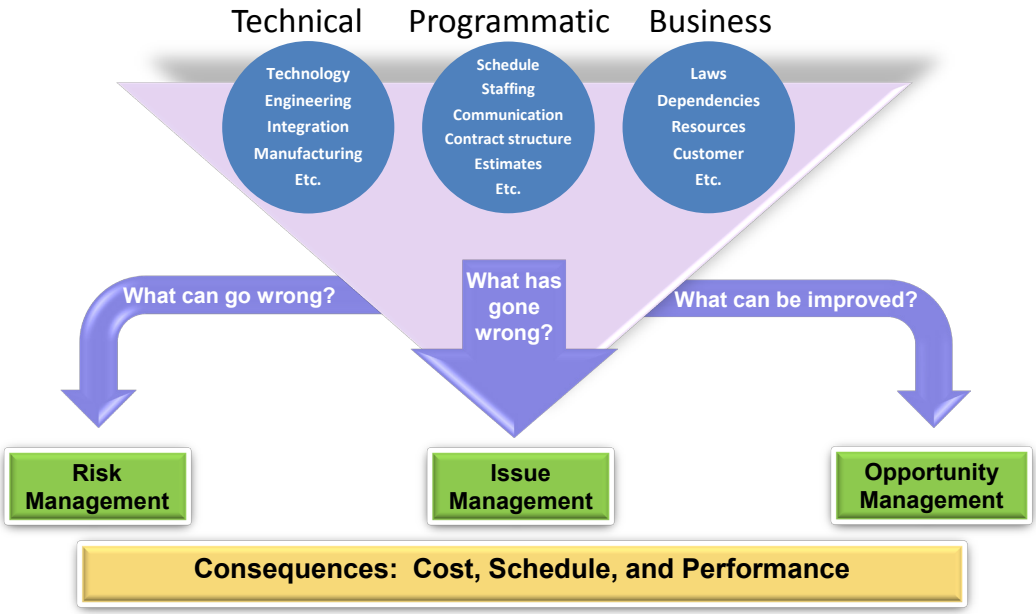


Figure 2-1. Risk, Issue, and Opportunity Relationship

2.2 Aligning Government and Contractor Risk Management

The Government program office, the prime contractor program office, and associated subcontractors should employ a consistent risk management process and establish a joint risk management database. Risk management is not a stand-alone program office task but should be integrated with other processes, such as requirements development; design, integration, and test (systems engineering); planning and management of system support and sustainment; schedule tracking; performance measurement; Earned Value Management (EVM) (when implemented); cost estimating; issue management; and so on.

Program offices usually create a Risk Working Group (RWG), with a representative from each IPT and led by a member of the Systems Engineering IPT. This group meets regularly and performs the risk management work. The RWG is empowered to draw on expertise from inside the program and from identified sources outside the program to help create individual risk plans and make needed recommendations that are forwarded to the Risk Management Board (RMB). The RMB is the approval authority for risk mitigation plans. The frequency of RMB meetings is tailorable and depends on the program.

The Government SEP and the contractor's Systems Engineering Management Plan (SEMP) are two important risk planning and management tools available to the PM. The SEP and SEMP are blueprints for all technical aspects of an acquisition program and at a minimum should describe:

- The process for how the program plans to manage risks
- How the risk management processes are integrated with the contractor(s) processes
- How the program identifies and analyzes risks
- How the program plans for, implements (including funding), and tracks risk control
- Key roles and responsibilities from working groups, through the IPT structure up to the executive level
- RMB, who chairs, membership, and meeting frequency
- Risk tool(s) that the program office and contractor use to perform risk management

2.3 Risk Management Plan

Although a program office summarizes the risk management approach and documents the program risk management planning activities in a SEP, SEMP, and Acquisition Strategy, the program may prepare a Risk Management Plan (RMP) to document the process in more detail. Risk management planning should be documented during the initial phase of program formulation and updated for each subsequent acquisition phase in all increments of the program. A good RMP should:

- Document an organized, comprehensive, and integrated approach for managing risks
- Define the goals, objectives, and the program office's risk management processes
- Document an approach to identify, analyze, mitigate, and monitor risks across the program
- Define the methods and processes used to execute a PM's RMP

- Help the program plan for adequate resources, including personnel, schedule, and budget
- Document sound issue and opportunity management approaches

Although not mandated by DoD policy, the RMP explains how the program manages risks to achieve future cost, schedule, and performance goals. For example, the RMP should outline how the program office resources the risk, issue, and opportunity management activities and subsequent risk mitigation plans to be effective. The program office should establish the basic approach and working structure it will use, and document that approach in an RMP. A comprehensive and consistent approach ensures all aspects of the program are examined for risk. As a program transitions through developmental and operational testing and sustainment, the program team should update the RMP to identify, assess, and control risks that have an impact on overall program cost, schedule, and/or performance. Following is an example of an RMP outline:

- **Introduction** – Overview of the purpose and objective of the RMP.
- **Program Summary** – Brief description of the program including the connection between the Acquisition Strategy, program management strategy, and technical strategy.
- **Definitions** – DoD definitions and definitions specific to the program to be used throughout the guide.
- **Risk Management Strategy –** Overview of the strategy to implement continuous risk management, to include communication between stakeholders and training of the program team in the risk management process and procedures.
- **Roles, Responsibilities, and Authorities –** Description of roles, responsibilities, and authorities within the risk management process for:
    - Reporting/identifying risks
    - Providing resources to control risks
    - Criteria used to determine if a "risk" submitted for consideration will become a risk or not (typically, criteria for probability and consequence)
    - Adding/modifying risks
    - Changing likelihood and consequence of a risk
    - Closing/retiring a risk
- **Risk Management Process and Procedures** – Description of the program risk management process, methodology, meeting battle rhythm, and guidance for implementing the plan, according to the tailorable four-step DoD process:
    - Risk Identification
    - Risk Analysis
    - Risk Mitigation
    - Risk Monitoring
- **Risk Management Tools –** List of the risk tool(s) the program (program office and contractor(s)) use to perform risk management. (If the program office and contractor(s) use

different risk tools, this section would include a description of how the information will be transferred between them. NOTE: In general, the same tool should be used. If the contractor's tool is acceptable, then this merely requires the contractor to provide Government access).

- **Risk Assessment Techniques** – Summary of the cost, schedule, and performance assessment processes, including procedures for assessing risks:
    - Overview and scope of the assessment process
    - Sources of information
    - Planned frequency of assessments
    - Products and formats
    - Assessment technique and tools
- **Communicating and Feedback Process** – Process for communicating the status of potential, current, and retired risks as well as opportunities that may exist to all personnel involved in risk management.

Typically, program offices define the documentation and reporting procedures as part of the risk management planning before contract award. The program office may add or modify this planning during contract execution as long as the efforts remain within the scope of the contract or are approved as part of a contract change. The program office should periodically review the RMP and revise it, if necessary. Events that may drive the need to update it include an upcoming acquisition milestone decision, following a system-level technical review, a change to the Acquisition Strategy after a contract award, or after program re-baselining.

Expectations

- The Government requires an RMP, IMP, and IMS in the Request for Proposal (RFP). The Government includes a copy of the risk, top-level schedule, WBS, and SEP in the proposal to inform the development of the contractor's proposal. The contractor's SEMP, provided with the proposal, provides the contractor's aligned approach to risk management.
- A SEP, SEMP, and RMP include a detailed plan of action for the management and identification of who, what, where, when, and how. These approved documents empower the lead systems engineer to execute the program's technical planning, including its risk management program.
- The Government and contractor team (prime and subcontractors) establish common risk management processes and definitions. The program office, prime contractor, and subcontractors also establish a joint risk management database.

2.4 Selecting a Risk Management Tool

Risk management tools support the implementation and execution of quantitative risk management. The PM needs to select the right risk management tool early and document details within the RMP. Some questions to consider when selecting the risk management tool are as follows:

- Support Objectives – Does the tool aid in meeting program objectives?
- Recurrence – Will the risk management process include continuous updates?
- Helpfulness – Will the tool be useful during the decision-making process?
- Accessibility – Will the tool be accessible to all users, perhaps remotely, including certain tool licensing requirements?
- Integration – Does the tool aid in the integration with other program management tools and processes?
- Requirements – Does the tool comply with IT security requirements?

Expectations:

- The Government program offices and contractors select and use a common risk management tool to collectively identify, analyze, mitigate, and monitor risks, issues, and opportunities. Access to the risk management tool is available through an Integrated Data Environment. When practical, key subcontractors and external programs employ the same risk management tool and processes.
- If multiple contractors are competing during an acquisition phase, firewalls are established in the tool to prevent contractors from viewing one another's data regarding technical and programmatic risks.

2.5 Risk Management Roles and Responsibilities

An effective risk management process requires the support and commitment of the entire acquisition team, including stakeholders, Government and contractor program offices, program teams, Sub-Integrated Product Teams, working groups, support personnel, and subject matter experts (SME). The program and contractor should clearly define the roles and responsibilities in the SEP, SEMP, Acquisition Strategy, and RMP and execute them throughout the acquisition life cycle.

When formulating roles and responsibilities, programs should consider resources. Design maturity and associated technical risks are key considerations when program offices and the Milestone Decision Authority select their contracting strategy. This requires PMs and contractors to balance program priorities with high-value risk mitigation activities.

For example, a firm fixed priced contract is usually employed on programs with mature designs or when the technical risks are minimal and can be predicted with an acceptable degree of certainty. On firm fixed priced contracts, PMs should reach an agreement with contractors on what key risks must be mitigated, when progress will be measured, and any appropriate contract options. Other than these agreed-to risks, prime contractors selectively resource risk mitigation activities that they feel are warranted to support delivering a system on time which meets the requirements in the specification.

On the other hand, cost type contracts are employed on programs where the inherent technical risks are less clear and potentially undefined so programs need to allocate sufficient resources to mitigate emerging risks. The sufficiency of funds available to address emerging risks should be reevaluated during budget cycle reviews as well as prior to acquisition milestones and the award of follow-on contracts. With both types of contracts, there is a defined process for allocating scarce resources to mitigate identified risks based on their likelihood and consequences (cost, schedule, and/or performance).

Communicating and reviewing the status of each risk is key to ensuring all personnel involved in risk management have a clear understanding of the progress being made in controlling risks. It involves presenting and sharing the current likelihood and consequence, along with an assessment of the current status of the mitigation plan chosen. This allows straightforward knowledge of delayed, missed, or failed mitigation actions. Figure 2-2 shows a sample of routine program-related meetings that are candidates for discussing risk status.

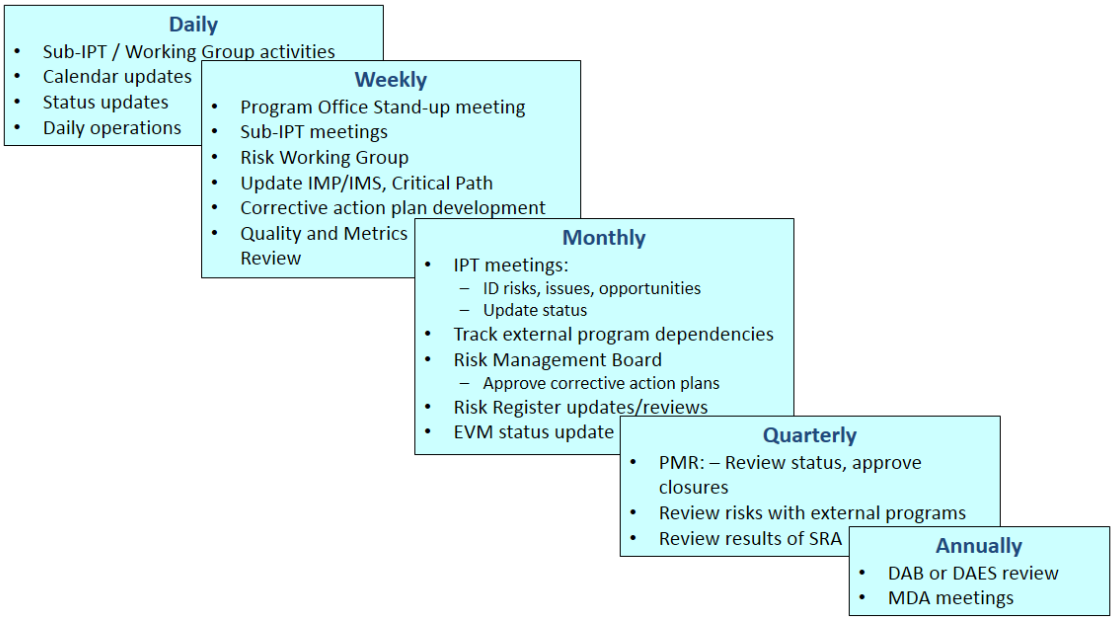


Figure 2-2. Sample Risk Management–Related Battle Rhythm

Organizing and training the team to follow a disciplined, repeatable process for conducting risk management is critical, since major program decisions during the program life cycle need the support of periodic assessments. Experienced teams do not necessarily require extensive training, but team members should review lessons learned from earlier programs. The program's risk manager, or an outside expert, may train the team, focusing on the program's risk management planning documented in the SEP, SEMP, Acquisition Strategy, and RMP. A risk management training package for the core team and SMEs is often beneficial and could be accomplished at the start-of-work meeting. This package typically includes the risk management approach, analysis criteria, documentation requirements, team ground rules, and a program overview.

Figure 2-3 displays the hierarchy typically involved in risk management. These core groups and individuals all play a part in the risk management process to identify, analyze, and report risks to the next higher level when they exceed that level's ability to mitigate. These groups provide an array of expertise in areas such as systems engineering, logistics, manufacturing, test, schedule analysis, contracting, cost control/estimating, earned value management, and software development.

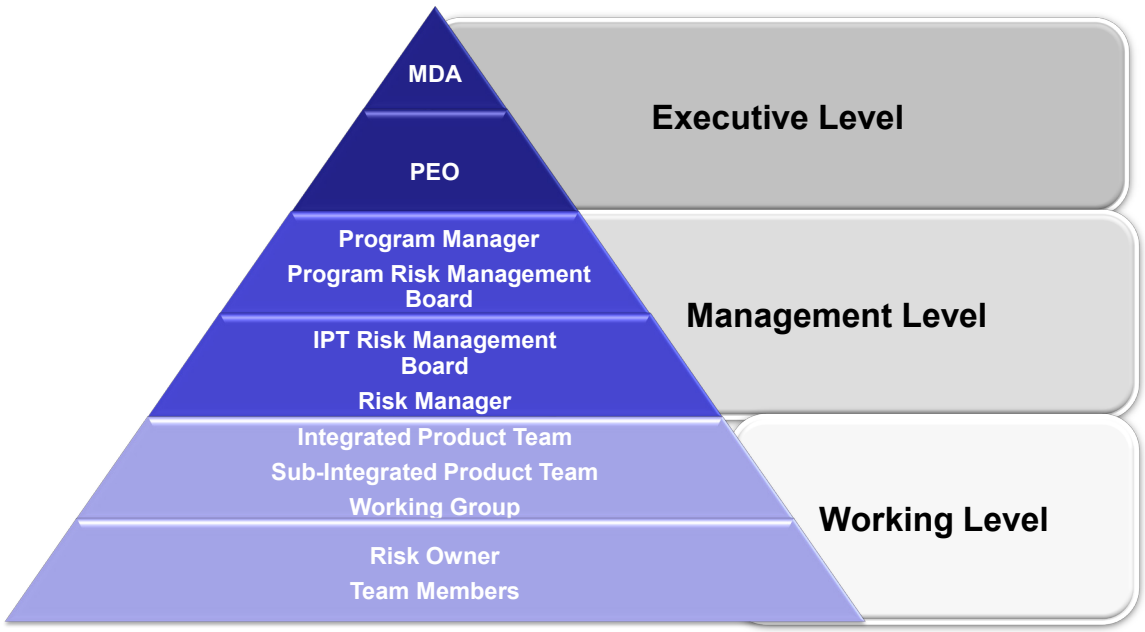


Figure 2-3. Roles and Responsibilities Tiering

Many impediments exist in implementing risk management, but it is the responsibility of everyone on the risk management team to work together to overcome obstacles that may prevent program success. The following responsibilities are recommended for inclusion in the RMP:

2.5.1 Executive Level

Milestone Decision Authority (MDA)

- Tailors program strategies and oversight, based on the specifics of the product being acquired including complexity, risk factors, and required timelines to satisfy validated requirements.
- Approves programs proceeding into the next acquisition phase based on an understanding of the technical, cost, and schedule risks of acquiring the product, and the adequacy of the plans and programmed funding to mitigate those risks.
- Considers the risks that could result from fielding incremental capabilities or features that provide military utility to the warfighter on schedule and within the allocated funding.
- Provides direction regarding management and control of cross-Service (external) program-level or "special interest" risks and issues.
- Ensures the program's planned risk activities, such as risk reduction and competitive and risk reduction prototyping during the Technology Maturation and Risk Reduction (TMRR) phase, are sufficient to reduce technology, engineering, integration, and life cycle cost risks to support authorizing a program to transition from development to production.
- Assesses the use of opportunity management to aid in proactive cost control throughout the acquisition life cycle and achieve "should" versus "will" costs.

Program Executive Officer

- Ensures program Statement of Objectives (SOO), Statements of Work (SOW), and Contract Deliverable Requirements Lists (CDRL) include provisions to support a defined program RMP and process.
- Approaches risk management not only from an individual program perspective, but also from a portfolio and system-of-systems perspective.
- Works with other Program Executive Offices (PEO) to identify shared concern, opportunities for leverage, and areas to optimize programs by identifying gaps and redundancies within portfolios.
- Executes program oversight by monitoring and assessing program-level and special interest risks and execution of risk mitigation plans.
- Provides direction regarding management and control of cross-PEO (external) and PEO portfolio (internal) program-level or special interest risks and issues.

2.5.2 Management Level

Program Manager

- Complies with statutory and regulatory risk management requirements.

- Establishes and executes an integrated risk management process with the contractor and key subcontractors.
- Ensures development and approves the program's RMP.
- Ensures the appropriate disciplines are involved in the program risk management process (program management, engineering, contracting, legal, financial management, EVM (cost account managers and cost schedule analyst), logistics, manufacturing, test and evaluation, quality assurance, system safety).
- Forms and chairs a program RMB to include Deputy PMs, IPT chairpersons, risk management coordinator, chief or lead systems engineer, program logistician, budget and financial manager, contracting officer, legal, prime contractor, and other members relevant to the program strategy, phase, and risks.
- Communicates program-level and special interest risk status, using the program's approved risk reporting format, during stakeholder meetings (Defense Acquisition Board (DAB), Overarching Integrated Product Team (OIPT), PEO review, user exchange meeting), program reviews, technical reviews, risk review board meetings, and other appropriate battle rhythm meetings.
- Assigns responsibility for risk management activities, monitors progress, and includes stakeholders in the formulation and acceptance of risk mitigation plans.
- Provides resources as necessary to effectively manage risks, issues, and opportunities. Maintains management reserve to allocate, as necessary, to IPTs if there are risks with executing the work packages within cost and schedule.
- Includes design, development, production, and support considerations in acquisition planning as well as the cost, schedule, and performance trade-space activities to manage risks.

Program Risk Management Board

- Ensures the risk management process is executed in accordance with the program's approved RMP, and risk management efforts at the working level are integrated.
- Reviews identified risks, approves proposed risk mitigation plans, to include adequacy of resources, and any changes to the approved plan.
- Monitors the status of risk mitigation efforts, inclusive of resource expenditures and quantitative assessment of risk reduction.
- Continually assesses the program for internal and external risks and changes in program strategy that might introduce new risks or change existing risks.
- Reports risk information, metrics, and trends using the program's approved risk reporting format, to senior management personnel (PM/PEO/MDA) and other stakeholder personnel.
- Determines which risks are managed at the program or special interest level and which are managed at the IPT or working group levels.

- Assigns valid risks to an owner for development of a plan.

IPT Risk Management Board/Risk Working Group

- Reviews the risks owned by the IPTs.
- Determines if new risk assessments and plans are adequate.
- Tracks the status of each IPT level risk mitigation plan.
- Approves risk closure for IPT level risks and notifies the program RMB of closure.
- Approves IPT level risk mitigation plans.

Risk Manager

- Manages the risk process and tools for effective use by teams.
- Serves as advisor at IPT and program RMB meetings.
- Maintains the RMP.
- Provides risk management training.
- Maintains the risk register.
- Facilitates risk assessments.
- Completes an initial screening of risks.
- Prepares risk briefings, reports, and documents required for program reviews.

2.5.3 Working Level

Integrated Product Teams, Sub-Integrated Product Teams, Working Groups

- Develop and implement the risk planning outlined in the SEP, SEMP, Acquisition Strategy, and/or RMP, and support the program PM and RMB as required.
- Identify internal and external risks in accordance with the procedures documented in the program's approved RMP. Recommend to the PM and RMB which risks should be tracked as program level or special interest risks.
- Identify risks that impact multiple IPTs, coordinate risk management efforts with affected IPTs, and recommend to the RMB which IPT should take the lead in managing the risk.
- Continually assess risks using documented risk assessment criteria. Conduct tailored program risk assessment for each of the applicable technical reviews and for each key program decision point.
- Recommend risk mitigation options, estimate funding requirements to implement risk mitigation options, support implementation of the selected risk mitigation plan, and track progress of risk mitigation efforts.

- Report risk status to the PM and RMB using the reporting requirements documented in the program's approved RMP.
- Assist the PM, as required, in reporting risk status to senior management personnel (PM/PEO/MDA) and other stakeholder personnel.
- Identify the need for risk management training of IPT personnel.
- Periodically revisit previously identified risks to verify the risk level is still accurate as the program progresses or changes over time.
- Support engineering trade-off analyses to ensure risk elements are considered during performance, cost, and schedule trade space excursions.

Risk Owner

- Determines the initial risk likelihood and consequence assessments.
- Develops the mitigation options and control plan for the risk item and a fallback plan for high-level risks.
- Develops cost consequence and mitigation strategy costs should the risk be realized.
- Presents changes to the baseline mitigation plan to the program or IPT RMBs, as appropriate, for approval.
- Controls the risk and implements the risk mitigation plan.
- Delegates risk events to other individuals or teams as required or dictated by expertise.

Team Members

- Identify and submit risk candidates.
- Support execution of the risk management process.

2.5.4 Government and Contractor Relationship

A close relationship between the Government and the contractor promotes an understanding of program risks as the team develops and executes management efforts. Although the Government PM has ultimate responsibility for risk management, the prime contractor's support and assistance are integral to a successful risk management program. The Government does not dictate how the contractor should manage risk, but both the Government and contractor need to share information, understand the risks, and develop and execute management efforts. To promote early mutual understanding, the RFP should address the general character of risk management execution, providing an opportunity for the offeror's proposal to include the nature of tasks, processes, and tools to be employed for risk management. The offeror should delineate the participation of the Government and the contractor in implementing a transparent, collaborative, and proactive risk management process. Contract type and terms should serve to align overall Government and contractor interests and should be consistent with an effective risk management program.

Government Responsibilities

- Involve the contractor as early as possible so that effective risk management can occur.
- Include contract provisions that foster contractor flow down of risk management requirements to subcontractors.
- Recognize that the contractor may treat risk differently from the Government due to differences in Government and contractor business and program viewpoints.
- Address with the contracting officer any subtleties in contract provisions that could affect the success of the risk management program, including applicable incentives for effective risk management as manifested by accomplishment of defined program objectives (known challenging design or integration tasks accomplished within constrained resources).
- Ensure systems engineering trade-off analyses show results of capability excursions around expected design performance points to highlight risk elements that can be used to establish cost and schedule trade space.
- Reflect program design and development considerations in acquisition planning and cost, schedule, and performance trade-space activities to manage risks.
- Evaluate the results of competitive and risk reduction prototyping to assess the risk related to design maturity and achieving program objectives.
- Conduct Schedule Risk Assessments of offerors' proposals to support the source selection decision process.
- Reflect the effectiveness of the contractor's risk management effort in the Contractor Performance Assessment Report System evaluation.
- Execute an effective risk management process to help achieve program objectives.

Contractor Responsibilities, Consistent with Contract Provisions

- Develop an internal risk management program and work jointly with the Government program office to develop an overall risk management program; include the risk management approach in the proposal.
- Flow down risk management requirements to subcontractors, to include consistent risk management processes and definitions, and integrate their risk management process with the overall program risk management effort.
- Conduct risk identification and analysis during all phases of the program, including proposal development, and apply appropriate risk mitigation strategies and plans.
- Assess the impact of risks during proposal and baseline development.
- Maintain a joint risk management tool and database; provide remote access to Government counterparts.

- Support, as required, Government risk management efforts, such as the RMB; reporting to senior management personnel and other stakeholders; and risk management training of IPT personnel.
- Report risk status to company management and Government personnel during program reviews, technical reviews, and other appropriate recurring meetings.
- Jointly conduct Integrated Baseline Reviews (IBR) with the Government team to reach mutual understanding of risks inherent in the program baseline plans.
- Conduct schedule risk analyses at key points during all phases of the program, including proposal development.
- Incorporate risk control activities into IMS and program budgets as appropriate.
- Synthesize and correlate the status of new and ongoing risk elements in the IMS, Contract Performance Report, risk control plans, estimates at completion, technical status documentation, program status reviews, and other sources of program status.

3 RISK MANAGEMENT PROCESS

Figure 3-1 depicts risk management as a four-step process to identify, analyze, mitigate, and monitor program risks.

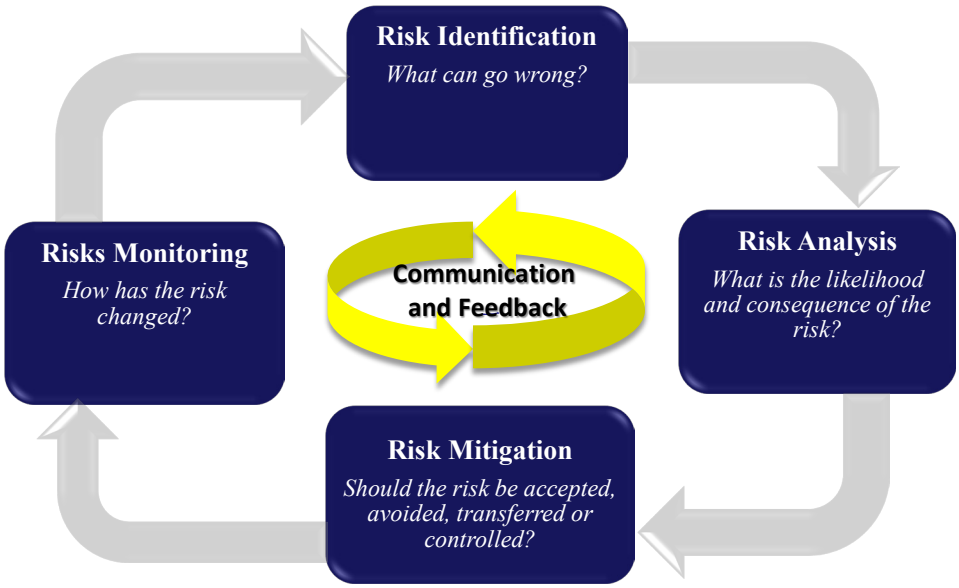


Figure 3-1. Risk Management Process

3.1 Risk Identification

The first activity in the risk management process is to identify risks by answering the question, *What can go wrong?* This step involves examining the technical aspects of a program to determine risk events (root causes) that may have negative cost, schedule, and performance impacts. To help identify risk root causes, the program team should ask "why" the event or condition is a risk, and then repeat the question "why" to reveal the causal factors that lead to the underlying root cause. The team continues the activity until it identifies the risk root cause as well as the specific causal factors.

This process is extremely important, not only for understanding the probability of the risk but also to help pinpoint the specific risk mitigation options and actions needed to address the root cause. It is the responsibility of every member of the program team, not just the PM, the systems engineer, the product support manager, or the risk manager, to identify risks. Risk identification is conducted continuously by all Government and contractor program team members.

The PM is responsible for examining and compiling identified risks, such as in a risk register (see section 3.2.4), and to summarize them at a manageable level of detail. This register allows for streamlining a large and diverse number of potential risks down to the most significant risks that warrant control activities.

In order to identify and manage risks, all personnel involved with the program should have a clear understanding of the program's requirements, goals, plans, and supporting analysis. An understanding of the following program-related documents helps the program personnel identify sources of potential risk:

- Analysis of Alternatives (AoA)
- Acquisition Strategy
- Acquisition Program Baseline (APB)
- Systems Engineering Plan (SEP)
- Systems Engineering Management Plan (SEMP)
- Integrated Master Plan (IMP)
- Contractor's Integrated Master Schedule (IMS)
- Contract structure and provisions

Early communication between the user requirements community and the acquisition community in the development of Joint Capabilities Integration and Development System (JCIDS) documents helps requirements leaders and acquisition leaders to identify poor requirements and technical risks for potential cost-performance trade-off decisions. Changes to a Key Performance Parameters (KPP) and Key System Attributes (KSA) introduce risk that could jeopardize a program's affordability, performance, and military utility.

The following activities are excellent opportunities to identify technical, business, and programmatic risks by Government and/or contractor program teams:

- Brainstorming activities with subject matter experts
- Interviews with program team leads, Systems Command/Center competencies, and/or program stakeholders
- Review of the lessons learned, including risks or issues on predecessor or similar programs
- In-service experience (reliability, safety mishap reports)
- AoAs, which evaluate the merits and risks of each technically feasible alternative
- New contract activity and proposals
- Systems engineering activities:
    - Trade studies, to include the identification of cost and schedule drivers
    - Systems Engineering Technical Reviews (SETR), to include the identification of problematic requirements and immature technologies
    - Evaluation of results from risk reduction and competitive and risk reduction prototyping

  - Evaluation of results from integration and test activities
  - Design changes, such as Class I Engineering Change Proposals (ECP) as well as the rate of Class I and II design changes
  - Failure Mode and Effects Analysis (FMEA), which helps the program identify possible failure modes and their consequences so risks can be identified, prioritized, and actions taken to control the risks
  - Specialty engineering efforts such as manning, human systems integration, reliability, supportability/sustainment, and security
- Independent assessments:
  - Red Teams, Non-Advocate Reviews, Program Support Assessments; technology and manufacturing assessments
  - Nunn-McCurdy and Critical Change Review assessments on Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) programs, respectively
- Trends in Technical Performance Measures (TPM), schedules, budgets, and other metrics:
  - Progress toward meeting KPPs and KSAs
  - Assessments of the performance to plan of TPMs, including an assessment of the reasons for deviation
  - Progress against the program's critical path
  - Schedule Health Checks and SRA
  - Earned Value Management System
- External influences:
  - Changes in user requirements – threats, Concept of Operations (CONOPS), and requirements creep
  - Externally driven cost and/or schedule constraints
  - Service or congressional changes to funding levels
  - Synchronization with critical external programs under development (e.g., schedule alignment, technology maturity assessment, technical issues, and funding priorities)
  - Synchronization of legacy systems availability and restrictions
  - Other interagency requirements or interests (e.g., FAA)
  - New Service or DoD policies and guidance
- Production:
  - Make-buy decisions, changes to suppliers, parts obsolescence, product delivery issues

Many risks can threaten program success in terms of meeting cost, schedule, and performance objectives. Figure 3-2 sites a few resources to use when identifying program risks.

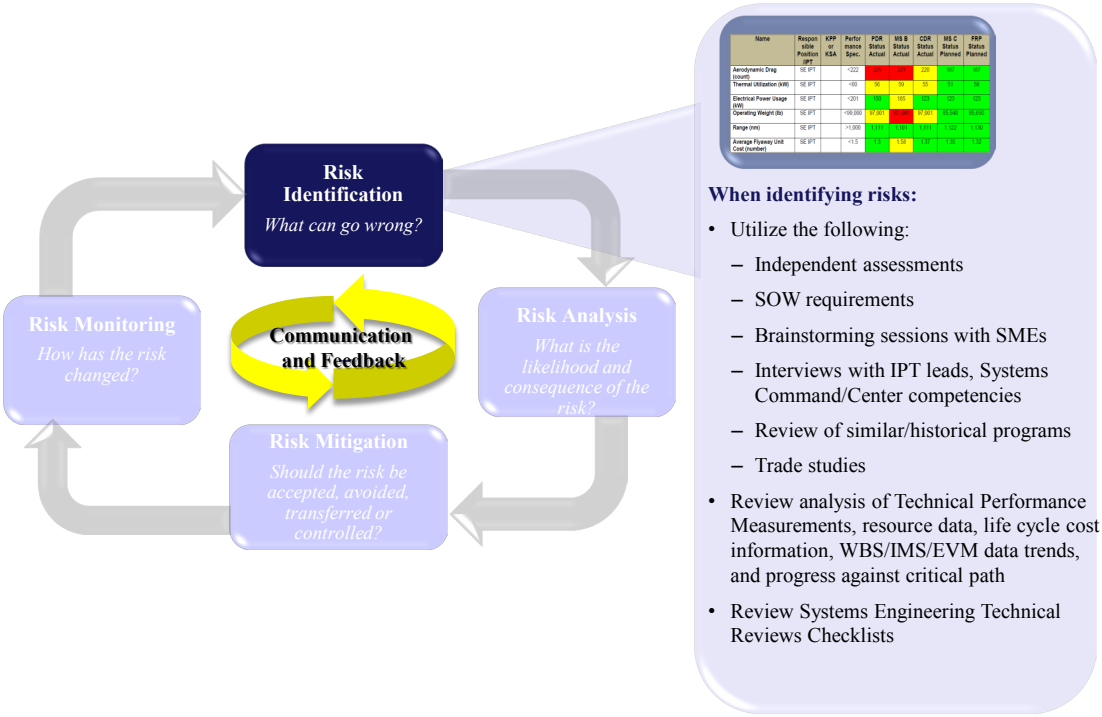


Figure 3-2. Risk Identification

In DoD, risks can be broadly grouped into three categories: technical, programmatic, and business (Figure 3-3). Top-level categories are defined as follows:

- **Technical** – Those risks that may prevent the end item from performing as intended or failing to meet performance expectations. Technical risks can be internally or externally generated. They typically emanate from areas such as requirements, technology, engineering, integration, test, manufacturing, quality, logistics, and training.
- **Programmatic** – Those risks that are generally within the control or influence of the PM or PEO. Programmatic risks can be associated with program estimating (including cost estimates, schedule estimates, staffing estimates, facility estimates, etc.), program planning, program execution, communications, and contract structure.
- **Business** – Those risks that generally originate outside the program office, or are not within the control or influence of the PM. Business risks can come from areas such as program dependencies, resources (funding, people, facilities, suppliers, tools, etc.), priorities, regulations, stakeholders (user community, acquisition officials, etc.), market, and weather.

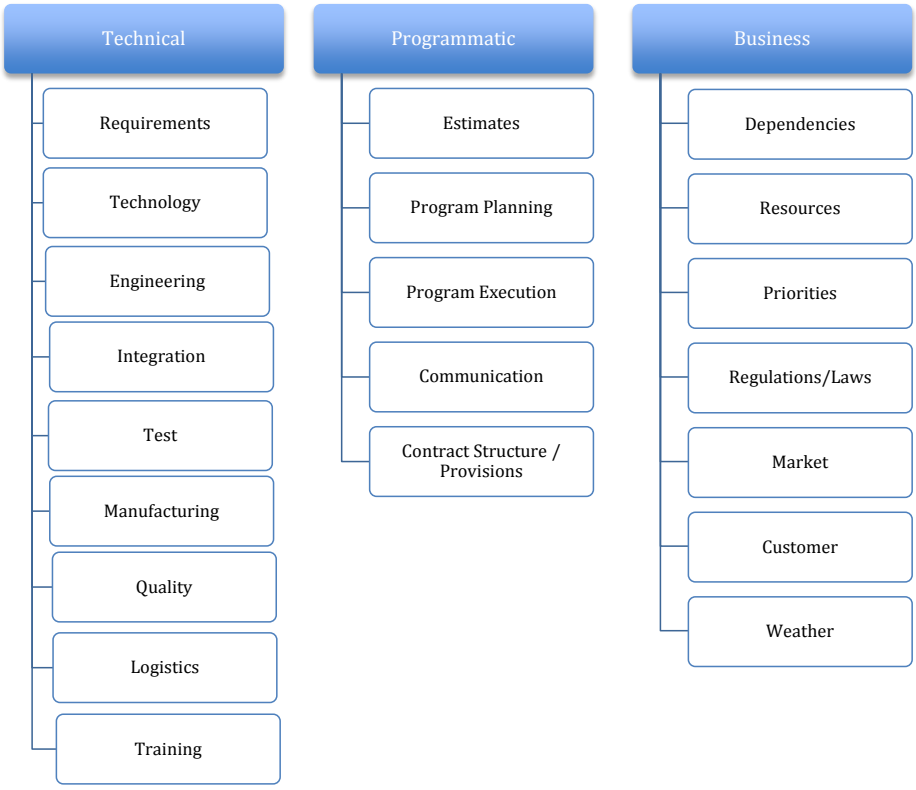


Figure 3-3. Risk Taxonomy

Among the predominant technical risks, the areas of technology, engineering, integration, and manufacturing are reflected in policy and guidance and are routinely discussed during OUSD(AT&L) program engagements and outreach events. These areas are defined as follows:

- **Technology** – Those risks associated with the transition of technical advances out of the laboratory, through prototyping, and into engineering. Technology risks include those associated with research, development, prototyping, and validation in laboratory/operational environments. Risks can also arise from an organization's first-time use of a technology.
- **Engineering** – Those risks associated with the multidisciplinary application of engineering principles to translate stakeholder requirements into effective and affordable systems. Engineering risks include those associated with engineering technical processes (functional analysis, design analysis and trade-offs, detail design, verification, validation); engineering technical management processes (decision analysis, configuration management, risk management, and technical assessment); and engineering products (technical baselines for operational, training, and support systems - inclusive of hardware and software).
- **Integration** – Those risks associated with the engineering and management activities to interface system elements within systems (internal integration) as well as systems with other systems (external integration). Integration risks include those associated with both functional and physical interface requirements, interface design, and management and control.

- **Manufacturing** – Those risks associated with the maturation of manufacturing feasibility, manufacturing technologies, development of critical manufacturing processes, demonstration of manufacturing processes in a pilot-line environment, and at full production rates. Manufacturing risks include those associated with design for producibility, materials, availability, manufacturing process maturity, supply chain management, manufacturing technology, tooling design and maintenance, special test and inspection equipment, process design/control, industrial base, and facilities/workforce considerations.
- **Requirements** – Those risks associated with achieving and delivering a needed capability. Requirements risks include those relating to the realization of KPPs, KSAs, TPMs, and other system attributes in the context of design, production, operation, and support constraints. Poor requirements definition at inception, requirements rigidity, and instability can lead to inefficiencies and sometimes program failure.

3.2 Risk Analysis

Risk analysis answers the question, *How big is the risk?* It is an iterative process that examines the cost, schedule, and performance parameters of risks in order to determine their likelihood and consequence to achieving program objectives.

Risk analysis is the activity of examining each identified risk to refine the description of the risk, isolate the cause, and determine the effects to aid in subsequent risk mitigation. It refines each risk in terms of its likelihood and consequence, and its relationship to other risk areas or processes. Analysis begins with a detailed study of the risks that have been identified. By analyzing each identified risk, the PM will have a better understanding of the cause, effects, and priorities in order to more effectively manage the risks.

Risk analysis also answers the question, *What is the likelihood and consequence of the risk*? by:

- Considering the likelihood the risk event will occur
- Identifying the possible consequences in terms of performance, schedule, and costs
- Identifying the risk level in the risk reporting matrix

Figure 3-4 depicts the how risks should be analyzed and what impact areas to quantify.

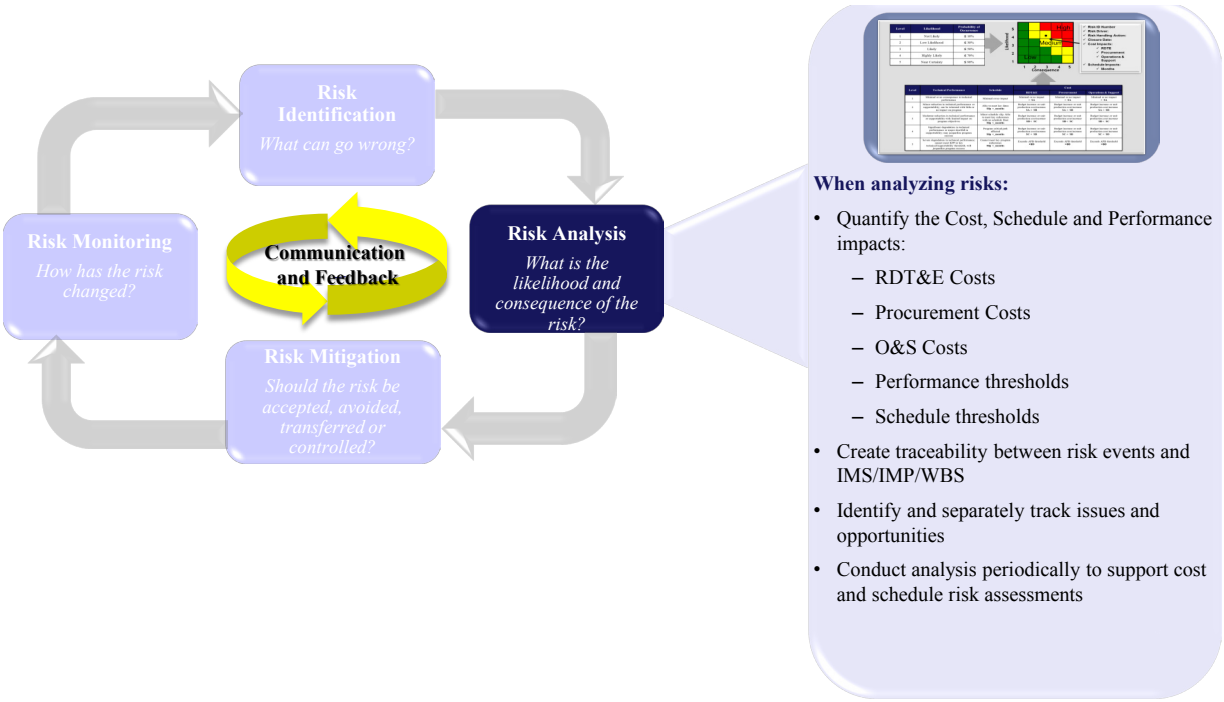


Figure 3-4. Risk Analysis

Program analysis integrates the technical performance assessment, schedule assessment, and cost estimates using established risk evaluation techniques. Likelihood and consequence analysis gives the PM insight into the detailed implications of risks from a quantitative perspective. It also provides a basis for prioritizing efforts and allocating resources to mitigate risks.

3.2.1 Likelihood

Risk likelihood is the assessed probability that a risk event will occur given existing conditions. It is important that the likelihood of the risk be tied to a specific risk event. Table 3-1 provides general criteria for establishing the likelihood of a risk occurring. The use of the predefined likelihood and consequence criteria provides a consistent means for evaluating risks so a program can make objective comparisons of risks. Risks can be characterized as high, moderate, or low based on rating thresholds.

Table 3-1. Levels of Likelihood Criteria

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~ 30%
3	Likely	~ 50%
4	Highly Likely	~ 70%
5	Near Certainty	~ 90%

3.2.2 Consequence

When analyzing risks, each risk should be rated in terms of impact to the program.(i.e., effect of the item on program technical performance, schedule, and/or cost). Risk consequence is measured as a deviation against the program performance, schedule, or cost baseline. While the Government and contractor may have a different perspective on sources of risk and priorities, they should seek to have a common framework for risk consequence analysis. Risk statements should be clearly written to define the potential event that could adversely affect the ability of the program to meet cost, schedule, and performance thresholds. Consequence levels should be defined and included in the SEP, SEMP, and RMP.

The consequence criteria in Table 3-2 may aid a program in distinguishing the type of technical performance, schedule, and cost (Research Development Test and Evaluation (RDT&E), Procurement, or Operations and Maintenance (O&M)) consequences. When assessing the consequence magnitude, the program team evaluates each risk as if it were going to occur. The impact is assessed qualitatively on a scale of 1 to 5, using the guidelines in the table.

PMs are encouraged to carefully consider their program's performance, schedule, and cost thresholds and to use these thresholds to set meaningful consequence criteria tailored to their program. For example, KPP and Acquisition Program Baseline (APB) thresholds should trigger Level 5 consequences. Lower-level consequences may serve as incremental "warning" points in the areas of performance, schedule, and cost. If employed properly, this approach can be effective in linking program management parameters with the risk management approach.

Typically risk control activities reduce the likelihood of the risk event occurring but do not affect the level of consequence (cost, schedule, or performance impact) if the risk event is realized. In addition, as part of risk control activities, the program may reduce the risk level if the system's design architecture changes or if the program addresses constraints, such as budget limitations, inflexible schedule, or inability to change requirements as part of the risk control activities.

Table 3-2. Levels and Types of Consequence Criteria

Level	Technical Performance	Schedule	Cost		
			RDT&E	Procurement	Operations & Maintenance
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact < $A or _% of budget	Minimal or no impact < $A or _% of budget	Minimal or no impact < $A or _% of budget
2	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program	Able to meet key dates Slip ≤ months	Budget increase or unit production cost increase $A ≤ $B or _% of budget	Budget increase or unit production cost increase $A ≤ $B or _% of budget	Budget increase or unit production cost increase $A ≤ $B or _% of budget
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float Slip ≤ months	Budget increase or unit production cost increase $B ≤ $C or _% of budget	Budget increase or unit production cost increase $B ≤ $C or _% of budget	Budget increase or unit production cost increase $B ≤ $C or _% of budget
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected Slip ≤ months	Budget increase or unit production cost increase $C ≤ $D or_ % of budget	Budget increase or unit production cost increase $C ≤ $D or _% of budget	Budget increase or unit production cost increase $C ≤ $D or _% of budget
5	Severe degradation in technical performance; cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones Slip ≤ months	Exceeds APB threshold >$D or _% of budget	Exceeds APB threshold >$D or _% of budget	Exceeds APB threshold >$D or _% of budget

It can sometimes be difficult to determine whether a risk is a performance risk, a schedule risk, or a cost risk. The following paragraphs clarify some of the distinctions.

3.2.2.1 *Performance Consequence Considerations*

Programs should first determine whether a risk has a direct performance consequence or impact. If so, the risk should be noted as a performance risk even though it may also have attendant schedule or cost implications. Performance risks have adverse consequences to capabilities, operations, user needs, or any derived requirements to effectiveness or suitability. Performance consequences can be manifested by performance shortfalls in a technical baseline artifact (specification, drawing, etc.), performance of a test article, or operational system performance.

3.2.2.2 *Schedule Consequence Considerations*

If the risk is judged not to have a performance impact, programs should next ask, "*Is there an impact to schedule and to what extent?"* If the risk affects the critical path, then it has an impact on both schedule and cost but should be carried as a schedule risk.

Program teams should analyze the impact of the risk to the IMS and the critical path(s), to:

- Evaluate baseline schedule (durations and network logic)
- Incorporate technical assessment dates and schedule uncertainties into the program schedule
- Evaluate impacts to program schedule based on engineering team assessment
- Perform schedule analysis on the program IMS, incorporating the potential impact and off-ramps from all contract schedules
- Quantify schedule excursions reflecting the effects of cost risks, including resource constraints
- Provide a Government schedule assessment for cost analysis and fiscal year planning, reflecting the technical foundation, activity definition, and inputs from technical and cost areas
- Document the schedule basis and risk impacts for the risk assessment
- Project an independent forecast of the planned completion dates for the SETRs and major milestones
- Conduct Schedule Health Checks and SRA to aid in the identification of schedule consequences

3.2.2.3 *Cost Consequence Considerations*

Programs should examine whether a risk has a cost consequence by asking, "*Does the risk affect the RDT&E, procurement, or O&M costs?"* If so, with no performance or schedule impacts, the risk is a cost risk and may have an impact on program efforts to:

- Assess technical and schedule results.

- Derive life cycle cost estimates by integrating technical assessment and schedule risk impacts on resources.
- Establish budgetary requirements consistent with fiscal year planning.
- Determine whether the adequacy and phasing of funding supports the technical and acquisition approaches.
- Provide program life cycle cost excursions from near-term budget execution impacts and external budget changes and constraints.
- Document the cost basis and risk impacts.

Note: Cost and funding are not the same. Cost is related to the amount of money necessary to acquire and sustain a commodity; funding is the amount of money available to acquire and sustain that commodity.

Expectations:

- Predefined likelihood and consequence criteria are used to provide a consistent means for evaluating risks so objective comparisons of risks can be made. Risks can be characterized as high, moderate, or low based on rating thresholds.
- Risk statements identify events that could adversely affect the ability of the program to meet performance, schedule, and cost thresholds or objectives.
- Trade studies inform risk mitigation activities, technology off-ramps, and the adjustment of requirements during Knowledge Point reviews and Configuration Steering Boards.
- Risk analysis is a snapshot in time and may change significantly during the program. Program teams conduct risk analyses periodically to align and support other program management activities such as technical, IMS (including critical path), and EVM reviews. All aspects of risk management are iterative.
- If the analyzed likelihood is at or near 100 percent, the program teams address the problem as an issue rather than a risk.

3.2.3 Risk Reporting Matrix

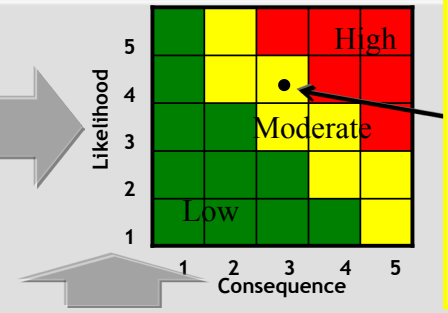
The purpose of risk reporting is to ensure that management receives all necessary information to make timely and effective decisions to manage risks. This allows for coordination of actions by the risk team, allocation of resources, and a consistent, disciplined approach. A primary goal of risk reporting should be to provide the PM with an effective tool for managing and communicating risk.

Programs should use a likelihood and consequence risk matrix to characterize risks. This characterization aids the program office in prioritizing risk mitigation activities.

The program should revisit and update the matrix on a regular basis. Once the analysis of likelihood and consequence is complete, program teams should then use the risk reporting matrix shown in

Figure 3-5. This risk reporting matrix allows the combination of likelihood and consequence to form an overall risk level for each risk: low (green), moderate (yellow), or high (red). Program teams can then use this rating level to more effectively communicate the level of risk and the urgency of program actions to control those risks.

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~ 30%
3	Likely	~ 50%
4	Highly Likely	~ 70%
5	Near Certainty	~ 90%



- **Risk ID Number:**
- **Risk Driver:**
- **Risk Mitigation Action:**
  - **Cost: $**
- **Closure Date:**
- **Cost Impacts:**
  - **RDTE: $ or %**
  - **Production: $ or %**
  - **O&M: $ or %**
- **Performance Impacts:**
- **Schedule Impacts:**
  - **Months:**

Level	Technical Performance	Schedule	Cost		
			RDT&E	Procurement	Operations & Maintenance
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact **< $A or _% of budget**	Minimal or no impact **< $A or _% of budget**	Minimal or no impact **< $A or _% of budget**
2	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program	Able to meet key dates **Slip ≤ months**	Budget increase or unit production cost increase **$A ≤ $B or _% of budget**	Budget increase or unit production cost increase **$A ≤ $B or _% of budget**	Budget increase or unit production cost increase **$A ≤ $B or _% of budget**
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float **Slip ≤ months**	Budget increase or unit production cost increase **$B ≤ $C or _% of budget**	Budget increase or unit production cost increase **$B ≤ $C or _% of budget**	Budget increase or unit production cost increase **$B ≤ $C or _% of budget**
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected **Slip ≤ months**	Budget increase or unit production cost increase **$C ≤ $D or_ % of budget**	Budget increase or unit production cost increase **$C ≤ $D or _% of budget**	Budget increase or unit production cost increase **$C ≤ $D or _% of budget**
5	Severe degradation in technical performance; cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones **Slip ≤ months**	Exceeds APB threshold **>$D or _% of budget**	Exceeds APB threshold **>$D or _% of budget**	Exceeds APB threshold **>$D or _% of budget**

Figure 3-5. Risk Reporting Matrix

Risk reporting documents should include recording, maintaining, and reporting of risk identification, risk analyses, risk mitigation approach, and tracking results. Risk reporting is performed as part of technical reviews, risk review board meetings, or periodic program reviews. Documentation includes all plans and reports for the PM and decision authorities, as well as reporting forms that may be internal to the program office. Predefined likelihood and consequence criteria should be used to provide a consistent means for evaluating risks so objective comparisons can be made.

Once the risks have been categorized by likelihood and severity of consequence, the risks can be prioritized onto the risk reporting matrix. This graphical representation of the analyzed risks offers some structure to risk management decisions that are often complex. The matrix focuses on the most logical and critical risks as demonstrated in Figure 3-6.

Risks can be characterized as high, moderate, or low based on rating thresholds. A risk level of high, moderate or low is calculated for each risk and serves as the means to rank the program risk. This difficult but important step in the risk management process helps the program determine resource allocation and the appropriate mitigation strategy. As implementation proceeds and additional risks

are identified, different scenarios may be used to analyze their impact on the program's cost, schedule, and performance requirements. This process allows the management of individual risks to be prioritized in terms of their impact.

Prioritizing risks is important during all acquisition phases, but especially when there has been a significant change in the Acquisition Strategy and prior to milestone reviews. Since every project is unique, the priorities of certain risks will vary. Risks also can be prioritized based on their relationship to other external risks. Risks that are high and have the most critical impact on program execution can be given the most priority. Figure 3-6 depicts a sample prioritized program risk matrix that summarizes the program risk picture.

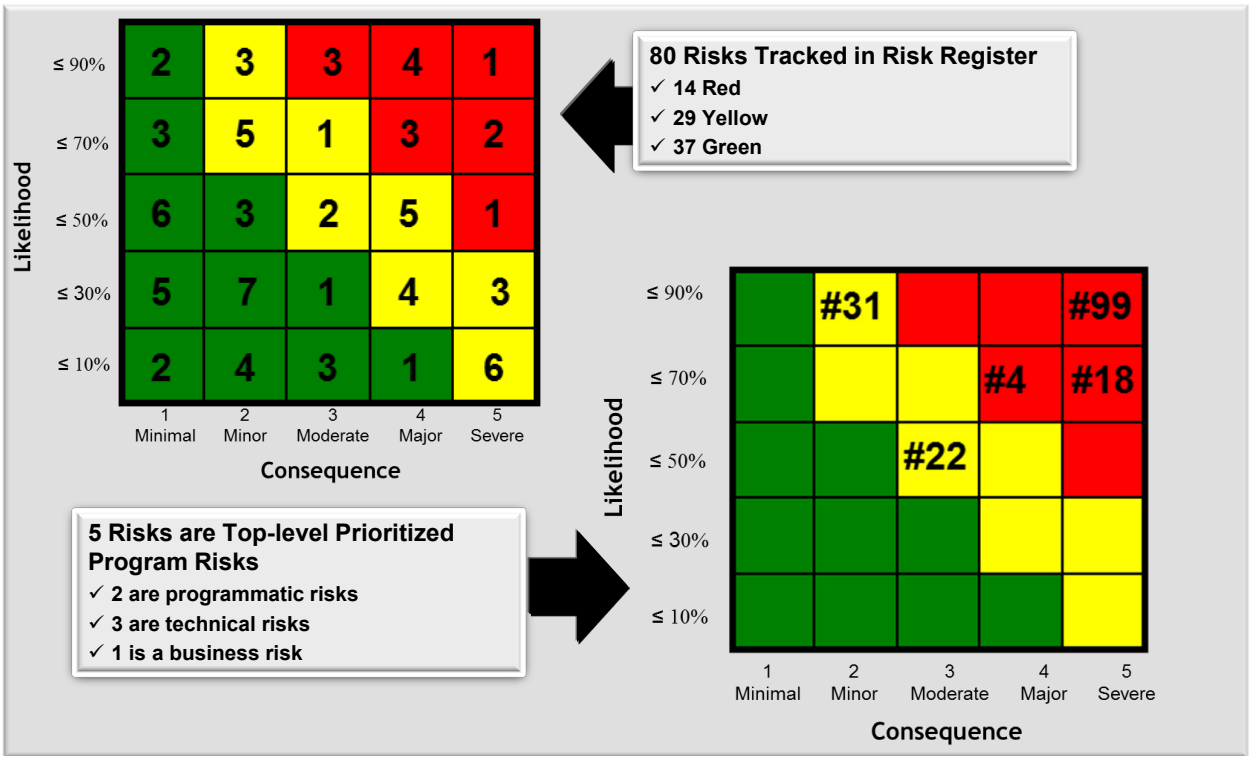


Figure 3-6. Prioritized Risk Matrix

Programs should use the risk tracking methodology that best suits them and might integrate a risk reporting matrix with risk control activities as outlined in Figure 3-7. This figure shows an example of an alternative approach for presenting the risk, performance, schedule, and cost (RDT&E, procurement, or O&M) consequences. This alternative risk reporting matrix also facilitates assessing performance to plan relative to risk control activities.

Risk	Likeli-hood (1-5)	Consequences					Control Activities	Planned (P) Actual (A)		Closure Date
		Funding			Schedule	Performance				
		RDT&E	Procurement	O&S			Activity	Date	Cost	
Risk 1 (describe the risk in terms of, "if… (something does or does not occur), then….(negative consequence X and Y will happen)	3	$450k			4 months	XX performance degraded	1 –Activity XX	(P) 6/16/14 (A)	(P) (A)	(P) 8/12/15
							2 –Activity YYY	(P) 10/12/13 (A) 11/1/13	(P) (A)	(A)
							3 – Activity ZZZ	(P) 8/12/15 (A)	(P) (A)	
Risk 2	4		$2.2M		8 months		1 –Activity aaa	(P) 7/13/14 (A)	(P) (A)	(P)7/13/14
							2 -	(P) (A)	(P) (A)	(A)
							3 -	(P) (A)	(P) (A)	
Risk 3	2		$520K		2 months		1 -	(P) (A)	(P) (A)	(P)
							2 -	(P) (A)	(P) (A)	(A)
							3 -	(P) (A)	(P) (A)	

Figure 3-7. Alternative Risk Reporting Matrix

Expectations:

- Risk statements are clearly written to define the potential root risk event that could adversely affect the ability of the program to meet cost, schedule, and performance thresholds.
  - The risk driver, mitigation activities, and closure are identified on the risk reporting matrix.
  - The magnitude and type of cost consequence (RDT&E, procurement, or O&M) are quantified on the risk reporting matrix.
  - The costs of control activities are shown on the risk reporting matrix.
  - Programs ensure that the risk consequences are based on the cost and schedule criteria defined in the SEP, SEMP, Acquisition Strategy, and RMP.

3.2.4 Risk Register

A risk register is a tool commonly used as a central repository for all risks identified by the program team and approved by the RMB. A risk register should be developed once the project and RMP have been approved. It provides a mechanism for maintaining awareness of the number and type of risks. The risk register records details of all risks identified throughout the life of the project. It includes information for each risk such as risk category, likelihood, consequence, planned mitigation or control measures, the risk owner, and, where applicable, expected closure dates. Figure 3-8 shows a sample format for a risk register. Risks should be linked to the appropriate WBS/IMS activities. Programs should regularly update and maintain the risk register as the status of risks change due to risk mitigation strategies. New risks should be added to the risk register when identified.

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood / Consequence Rating	Risk Reporting Matrix	Risk Mitigation Strategy	Submitted Date	Board Review	Planned Closure	Expected Risk Rating	Plan Status
8231	3.2.2	Mr. Bill Smith	Technical	Open	II	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	3/4	Yellow	Control - Program will apply management reserve to retain adequate software engineers to burn-down SW defects	8/23/2013	1/14/2014	2/12/2014	Green (1-4)	On track

Figure 3-8. Risk Register

3.3 Risk Mitigation

Risk mitigation incorporates a strategic approach to addressing risks. A risk mitigation approach answers the question, *What is the plan?* After the program's risks have been assessed, the PM should develop approaches to manage risks by analyzing various mitigation techniques and selecting those best fitting the program's circumstances. The selected mitigation approaches for program-level risks should be reflected in the program's Acquisition Strategy and include the specifics of *what* should be done, *when* it should be accomplished, *who* is responsible, the cost and schedule impact, and the *funding/resources* required to implement the risk mitigation plan. Figure 3-9 highlights key aspects of risk mitigation.

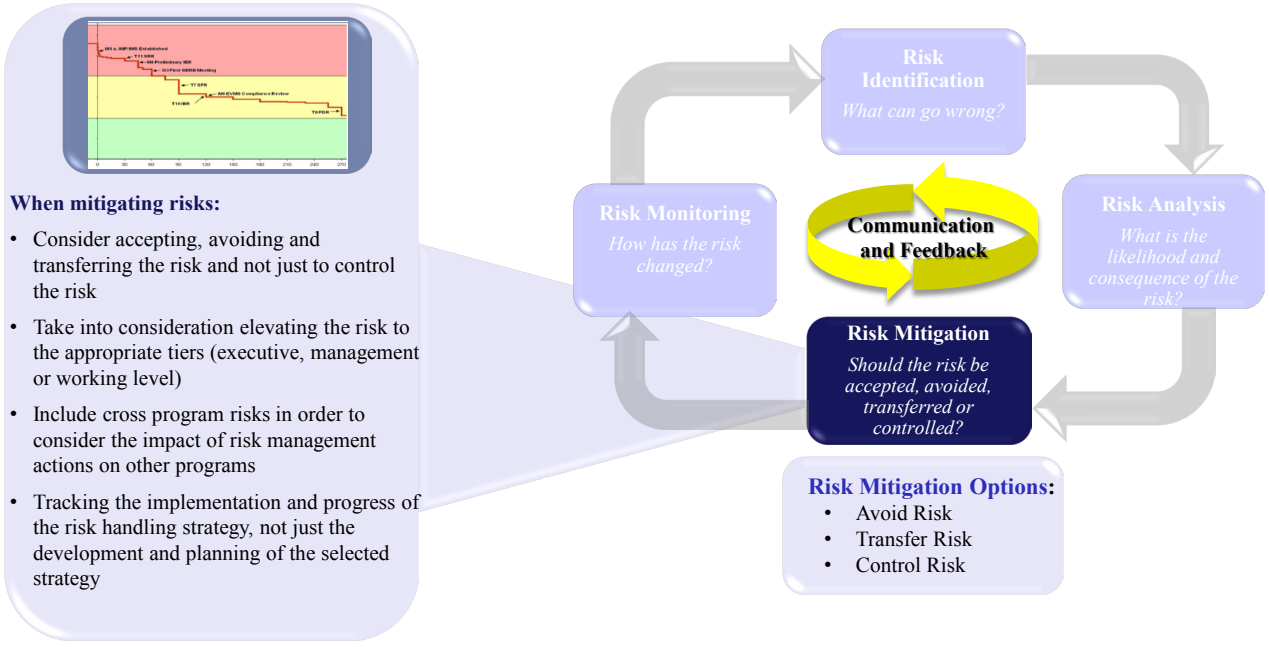


Figure 3-9. Risk Mitigation

Through risk mitigation the program identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. For each risk, program teams should select the most appropriate program approach from the four mitigation options listed and document the planned approach in a risk mitigation plan.

The level of detail in planning depends on the program life cycle phase and the nature of the risks to be addressed. However, there should be enough detail to allow an estimate of the effort required and technical scope needed based on system complexity. Figure 3-10 provides a sample risk reporting matrix that highlights the details that should be addressed when quantifying the impact of risks.

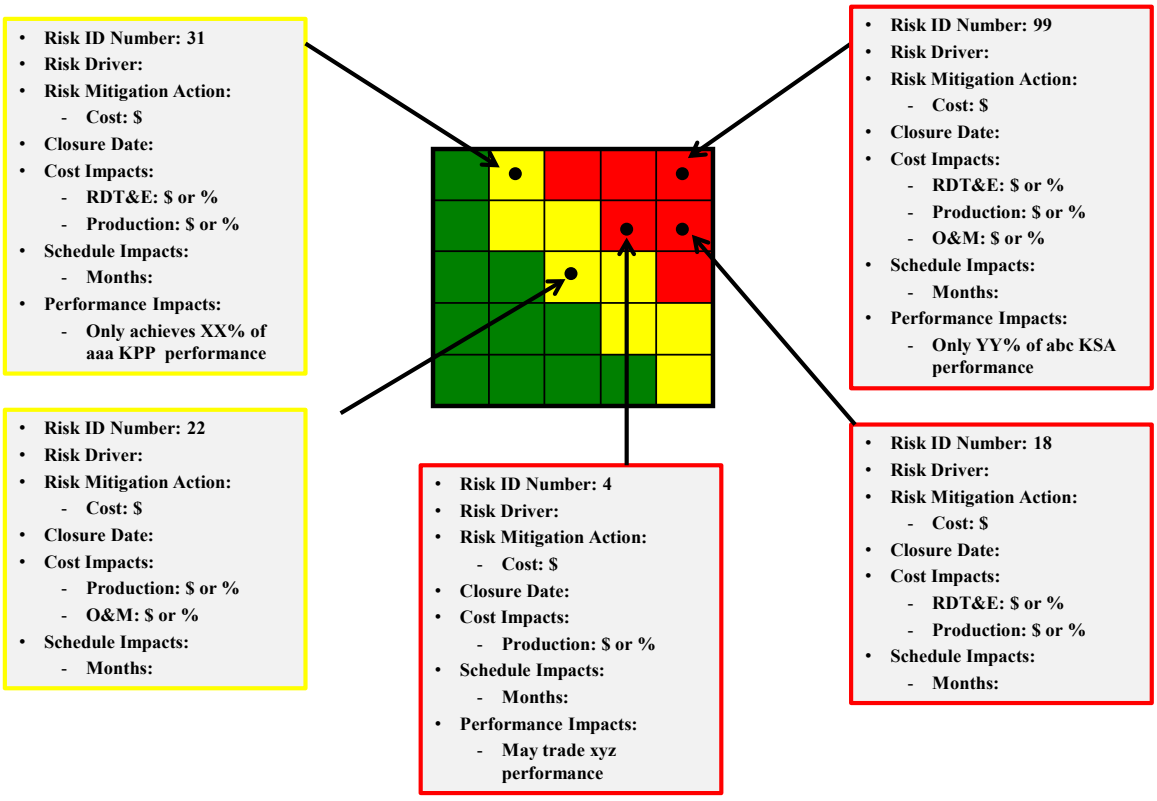


Figure 3-10. Sample Program Tier 1 Risk Reporting Matrix

When formulating the mitigation approach, the RMB should compile a list of criteria that answers questions such as:

- Is the approach feasible in implementation?
- Are the expectations realistic in effectively reducing program risk to an acceptable level?
- Is the approach affordable in terms of dollars and resources?
- Is adequate time available to develop and implement the approach?
- What impact do these approaches have on the overall program schedule?
- What impact will the mitigation approach have on the technical performance of the system?

Successful mitigation requires the Government and the contractor to communicate all program risks for mutual adjudication. Both parties may not always agree on risk likelihood/consequence, but the RMB is the mechanism for risk definition and assignment. Programs often fall into the trap of identifying ongoing program activities as risk mitigation actions, without making changes to the planning, requirements, budget, or the program budget/resource allocation. This approach of not changing the planning, requirements, budget or program allocation typically is not sufficient to adequately address the identified risks. In most situations, relying on previously planned program activities without modifying them will not control the risk but may result in the program's simply accepting the risk and its consequence, as part of the program approach. It is important for programs to recognize this distinction when communicating risk mitigation approaches to higher program and technical authority.

If the risk changes significantly, the program team should adjust the risk mitigation approaches accordingly. If the risks are lower in severity than previously assessed, then the program team can reduce or cancel the specific risk mitigation approach and consider using the resources for other uses. If risks are higher in severity or new events are found, appropriate risk mitigation efforts should be implemented. Notwithstanding the actions taken, the rationale for the changes to the risk (and control implementation) should be documented and maintained in a history file.

3.3.1 Risk Acceptance

By risk acceptance, the program acknowledges that the risk event or condition may be realized and willingly accepts the risk with the consequences. Accepting a risk does not mean that it is being ignored. Before accepting the risk, the program should identify the resources, schedule, and cost needed to overcome the risk. The executive, management, and working levels occasionally have to seek relief from the next higher level or accept a risk without making a clear effort to control it, depending on the scope of the consequence. For example, risks may also be accepted if further control exceeds cost or schedule allocations. However, the program should make every attempt to identify and understand the risk so that any future efforts can be strategically planned.

3.3.2 Risk Avoidance

Through risk avoidance, the program eliminates the risk event or condition by taking an alternate path. Analyzing and reviewing the proposed system in detail provides insight to determining the risk drivers for each technical requirement. Examples might be changing operating procedures or substituting a low-risk mature technology. Risk avoidance also provides the PM with an understanding of what the real needs are and ways of avoiding the risks that are not critical to performance. This may involve a change in the requirements and specifications that reduce risk to an acceptable level. Risk avoidance should be supported by a cost-benefit analysis.

3.3.3 Risk Transfer

Risk transfer includes reassigning the risk responsibility to another entity. This approach may reallocate a risk from one program to another, between the Government and the prime contractor, or within Government agencies. The prerequisite for transferring a risk is the acknowledgement from the receiving entity that it now owns the risk. For example, a performance risk can be transferred to an external program to improve the performance of that subsystem. Reallocating risk drivers such as design requirements that are transferred may lead to lower system risks while maintaining system-level requirements.

3.3.4 Risk Control

Risk control entails controlling the risk by taking action to reduce the likelihood of a risk event or condition. This approach does not seek to eliminate the risk but attempts to reduce the risk and monitor its impact/effect on the program. The intent of the risk control plan implementation is to reduce the level of program risks by:

- Directing the teams to execute the defined and approved risk control plans
- Applying resources (manpower, schedule, budget) to reduce the likelihood and/or consequence of risks
- Tracking resource expenditure, technical progress, and risk impacts (benefits)
- Providing a coordination vehicle with management and other stakeholders
- Outlining the risk reporting requirements for ongoing monitoring, to include "trip wires" which warrant elevating the risk to the next management level
- Documenting the change history
- Providing information to further enhance risk tracking and risk communication

It is also possible that throughout the system life cycle there may be a need for different near-term and long-term control approaches. Programs should avoid the tendency to select control as the risk mitigation approach without seriously evaluating acceptance, avoidance, and transfer.

3.3.5 Risk Burn-Down

Once a program team has determined that the mitigation strategy for a risk is to control it, part of the control plan may include a risk burn-down plan for high risks. The program identifies mitigation activities in a burn-down strategy. For most risks, the burn-down plan consists of steps, tied to the project schedule, that allow the program to control and retire risks. A burn-down plan consists of 6 steps to plan for risk mitigation:

1. Identify risk start and end points on a graph
2. Assign numerical values to these points

3. Identify activities that will burn-down risk
4. Estimate the time basis for these activities
5. Estimate their relative risk burn-down contribution
6. Chart the relationship of activities on a date basis

Figure 3-11 shows a sample risk burn-down chart and associated activities. A risk burn-down chart includes:

- An instant snapshot of the progress of a risk over time
- Actual progress against the planned reduction of risk levels
- Effectiveness of previous risk control activity
- IMS tasks

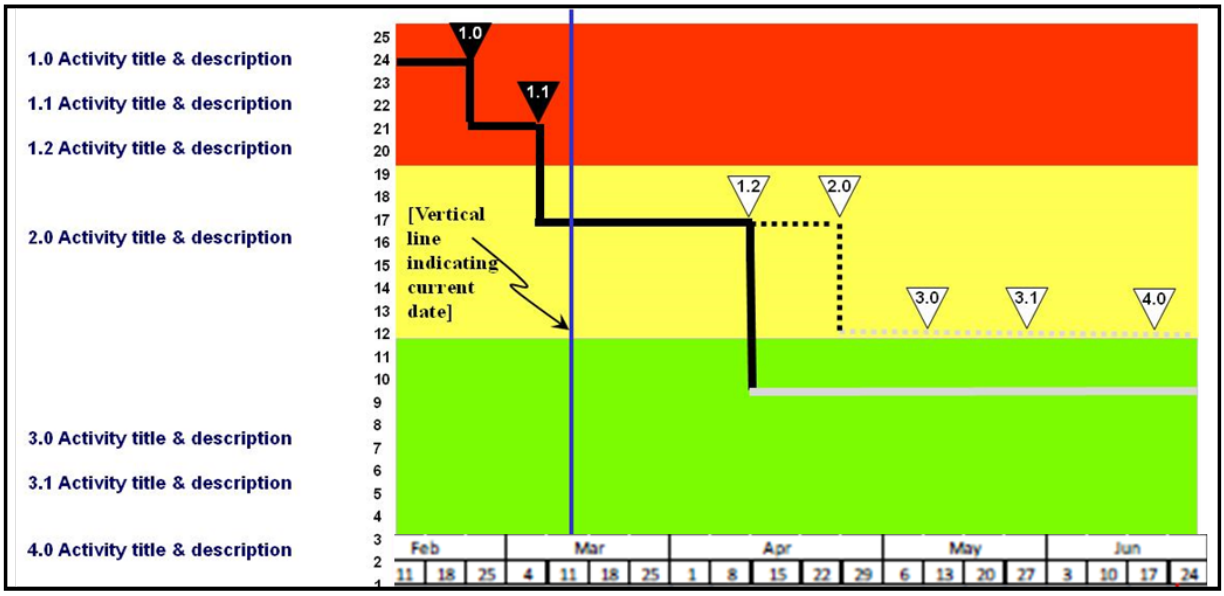


Figure 3-11. Risk Burn-Down

Expectations:

- Risks are either:
  - Accepted: The program assumes responsibility for potential consequences.
  - Avoided: The program eliminates the risk event or condition by taking an alternate path.
  - Transferred: The program assigns risk responsibility to another entity. Programs should not transfer a risk to another program unless the receiving organization accepts it and has the resources to control it.
  - Controlled: The program develops, resources, and monitors control plans.
- The risk register captures the risk mitigation approach (Accept, Avoid, Transfer, Control) for each risk.
- Risks that are assessed as "High" or "Moderate" have resourced risk control plans.
  - Due to potential adverse impact to the program, risks assessed as "High" and remaining such for longer than 3 months require fallback or alternative plans.
  - Risks that are assessed as "Low" do not require control plans but, upon further review by management, may have elements that require monitoring. If so, risk control plans may be formally or informally implemented.
- The risk reporting matrix should not list issues.
- Risks are managed at the appropriate organizational level (executive, management, or working). The program tracks implementation of risk control, not just development of a control plan. The program allocates appropriate budget. Programs continually monitor control plans/implementation for new and changing risks.
- Typically risk control activities reduce the likelihood of the risk event occurring, not the consequences (cost, schedule, or performance impact).

3.4 Risk Monitoring

Risk monitoring answers the question, *How have the risks changed?* Risk monitoring includes a continuous process to systematically track and evaluate the performance of risk mitigation approaches against established metrics throughout the acquisition process. During this time, the program office should reexamine and conduct assessments with the risk mitigation approaches to determine effectiveness.

Successful risk monitoring includes timely, specific reporting procedures as part of effective communications among the program office, contractor, and stakeholders. Figure 3-12 highlights selected components of risk monitoring. Risk monitoring documents may include: TPM status, other program metrics, risk register reports/updates, technical reports, earned value reports, watch lists, schedule performance reports, technical review minutes/reports, IMSs, test results, and operational feedback.

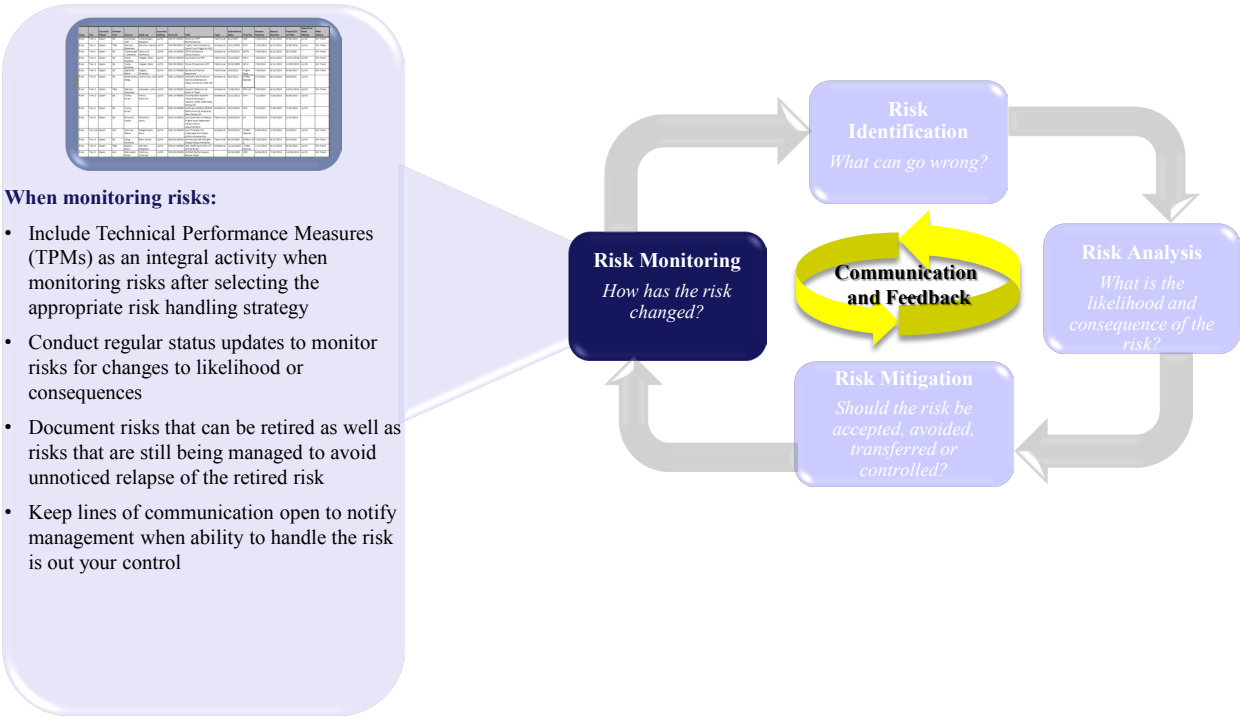


Figure 3-12. Risk Monitoring

Program offices and contractors should establish a regular schedule for reviewing risks, issues, and opportunities. At a top level, periodic program management reviews and technical reviews provide much of the information used to identify any performance, schedule, readiness, and cost barriers to meeting program objectives and milestones. Therefore, throughout the program, the program office should reevaluate known risks on a periodic basis and examine the program for new events by:

- Monitoring risks for any changes to likelihood or consequence as a result of program progress
- Reviewing regular status updates
- Displaying risk management dynamics by tracking risk status within the risk reporting matrix and risk register reports/updates
- Alerting management as to when risk mitigation plans should be implemented or adjusted
- Citing those risks that can be retired due to program progress or control
- Reviewing retired risks on a periodic basis to ensure they have not relapsed

The key to risk monitoring is to establish a management indicator system over the entire program. The PM uses this indicator system to evaluate the status of the program throughout the life cycle. A risk's likelihood and consequence may change as the acquisition process proceeds and updated information becomes available. Program teams should use the management indicator system to

provide an early warning when the likelihood of occurrence or the severity of consequence exceeds pre-established thresholds/limits or is trending toward exceeding preset thresholds/limits. Risk monitoring allows the program team to take timely management actions to control these problems.

Figure 3-13 illustrates the results of risk control actions against established metrics throughout the acquisition process. The plotted position on the risk reporting matrix should show the PM's current assessment of the risk's likelihood and the estimated severity of its effect on the program if control fails. Figure 3-13 also provides an example of changed risk status after risk mitigation. As risk control succeeds in a program, a yellow or red risk's position on the risk reporting matrix migrates in successive assessments from its current location toward the green. Therefore, the program office should reexamine risk assessments and risk control approaches concurrently and feed information back to the other risk activities of identification, analysis, and mitigation.

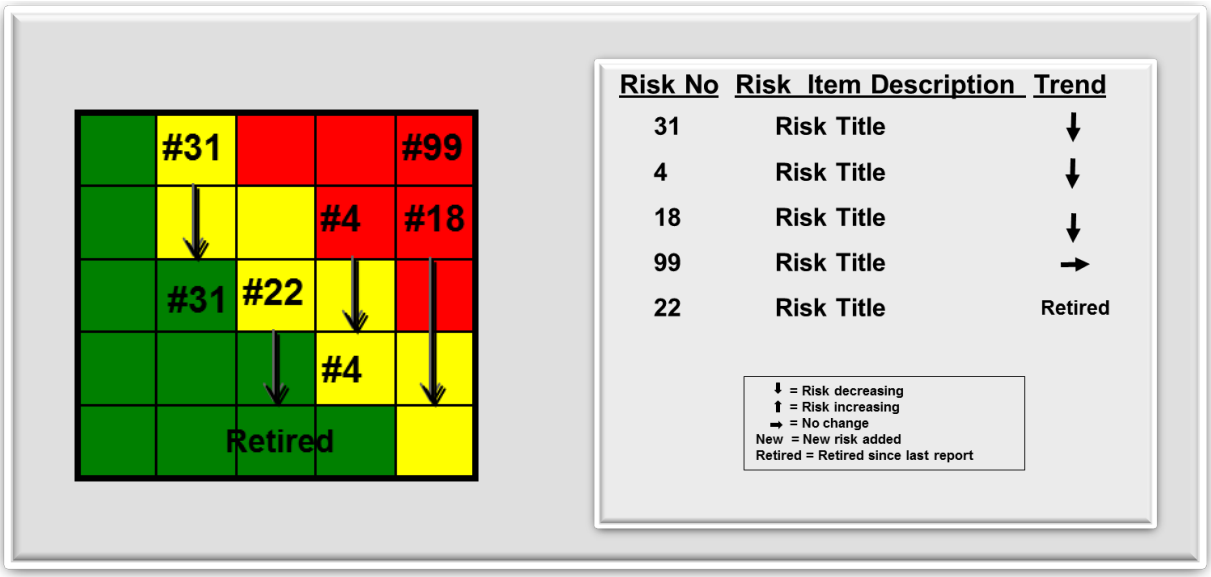


Figure 3-13. Risk Monitoring Matrix

Expectations:

- The program team conducts regular status updates to monitor risks for any changes to likelihood or consequence as a result of program progress. Program offices and contractors establish a regular schedule for reviewing risks, issues, and opportunities.
- The team alerts management when risk mitigation plans should be implemented or adjusted.
- Managers alert the next level of management when the ability to mitigate a risk exceeds the lower level's authority or resources.
- The program team tracks implementation of risk control against the plan.
- The program establishes a management indicator system over the entire program to monitor risk activity.
- The program reviews closed risks periodically to ensure their risk level has not changed.

4 INTEGRATING RISK MANAGEMENT WITH OTHER PROGRAM MANAGEMENT TOOLS

Programs need to integrate risk management with other program management tools during all phases of the program. Four examples of program management tools discussed in this guide are the WBS, IMP, IMS, and EVM.

The program should use the WBS and IMS to identify risks during periodic reviews of work packages. The program should then enter risks into the register along with the associated control plans, and whenever possible, link the risks to the work packages associated with the control effort. For control efforts that represent new or out-of-scope work, the program may need new resource-loaded work packages to track the effort. The IMP should include major program-level risks. Risk control efforts should include assigned resources (funded program tasks) reflected in the IMP, IMS, and EVM baselines.

Collectively, the WBS, IMP, IMS, and EVM help the PM gain insight into balancing program requirements and constraints against cost, schedule, or technical risk. A good risk management process allows the program to deal with risk in a timely manner and at the appropriate management level. A stable and recognized program baseline is critical to effective risk management.

4.1 Work Breakdown Structure

The WBS is a product-oriented family tree composed of hardware, software, services, data, and facilities. It displays and defines the product, or products, to be developed and/or produced and is an organized method to break down a product into sub-products at lower levels of detail. Produced from systems engineering efforts, it breaks down and decomposes all authorized program work into appropriate elements for planning, budgeting, scheduling, and cost accounting. The WBS facilitates communication as it provides a common frame of reference for all contract line items and end items. Figure 4-1 depicts a simplified WBS decomposed to Level 3.

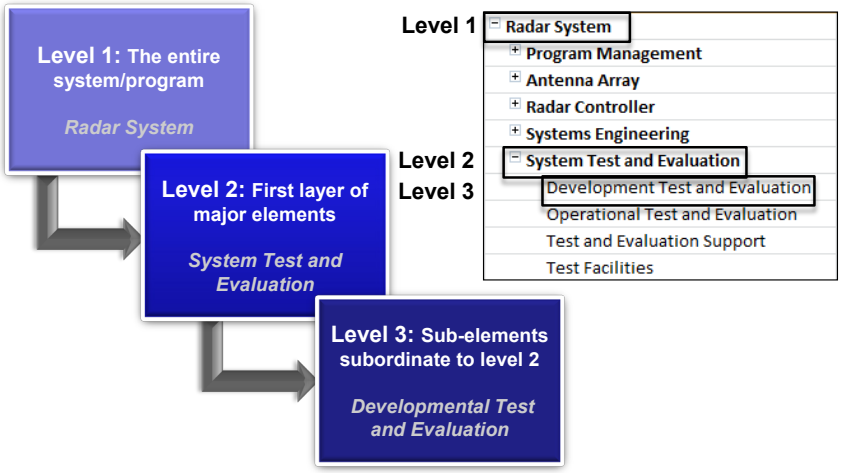


Figure 4-1. Example of WBS Levels

The program should use the WBS as a basis for identifying and analyzing risk, for monitoring risks at their respective levels (primarily for impact on cost and schedule performance), and for assessing the resulting effect of risks on the overall program or product. Following risk mitigation planning, the program should update the WBS as needed to reflect selected mitigation options.

Figure 4-2 provides examples of a program and contractor WBS relationship. See MIL-STD-881 for more details on preparing, understanding, and presenting the program WBS and contractor WBS.

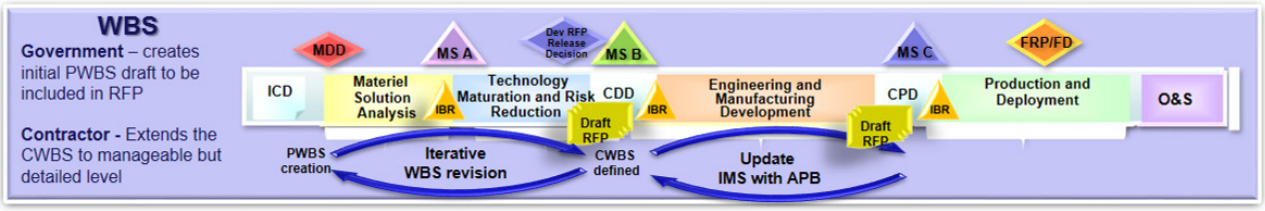


Figure 4-2. Government and Contractor WBS Relationship

4.2 Integrated Master Plans and Integrated Master Schedules

Effective risk management requires a stable and recognized baseline from which to identify program risks. The IMP and IMS help establish and maintain that baseline. The IMP is an overarching event-based plan that displays each milestone and supporting accomplishments needed for program completion. The IMS documents the more detailed, logical sequence of work, including relationships among tasks and significant interdependencies. The IMP and IMS facilitate effective planning and forecasting that are critical to project success. Distinct IMS tasks are summarized by WBS identifiers so the program can track progress and measure schedule performance. Assigning the same WBS codes to each task in the IMP and IMS allows direct traceability to the WBS (shown in figure 4-3). This structure serves as the basis for meeting the RFP requirements.

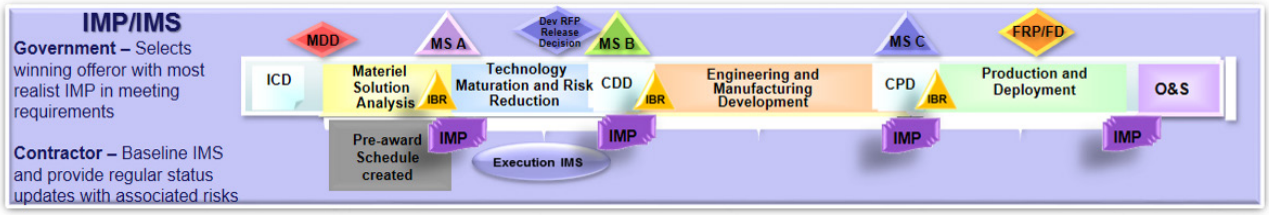


Figure 4-3. IMP/IMS Creation and Implementation

The IMS is critical as the program develops "what-if" scenarios to assess the likelihood and consequence of each risk. Using the IMS, the program should identify risk drivers to gain a better understanding of the risks and therefore identify the best mitigation strategy. In order to better track progress in controlling risk, the program should reflect resources in the IMS.

4.2.1 IMS Health Assessment

Programs should regularly assess the health of the IMS through a schedule health assessment. Schedules should be resource loaded and trace to TPMs. The following schedule health characteristics aid the program office to assess the quality and structural integrity of schedules. These characteristics provide the analyst with a framework for asking educated questions and performing follow-up research.

- **Logic:** A good schedule identifies and links all work package elements in the order they should be executed using predecessors and/or successors.
- **Type of Relationship:** Relationships establish the order in which each task should be completed. The finish-to-start relationship is the preferred method as established by auditing agencies and is the default for many scheduling tools. A good schedule establishes a finish-start hierarchy, with few exceptions.
- **Hard Constraints:** Hard constraints fix a task's finish date and prevent tasks from moving as their dependencies finish, thereby preventing the schedule from being logic-driven. The critical path and any subsequent analysis may be adversely affected. Good schedules will not have any hard constraints.
- **High Duration:** Any unfinished task with a baseline duration greater than 44 working days (2 months) is considered high duration. Good schedules will break down tasks that have durations greater than 44 days into smaller, more manageable efforts that provide better insight into cost and schedule performance.
- **Leads:** A lead is an overlap between tasks that have a dependency. For example, if a task can start when its predecessor is half finished, the program can specify a finish-to-start dependency with a lead time of the applicable number of days for the successor task. Programs should minimize leads as they can distort the critical path and cause resource conflicts.
- **Lags:** Any duration between a task's completion and its predecessor's start date is defined as a lag. Lags should be avoided because they can adversely affect the critical path and any subsequent analysis.
- **High Float:** Float (or slack) is the amount of time a task can be delayed without causing a delay to subsequent tasks. A task with float more than 44 working days is considered high float and may be a result of missing predecessors and/or successors. If the percentage of tasks with high float exceeds 5 percent, the critical path may be unstable and will not be logic-driven. Good schedules avoid high float.
- **Negative Float:** Any task with negative float (less than zero) may indicate that the forecasted date (start-to-finish) is unrealistic and will affect the schedule's overall realism. Good schedules will have a corrective action plan (get-well plan) to mitigate the negative float and its impact.
- **Invalid Dates:** If a status to actual start/finish dates reflects a future beyond the current status date, it is considered invalid. Tasks that have actual start and/or actual finish dates that meet these criteria indicate that the IMS has not been properly statused. Accurate, updated actual start and finish dates are necessary for program management decisions and for calculating a valid critical path.
- **Resources:** Tasks that have durations of one or more days require the allocation of resources (hours/dollars) to complete the assigned work. Good schedules use resource allocations to

assist the PM in ensuring the scheduled efforts are executable as planned and increase effectiveness of schedule risk assessments.

- **Missed Tasks:** Tasks that do not finish as planned are considered missed tasks. An excessive amount of missed tasks indicates that the program is performing poorly to the baseline plan and may be a result of inadequate resources and/or unrealistic planning. Good schedules provide advanced warning to the PM, helping to minimize the impact.
- **Critical Path Test:** Properly established schedules map tasks in a sequential order. The schedule of sequential tasks with zero float creates a critical path. A failed critical path test indicates broken logic somewhere in the schedule. Good schedule management ensures the critical path remains intact.
- **Critical Path Length Index (CPLI):** The CPLI measures the schedule's efficiency to finish on time. The CPLI uses the negative float in a schedule to calculate the longest, continuous sequence of tasks/activities through the schedule from contract start (or current status date) to contract completion. A CPLI of 1.00 or greater indicates there is no negative float in the schedule. Good schedules approach a CPLI of 1.00.
- **Baseline Execution Index (BEI):** The BEI is the efficiency with which actual work has been accomplished when measured against the baseline plan. This efficiency measure is an indication of how well the program is executing to plan. Well-executed schedules have a calculated BEI not less than 0.95 with a target of 1.00.

As displayed in Figure 4-4, the designation of a "red" assessment is not synonymous with failure, but rather an indicator of potential lower schedule quality.

Logic	0.3% (7/2757 tasks) have a missing schedule relationship
Leads	0% (0/2757 tasks) have lead time
Lags	0.4% (11/2757 tasks) have lag time
Relationship Types	2.6% (72/2757 tasks) have an improper schedule relationship
Hard Constraints	0.4% (12/2757 tasks) have hard constraints
High Float	6.4% (176/2757 tasks) have excessive float
Negative Float	2.5% (68/2757 tasks) have negative float
High Duration	18.6% (512/2757 tasks) have excessive duration
Invalid Forecast/Actual Dates	0.8% (85/10425 tasks) have invalid dates
Resources	93.1% (2567/2757 tasks) have improper resources assigned
Missed Tasks	32.9% (3425/10425 tasks) have missed their finish dates
Critical Path Test	0 day(s) of float
Critical Path Length Index (CPLI)	1 CPLI
Baseline Execution Index (BEI)	1.01 BEI. 0% (2/7584 tasks) prior to the status date were not completed

Figure 4-4. Sample Schedule Health Characteristics Assessment

4.2.2 Schedule Risk Assessment

Schedule risk assessments (SRA) provide a means to determine the level of risk associated with various tasks that make up the program and their effect on overall program schedule objectives. The analyst reviews the schedule to determine schedule risk and supplemental risk drivers and identifies high-risk tasks that should be on the critical path. Using a Monte Carlo simulation or other analytical tools, the analyst should develop a probability distribution based on the duration of each task. The critical path within the schedule should indicate a realistic estimate of the schedule risk.

An SRA provides an estimate to notify the PM early on if there is a significant likelihood or probability of overrunning the program schedule and by how much. Although schedule probability distribution should be developed as soon as the IMS is available, the distribution can be performed starting at the completion of the first statement of work.

The WBS is best used as a starting point for identifying the lowest level activity for which duration and probability can be assessed. The WBS level selected depends on the program phase. An SRA should be at the program level and should include all contractor schedules; however, it is possible to run an assessment on each contractor's schedule, if it is properly loaded.

Monte Carlo simulation produces cumulative probability associated with different duration values in order to indicate the level of schedule risk and to identify the specific schedule drivers. It also provides overall schedule risk at the program level, accounting for the combined effects of multiple individual risks affecting program activities. Since the IMS, which was derived from the WBS elements, is used in loading the chosen risk assessment tool, it is possible to determine the risk drivers and link them back to the appropriate performance risks.

Figure 4-5 shows the process and components of schedule risk assessments. Accurate analysis requires continuous cooperation between the schedule analysts and the PM.

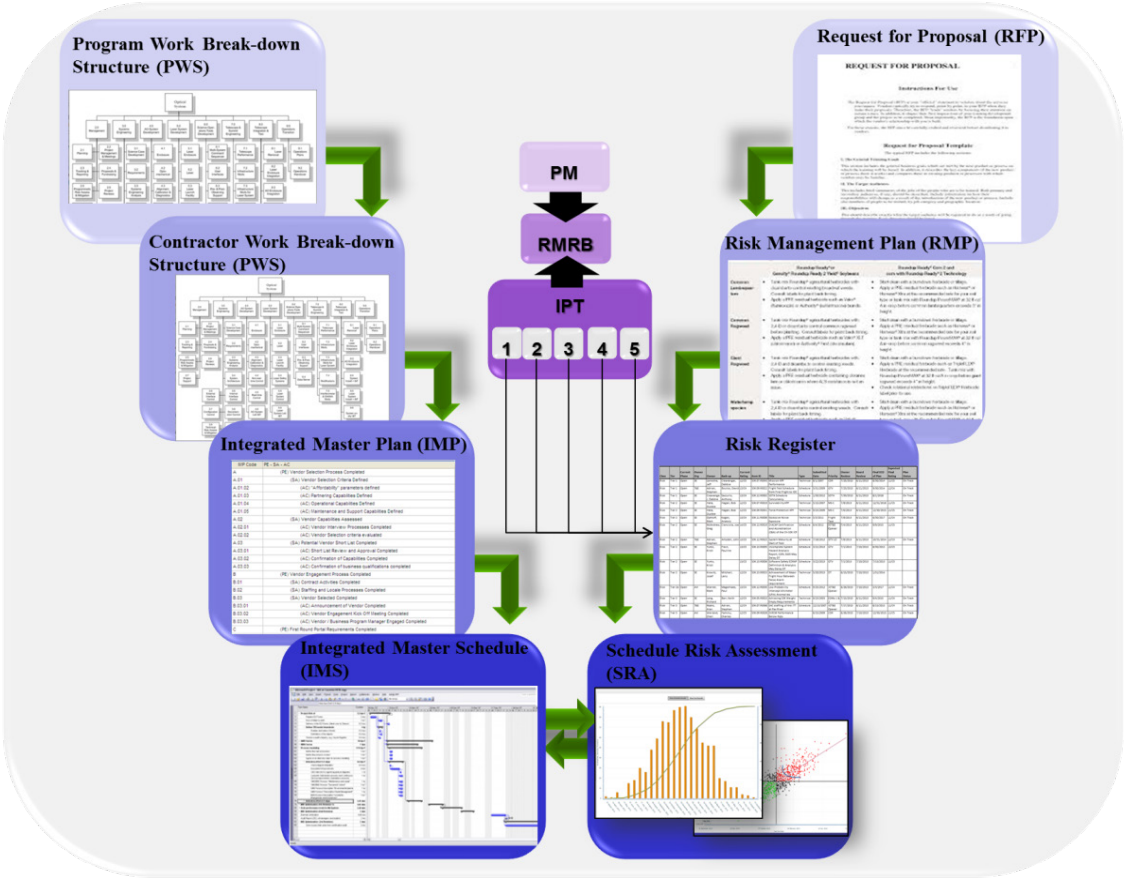


Figure 4-5. Schedule Risk Assessments

4.2.3 Cost Risk Assessment Technique

If the IMS is well constructed and fully resourced, it can be used to conduct cost risk assessments. These assessments can provide a realistic cost Estimate at Completion (EAC) that permits the evaluation of performance and technical parameters or schedule causes of cost risks in order to determine the actual risk of cost overruns and to identify cost drivers. The cost risk is determined by comparing the EAC with the cost baseline developed as part of the acquisition program baseline. The risk-adjusted program cost estimate displays the probability of a program completing within a dollar threshold and forecasts a recommended budget baseline required to complete the program within certain cost parameters.

Although this assessment can be used throughout the acquisition phases, it should be used in conjunction with technical performance and schedule risk assessment. Cost risk assessments should address both the probability of occurrence and the consequences/impacts of potential risk events. As the program advances through the acquisition life cycle and the WBS is expanded, specific technical performance and schedule risks can then be identified down to the lowest (4, 5, or lower) level. The WBS elements may encompass cost estimating uncertainties, schedule risks, and technical

performance risks; therefore, the validity of the cost data used to construct the cost risk assessments is critical. Collecting good data is the most critical part of the cost assessment process.

A number of analytical tools can be used to perform cost risk assessments. As with SRAs, Monte Carlo simulation can be used to determine the cost probability distributions for a program. This technique is often chosen for its quick results and fairly accurate estimates.

4.3 Earned Value Management

EVM is a program management tool that provides insight into the contractors' cost and schedule performance against planned performance. By integrating the technical, cost, and schedule parameters of a contract into an integrated baseline, work is performed and measured against this baseline whereby a corresponding budget value is "earned."

If variances in cost and schedule begin to appear in Contract Performance Reports (CPR), the program team can then use EVM to analyze the data and isolate causes of the variances and identify any risks that may be associated with the variance. Using the earned value metric, cost and schedule variances can be determined and the program manager can identify significant risk drivers, forecast future cost and schedule performance, and implement corrective action plans to get back on track.

EVM is effective in helping a program monitor WBS elements that are experiencing risks. The strength of EVM lies in its rigorous examination of what has already occurred on the project, using quantitative metrics to evaluate project past performance. The program can then analyze what actions are necessary to establish or modify a mitigation approach.

If the program contract is required to comply with ANSI/EIA-748, Earned Value Management Systems, risk management should be integrated with EVM to expose underlying drivers of performance risk.

Expectations:

- Programs integrate risk management with other management tools (WBS, IMP, IMS, EVM, as applicable) during all phases of the program.
- Programs establish traceability between risk management activities and the WBS, IMP, and IMS.

5 ISSUE MANAGEMENT PROCESS

Through issue management, the program identifies issues that have already occurred and assesses the severity and urgency of their possible impact on the program. This process results in a strategy for resolving, transferring, or assuming the issues.

OSD has found that program issues are, too often, mistakenly characterized as risks. This practice is reactive and tends to blind the program to true risk management. Risk management applies resources to lessen the likelihood, or in some cases, the consequence, of a future event. Issue management, on the other hand, applies resources to address and resolve a past or occurring event and its related consequences. When a negative event has been identified and has a past or present impact to the cost, schedule, or performance of a program, it is not a risk. These events should be cataloged as issues and should be addressed within the program's normal issue management process. In addition, even though an issue may introduce a likely future consequence, this does not make it a risk. To ensure issues and risks are properly identified, programs should have an issue management approach to identify problems and track associated closure plans. Programs should also assess whether issues are spawning prospective risks.

Figure 5-1 displays the issue management process. Similar to the risk management process, issue management should have its own cost-effective approach for identifying, analyzing, handling, and monitoring program issues. PMs and chief engineers should develop a Plan of Action and Milestones (POA&M) to address and manage all program issues. Issues should be reviewed during the program office and contractor's regularly scheduled meetings. Issue management, when properly applied and communicated, can shift management action from reactive to proactive.

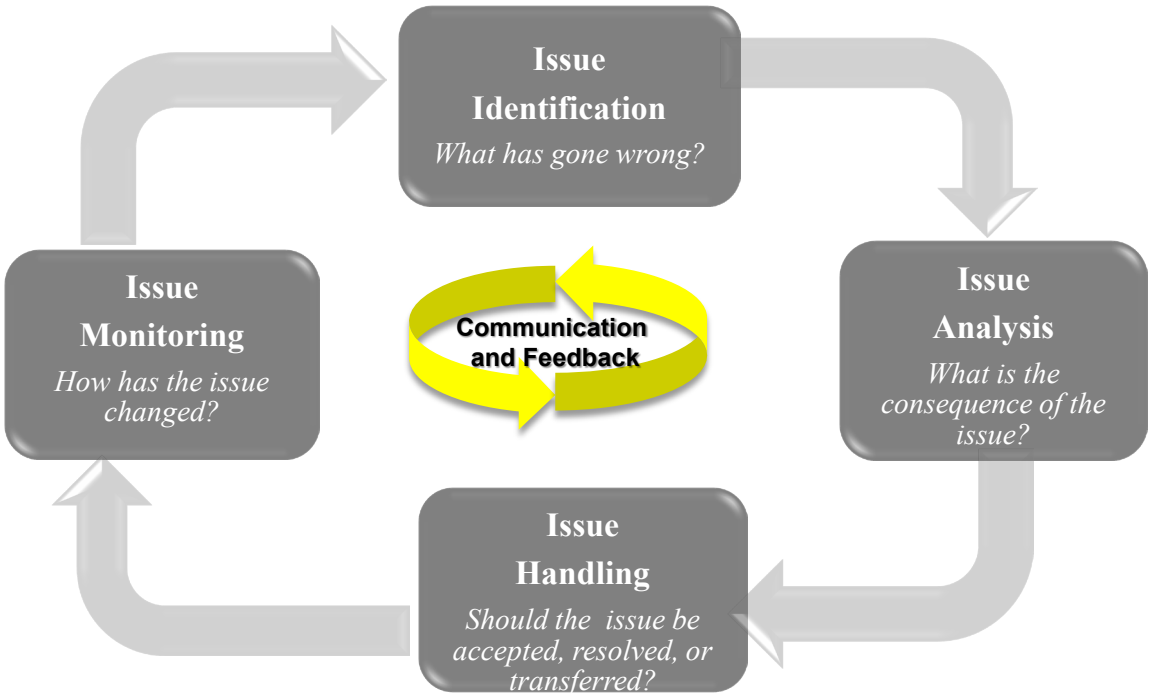


Figure 5-1. Issue Management Process

Issues are best identified before the beginning of a new project or contract and should be updated and reviewed periodically throughout the life cycle of the program. Unlike opportunities and risks, there is no assessment of their likelihood because issues have either already occurred or are in the process of occurring. The issue management matrix in Figure 5-2 provides a graphical representation of the issue status. Issues are mapped according to their consequences. The yellow, orange, and red regions on the matrix indicate areas of low, moderate, and high issues, respectively.

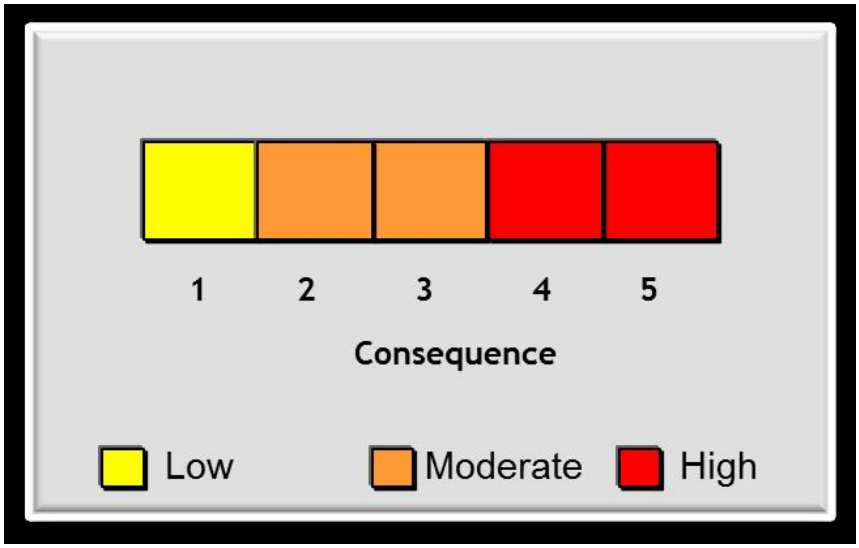


Figure 5-2. Issue Reporting Matrix

Once an issue has been analyzed for severity and urgency, the program should develop and implement a corrective action plan. The program monitors issues using the following mitigation options:

- Transfer – Reallocating ownership of the issue to a team more capable of reducing or accepting the issue.
- Assume – Accepting the issue based on results of cost-benefit analysis that displays a benefit in accepting the consequences of the issue.
- Resolve – Implementing a strategy to undertake the issue by correcting the issue at hand and ensuring that it does not recur.

The program should track the resolution of issues against the POA&M. Figure 5-3 shows a sample issue tracking matrix.

Issue	Consequence	Type T/B/P	Plan of Action at Milestones			
			Closure Activities	Closure Date Planned (P) Actual (A)	Cost	
					Type (RDT&E, Procurement, O&M)	Amount ($)
Issue X (Describe the issue that has occurred, the type of issue, technical, business, or programmatic, and what are the resulting cost, schedule and performance consequences)		Tech (T)	Activity 1	(P) – 10/12/13 (A) - 11/1/13	RDT&E	$420K
			Activity 2	(P) (A)	Procurement	$2.1M
			Activity 3	(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		

Consequence Table Key

- More than z days behind plan
- Between y and z days behind plan
- Less than x days behind plan

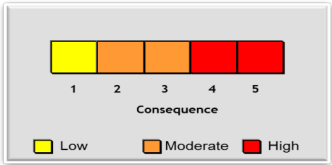


Figure 5-3. Issue Tracking Matrix

Expectations:

- Do not confuse issues with risks. Both have consequences, but issues have already occurred. Therefore, programs should have an issue management process separate and distinct from the risk management process.
- A program should develop a POA&M for all issues and should review the POA&M during the program office and contractor's battle rhythm of meetings (see Figure 2-2).
- Programs track cost, schedule, and performance issues and report to the appropriate management level based upon the level of the consequence impacts.

6 OPPORTUNITY MANAGEMENT PROCESS

An opportunity is the potential for improving the program in terms of cost, schedule, and performance. Opportunity management supports USD(AT&L) Better Buying Power initiatives to achieve "should cost" objectives. In Better Buying Power 2.0, the USD(AT&L) discussed implementing "should cost" management, stating, "Our goal should be to identify opportunities to do better and to manage toward that goal. Managers should scrutinize each element of cost under their control and assess how it can be reduced without unacceptable reductions in value received."

Figure 6-1. Opportunities Help Deliver Should Cost Objectives

PMs should use opportunity management (OM) to identify, analyze, plan, implement, and track initiatives that can yield improvements in the program's cost, schedule, and/or performance baseline by reallocating program resources. Identifying opportunities starts with forecasting potential enhancements within the program's technical mission, stakeholder objects, and contract extensions.

By focusing on the downside of risk, programs may overlook opportunities that provide possibilities for innovation. As opportunities emerge, the program can shift focus toward understanding how to take advantage of opportunities while continuing to manage risks. Opportunity management measures program improvement in terms of likelihood and benefits. Figure 6-2 shows the opportunity management process.

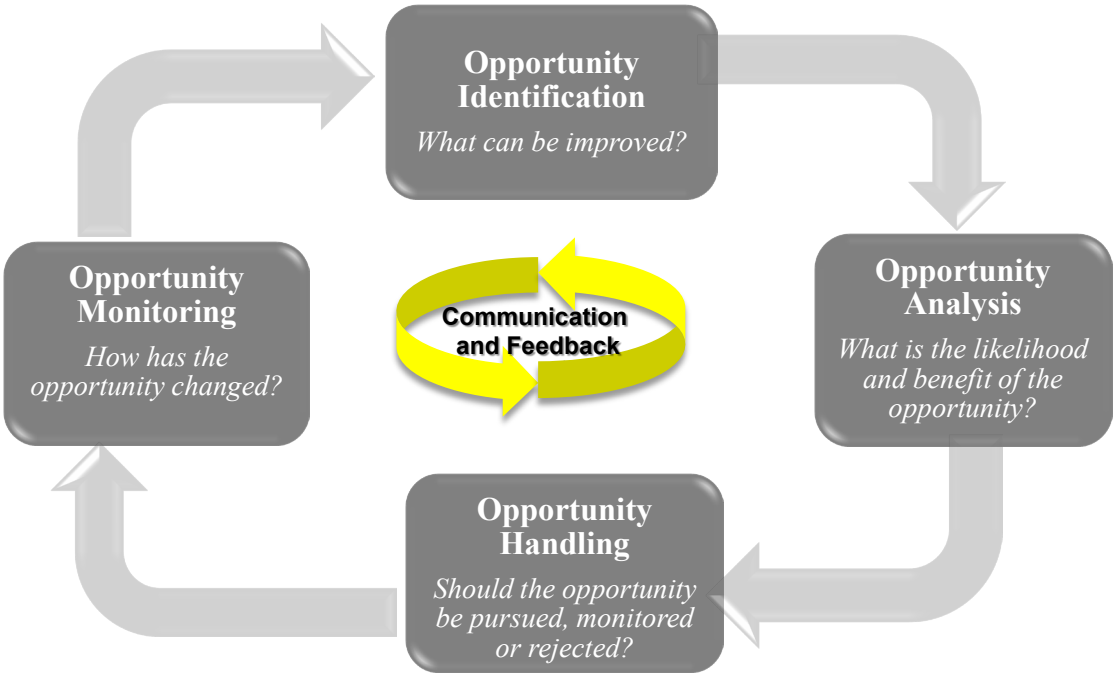


Figure 6-2. Opportunity Management Process

The program should consider the following while outlining the OM process:

- Define the effort.
- Identify roles and responsibilities.
- Acknowledge boundaries that may exist.
- Maintain leadership support.

Opportunities should be assessed for both advantages and disadvantages. Through the OM process, the program identifies potential enhancements to pursue cost, schedule, and performance benefits that enable the program to perform better than planned. Program teams should seek out opportunities across the entire system life cycle. For example, important sources of opportunities include system and program changes that yield reductions in total ownership cost. These reductions can be in any aspect of life cycle cost, including research and development, production, personnel, training, spares, and operations and maintenance. Each of these elements of life cycle cost should be considered for reduction opportunities early on and throughout the program life cycle.

During production, the program should continuously analyze opportunities for design changes that yield reductions in production costs. Design changes to production configurations (and the product baseline) may take the form of Value Engineering Change Proposals within the context of ongoing production contracts. These do not change the system performance, but they may change the design to yield production or support cost reductions.

Although there is an upside to pursuing the desired benefits of OM, there are also downsides resulting from changes in the baseline plan and scope of the program. The program should perform

a cost-benefit analysis to justify the added cost or schedule that may be needed to achieve the intended benefit. Next, the program should weigh the benefit with the cost and likelihood of achieving it. Figure 6-3 illustrates the progression of the opportunity management process.

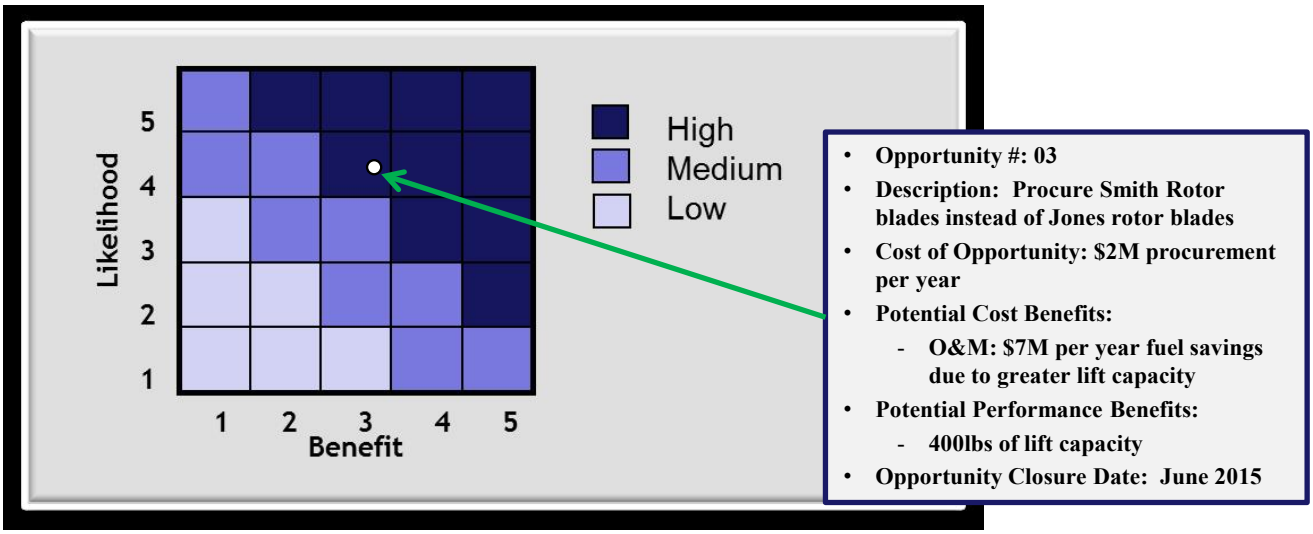


Figure 6-3. Opportunity Reporting Matrix

Opportunities can be discovered before program execution and throughout the life of the program. These events should help improve the technical capabilities, ease schedule restrictions, and decrease costs. Once the opportunities are identified, the next step is to analyze the likelihood of occurrence and the benefit of pursuing the opportunities. In arranging the strategy to pursue opportunities, the program should assess the potential benefit and achievability as follows:

- Low – Little benefit, and minimal oversight needed to engage opportunity
- Moderate – Some benefit, and oversight may be required
- High – Major benefit, and oversight will be required

The opportunity assessment matrix provides a graphical representation of opportunity status. Opportunities are mapped on the matrix according to their likelihood and potential benefit.

The most important difference between an opportunity and a risk is that an opportunity needs to be supported and proven beneficial to the program. One should be careful to assess whether improvements to system performance above threshold, above either the operational capability documented in the JCIDS document or the specification, could be considered "gold plating" even though seemingly a good idea. It is also important to remember that the Government and vendor may see different opportunity benefits and costs. A vendor is not likely to propose an opportunity not benefiting itself, nor facilitate one. Programs should manage this relationship focusing on how the vendor profitability may be impacted and how they may be incentivized.

Factors such as cost, schedule, and the onset of risks associated with the opportunity can play a big role in how the opportunity is handled. The handling approach is evaluated so that the best option

can be selected, and then either rejected (because it is not feasible), monitored, or taken into consideration in the revised baseline plan. Common opportunity-handling options include:

- Reject – Intentionally ignore an opportunity due to cost, technical readiness, resources, and schedule burden.
- Monitor – Continuously evaluate the opportunity for changes in circumstances.
- Pursue – Fund and implement a plan to pursue the opportunity.

Example: If using a new technology and lighter materials could lower a ship's weight, the program may have an opportunity to add other capabilities such as increased armament and increased speed. The program may opt to monitor the opportunity and revisit improving the product after Low-Rate Initial Production (LRIP).

- Once there is a plan in place to reject, monitor, or pursue the opportunity, the program office should continue to observe the opportunity for a status change. The program should conduct a cost-benefit assessment regularly and report the results to decision makers. Figure 6-4 shows a sample opportunity tracking matrix.

Opportunity	Likeli-hood	Cost	Benefit					Activity	Expected Closure
			RDT&E	Procurement	O&M	Schedule	Performance		
1. **Opportunity 1: Procure Smith Rotor blades instead of Jones rotor blades**		$2M			$7M	6 month margin	4% greater lift	Summarize the activity to realize the opportunity	June 2016
2. Opportunity 2 (describe the opportunity in terms of what it will provide the program, the benefit to the program, and the cost to the program)		$15K	$25K		$1.1 M				May 2015
3. Opportunity 3 (describe the opportunity in terms of what it will provide the program, the benefit to the program, and the cost to the program)		$211K		$0.4M	$3.6 M	4 months less long lead time needed			

Figure 6-4. Sample Opportunity Tracking Matrix

Expectations:

- Program managers use opportunity management to identify, analyze, plan, implement, and track initiatives that can yield improvements in the program's cost, schedule, and/or performance baseline through the reallocation of program resources.
- PMs seek to improve a program through exploitation of available opportunities.
- Risk, issue, and opportunity management is reviewed during a defined battle rhythm of meetings.

7 MANAGEMENT OF CROSS-PROGRAM RISKS

Programs should identify and manage internal and external interfaces. These interfaces can be a significant source of risk. An integration activity involving mature hardware and software such as Government-furnished equipment generally goes smoothly because it uses established and stable interfaces; however, the design, integration, and test activities associated with new development usually results in technical, business, and programmatic risks. Interdependent programs may have differing priorities regarding funding levels; hardware and software development schedules; space, weight, power and cooling (SWAP-C) requirements; immature technologies; testing results; or other areas that could introduce risks. To control cross-program risks, the programs should have strong risk management processes and an environment of "shared destiny."

The following activities can aid a program to manage activities when it is fielding a new system that should depend on programs outside the PEO's portfolio or from another Service:

- Seek program champions within the Service(s) and OSD who can:
    - Exert strong management control over critical interfaces with external programs.
    - Align funding and priorities (funding, schedule, form factors requirements, etc.) of external programs.
    - Instill in subordinates a sense of urgency in the system's development and fielding.
- Ensure interface management is in place to meet cost, schedule, and performance requirements.
    - Ensure internal and external interface requirements are documented in the Interface Control Documents and Interface Requirement Specifications.
    - Establish an Interface Control Working Group to identify and resolve interface issues at the lowest possible level.
    - Develop a time-phased, fast-track issue identification and resolution process that raises issues sequentially to the PM, PEO, Service acquisition level, and Defense Acquisition Executive in order to align priorities and resources. For example, if an issue is not resolved within a specified period such as 2 weeks, it should be elevated to the next management layer until it is resolved.
- Develop Memorandums of Agreements (MOA) with all external programs to identify and manage critical interfaces. These MOAs should be documented in the Acquisition Strategy and SEP.
    - MOAs between interdependent programs establish roles and responsibilities associated with dependency. They should include agreements on cost, schedule, performance, and details (or planning) of any functional and/or physical interfaces. The status of required MOAs is covered by a mandated table in each program's SEP.
    - The MOAs should contain cost/schedule and performance "tripwires" that require a program to inform other programs within the family of systems/system-of-systems of any significant (nominally > 10%) variance in performance, schedule, or cost.
    - The contractors should establish Associate Contractor Agreements to facilitate working relationships.

Table 7-1 is an example of a notional table of required MOAs from the Acquisition Strategy Outline.

Table 7-1. Notional Table of Required MOAs from the Acquisition Strategy Outline

REQUIRED MEMORANDA OF AGREEMENT				
Interface	**Cooperating Agency**	**Interface Control Authority**	**Required By Date**	**Impact if Not Completed**

- Develop and maintain a synchronized schedule that shows prototyping, technical reviews, integration and test activities, and acquisition milestones for associated programs. Assess schedule performance to plan on a regular basis to inform risk identification activities. Figure 7-1 is an example synchronization schedule from the SEP Outline.

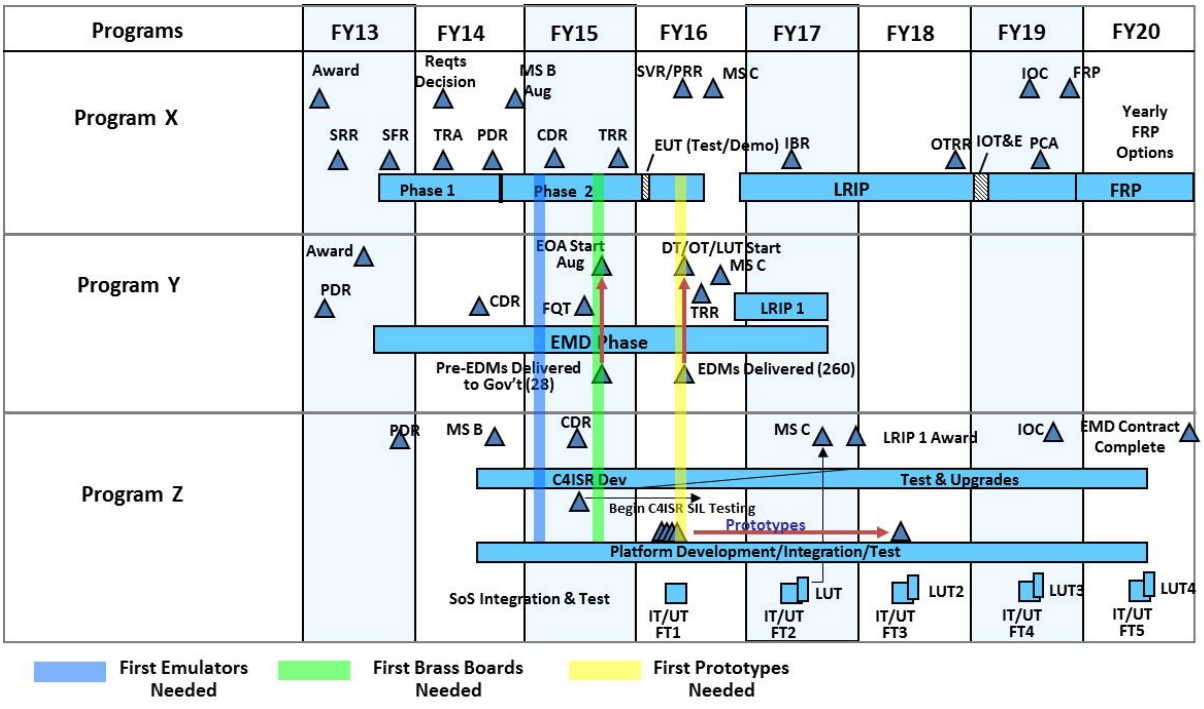


Figure 7-1. Notional Synchronization from the SEP Outline

- Develop an integration plan that tracks interdependent program touch points, identifies risks, and institutes a plan to mitigate them. The integration plan should:
  - Document the approach to identify interface requirements.
  - Define the interface products.

  - Describe the candidate integration sequences.
  - Show a coordinated delivery of verified Configuration Items.
  - Describe the integration test approach and facilities.

The following activities can assist the program to mitigate integration risks and promote strong communication and teamwork between the PMs of external programs and their contractors.

- Hold periodic meetings with all program, contractor, Service, and/or OSD stakeholders to review cross-program progress, risks, and issues. Build alliances to garner support in the event of unforeseen risks and issues.
- Establish a tiered, regular schedule of meetings with external programs and associated contractors to promote collaboration and information exchanges. Examples include program team meetings, risk review boards, Program Management Reviews, meetings among the PMs, PEOs, and/or the Service Acquisition Executives as issues warrant, etc.
  - At a minimum, the meetings should address the synchronization of program schedule activities, the results of a schedule risk assessment, and the technical, business, and programmatic risks. The meetings should track performance to plan of planned maturation activities, as well as any deviations from plans in order to inform risk control activities; integration and test activities; the adequacy of resources (funding and personnel); and a review of risks, issues, and opportunities.
  - Programs with key external dependencies should have representatives attend each other's technical reviews and meetings with Service and OSD leadership (OIPT, DAB, and Defense Acquisition Executive Summary meetings, etc.) as interface issues warrant.
  - Programs with key external dependencies with other programs in development should consider inserting liaisons into one another's program offices to facilitate coordination, as well as assess progress and risks.
  - To maintain visibility into the health of the interfaces between programs, the traditional interdependency chart can depict program health and challenges. Figure 7-2 shows an example of a program's tracking of the cost, performance, schedule, technology, and system-of-systems management with external programs.

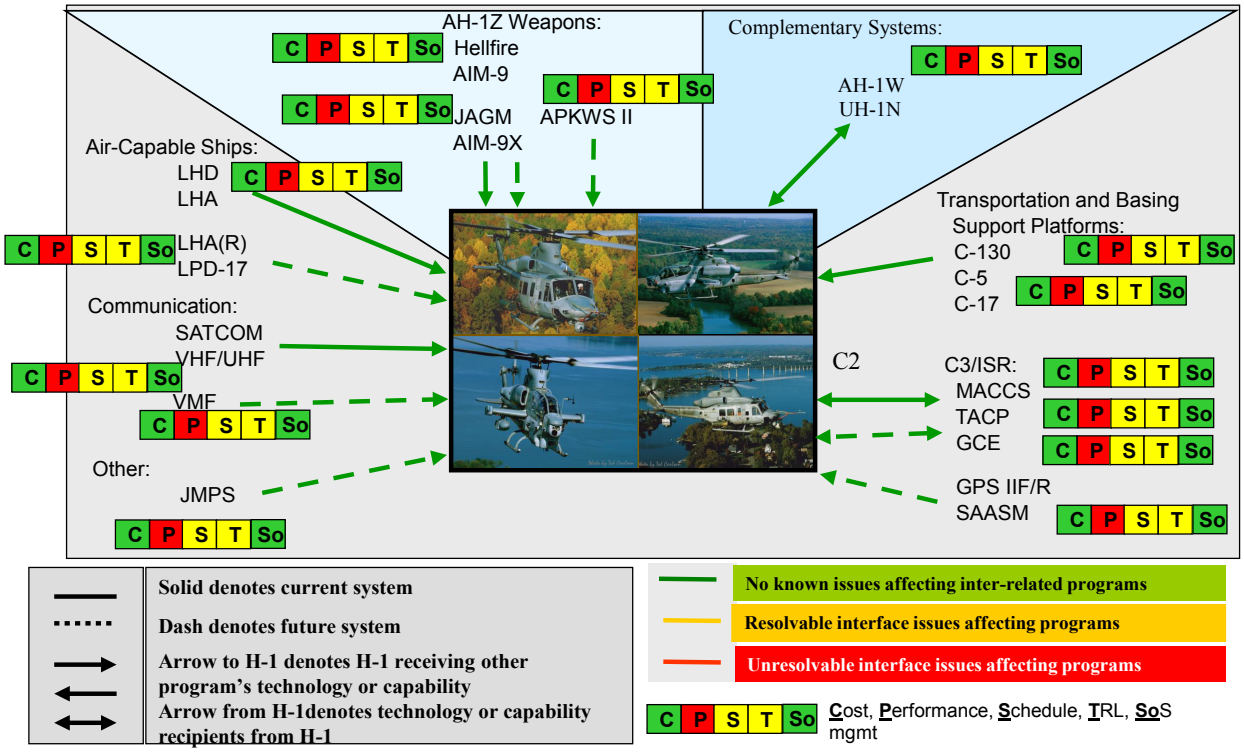


Figure 7-2. Tracking Interdependency Risks

Expectations:

- There is collaboration and a sense of "shared destiny" between programs with critical dependencies.
- Programs are bound by the agreements documented in MOAs.
  - External programs know and accept their space, weight, power, cooling, and performance allocations.
  - Programs that are critically dependent on others agree to provide early warning to associated programs if their systems exceed the cost, schedule, and/or performance tripwires established in the SEP and MOAs.
- The program schedule reflects sufficient time for integration and test, as well as corrective actions.
- Senior managers implement external risk management, which includes cross-program risks and risks that the program may be generating for other programs.

This page intentionally blank.

APPENDIX A. RISK MANAGEMENT CONSIDERATIONS DURING ACQUISITION LIFE CYCLE PHASES

Many criteria should be met during the course of the system's life cycle. Some of these criteria are used as measures of the program's progress, such as the Acquisition Decision Memorandum (ADM) requirements entry criteria for event-driven technical reviews. Failure to meet one or more of these criteria can have undesirable consequences for the program, so it is prudent to look for risks among them. Figure A-1 depicts the DoDI 5000.02 acquisition life cycle.

The program team should assess any risks related to achieving the objectives of each acquisition phase upon entrance. The program team should assess the phase objectives by assessing, at a minimum, three aspects: (1) any applicable ADM requirements (phase exit criteria), (2) entry criteria for the next phase (per DoDI 5000.02), and (3) entry/exit criteria for the SETRs applicable to the phase (consistent with the program's SEP).

All of these aspects should be considered as part of performing Risk Identification. SETR checklists should be used continuously during the acquisition phase to identify the source of potential risks to preclude "discovery" just prior to the technical review. Tailorable checklists for each review can be found at the Acquisition Community Connection Practice Center website: https://acc.dau.mil/CommunityBrowser.aspx?id=25710.

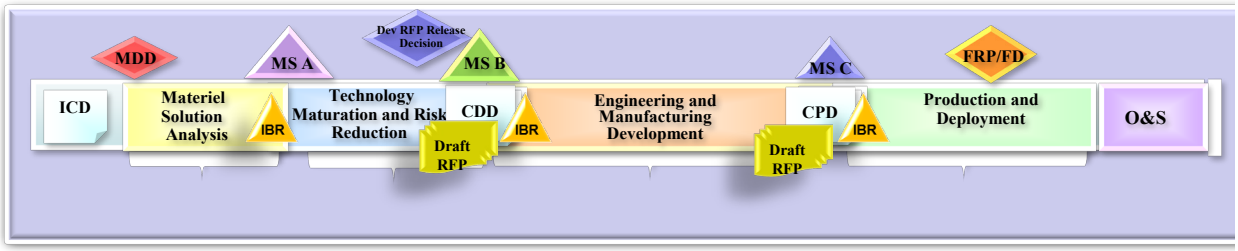


Figure A-1. Acquisition Life Cycle

Expectations:

- Programs continuously use DoDI 5000.02 acquisition phase entry criteria, ADM requirements, and entry/exit criteria for upcoming SETRs as a framework for the program's risk management process.
- Risk management is included in RFP formulations, evaluation criteria and the offeror's proposed SOW including tasks and processes to be employed for risk management. Risk management processes and reporting requirements are flowed down to subcontractors and suppliers.

1. Pre-Materiel Development Decision

While not an actual acquisition life cycle phase, the key activities accomplished prior to the Materiel Development Decision (MDD) are the finalization of the ICD, formulation of the Analysis of Alternatives (AoA) guidance for the conduct of the AoA during the MSA phase, and initial development of effective acquisition approaches for the different alternatives under consideration.

Because the ICD described capability gaps form the basis around which capability requirements and performance requirements will be matured, it is important for acquisition community engineers (at the program, Service or OSD level) to review the ICD. Conducting engineering analysis of the ICD is a key risk management activity early in the program lifecycle. In order to better frame the AoA to identify risks, the ICD should be evaluated during the ICD coordination process by the acquisition community in the following areas:

- Does the ICD describe the attributes of the desired capabilities in terms of desired outcomes? Does the ICD contain broad descriptions of desired outcomes help ensure that the required capabilities are addressed without constraining the solution space to a specific, and possibly limited, materiel system?
- If a materiel approach is recommended, does the ICD contain rationale for the recommended best solution? Does the ICD make a recommendation on the type of materiel approach preferred for each capability gap: information system approach, evolutionary development of an existing capability, or a transformational approach?
- Does the ICD describe the capability gaps clearly? Are the capability gaps and the attributes of the desired capabilities described in terms of desired effects? Are the desired effects general enough so as not to prejudice decisions in favor of a particular solution?
- Are the ICD parameters for the capability attributes stated in measurable terms with measures and metrics with defined criteria so that the AoA can identify and assess a broad range of alternatives including near-term options?
- Is the expected environment and operating condition of the capability clearly stated in the definitions of the measures of effectiveness and suitability?

In preparing for the AoA, the acquisition community should assist the sponsoring Service in drafting the AoA guidance to assess the cost and feasibility of potential solutions to meet identified capability gaps. In so doing, the acquisition community helps to ensure the AoA identifies risks for each potential solution being considered, including relative risks between alternatives. The AoA guidance should require the AoA team to:

- Provide early assessment of the risks and acquisition impacts of alternatives under consideration
- Include a requirement for in-depth analysis of cost, schedule performance, and risk with each proposed alternative.

- Ensure all cost and schedule drivers for alternative solutions and requirements are clearly identified.
- Consider possible tradeoffs among risk, life cycle cost, schedule, and performance objectives (including mandatory Key Performance Parameters) for each alternative considered
- Require an assessment of whether the military requirement can be met in a manner consistent with the cost and schedule objectives recommended by the requirements validation authority
- Consider affordability analysis results and affordability goals if established by the MDA

The acquisition community should expect to support early systems engineering analyses and conduct an assessment of how the proposed candidate materiel solution approaches are technically feasible and have the potential to effectively address capability gaps, desired operational attributes, and associated external dependencies. Because the acquisition community is likely familiar with the alternatives being considered for the AoA, it can draft effective acquisition approaches for the different alternatives prior to the MDD. Developing notional schedules for each alternative based on analogous programs, assessing the technical feasibility of each alternative in areas of software development, integration, manufacturing, and reliability helps identify risks to be mitigated.

2. Materiel Solution Analysis (MSA) Phase

The purpose of this phase is to conduct the analysis and other activities needed to choose the concept for the product to be acquired, to refine the requirements, and to conduct planning to support a decision on the acquisition strategy for the product. Key engineering activities during this phase include trades between cost and performance, affordability analysis, risk analysis, and planning for risk management.

To help refine requirements, Sponsors should consider providing draft technical requirements to industry and involve industry in funded concept definition to support requirements definition. In doing so, the acquisition community receives industry feedback and recommendations on early stage draft requirements. Funded competitive concept definition studies (e.g., early design trade studies and operations research) inform decisions about requirements and are valuable inputs to formal Analysis of Alternatives conducted after the Material Development Decision.

Figure A-2 displays the risk touch points during the Materiel Solution Analysis Phase.

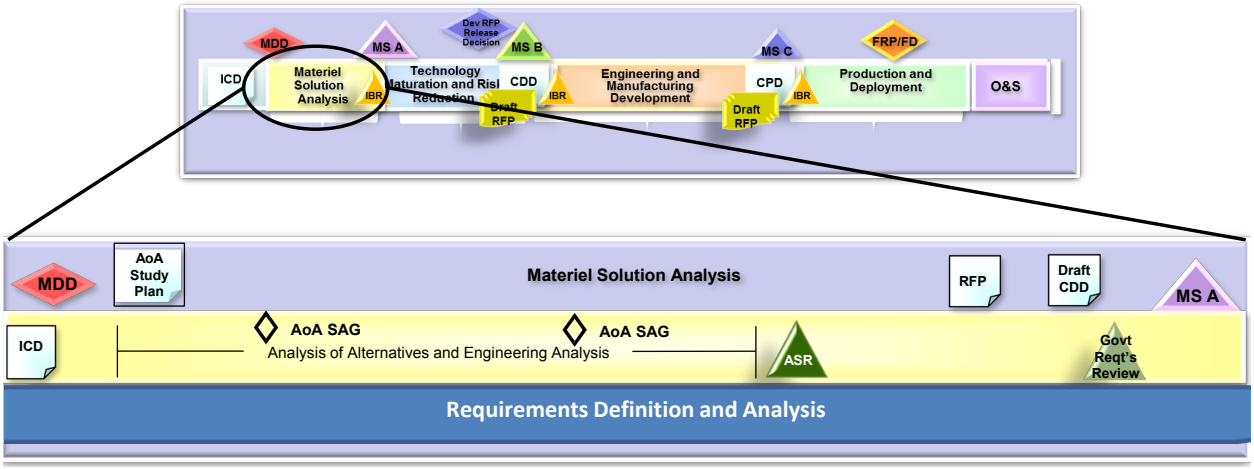


Figure A-2. Materiel Solution Analysis Phase[1] Risk Touch Points

Plans are made for an AoA to support the selection of a materiel solution by the Service sponsor. The plans include AoA Guidance and an AoA Study plan. Cost, schedule, technical, and programmatic risk should be assessed as part of any AoA. This is necessary to inform the available trade space and to inform the cost benefit analysis that is used to shape affordable technical development initiatives. DoDI 5000.02 identifies risks as a core element of AoA assessments.

While all known sources of risk should be considered, the program should focus on the following:

- Uncertainty (or confidence level) associated with each alternative's schedule estimate, proposed performance and associated technical risks. Each of these aspects should be assessed for realism relative to prior analyses and related systems (Engineering and Schedule Risk).
- Interfaces and dependencies that involve other programs. Consideration should be given to program maturity and risks associated with the interfaces themselves (Integration Risk).
- Critical technologies required for each alternative. What is the present maturity of each? What are the risks associated with bringing the critical technologies to the needed levels of maturity in a timely and cost effective manner (Technology Risk)?

Key to reducing risk early in the lifecycle is good communications between the requirements community and the acquisition community in the development of system requirements in JCIDS documents. The USD(AT&L) BBP 2.0 memo states, "acquisition leaders must work with requirements leaders early and effectively throughout the lifecycle of a product. Poor requirements definition at inception, requirements rigidity, and instability invariably lead to inefficiencies and sometimes to program failure. Acquisition leaders need to understand user priorities, and requirements leaders need to understand cost performance trade-offs and technical risk implications."

[1] Descriptions of activities by phase presented here emphasize risk management. Comprehensive descriptions of program phases are in the Defense Acquisition Guidebook, Chapter 4 (15 May 2013).

The SETR conducted during the MSA phase to assess and mitigate risk is the Alternative System Review (ASR). Following the selection of the preferred materiel solution, the program should hold an ASR. One purpose of the ASR is to ensure technical risk items are identified and analyzed, and appropriate control plans are in place. This is an extension of the work begun during the AoA, but now focused on a single materiel solution. The previous list covers those risks that need to be dealt with explicitly at this stage. Other sources of risk, peculiar to the chosen solution, should also be included in the analysis. During the MSA phase, risks of achieving phase exit criteria, as well as achieving the ASR's entry and exit criteria should be assessed and identified as part of Risk Identification.

The program needs to plan for the TMRR phase as part of the Milestone A decision. The TMRR phase is intended to mature an understanding of achievable requirements and develop a sufficient understanding of the materiel solution to support sound investment decisions at the pre-Engineering and Manufacturing Development (EMD) Review and at Milestone B. Specific outputs from the Milestone A decision include an assessment of technical risk and an understanding of the unique program interdependencies, interfaces, and associated MOAs. Specific risks should be identified for risk reduction, with exit criteria to be assessed at the end of TMRR. These risks should be captured in the RFP, inform the development of the program cost and schedule, and inform the acquisition strategy and any risk reduction prototyping plans.

Expectations:

- Programs explicitly assess integration, engineering, schedule, and technology risks related to alternative materiel solutions.
- Programs that depend on products and/or services from other programs are aware of the risks posed by changes that can occur in the complementary program's schedule and technical plans. Portfolio managers are aware of the risk of cascading events across the portfolio.
- Programs use the ASR risk assessment checklist to help identify and analyze risks.
- MSA phase outputs include a technical strategy that addresses the reduction of technical risk during the TMRR phase.

3. Technology Maturation and Risk Reduction (TMRR) Phase

The purpose of this phase is to reduce technology, engineering, integration, and life cycle cost risk(s) to the point that a decision to contract for EMD can be made with confidence in successful program execution for development, production, and sustainment.[2]

The key activities during the TMRR phase which reduce technical risk are:

[2] Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013.

- Risk reduction prototyping (at the system level or at the technology, subcomponents, or components level if appropriate) if they materially reduce engineering and manufacturing development risk at an acceptable cost.
- Competitive prototyping of the system, or for critical subsystems prior to Milestone B.
- Systems engineering trade-off analyses prior to the Requirements Decision Point to show how cost varies as a function of the major design parameters and support the assessment of final requirements in the Capability Development Document (CDD).
- Preliminary design activities (for example functional analysis, functional allocation, and preliminary design) up to and including a Preliminary Design Review (PDR) prior to source selection for the EMD phase.

Figure A-3 displays the risk touch points during the Technology Maturation and Risk Reduction phase. The SETRs conducted during the TMRR phase to assess and mitigate risk are the System Requirements Review (SRR), the System Functional Review (SFR), and the PDR. Throughout the TMRR phase, the program team is expected to conduct a rigorous assessment of technical risk, determine risk mitigation plans, and work with the PM to resource the mitigation plans.

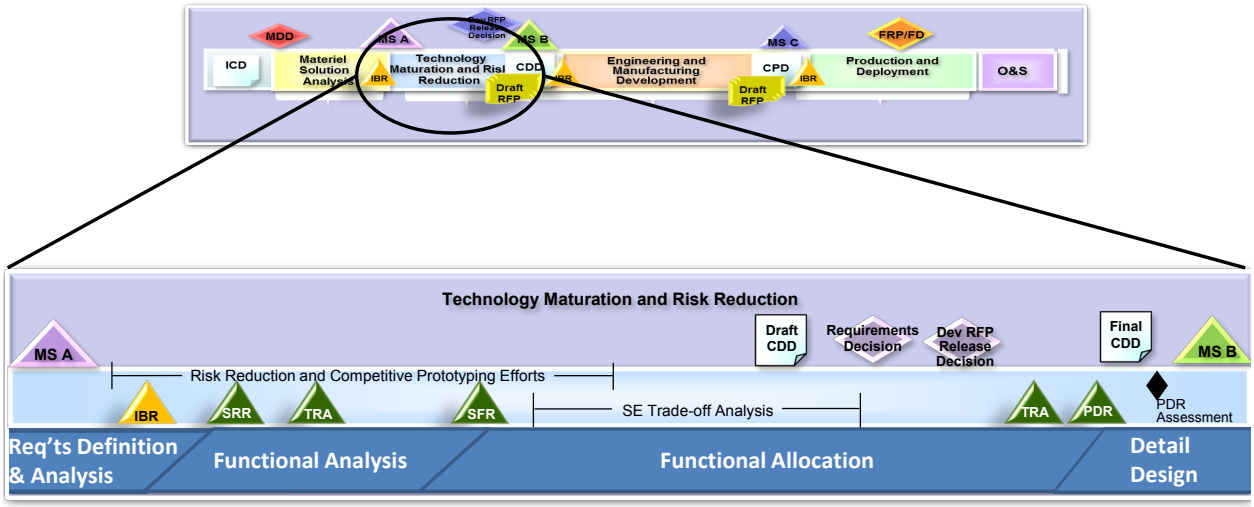


Figure A-3. Technology Maturation and Risk Reduction Phase Touch Points

The program can reduce technology risk by maturing the program critical technologies, demonstrations in a relevant environment, and assessment of demonstration results against requirements and stakeholder expectations. The character of risk reduction expected during the TMRR phase was explained in the directive memorandum for USD(AT&L) initiative Better Buying Power 2.0 and captured in DoDI 5000.02 as follows:

"*Technology Readiness Levels, …. should he used to benchmark technology risk during this phase; however, these indices are rough benchmarks, and not conclusive about the degree of risk mitigation needed prior to development. Deeper analysis of the actual risks associated with the preferred design and any recommended risk mitigation must be conducted and provided to the MDA." [(November 26, 2013)]*

During competitive and risk reduction prototyping, risks of achieving SRR entry criteria should be identified as part of Risk Identification.

The SRR confirms that the user requirements have been translated into system specific technical requirements, critical technologies are identified, required technology demonstrations are planned, risks are well understood, and mitigation plans are in place. The SRR ensures that the system under review is ready to proceed into end-item development, functional analysis, and development of the system functional baseline with acceptable risk.

The System Functional Baseline is established at the SFR. The SFR ensures that the system under review is ready to proceed into preliminary design, and that all system requirements and functional performance requirements derived from the system/subsystem specification (S/SS) are defined, aligned with the external environment (systems and infrastructure) and consistent with cost (program budget), schedule (program schedule), acceptable technical risk, and other system constraints. Risk items associated with functional requirements are identified and analyzed, and control plans put in place. This checklist can also assist in identifying technical risks associated with the Milestone B decision.

The PDR occurs following completion of functional allocation and preliminary design. The PDR confirms that all functions and performance requirements derived from the system specification and functional baseline are fully decomposed to their lowest level, inclusive of the operational, training, and support systems, aligned with the external environment (systems and infrastructure) and consistent with cost (program budget), schedule (program schedule), and other system constraints. The PDR supports the Milestone B decision and ensures that the system under review is ready to proceed into detail design (development of manufacturing drawings, software code-to documentation and other fabrication documentation) with acceptable risk.

The risk-related outputs of the TMRR phase are:

- Assessment of whether TMRR phase risks were adequately mitigated. Confirmation at the end of TMRR phase that critical technologies have been demonstrated in a relevant environment.
- EMD schedule, integration, (including program interdependencies), and manufacturing risks are acceptable.
- Determination that system requirements, as documented in the CDD are achievable as shown by fully traceable allocation to CIs and a completed allocated baseline.
- Risk control in connection with the unique program interdependencies, interfaces, and associated MOAs.

Beyond the structure of a risk management process, it is important that programs establish a viable means of addressing emerging risks that recognizes the realities of funding allocations on work priorities. Since emerging risk control alternatives often require additional resources, the outcome can be inaction or "accepting the risk." Accordingly, good risk management practices should include consideration of contingency funding tailored to the program nature and circumstance.

Expectations:

- During the TMRR phase the program team conducts rigorous and persistent assessments of technical risk, determines risk mitigation plans, and works with the Program Manager to resource the control plans.
- The SFR and PDR risk assessment checklists are used to help identify and analyze risks.
- Risks related to completion of each of the artifacts comprising the Functional and Allocated Baselines were addressed.
- The IMS is regularly updated to help manage risks and link identified risks to a specific task traceable to the IMP and WBS.
- Competitive and risk reduction prototyping focused on reducing the specific technical risks in the design for the actual product to be built and tested in EMD.
- All sources of risk have been adequately controlled to support a commitment to design for production. This includes technology, engineering, integration, manufacturing, sustainment, and cost risks.
- The technical, cost, and schedule risks of acquiring the product are understood, and have adequate plans and programmed funding to mitigate those risks prior to Milestone B.
- Requirements, technology, engineering, integration, manufacturing, logistics, and life cycle cost risks are addressed to the point that a decision to contract for Engineering and Manufacturing Development can be made with confidence in successful program execution for development, production, and sustainment.

4. Engineering and Manufacturing Development (EMD) Phase

The purpose of the EMD phase is to develop, build, and test a system or one or more increments of capability to verify that all operational and derived requirements have been met, support subsystem functionality, and all internal and external interfaces.[3] This phase completes all needed hardware and software detailed design, develops the product baseline, verifies it meets the functional and allocated baselines, and transforms the preliminary design into a producible design. The phase includes the completion of all needed hardware and software detailed design. The EMD phase systemically reduces risks to an acceptable level, builds and tests prototypes or first articles to verify compliance with requirements, and prepares for production or fielding. It includes the establishment of the

[3] Interim DoD Instruction 5000.02, "Operation of the Defense Acquisition System," November 25, 2013.

product baseline for all configuration items, future production or fielding decision. EMD completes the design process to include defining system

Figure A-4 illustrates the risk touch points during the EMD phase. The SETRs conducted during the EMD phase to assess and mitigate risk are the Critical Design Review (CDR), the System Verification Review (SVR), the Functional Configuration Audit (FCA), and the Production Readiness Review (PRR). The risk management activities turn from a focus on technology maturation to transition from development to production. The program identifies risks related to critical manufacturing process and key product characteristics. Specific risk areas are:

- Requirements Stability
- Integration and Interdependency
- Manufacturing
- Supply Chain

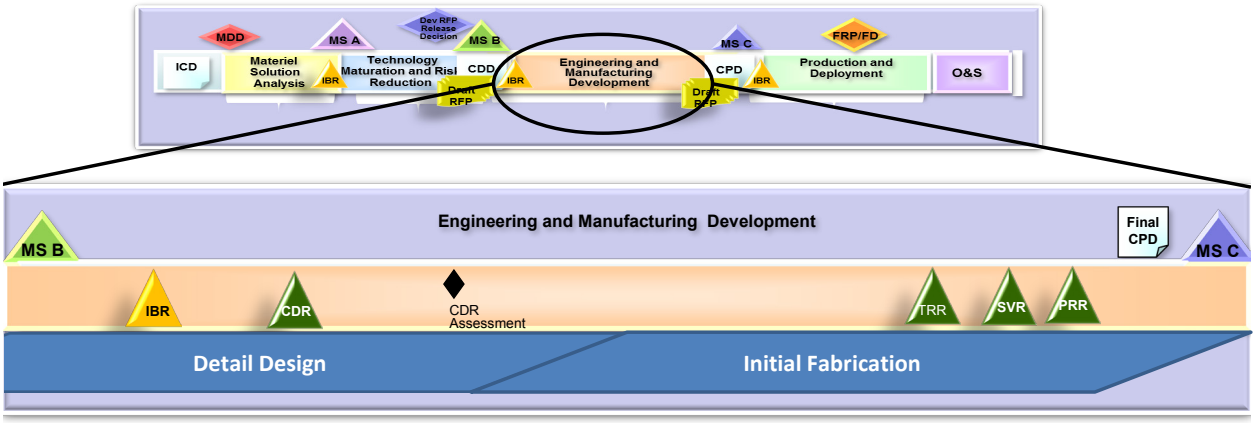


Figure A-4. Engineering and Manufacturing Development Phase Risk Touch Points

As in the TMRR phase, consideration of risk and risk control are important components of the successive technical reviews. Following Milestone B and during the detail design work effort, risks of achieving CDR entry criteria should be identified.

The CDR confirms that all functions and performance requirements derived from the system specification, functional baseline, and allocated baseline are captured in the initial product baseline (build-to documentation), inclusive of the operational, training, and support systems, aligned with the external environment (systems and infrastructure) and consistent with cost (program budget), schedule (program schedule), and other system constraints. The CDR ensures that the system under review is ready to proceed into hardware fabrication and software coding with acceptable risk.

Following CDR and during the initial fabrication work effort, risks of achieving SVR, FCA, and PRR entry criteria should be identified.

The SVR confirms that all tests and verification of functions are complete, and establishes and verifies final product performance. The SVR ensures that the system under review can proceed into LRIP with acceptable risk.

A FCA may also be conducted concurrently with the SVR. The FCA is the formal examination of the as-tested characteristics of a configuration item (hardware and software) with the objective of verifying that actual performance complies with design and interface requirements in the functional baseline. A successful FCA typically demonstrates that the EMD product is sufficiently mature for entrance into Low-Rate Initial Production (LRIP).

The PRR reviews the readiness of the manufacturing processes, the quality system, the availability of materials, and the production planning (facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.). Successful completion of the PRR establishes that the system requirements are fully met in the final production configuration and that production capability forms a satisfactory basis for proceeding into LRIP with acceptable risk.

The SVR, the FCA, and the PRR, are sometimes held concurrently. These SETRs have as a single goal, from the risk perspective, to be an assessment of the product and processes to ensure the system under review can proceed to validation and LRIP and full-rate production within cost, schedule, risk, and other system constraints. Success in these reviews reduces the risk in operational test and evaluation.

Expectations:

- Programs use the CDR risk assessment checklists to help identify and analyze risks.
- Risks related to completion of each of the artifacts comprising the Initial Product Baseline are addressed.
- The program completes a technical risk assessment for entering into fabrication of hardware and software configuration items with a determination of acceptable risk for full commitment to fabrication, construction/coding, and/or purchase.
- Programs use the SVR/FCA/PRR risk assessment checklists to assist in identifying and analyzing technical risks for Milestone C.
- Programs assess the maturity of critical manufacturing processes to ensure they are affordable and executable.

5. Production and Deployment (P&D) Phase

The purpose of the Production and Deployment (P&D) Phase is to produce and deliver requirements-compliant products to receiving military organizations. Figure A-5 displays the risk touch points of the P&D phase. The program teams develop rigorous P&D risk mitigation options to plan and resource effective risk control actions.

Specific actions include:

- Identifying acceptable risks and mitigation plans for achieving Initial Operational Capability (IOC) and Full Operational Capability (FOC)
- Updating the RMP to reflect the sustainment risk assessment
- Supplier and Supply Chain Risk Management

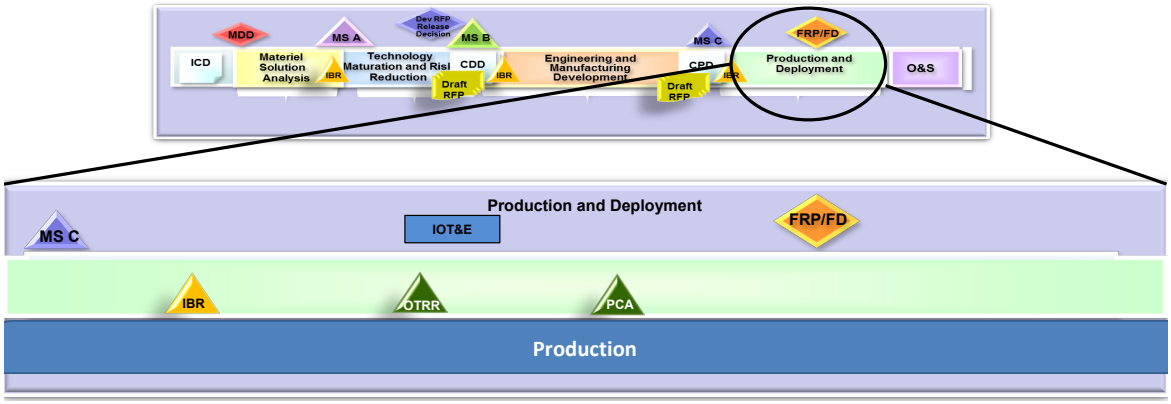


Figure A-5. Production and Deployment Phase Risk Touch Points

Following Milestone C and during Production, the risks of successfully completing Initial Operational Test and Evaluation and achieving the Physical Configuration Audit (PCA) should be identified as part of Risk Identification. The PCA, which may be conducted during the P&D phase, is a formal audit of the verification and validation results against the Product Baseline and the Capability Production Document. One exit criterion is the determination of acceptable technical risk for fielding and sustainment.

Expectations:

- The program team conducts rigorous production risk assessments and puts in place plans and resources to effectively mitigate any unacceptable risks.
- Programs use the PCA risk assessment checklists to help identify and analyze risks.
- IOC and FOC risks are acceptable.
- The RMP is updated to include assessment of sustainment related risks.
- For mission-critical functions and components, the program obtains an analysis of supply chain risk.
- Prior to the production decision, the program ensures that all unacceptable manufacturing risks are addressed and that applicable manufacturing processes are under statistical process.

6. Operations and Support (O&S) Phase

In the O&S phase, the risk activities include monitoring in-service usage, problem reports, parts availability/obsolescence, engineering modifications, technology insertions, and operational hazard risks. Following declaration of the system IOC, risks of achieving the In-Service Review (ISR) exit criteria should be identified. The ISR is a multi-disciplined assessment to characterize the in-service health of the deployed system and enabling system elements (training, user manuals, documentation, etc.). Risk management activities in the course of the ISR include risk assessment of operational hazards, product baseline integrity, supply chain status, determination of acceptable operational hazard risk, and in-service usage/support risk.

Expectations:

- The program team continuously monitors service usage, problem reports, parts availability/obsolescence, engineering modifications, technology insertions, and operational hazards.
- When necessary, program teams implements plans and resources to effectively mitigate any identified unacceptable risks.

7. Systemic Areas of Risk Found in DoD Acquisition Programs

As indicated in paragraph 3.1 of the main body, independent assessments are a risk identification activity that can provide early warning of potential risk areas. The Office of the Deputy Assistant Secretary of Defense (Systems Engineering) conducts independent technical assessments (Program Support Assessments). Below are the top systemic findings observed over 120 of these assessments which provide insight into common risk areas. Each of these systemic issues has been found in at least 25 percent of the assessments conducted and should be considered when initiating a program.

- Program Schedule – technical assessments have found 42% of program schedules are not realistic and 28% of programs are not likely to achieve the planned schedule
- Budget – 38% of program budgets are not sufficient for the effort required
- Acquisition Strategy – assessments have found 32% of programs need restructuring of the program's acquisition strategy
- Design Verification – Planned testing is incomplete or inadequate in 26% of programs
- Reliability Performance – 26% of programs have not established a reliability growth plan
- Risk Management – 25% of programs do not have sufficient risk management tools or do not use appropriate risk management methodologies
- Requirements Development – Requirements are vague, poorly stated, or not defined in 25% of programs

APPENDIX B. COMMON RISKS AND MITIGATION ACTIVITIES

Common risks associated with selected technical, programmatic and business risks realized by programs, as well as proactive activities to mitigate them are provided below for consideration in improving program planning and execution activities:

1. Risk: Technical (Requirements)

Proactive risk mitigation activities:

MSA Phase

- Establish an affordability goal.
- Develop design concepts to assess the state of the possible and inform requirements, RFP, and source selection activities.
- Hold a Government only requirements review to ensure the proper translation of the user requirements into the performance specification.
- To facilitate the success of the program, ensure that it is guided by a small set of key requirements (e.g., minimize the number of KPPs and KSAs per CJCSI 3170 to preclude impacting the contractors trade space).
- Ensure that the Government and bidding contractors have a complete and common understanding of the requirements:
    - Solicit Industry feedback regarding the feasibility of requirements, unit costs, and maturity of envisioned technologies via industry days, individual meetings with prospective bidders, and requests for information.
    - Provide a crosswalk between the performance specification and draft CDD in the Request for Proposal.
- Establish the requirement in the performance specification for an open systems architecture which enables a cost effective and rapid development of systems that are interoperable in the joint battle space. Open systems architecture contains vendor-independent, non-proprietary system or device design based on official and/or popular standards. It allows all vendors (in competition with one another) to create add-on products that increase a system's (or device's) flexibility, functionality, interoperability, potential use, and useful life.
- When evaluating the potential use of commercial and Government off-the-shelf (COTS/GOTS) hardware and software, be mindful of required modifications that affect SWAP-C allocations, integration challenges, performance degradations resulting from the integration in a new platform, and support implications.

TMRR Phase

- Ensure that contractors are required to identify problematic requirements as well as cost/schedule driving requirements in their proposals and early in the TMRR phase to support the maturation of the CDD requirements.
- Conduct systems engineering trade-off analysis to assess their affordability and technical feasibility. The systems engineering trade-off analysis should:
    - Depict the relationship between life cycle cost, system performance requirements, design parameters and delivery schedules.
    - Show how cost varies and a function of system requirements (including Key Performance Parameters, major design parameters and schedule.
    - Identify affordability drivers to the MDA and how the program meets affordability constraints.
    - Be reassessed over the acquisition life cycle as system requirements, design, manufacturing, test, and logistics activities evolve and mature.
- For trade studies affecting KPP/KSAs, a defined decision hierarchy should be developed to timely mitigate technical risks and their potential impact on the schedule.
    - If trade study decisions are not made within 2 weeks after the completion of the trade study, they need to be continually escalated to the next level until a binding decision is made.
    - To ensure timely decisions, the PM should be empowered to make decisions on all requirements below the KSA level.
- Prototyping activities conducted during the TMRR phase should be representative of the planned end item design in order to have merit in informing trade-studies and mitigating integration, technology, technical and/or engineering risks.
    - Ensure stable requirements to preclude requirements changes which negate the relevance of prototyping and associated investments.
- Prepare a post Milestone SEP update (Service Approved) that reflects the contractor(s) technical planning (e.g., detailed schedule, TPMs, the contractor's organization, etc.). This establishes the baseline for assessing performance to plan in order to inform risks and required risk mitigation activities.
    - Interim values for TPMs should be developed and reviewed during the normal battle rhythm of program activities to inform areas of potential risk.

EMD Phase

- Avoid requirements creep. All new requirements should be pushed to the next increment resultant to mitigate resultant performance, cost, and schedule risks.

- Hold annual Configuration Steering Board (CSB) meetings to ensure technical performance requirements are balanced with the allocated schedule and funding.
    - CSBs and/or Knowledge Point reviews should include the requirements community and assess: problematic requirements; Systems engineering trade-off analysis; cost and schedule driving requirements; and the sensitivity of requirements.
    - In accordance with BBP 2.0, CSBs should be highly visible to and coordinated with the JROC , particularly when required changes to KPPs or KSAs could jeopardize a program's military utility or affordability
- In order to mitigate technology, technical, integration, or performance risks; work with the user to define a capabilities roadmap that facilitates fielding the initial increment of capability within the allocated schedule and funding.
- Based on insights from the critical design review and testing, ensure that the final CDD reflects low risk achievable requirements to reduce performance risks during the OT&E.

TMRR, EMD, and PD Phases

- Plan for contingencies and technical risk mitigation activities, by establishing schedule, performance and cost margins.
- Allocate SWAP-C requirements to all components and systems, and ensure that realistic growth margins are established to accommodate growth as the program progresses through development and transitions into production.

2. Risk: Technical (Technology)

Proactive risk mitigation activities:

MSA and TMRR Phase

- Limit the number of critical technologies (<Technology Readiness Level (TRL) 6).
    - Structure TMRR phase activities to confirm during the hardware build, integration, and test activities that performance at TRL 6 or higher can been demonstrated by MS B.
- Ensure that the TMRR phase RFP requires the contractors' TMRR phase proposals to:
    - Include an assessment of the maturity of proposed technologies.
    - Identify mature alternative technologies for any technology that is assessed to be less that TRL 6.
    - Identify resourced off-ramps in the Integrated Master Schedule (IMS), submitted with the contractor's proposal, for technologies that are not maturing as planned.

TMRR, EMD, and PD Phases

- Conduct a Government Technology Readiness Assessment early in the TMRR phase to identify and assess critical technology elements in the contractors' proposal.
    - Develop detailed time phased maturation plans.
- Keep sponsors/leadership informed of associated technology risks and mitigation plans.
- Ensure that the IMS includes resourced off-ramps for technologies that are not maturing as planned; Execute off-ramps as planned to mitigate performance and schedule risks.

EMD and PD Phase

- Plan/implement technology refresh cycles in the development and operations phases to proactively address technology obsolescence risks.

3. Risk: Technical (Integration, Testing, Manufacturing)

Proactive risk mitigation activities:

MSA Phase

- Develop a competitive and risk reduction prototyping strategy is focused on burning down technical risk areas in order to give the program a clear understanding of technical risks (e.g., technology, engineering and integration).
- Solicit an integration plan, IMS through prototype delivery, and drawings/models in the TMRR phase Request for Proposal to assess the bidding contractors' understanding of the technical associated with developing the systems effort and required planning to execute it.

TMRR and EMD Phases

- Be proactive in the early identification and mitigation of risks by planning to conduct an effective developmental test and evaluation program which:
    - Contains risk reduction and competitive prototyping of the system or key subsystems which are representatives of the actual end item in order to: reduce technical risk, validate designs and cost estimates, evaluate manufacturing processes, refine requirements, and inform the preliminary design of the end-item. In the end, prototyping should reduce the time to fielding.
        - This precludes the discovery of serious design issues late in the development process which can delay a program at a great expense due to the delays in the contractor team's efforts.
        - These activities prior to the commitment to EMD can make all the difference between a successful EMD and one that experiences massive overruns.

  - Reflects a full set of event driven developmental test activities across the program's acquisition lifecycle (e.g., hardware in the loop testing in system integration laboratories, environmental stress screening at the subsystem level, reliability growth testing and software testing in emulators) to support risk reduction, design validation, and requirements verification.

- Is planned conducted as efficiently as possible to avoid costs by discovering problems as early as possible.
- Is structured to provide program management and technical leadership insights into the technical, technology, and integration risks, which may impact the system's compliance with user and specification requirements[4].
- Ensure that the RFP contains a requirement for the winning contractors to perform shakedown testing with defined success criteria to facilitate resolving integration activities and early failures modes prior to the start of Government testing.

EMD Phase

- Burn down integration risks through the use of a combination of component/subsystem hot benches, Systems Integration Labs (SIL), high value test assets, early prototypes and full prototypes.
- Utilize early prototypes as part of the normal integration process for complex systems to:
  - Facilitate the integration of major subsystems and infrastructural components; as well as the discovery/resolution of subsystem-level interaction issues.
  - Provide evidence of systems integration maturity and risk burn down through the Government check out of the system prior to full prototype build and qualification testing.
  - Provide the first exposure of the system to stressing environments.
  - Provide early feedback of the system design to inform the Critical Design Review.
  - Help mitigate technical, cost and schedule risks associated with full prototypes. Examples of technical issues uncovered by early prototypes:
    - Mechanical fit, alignment and interface issues between subsystems or with structures.
    - Assembly/maintenance access issues.
    - Shielding and grounding issues with cables and boxes.
    - Communications issues such as boxes not responding as expected or signal noise caused by impedance mismatches, shielding and grounding

[4] Frank Kendall, "Perspectives on Developmental Test and Evaluation," March 2013 https://acc.dau.mil/adl/en-US/653463/file/72222/March_2013_ITEA_Journal_Kendall_Dev_Test.pdf

        - Fault thresholds set too tight that contribution to the unnecessary shutdown of boxes or subsystem

- The EMD phase schedule reflects the completion of qualification testing prior to the Low Rate Initial Production decision.

4. Risk: Programmatic (Schedule)

Proactive risk mitigation activities:

MSA Phase

- Develop a low risk program schedule early in the program. The schedule should:
    - Be representative of historical programs vice being externally driven.
    - Reflect the full suite of SE technical reviews.
    - Contain the appropriate phasing between activities.
    - Contain sufficient time for integration, test, and corrective actions.
    - Contain schedule margin to accommodate unplanned risks and issues.
    - Be "event" versus "schedule" driven to ensure that risks are mitigated prior to proceeding to the next phase.
    - Be structured to ensure that system performance is demonstrated prior to significant financial commitments.
    - Contain an acceptable level of concurrency.

Include an IMP, top level schedule, and risks in the RFP to inform the contractors' proposal.

- Assess the contractor's Integrated Master Schedule during source selection to assess the contractor's understanding of the technical effort and required phasing of the work package.

TMRR, EMD, and PD Phases

- Avoid the urgency of schedule need outweighing good engineering and program management.
- Ensure that the program schedule reflects realistic and event-driven phasing for systems engineering, integration, and test activities, to include sufficient time for integration activities and corrective actions.
- The program has Tier 2 and below schedules that show technical and integration activities such as:
    - Technical reviews, program management reviews, technical interchange meetings which address technical and integration efforts reflected.
    - Stand-up of system integration laboratories and contractor and/or Government facilities.
    - Integrated system performance of full-up prototype prior to MS C.
    - Development, integration, and test activities with external programs.

  - A bridge contract to maintain engineering and manufacturing expertise/qualification of production line, when warranted.

- Program management control efforts include the linkage between the Integrated Master Plan (IMP), Integrated Master Schedule (IMS), Technical Performance Measures, risk management, and earned value management.
  - The IMS depicts a likely progression of effort and work through the remaining activities and events in the acquisition phase.
  - The IMS contains activities to perform all integration activities (e.g., modeling & simulation, hardware and software integration, distributed simulation, component, subsystems, system, Family of Systems and/or system-of-system-level integration). The IMS reflects:
    - Resourced off-ramps related to high risk technologies and integration challenges.
    - The integration of schedules with key subcontractors and suppliers.
    - Delivery schedules and integration activities with external programs.

- Conduct Schedule Risk Assessments on a regular basis to assess risks and inform mitigation activities associated with achieving the next systems engineering technical review, major test event, and acquisition milestones.

5. Risk: Programmatic (Communication)

Proactive risk mitigation activity:

MSA, TMRR, EMD, and PD Phases

- Ensure horizontal communications across IPTs and vertical communications up through management (e.g., the lead systems engineer, PM, PEO, etc.).

- To mitigate program execution risks, garner and sustain the support of senior leadership from within the acquiring command and user.
  - Build and maintain a robust external senior leader stakeholder group.
    - Establish an empowered working group with representatives from each organization.
    - Pull in every organization that could possibly support/derail the program.

- Ensure stakeholders understand the basis for the technical requirements, so they "own" and support them.
    - Ensure they understand the need to control requirements creep.
  - Track key leader turnover in each organization; brief the new leadership on the importance of the program.

- Build alliances with all stakeholders who can provide support in mitigating inevitable technical, programmatic, and business risks.
    - Ensure transparency with Service, user, OSD, and Congressional stakeholders by providing them with progress of ongoing efforts (e.g., competitive and risk reduction prototyping, systems engineering trade-off analysis, and knowledge point reviews) on a regular basis and the impact of any proposed funding reductions.
    - Hold Working Integrated Product Team (WIPT) meetings (e.g., systems engineering, acquisition, test and evaluation, etc.) with the Office of the Secretary of Defense and Service staff engineers on a regular basis to the assess system maturation (e.g., performance to plan of Technical Performance Measures) as well as any associated risks, issues, and/or opportunities.

6. Risk: Business (Dependencies)

Proactive risk mitigation activities:

TMRR, EMD, and PD Phases

When the fielding of a new system that is critically dependent on other programs outside of the PEOs portfolio or from another Service, the following activities can aid in the management and alignment of activities:

- Seek program champions within the Service(s) and Office of the Secretary of Defense who can:
    - Exert strong management control over critical interfaces with external programs.
    - Align funding and priorities (funding, schedule, form factors requirements, etc.) of external programs.
    - Instill in subordinates a sense of urgency in the system's development and fielding.
- Ensure interface management is in place to meet cost, schedule, performance requirements, and ultimately program success.
    - Internal and external interface requirements are documented in the Interface Control Documents and Interface Requirement Specifications.
    - Establish an Interface Control Working Group to identify and resolve interface issues at the lowest possible level.
    - Develop a time phased fast track issue identification and resolution process established that raises issues sequentially to the PM, PEO, Service Acquisition Level, and Defense Acquisition Executive in order to align priorities and resources (e.g., if an issue is not resolved within a specified period such as two weeks, it should be elevated to the next management layer until it's resolved).

- Develop Memorandums of Agreements (MoA) with all external programs in order to identify and manage the critical interfaces. These MOAs should be documented in the Acquisition Strategy and SEP.
    - MOAs between inter-dependent programs establish roles and responsibilities associated with dependency. They should include agreements on cost, schedule, performance, and details (or planning) of any functional and/or physical interfaces. The status of required MOAs is covered by a mandated table in each program's SEP.
    - The MoAs should contain cost/schedule and performance "tripwires" that require a program to inform other programs within the Family of Systems/System-of-systems of any significant (nominally > 10%) variance in cost, schedule, or performance.
    - Associate Contractor Agreements should also be put in place between the contractors to facilitate working relationships between them.
- Develop and maintain a synchronized schedule that shows prototyping, technical reviews, integration and test activities, and acquisition milestones for associated programs. Assess schedule performance to plan on a regular basis to inform risk identification activities.
- Develop an integration plan which tracks interdependent program touch points, identifies risks, and institutes a plan to mitigate them. The integration plan should document the approach to identify interface requirements, interface products, candidate integration sequences, a coordinated delivery of verified Configuration Items, along with the integration test approach and facilities.
- To mitigate **integration** risks, promote strong communication and teamwork between the PMs of external programs, and the Contractors.
- Hold periodic meetings with all program, contractor, Service and/or Office of the Secretary of Defense stakeholders to review cross program progress, risks and issues. Build alliances to garner support in the event of unforeseen risks and issues.
- Establish a tiered battle rhythm of meetings with external programs and associated contractors (e.g., meetings at the IPT level, as well as PM and PEO levels) to promote collaboration and information exchanges. Examples include IPT meetings, risk review boards, Program Management Reviews, meetings between the PMs, PEOs and /or the Service Acquisition Executives as issues warrant; etc.).
    - At a minimum, the meetings should address the synchronization of program schedule activities; results of schedule risk assessments; technical, business and programmatic risks; the performance to plan of planned maturation activities as well as any deviations from plans in order to inform risk control activities; integration and test activities; and the adequacy of resources (funding and personnel); and a review of risks, issues and opportunities.
    - Programs with key external dependencies should have representatives attend each other's technical reviews, and meetings with Service and OSD leadership

(Overarching Integrated Product Team (OIPT), Defense Acquisition Board (DAB), and Defense Acquisition Executive Summary (DAES) meetings, etc. as interface issues warrant.

- Programs with key external dependencies with other program in development should consider inserting liaisons into each other's program offices to facilitate coordination as well as assess progress and risks.

7. Risk: Business (Resources)

Proactive risk mitigation activities:

TMRR, EMD, and PD Phases

Establish a funding instability risk in the risk register to be prepared to substantiate the impact of any proposed funding reductions, including any resultant technical, technology, integration and/or engineering risks.

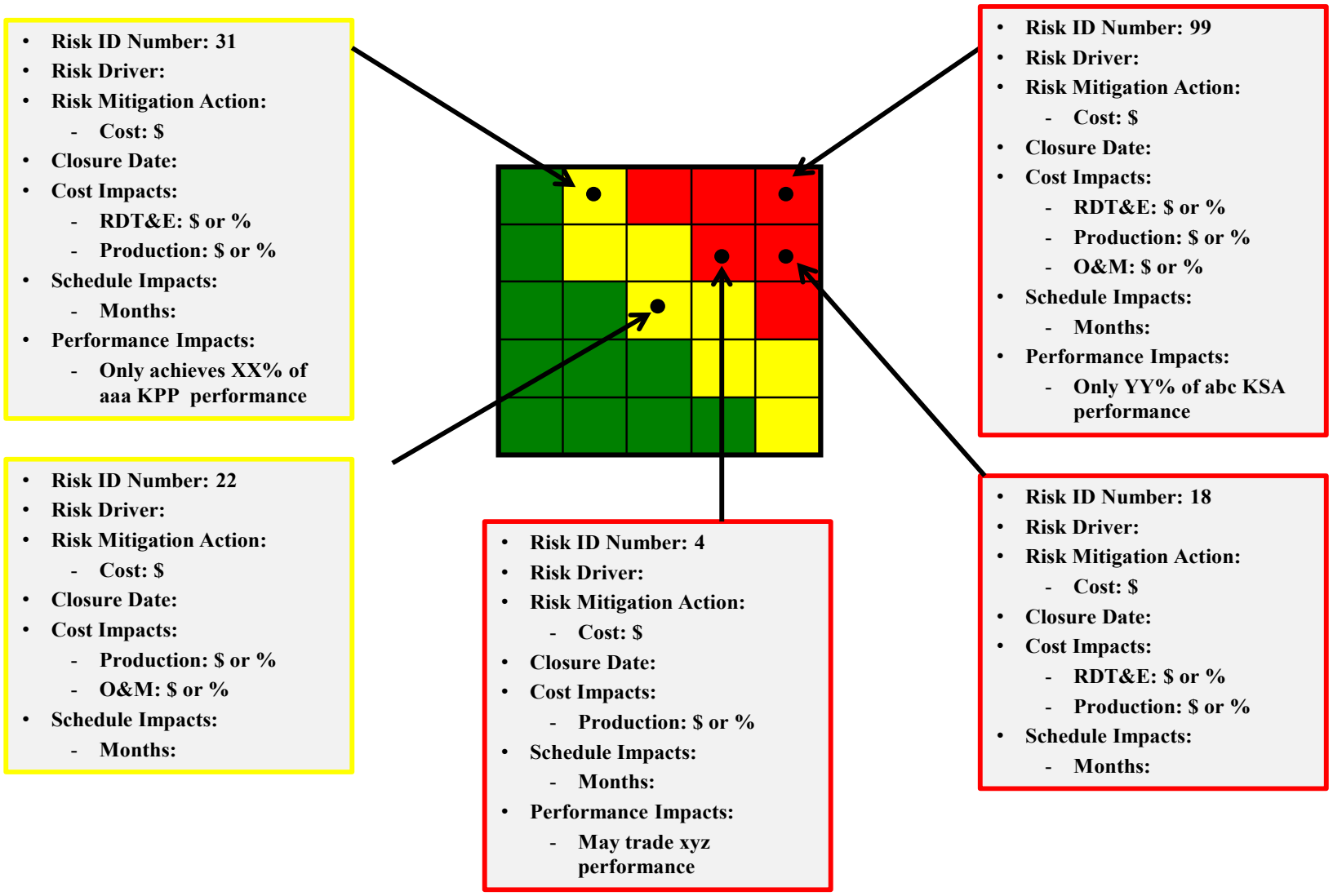
- Keep the cost team busy with quantifying the technical impact of "what if" funding cut scenarios, such as 5%, 10%, 15%, etc. reductions.
    - Understand the impacts and mitigations before the question is asked.
- Solicit information from the requirements sponsors who know the capability priorities which cannot be deferred.
- Don't mask the impacts of proposed realized funding reductions. Ensure that leadership fully understands the implications of the funding cut. On the other hand, don't overstate the impact either – since program credibility is on the line.

APPENDIX C. SAMPLE TEMPLATES: REPORTING MATRICES FOR RISKS, ISSUES, AND OPPORTUNITIES

1. Sample Risk Register

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood Rating	Consequence Rating	Risk Reporting Matrix	Risk Mitigation Strategy	Submitted Date	Board Review	Planned Closure	Expected Risk Rating	Plan Status
8231	3.2.2	Mr. Bill Smith	Technical	Open	II	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	3	4	Yellow	Control - Program will apply management reserve to retain adequate software engineers to burn-down SW defects	8/23/2013	1/14/2014	2/12/2014	Green (1-4)	on-track

2. Risk Cube


• Risk ID Number: 31
• Risk Driver:
• Risk Mitigation Action:
- Cost: $
• Closure Date:
• Cost Impacts:
- RDT&E: $ or %
- Production: $ or %
• Schedule Impacts:
- Months:
• Performance Impacts:
- Only achieves XX% of aaa KPP performance
• Risk ID Number: 99
• Risk Driver:
• Risk Mitigation Action:
- Cost: $
• Closure Date:
• Cost Impacts:
- RDT&E: $ or %
- Production: $ or %
- O&M: $ or %
• Schedule Impacts:
- Months:
• Performance Impacts:
- Only YY% of abc KSA performance
• Risk ID Number: 22
• Risk Driver:
• Risk Mitigation Action:
- Cost: $
• Closure Date:
• Cost Impacts:
- Production: $ or %
- O&M: $ or %
• Schedule Impacts:
- Months:
• Risk ID Number: 4
• Risk Driver:
• Risk Mitigation Action:
- Cost: $
• Closure Date:
• Cost Impacts:
- Production: $ or %
• Schedule Impacts:
- Months:
• Performance Impacts:
- May trade xyz performance
• Risk ID Number: 18
• Risk Driver:
• Risk Mitigation Action:
- Cost: $
• Closure Date:
• Cost Impacts:
- RDT&E: $ or %
- Production: $ or %
• Schedule Impacts:
- Months:

3. Alternate to the Risk Reporting Matrix

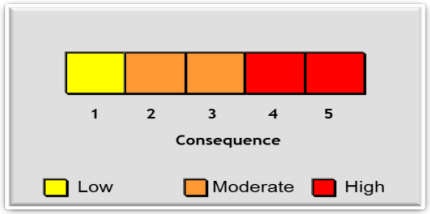
Risk	Likeli-hood (1-5)	Consequences					Control Activities	Planned (P) Actual (A)		Closure Date
		Funding			Schedule	Performance				
		RDT&E	Procurement	O&S			Activity	Date	Cost	
Risk 1 (describe the risk in terms of, "if… (something does or does not occur), then….(negative consequence X and Y will happen)	3	$450k			4 months	XX performance degraded	1 –Activity XX	(P) 6/16/14 (A)	(P) (A)	(P) 8/12/15
							2 –Activity YYY	(P) 10/12/13 (A) 11/1/13	(P) (A)	(A)
							3 – Activity ZZZ	(P) 8/12/15 (A)	(P) (A)	
Risk 2	4		$2.2M		8 months		1 –Activity aaa	(P) 7/13/14 (A)	(P) (A)	(P)7/13/14
							2 -	(P) (A)	(P) (A)	(A)
							3 -	(P) (A)	(P) (A)	
Risk 3	2		$520K		2 months		1 -	(P) (A)	(P) (A)	(P)
							2 -	(P) (A)	(P) (A)	(A)
							3 -	(P) (A)	(P) (A)	

4. Issue Tracking Sheet

Issue	Consequence	Type T/B/P	Plan of Action at Milestones			
			Closure Activities	Closure Date Planned (P) Actual (A)	Cost	
					Type (RDT&E, Procurement, O&M)	Amount ($)
Issue X (Describe the issue that has occurred, the type of issue, technical, business, or programmatic, and what are the resulting cost, schedule and performance consequences)		Tech (T)	Activity 1	(P) – 10/12/13 (A) - 11/1/13	RDT&E	$420K
			Activity 2	(P) (A)	Procurement	$2.1M
			Activity 3	(P) (A)		
				(P) (A)		
				(P) (A)		
				(P) (A)		

Consequence Table Key

- More than z days behind plan
- Between y and z days behind plan
- Less than x days behind plan



5. Sample Opportunity Tracking Matrix

Opportunity	Likeli-hood	Cost	Benefit					Activity	Expected Closure
			RDT&E	Procurement	O&M	Schedule	Performance		
1. **Opportunity 1: Procure Smith Rotor blades instead of Jones rotor blades**		$2M			$7M	6 month margin	4% greater lift	Summarize the activity to realize the opportunity	June 2016
2. Opportunity 2 (describe the opportunity in terms of what it will provide the program, the benefit to the program, and the cost to the program)		$15K	$25K		$1.1 M				May 2015
3. Opportunity 3 (describe the opportunity in terms of what it will provide the program, the benefit to the program, and the cost to the program)		$211K		$0.4M	$3.6 M	4 months less long lead time needed			

APPENDIX D: BETTER BUYING POWER INITIATIVES AND THE RISK MANAGEMENT GUIDE

Better Buying Power Initiative		Where Addressed in this Guide
1.0	At Milestone B, establish engineering trades showing how each key design feature affects the target cost	Section 2. Government Responsibilities; Section 3. Risk Identification; Appendix A, RM Considerations During Acquisition Life Cycle Phases
1.0	Present a competitive strategy at each program milestone	Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
2.0 3.0	Emphasize competition strategies and create and maintain competitive environments	Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
2.0	Use technology development phase for true risk reduction	Section 3. Risk Management Process, 3.2 Risk Analysis; Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
1.0 2.0 3.0	At Milestone A, set affordability target as a Key Performance Parameter. Mandate affordability as a requirement. Continue to set and enforce affordability caps	Section 3.3. Risk Mitigation; Appendix A RM Considerations During Acquisition Life Cycle Phases
1.0 2.0 3.0	Strengthen and expand "should cost" based cost management	Section 6. Opportunity Management
2.0 3.0	Build stronger partnerships between the acquisition, requirements, and intelligence communities	Section 3.1. Risk Identification; Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
3.0	Increase the use of prototyping and experimentation	Section 2.5. Roles and Responsibilities (2.5.1, 2.5.4); Section 3.1. Risk Identification; Section 7. Management of Cross-Program Risks; Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
3.0	Provide draft technical requirements to industry early and involve industry in funded concept definition to support requirements definition	Section 3.1. Risk Identification; Appendix A RM Considerations During Acquisition Life Cycle Phases; Appendix B Common Risks and Mitigation Activities
3.0	Improve our leaders' ability to understand and mitigate technical risk	7th Edition focused on Technical Risk; Section 3. Risk Management Process; 3.1 Risk Identification; Section 7 Management of Cross-Program Risks; Appendix B Common Risks and Mitigation Activities

ACRONYMS

APB	Acquisition Program Baseline
C	Cost
CDD	Capability Development Document
CDR	Critical Design Review
COTS	commercial-off-the-shelf
CPD	Capability Production Document
CPR	Contract Performance Report
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DAG	Defense Acquisition Guidebook
DAP	Defense Acquisition Portal
DAU	Defense Acquisition University
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EAC	Estimate at Completion
ESOH	Environment, Safety, and Occupational Health
EVM	Earned Value Management
FAA	Federal Aviation Administration
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOT&E	Initial Operational Test and Evaluation
IPT	Integrated Product Team
JCIDS	Joint Capabilities Integration and Development System
KPP	Key Performance Parameter
KSA	Key System Attribute
LCC	Life Cycle Cost
LCCE	Life Cycle Cost Estimate
LCSP	Life Cycle Support Plan
LRIP	Low-Rate Initial Production

MAIS	Major Automated Information System
MDAP	Major Defense Acquisition Program
M&S	Modeling and Simulation
MDA	Milestone Decision Authority
MDD	Materiel Development Decision
OIPT	Overarching Integrated Product Team
O&M	Operations and Maintenance
O&S	Operations and Support
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
P	Performance
PDR	Preliminary Design Review
PEO	Program Executive Office or Program Executive Officer
PM	Program Manager
PMR	Program Management Review
RFP	Request for Proposal
RM	Risk Management
RMB	Risk Management Board
RMP	Risk Management Plan
SE	Systems Engineer
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SME	Subject Matter Expert
SRA	Schedule Risk Assessment
TDS	Technology Development Strategy
TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
TPM	Technical Performance Measure
TRA	Technology Readiness Assessment
WBS	Work Breakdown Structure

REFERENCES

Department of Defense Directive (DoDD) 5000.01. 2003. "The Defense Acquisition System." Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics.

Interim Department of Defense Instruction (DoDI) 5000.02. November 25, 2013. "Operation of the Defense Acquisition System." Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics.

MIL-STD-881C. 2011. "Work Breakdown Structures for Defense Materiel Items." Washington, D.C.: Office of the Assistant Secretary of Defense for Acquisition, Performance Assessments, and Root Cause Analysis.
https://acc.dau.mil/CommunityBrowser.aspx?id=482538

Public Law 111-23, 111th Cong. (May 22, 2009.) *Weapon Systems Acquisition Reform Act of 2009.*

Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (PDUSD(AT&L)). 2011. "Document Streamlining –Document Streamlining–Program Strategies and Systems Engineering Plan (SEP)." Memorandum (April 20). Washington, D.C.: PDUSD(AT&L).
http://www.acq.osd.mil/se/docs/PDUSD-ATLMemo-Expected-Bus-Practice-TDS_AS_SEP-20Apr11.pdf
http://www.acq.osd.mil/se/docs/PDUSD-Approved.SEP_Outline-04-20-2011.docx

Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). 2012. "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending." Memorandum (November 13). Washington, D.C.: USD(AT&L).

Resources

Best Manufacturing Practices Center of Excellence
http://www.bmpcoe.org/

Circular No. A–11 , Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets
http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf

Defense Acquisition Guidebook
https://dag.dau.mil/Pages/Default.aspx

Defense Acquisition Portal
https://dap.dau.mil/Pages/Default.aspx

DoDD 5200.01, DoD Information Security Program
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

DoDD 5200.39, Critical Program Information (CPI) Protection Within the Department of Defense
http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

DoD Earned Value Management
http://www.acq.osd.mil/evm/

DoD Earned Value Management Implementation Guide (EVMIG)
https://acc.dau.mil/CommunityBrowser.aspx?id=386074

MIL-STD-882E, Standard Practice for System Safety
http://acqnotes.com/acqnote/tasks/mil-std-882e-system-safety

Program Managers' Guide to the Integrated Baseline Review Process
https://acc.dau.mil/CommunityBrowser.aspx?id=37635

Risk Management Community of Practice
https://acc.dau.mil/CommunityBrowser.aspx?id=17607

Department of Defense Risk Management Guide for Defense Acquisition Programs, 7th Edition (Interim Release)

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030

Email: osd.atl.asd-re.se@mail.mil
Website: www.acq.osd.mil/se