Department of Defense
Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs

June 2015

Office of the Deputy Assistant Secretary of Defense for
Systems Engineering

Washington, D.C.

Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs

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

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

Contents

FIGURES

TABLES

Preface

This guide is one of several Department of Defense (DoD) policy and guidance documents that address the Department's focus on risk management. As evidenced in these documents, the Department recognizes a significant relationship between effective risk management and program success.

This guide builds from previous editions of the *DoD Risk Management Guide* but reflects revisions to emphasize managing not only program risks but also issues and opportunities. Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, requires program managers (PM) to implement effective risk management, noting "the goal is to both mitigate risks and create opportunities for technology development outcomes that could have a positive impact on meeting performance objectives as well as thresholds."

In 2015, the Under Secretary of Defense for Acquisition, Technology, and Logistics emphasized risk management as a focus of the DoD Better Buying Power initiative:

> Risk management is an endeavor that begins with requirements formulation and assessment, includes the planning and conducting of a technical risk reduction phase if needed, and strongly influences the structure of the development and test activities. Active risk management requires investment based on identification of where to best deploy scarce resources for the greatest impact on the program's risk profile. PMs and staff should shape and control risk, not just observe progress and react to risks that are realized. Anticipating possible adverse events, evaluating probabilities of occurrence, understanding cost and schedule impacts, and deciding to take cost effective steps ahead of time to limit their impact if they occur is the essence of effective risk management. Risk management should occur throughout the lifecycle of the program and strategies should be adjusted as the risk profile changes.

Risk management is an integral part of program management and systems engineering. A program must align risk appetite with organizational capacity to manage and handle risks and apply informed judgment to allocate limited resources to the best effect. Sound judgment to achieve this balance is at the core of program management.

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

Although this guide focuses primarily on the government program office, DoD recognizes that industry plays a central role in executing the management necessary for delivery of acquisition products. A close collaboration between government and industry is an essential ingredient of

productive and economic risk, issue, and opportunity management. Government and industry may on occasion differ in the prioritization of risks, driven in part by differing perspectives or incentives. Nevertheless, a shared commitment to a disciplined process, realism, and openness to observations borne of knowledge, even when inconvenient, underpins the value of the collective effort.

The guide is organized as follows:

Section 1: Introduces the scope and changes in this revised edition of the guide.

Section 2: Describes the planning and documentation of the program's risk management process. Highlights planning as the first step in the risk management process.

Section 3: Discusses the five steps in the risk management process: planning, identification, analysis, handling, and monitoring. Provides detailed guidance and examples to assist programs to build and customize the process.

Section 4: Describes proactive risk management through integrating with other program management tools such as the Work Breakdown Structure (WBS), Integrated Master Plan (IMP), and Integrated Master Schedule (IMS). It also discusses other techniques and metrics such as schedule risk analysis (SRA), cost risk analysis (CRA), performance risk analysis (PRA), and Technical Performance Measures (TPM).

Section 5: Defines the issue management process as a distinct and complementary management process. An issue is an event or situation with negative consequences that has already occurred or is certain to occur. This distinction between an issue and a risk differentiates how they are managed.

Section 6: Describes the application of opportunity management including the similarities and differences between opportunity and 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.

Section 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.

Appendixes: The appendixes provide additional information, lessons on common risks previously observed, templates, and a vignette that may help program offices manage risks, issues, and opportunities.

Most sections also contain a text box with expectations that program office leadership should have in mind as they seek to improve the planning and execution of risk management processes and techniques.

1 INTRODUCTION

1.1 Purpose

This guide seeks to inform program office personnel, ranging from junior personnel to PMs, regarding the effective use of and expectations related to DoD processes to identify and manage program risks, issues, and opportunities. Proactively managing these areas will help programs achieve cost, schedule, and performance objectives throughout the life cycle.

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

- **Risks** are future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance. Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur.
- **Issues** are events or conditions with negative effect that have occurred (such as realized risks) or are certain to occur (probability of 1) in the future that should be addressed.
- **Opportunities** are potential future benefits to the program's cost, schedule, and/or performance baseline, usually achieved through reallocation of resources.

Figure 1-1 shows a simple portrayal of technical, programmatic, and business events that may lead to risks, issues, or opportunities, each with cost, schedule, or performance consequences.

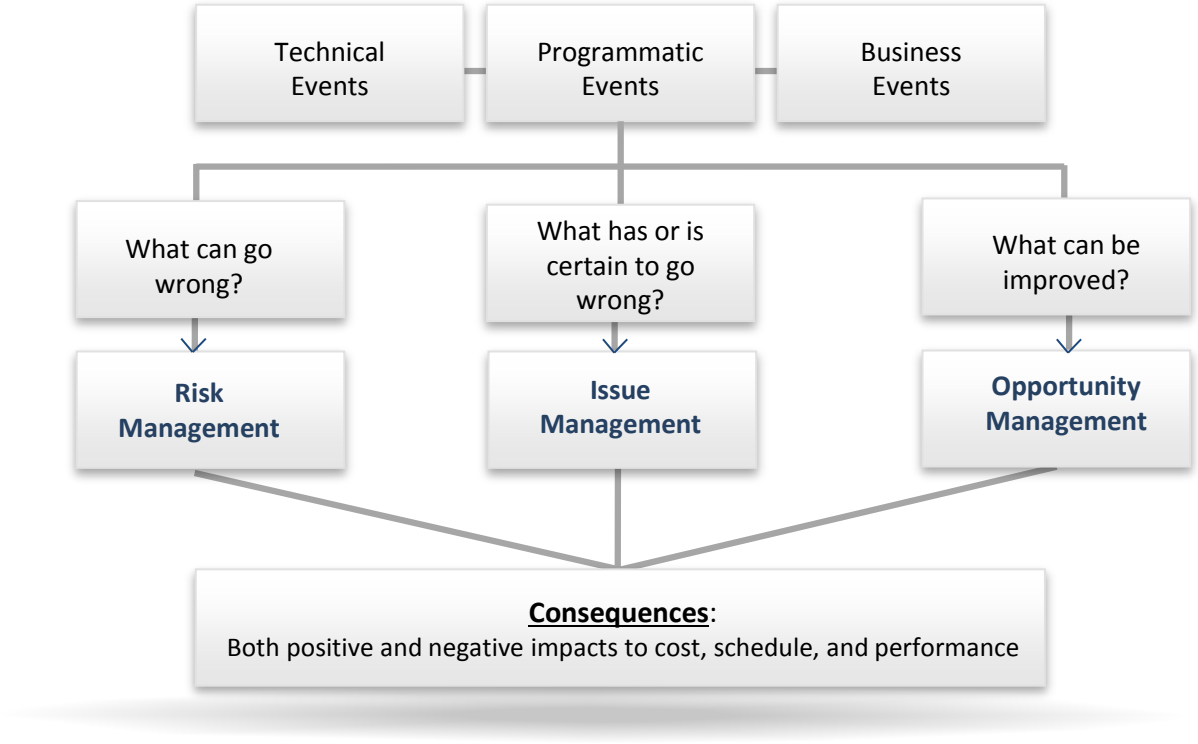


Figure 1-1. Overview of Potential Sources of Program Risks, Issues, and Opportunities

The DoD risk management process is fundamental to acquisition program success. 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; *Defense Acquisition Guidebook;* Military Department guidance; and other instructions, policy memorandums, and regulations.

1.2 Scope

The practice of risk management draws from many disciplines, including program management, systems engineering, requirements definition, earned value management (EVM), production planning, quality assurance, and logistics. Programs should strive to follow sound risk management processes as outlined; however, the Department recognizes some tailoring will be required as programs adapt to fit within program-specific circumstances.

DoD distinguishes mandatory policy from recommended guidance. This document serves solely as guidance for risk management approaches for DoD acquisition programs. This guide builds on previous editions of the *DoD Risk Management Guide* while emphasizing areas for improvement that have emerged during Office of the Secretary of Defense (OSD) program reviews across the range of DoD programs:

- Risk management in relation to other program management tools
- Issue management
- Opportunity management
- Managing risks with external programs
- Proactive handling activities throughout the acquisition life cycle phases

This guide does not attempt to address, or circumvent, the specific requirements to prevent and manage system safety or system hazards, including environment, safety, and occupational health (ESOH) hazards. The reader should refer to DoDI 5000.02, Enclosure 3 and MIL-STD-882, Standard Practice for System Safety, for guidance in these areas. Likewise, this guide does not attempt to address specialized cybersecurity risks in information technology systems. Programs should refer to DoDI 8510.01, Risk Management Framework for DoD Information Technology (IT), for policy and procedures regarding the integrated enterprise-wide structure for cybersecurity risk management. Programs should develop a method to map these specialized ESOH and cybersecurity risks or issues into their overall risk/issue management processes, to include the risk and issue matrixes and registers discussed in Sections 3 and 5.

1.3 Risk Management Overview

Successful risk management requires thoughtful planning and resourcing, and should be implemented as early as possible in the life cycle beginning with the Materiel Solution Analysis phase. The goal is to identify risks to inform decisions and handling strategies before the risks become issues.

Risk management needs to be both top-down (embraced by the PM and others) and bottom-up (from working-level engineers) to be successful. PMs should encourage everyone on their program to take ownership of the risk management program and should be careful not to cultivate a "shoot the messenger" culture. All personnel should be encouraged to identify risks, issues, and opportunities and, as appropriate, to support analysis, handling, and monitoring activities.

Organizational implementation and process quality are equally important in determining a program's risk management effectiveness. A poorly implemented risk management process will not contribute to program success but may lead to program inefficiency. 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 (Figure 1-2):

1. Risk Planning: What is the program's risk management process?
2. Risk Identification: What can go wrong?
3. Risk Analysis: What are the likelihood and consequence of the risk?
4. Risk Handling: Should the risk be accepted, avoided, transferred, or mitigated?
5. Risk Monitoring: How has the risk changed?

Figure 1-2. Risk Management Process

2 ESTABLISHING AN EFFECTIVE RISK MANAGEMENT PROCESS

Risk management is integral to effective program management. As such, the program should initiate risk management planning and execution as soon as possible in the life cycle. All functional disciplines supporting program planning and execution have a role in risk management.

This section discusses the risk management process as the primary framework. Issues and opportunities are managed similarly as indicated in Sections 5 and 6. The basic risk management concepts should be incorporated or adapted to issue and opportunity management as applicable.

2.1 Framing Assumptions and Ground Rules

Program leadership should consider and document program framing assumptions because of the risks they may introduce should the assumptions prove invalid. Examples of framing assumptions may include priority of requirements, schedule dependencies, or accuracy of models and simulations.

In addition, the program should document key risk management ground rules to be used across the risk management program. Typical ground rules for risk management relevant to programs include time frame, time of risk event, and WBS level:

- Time frame: Current probability and impact estimates, discussed in Section 3, are based upon the status of the item or event as assessed, not upon projected or planned activities. For example, the risk consequence should be evaluated as the impact if the risk were to be realized without further mitigation, avoidance, etc.
- Time of risk event: In order to properly analyze a risk, the time at which the risk hypothetically will occur should be considered and documented, as occurrence or realization timing is most likely a primary factor in the impact. (This time is often specified during risk analysis on previously approved risks and is different from the time frame associated with implementing a risk handling strategy to avert or accept the risk.)
- WBS level: Hardware and software risk events should be identified to the lowest level possible to facilitate identification of causal factors and handling strategies.

2.2 Aligning Government and Contractor Risk Management

The government program office, the prime contractor(s), and associated subcontractors should employ a consistent, though not necessarily identical, risk management process. This will facilitate risk register alignment and transference of data between parties. Risk management is not a stand-alone process and should be integrated with other program processes, such as requirements development; the design, integration, systems engineering, planning, and management of system support and sustainment; schedule tracking; performance measurement; EVM; cost estimating; issue management; and so on. Programs should include appropriate language in the Request for Proposal (RFP) and resulting contract.

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 success. 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 occasion 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.

On firm-fixed-price contracts, PMs and their contracting officers should reach an agreement with contractors during contract negotiations on what key risks must be handled, when progress will be measured, and any appropriate contract options. 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 handle emerging risks. The sufficiency of funds available to address emerging risks should be reevaluated during budget cycle reviews and before acquisition milestones and the award of follow-on contracts. The government must be aware that while a contractor may have responsibility for handling a risk, the government still has ownership and interest in the efforts.

Appendix D contains a summary listing of typical government and contractor responsibilities regarding risk management.

2.2.1 Risk Management Board and Risk Working Group

The PM establishes and typically chairs the Risk Management Board (RMB), the approval authority for risk management–related products. The RMB usually includes the individuals who represent the various functionalities of the program office, such as program control, the chief engineer, logistics, test, systems engineering, Risk Working Group (RWG) lead, contracting officer as warranted, potentially a user representative (if resident, or by invitation), and others depending on the agenda. The RMB should document actions and decisions in meeting minutes and/or the risk register as necessary. Programs should consider integrated government-contractor RMBs where practical. Often these joint RMBs are co-chaired by the two PMs. Whenever there is disagreement between the chairs, the type of contract plays a role in the decision making and therefore the contracting representatives are participants, if appropriate. Ultimately the RMB structure should define decision-making responsibilities and accountability.

A tiered structure is often implemented and provides a viable approach to manage lower-level risks. If used, it is imperative these lower-level boards have the authority and resources required to fully implement handling strategies. The program should ensure recurring visibility into these lower-level risks, issues, or opportunities. Regardless of approach, the established process should lead to consistent enterprise processes with the government PM ultimately responsible and accountable for

program-level risk management. These boards may also address opportunities and if so are sometimes referred to as risk and opportunity management boards (ROMB) or other variations. The frequency of RMB meetings can be tailored; however, the program's battle rhythm should ensure risk management activities remain timely and relevant.

Program offices should create a RWG led by a member of the Systems Engineering Integrated Product Team (IPT) or Program Management IPT, with a representative from other IPTs. The program should describe the roles and responsibilities of the RWG in a charter or equivalent. An effective RWG is empowered to draw on expertise from inside the program and from identified sources outside the program to develop individual risk plans and recommendations for the RMB. Figure 2-1 shows a sample of routine program meetings that are candidates for discussing risk status.

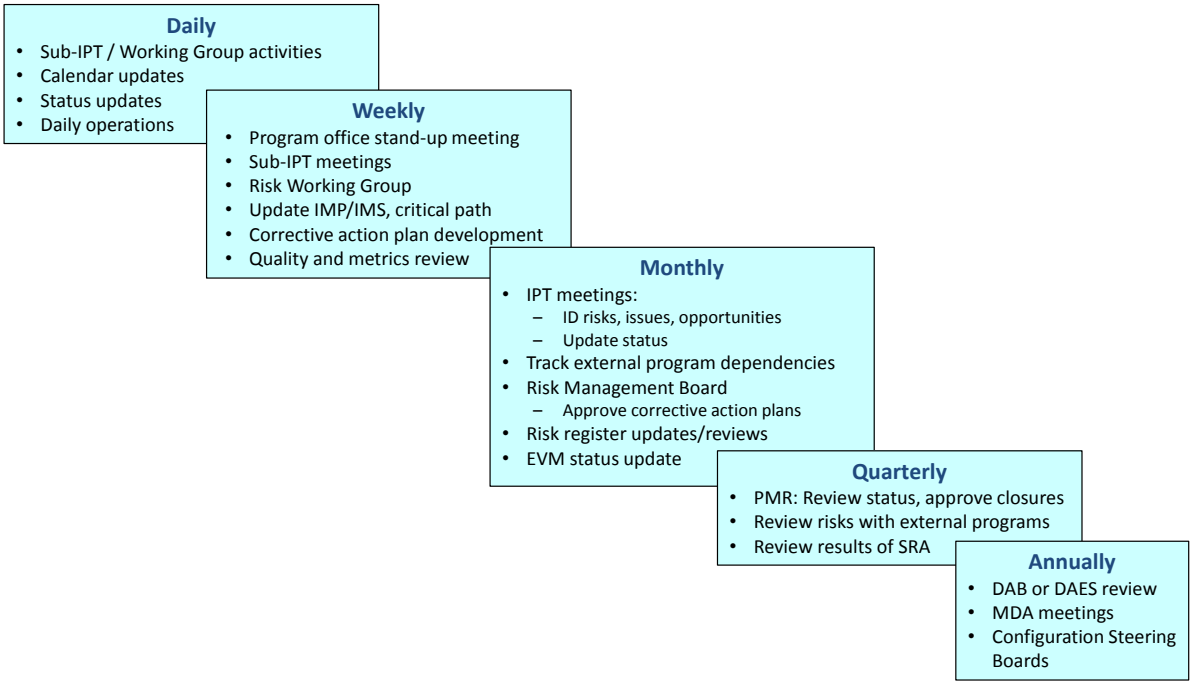


Figure 2-1. Sample Risk Management–Related Battle Rhythm

2.2.2 Acquisition Strategy, SEP, and SEMP

Programs address risk management at a general level in the Acquisition Strategy, for which the 2011 Acquisition Strategy Outline provides applicable guidance. The government Systems Engineering Plan (SEP) and contractor Systems Engineering Management Plan (SEMP) should describe:

- The process for how the program plans to manage risks.
- How risk management processes are integrated with the contractor(s) processes.
- How the program identifies and analyzes risks.
- How the program plans, implements (including funding), and tracks risk handling activities.
- Key roles and responsibilities from working groups, IPTs, RWGs, and RMBs up to the PM.

- The RMB, including who chairs the board, the membership, and meeting frequency.
- Risk tool(s) that the program office and contractor use to perform risk management.

2.3 Risk Management Plan

DoD programs are required to summarize the risk management approach and planning activities in the SEP and Acquisition Strategy. Some programs document their plans in a combined Risk, Issue, and Opportunity (RIO) Management Plan. Others document their plans in separate documents. Programs should make a deliberate decision whether or not to combine the plans into one document so as to best manage all three areas. This section provides details for developing a Risk Management Plan (RMP), but the same principles apply for issues and opportunities, which programs should likewise develop and document.

The RMP should:

- Explain how the program manages risks to achieve cost, schedule, and performance goals.
- Establish the basic approach and risk management working structure.
- Document an organized, comprehensive, and integrated approach for managing risks.
- Define the goals, objectives, and the program office's risk management processes.
- Define an approach to identify, analyze, handle, and monitor risks across the program.
- Document the process to request and allocate resources (personnel, schedule, and budget) to mitigate risks.
- Define the means to monitor the effectiveness of the risk management process.
- Document the integrated risk management processes as they apply to contractors, subcontractors, and teammates.

The RMP should be documented early in the program's initial formulation and updated at certain intervals as a program progresses through the acquisition life cycle (e.g., when a program is rebaselined, changes in program phases, developmental and operational testing, and sustainment). Programs may include aspects of issue and opportunity management planning, as appropriate. 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 among the Acquisition Strategy, Program Management Plan, and technical strategy.
- **Definitions** – Definitions specific to the program to be used in the plan.
- **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.

- **Risk Management Board(s) and Risk Working Group(s)** – Description of the formation, leadership, membership, and purpose of these groups.
- **Roles, Responsibilities, and Authorities –** Description of roles, responsibilities, and authorities within the risk management process for:
  - Identifying, adding, modifying, and reporting risks
  - Providing resources to handle risks
  - Developing criteria to determine whether a candidate risk is accepted
  - 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 five-step DoD process:
  - Risk planning
  - Risk identification
  - Risk analysis
  - Risk handling
  - Risk monitoring
- **Risk Management in Relation to Other Program Management Tools –** List of the risk tools the program (program office and contractor[s]) uses to perform risk management. Preferably, the program office and contractor(s) should use the same tool. If they use different tools, the tools should be capable of seamlessly exchanging data. This section would include a description of how the information would be transferred.
- **Risk Evaluation Techniques** – Summary of the cost, schedule, and performance evaluation processes, including procedures for evaluating risks.
  - Overview and scope of the evaluation process
  - Sources of information
  - Planned frequency of assessments
  - Products and formats
  - Evaluation technique and tools
  - Likelihood and consequence parameters and thresholds
- **Communication and Feedback Process** – Process for communicating and/or elevating the status of potential, current, and retired risks as well as opportunities that may exist to all personnel involved in risk management.

Program offices define the documentation and reporting procedures as part of risk management planning before contract award. The program should add to or modify this planning after contract

award or during contract execution if it becomes necessary, to include review and revision of the RMP. Events that may drive updates include acquisition milestones, contract award, system-level technical reviews, a change to the Acquisition Strategy, or program rebaselining.

➢ ***Expectations***

- The government should inform the program's risk management approach through carefully crafted language in the RFP, which should include the top-level schedule, WBS, and SEP. In turn, the contractor's proposal should reflect a consistent and integrated risk management approach as evidenced in the RMP, IMP, IMS, and SEMP.
- Programs establish and document a risk, issue, and opportunity management structure for appropriate implementation and oversight (RMB, RWG, etc.).

2.4 Selecting a Risk Management Tool

Risk management tools support the implementation and execution of risk management. The PM needs to select the appropriate risk management tool(s) early and document details in the SEP. Some areas to consider when selecting the risk management tool are:

- Support Objectives: Does the tool aid in meeting program objectives?
- Recurrence: Will the risk management tool accommodate recurring updates to the risk management process?
- 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 meet the requirements for the program office and contractor(s)?

➢ ***Expectations***

- The government program offices and contractors select a common or electronically compatible risk management tool to collectively identify, analyze, handle, 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. All parties must establish appropriate firewalls and take care to protect sensitive government or contractor proprietary risk and technical data.

2.5 Risk Management Roles, Responsibilities, and Relationships

Design maturity and associated technical risks are key considerations when program offices and the Milestone Decision Authority (MDA) select an acquisition approach. Constrained budgets require PMs and contractors to balance program priorities with high-value risk handling activities. Given these constraints, an effective risk management process requires the support and commitment of the entire acquisition team. To ensure effective management, the program and contractor need to clearly define the roles and responsibilities in the Acquisition Strategy, SEP, SEMP, and RMP.

Regularly communicating and reviewing the status of each risk is key to ensuring personnel involved in risk management have a clear understanding of the progress being made in managing risks. These activities involve reviewing likelihood and consequence assessments, along with the status of selected handling plans.

Organizing and training the team to follow a disciplined, repeatable risk management process is critical since periodic assessments support major program decisions throughout the life cycle. While experienced team members may not require extensive training in risk management, all team members would benefit from periodic review of lessons learned from earlier programs. A risk management training package for the core team and subject matter experts (SME) is often beneficial.

Figure 2-2 displays the hierarchy typically involved in risk management. These core groups and individuals all play a vital role in the risk management process and in helping to identify, analyze, report, and handle risks at the appropriate level. These groups provide an array of expertise in areas such as systems engineering, logistics, manufacturing, test, schedule analysis, contracting, cost control/estimating, EVM, and software development.

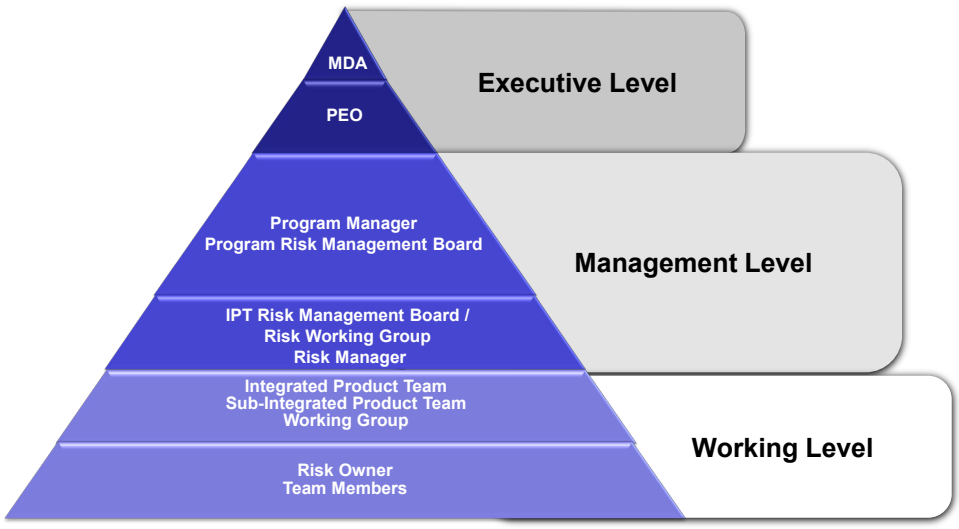


Figure 2-2. Roles and Responsibilities Tiering

Specific risk management roles and responsibilities for each tier level of management and authority are included at Appendix D. Programs should consider those listed in the appendix when developing their RMP.

3 RISK MANAGEMENT

Figure 3-1 depicts risk management as a five-step process to plan, identify, analyze, handle, and monitor program risks. This section will provide more detail in each iterative step in the process.

Figure 3-1. Risk Management Process

3.1 Risk Management Planning

Section 2 discussed risk management planning in detail. In short, risk planning consists of the activities to develop, implement, and document the risk management process. Effective planning should outline each of the risk management steps described in the following sections. Figure 3-2 depicts key aspects of risk planning.

Risk planning should be summarized in the SEP and the RMP and should address the program's risk management organization (e.g., RMBs, frequency of meetings and members), ground rules and assumptions, candidate risk categories, and use of any risk management tools. The plan should describe how often the RMP will be reviewed and updated. It should address risk management training for program personnel, define an appropriate risk management culture, provide a description of the program's risk management processes, and describe how to use the program's adopted risk management tools.

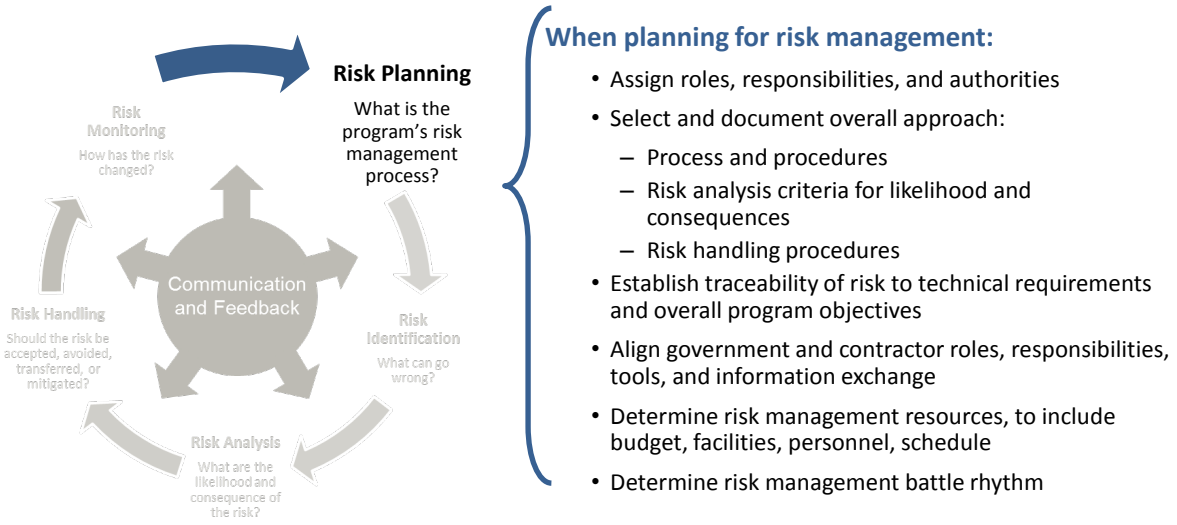


Figure 3-2. Risk Planning

3.2 Risk Identification

The next activity in the risk management process is to identify risks by answering the questions, *What can go wrong?* or *What is uniquely hard or difficult?* This step involves examining the program to determine risk events and associated cause(s) that may have negative cost, schedule, and/or performance impacts. While the root cause of some risks may not be known or be determinable at the time the risk is evaluated, the program should attempt to drill down far enough to understand underlying root cause(s) to inform risk analysis and the development of handling strategies discussed in Section 3.4.

All program personnel are encouraged to identify candidate risks. Limiting risk identification to managers or other small groups can result in risks being missed. Risk identification is conducted continuously by all government and contractor program team members. The risk manager is responsible for examining and compiling identified risks in a program risk register (see Section 3.3.4), and summarizing them at a manageable level of detail.

3.2.1 Risk Identification Methodologies

A wide variety of risk identification approaches exist. They can be grouped loosely into top-level (e.g., assessment or review of key processes and documents) or lower-level methods (e.g., brainstorming, Delphi method, diagramming methods). A more systematic method using a top-level approach combined with a variety of lower-level methods is recommended. Program personnel should have a clear understanding of the program's requirements, goals, plans, and supporting analysis. An understanding of the following program-related documents helps 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)
- Test and Evaluation Management Plan (TEMP)
- Technology Readiness Assessment (TRA)
- Program Protection Plan (PPP)
- Life-Cycle Sustainment Plan (LCSP)
- Life-Cycle Mission Data Plan (LMDP)
- Integrated Master Plan (IMP)
- Integrated Master Schedule (IMS)
- Contract structure and provisions
- Government technical requirements and specifications documents
- Joint Capabilities Integration and Development System (JCIDS) documents

Early and recurring communication between the user and acquisition communities involved in the development of JCIDS documents helps requirements leaders and acquisition leaders identify high-risk requirements and inform potential technical risk-based trades. All participants should recognize that requirements churn, especially changes to Key Performance Parameters (KPP) and Key System Attributes (KSA), should be analyzed to determine what risks may be introduced that could jeopardize affordability, schedule, and performance.

The following lower-level approaches should be considered to help identify technical, programmatic, and business risks by government and/or contractor program teams:

- SME brainstorming activities, affinity method for grouping results and other inputs, and diagramming methods (e.g., cause/effect, influence diagrams, process flow charts)
- Interviews with program team leads, SMEs, and/or program stakeholders, review of lessons learned, including risks or issues on predecessor or similar programs
- Examination of new contract activity and proposals, e.g., the Integrated Baseline Review
- Systems engineering activities:
    - Systems Engineering Technical Reviews (SETR) and design reviews, to include the identification of problematic requirements, immature technologies, and design shortfalls
    - Trade studies, to include the identification of cost, schedule, and performance drivers
    - Maturity of critical technologies and progress to technology maturation plans
    - Checklists and trigger questions focused on key processes associated with development, production, and/or support activities
    - Evaluation of results from competitive and risk reduction prototyping
    - Evaluation of results from integration and test activities
    - Design changes, such as Class I Engineering Change Proposals as well as the rate of Class I and II design changes
    - Failure mode and effects analysis, fault tree analysis, and additional reliability analyses

  - Specialty engineering efforts such as manning, human systems integration, reliability, supportability/sustainment, and security
- The use of other leading indicators that may provide earlier indications of risks
- Independent assessments such as Red Teams, Non-Advocate Reviews, Program Support Assessments, Nunn-McCurdy Reviews, and Critical Change Reviews
- Trends in progress toward meeting KPPs, KSAs, TPMs, schedules, budgets, the program's Earned Value Management System, and other metrics
- External influences:
  - Changes in user requirements: threats, Concept of Operations, and requirements creep
  - Externally driven cost and/or schedule constraints, or 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 stakeholder or interagency requirements or interests (e.g., Federal Aviation Administration)
  - Statutory changes, or changes in Service or DoD policy and guidance
- Production:
  - Make-buy decisions, changes to suppliers, parts obsolescence, product delivery issues
  - Manufacturing: manufacturing readiness, tooling, process maturity, etc.
  - Other considerations such as government-furnished equipment availability, business consolidations, sole and single source suppliers, access to raw materials, export control, etc.

The risk identification methodology contained in *Risk Identification: Integration and Illities (RI3)* (2008) is just one example of a top-level risk identification approach combined with a lower-level approach. In this methodology, a top-level approach (key processes) is combined with topics (e.g., design maturity and stability) and associated trigger questions for each topic (lower-level approach).

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

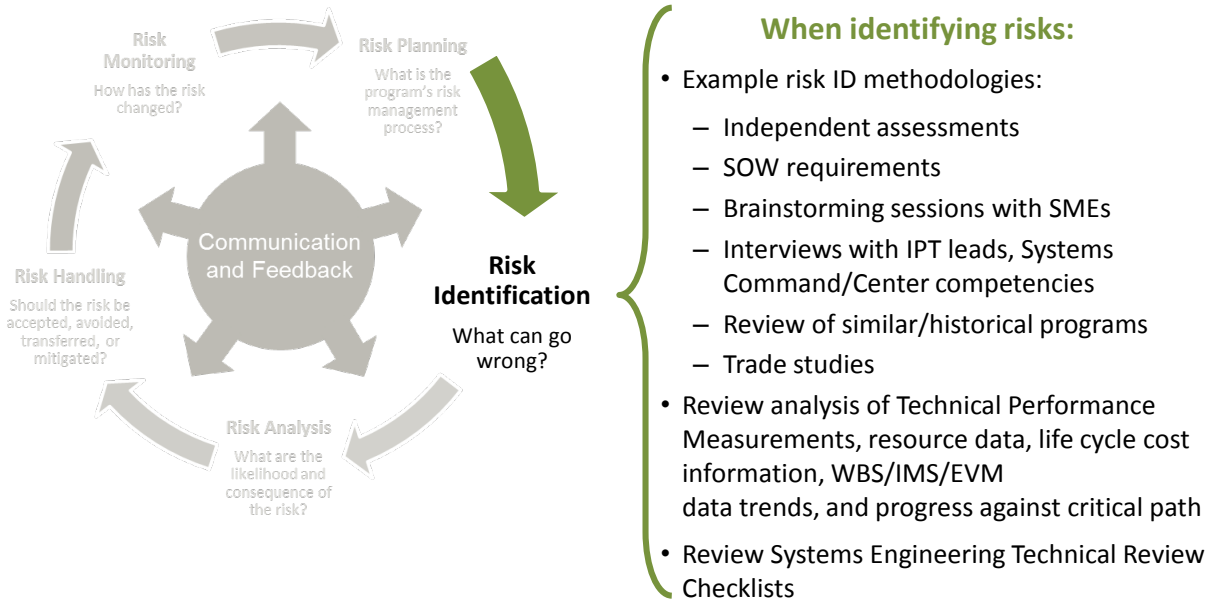


Figure 3-3. Risk Identification

3.2.2 Risk Categories

Acquisition risks with cost, schedule, and performance impacts can be grouped broadly into three categories: technical, programmatic, and business (Figure 3-4):

- **Technical** – Those risks that may prevent the end item from performing as intended or from meeting performance expectations. Technical risks can be internally or externally generated and may have cost, schedule, and/or performance consequences. They typically emanate from areas such as requirements, technology, engineering, integration, test, manufacturing, quality, logistics, system security, and training.
- **Programmatic** – Those non-technical risks that are generally within the control or influence of the PM or Program Executive Office (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 (External)** – Those non-technical 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 factors; and weather.

PMs should generally focus government and contractor efforts on risks over which they have or can influence control and elevate risks for which they do not have control (often external or business risks) to the next level.

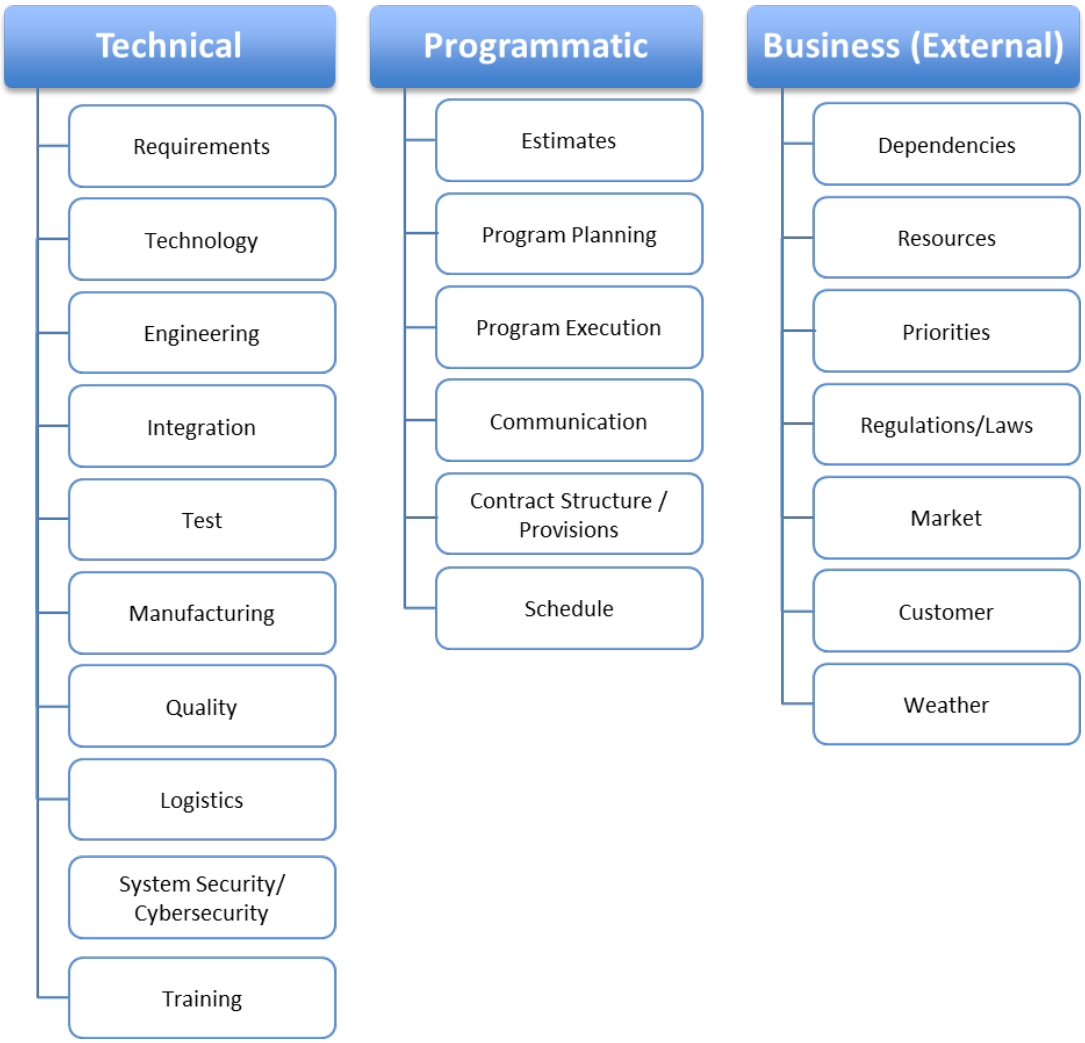


Figure 3-4. Risk Taxonomy

It is important to distinguish between technology, engineering, and integration risks. All three fall under the area of technical risk and are discussed below:

- 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.
- 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; engineering technical management processes; and engineering products. Software engineering risks include those associated with software design requirements, design of architecture, and development of 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. It can be associated with hardware or software from component through system-of-systems level.

3.2.3 Risk Statement

A key aspect of risk identification is a well-framed risk statement. A good risk statement contains two elements: the potential event and the associated consequences. If known, the risk statement should include a third element: an existing contributing circumstance (cause) of the risk. Risk statements should be written to define the potential event that could adversely affect the ability of the program to meet cost, schedule, and performance objectives. A structured approach for specifying and communicating risk precludes vague and/or inconsistent risk statements.

Multiple approaches exist in writing a risk statement. Several possible formats are illustrated below. Whenever possible, programs are best served by using a single approach for consistency. The following examples state the event or condition and outcome in a clear, concise statement written in easy-to-understand language. The statements do not include a potential risk handling strategy, other solution, or other extraneous information.

The preferred method includes a two-part statement in the **"if–then"** format. This format characterizes the possible risk event or condition ("if") and the outcome or consequence(s) ("then").

- *"If" some event or condition occurs, "then" a specific negative impact or consequence to program objectives will result.*

Example statements using the "if–then" format:

- *"If the real-time software design does not meet schedule requirements due to laboratory unavailability, then the payload integration schedule will slip."*
- *"If the structural properties of the wing skin material that were anticipated cannot be consistently achieved due to difficulty controlling processing variables, then increased wing weight or reduced aircraft maneuvering envelope (from 7.0g's to 6.0 g's) will be the result."*

Other formats include the **"condition–consequence"** format. In this format, the "consequence" is the possible outcome of the existing "condition," which has the following structure:

- *A "condition" that is causing concern or uncertainty exists, therefore a negative impact or "consequence" to a program objective may result.*

An example statement using the "condition–consequence" format:

- *To date, lower than expected structural properties are being achieved with the selected wing skin material; therefore a heavier wing design or reduced high g maneuver capability (7.0g's to 6.0g's) may result.*

Another approach adds a "because" to the statement construct, producing a **"because-event-consequence"** format. This leads to statements with the following structure:

- *"Because" of a fact or existing condition, "an event" may occur, resulting in a negative impact or "consequence" to a program objective.*

An example risk statement using this format:

- *Because the contractor is experiencing tooling problems, actuator P/N 123 may not be delivered by June 8, causing a day-for-day schedule slip to integration of the X-Y-Z subsystem.*

The formulation of a risk statement should provide a clear conditional relationship between the risk event and its effects (relatable to the likelihood and consequences discussed in Section 3.3).

Recognizing a Weak Risk Statement

Poorly written risk statements do not promote understanding or support productive action. Weak statements may confuse cause, risk, and consequence, or they may not describe consequence accurately. The statements may be overly general, circular, or self-evident. Following are examples of poorly formed risk statements with a rationale for why they are inadequate.

1. Makes an overly general observation:

   - *Weak: If the high vacancy rate in engineering staff persists, then the program staffing will be inadequate.*

This is an overly general statement, with somewhat circular logic that provides no impact on program objectives or lends any insight into underlying or existing causal conditions.

In contrast, the statement below is more informative.

- *Stronger: If the high vacancy rate in software engineering staff persists due to aggressive recruiting by competitors, then the commitment to deliver first software builds in 6 months will not be met.*

2. Identifies an issue rather than a risk:

   - *Weak: Fatigue cracks discovered in already produced vehicles may shorten service life unless remedied.*

This statement describes an issue, not a risk. The statement depicts an event that has already occurred, causing a problem with consequences that must be evaluated and addressed.

3. Diverts focus from the program's controllable activities:

   - *Weak: If the program's funding is withheld due to poor test results, then the program schedule will be jeopardized.*

In this case, the potential for curtailed funding is actually a consequence of the program's poor test results, which should be the focus of attention but is not directly or centrally addressed in the risk statement.

- *Stronger: If the vehicle reliability test performance is below XX MTBF during test, then the resulting schedule delay to fix failures could jeopardize FY 2018 funding.*

3.2.4 Evaluation of Candidate Risks

Candidate risks should be analyzed at the working level and the resulting data presented to the program's RMB (or equivalent) for evaluation. Potential outcomes include (1) approved, (2) rejected, (3) need more information (deferred), (4) management action, and (5) engineering process/practice item. Note: Management actions and engineering process should be used to address candidates that can be handled simply and expeditiously without being raised to the program's risk management process (e.g., a paragraph is needed before an RFP is released, or a requirements document must be completed before a component design can be initiated). This approach assumes that the program will actively resolve the item in a timely manner, and if any limiting constraints appear the item will be brought back to the risk management process as a candidate risk.

3.3 Risk Analysis

Risk analysis answers the questions, *What are the likelihood and consequence of the risk?* and *How big is the risk?* During risk analysis, the program will:

- Estimate the likelihood the risk event will occur.
- Estimate the possible consequences in terms of cost, schedule, and performance.
- Determine the resulting risk level and prioritize risks.

Risk analysis provides an estimate of each risk's likelihood and consequence, and the resulting risk level in order to more effectively manage risks and prioritize handling efforts. The use of consistent predefined likelihood and consequence criteria provides a structured means for evaluating risks so decision makers and program office staff can make objective comparisons of risks. The government and the contractor should use a common framework for risk analysis and estimation.

The detailed analysis described in the following sections will provide the program with the requisite insight into the potential risk implications and a basis for prioritizing resources if and when warranted. While there is a level of subjectivity and qualitative analysis associated with risk analysis, programs should strive to underpin the analysis with quantitative data to the maximum extent possible. To efficiently accomplish this step, the risk practitioner or team may consider working from the impact or consequence first. Figure 3-5 depicts how risks should be analyzed and what impact areas to quantify.

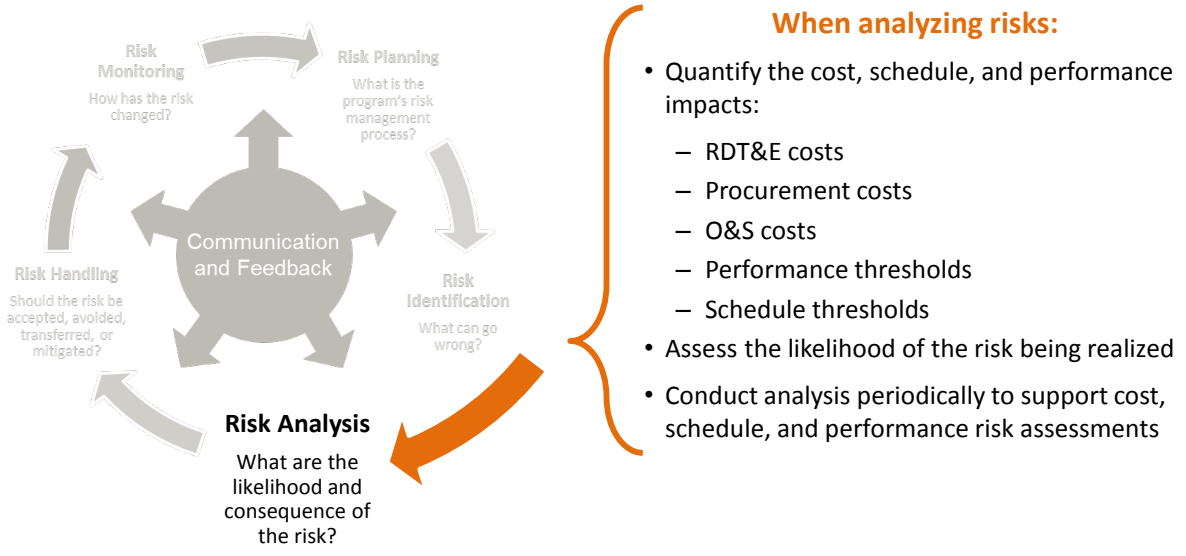


Figure 3-5. Risk Analysis

The following subsections address risk analysis using qualitative consequence (Section 3.3.1) and likelihood (Section 3.3.2) scales plus a standard risk matrix (Section 3.3.3) to convert likelihood and consequence values to relative risk levels. Cost, schedule, and performance risk analyses that are generally simulation-based are briefly addressed in Sections 4.2.2 (Schedule Risk Analysis), 4.2.3 (Cost Risk Analysis), and 4.2.4 (Performance Risk Analysis).

3.3.1 Consequence

When analyzing risks, each risk should be evaluated in terms of impact to the program (i.e., effect of the event on program cost, schedule, and performance) should the risk be fully realized. Risk consequence is measured as a deviation against program cost, schedule, and performance baselines. While the government and contractor will at times have different perspectives on risks and priorities, they should seek to have a common framework for risk consequence and likelihood criteria.

The Department recognizes programs may need to tailor criteria based on program-specific circumstances. However, programs should ensure the tailoring enables meaningful consequence criteria and a consistent means of communication to senior leadership. For example, a risk breaching KPP and/or Acquisition Program Baseline (APB) thresholds should trigger a Level 5 performance consequence rating. In crafting absolute dollar values, programs should recognize that the absolute scale of the magnitude of dollars also carries significance from a departmental or portfolio perspective. Programs should establish and document specific criteria, to include program-specific dollar and schedule thresholds, in program planning documents such as the SEP and RMP.

Programs should use the consequence criteria in Table 3-1 as a guideline in assessing cost, schedule, and performance consequences.

Table 3-1. Recommended Consequence Criteria for an MDAP

Level	Cost*			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance/ Sustainment		
5	Major impact. 10% or greater increase over APB threshold; or >$D. Management reserve depleted.	Major impact. Budget or unit production cost (e.g., APUC) increasing to a significant Nunn-McCurdy breach; or increase of more than $XX in programmed dollars (POM).	Costs exceed life cycle ownership cost by 10%. Ability to sustain system in jeopardy.	Schedule slip that requires a major schedule rebaselining; precludes program from meeting its APB schedule objectives by more than 6 months; negative float to program completion.	Severe degradation precludes system from meeting a KPP or key technical/ supportability threshold; will jeopardize program success; design or supportability margins exceeded; unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP).
4	Significant impact. 5% -<10% increase over APB threshold; or $C-≤$D. Requires use of significant management reserves.	Significant impact. Costs that drive a unit production cost (e.g., APUC) increasing to an APB threshold breach of $C - ≤ $D; or increase of $YY-XX in programmed dollars (POM).	Costs drive increase of more than z% over program's life cycle cost estimate; costs drive program to exceed life cycle ownership cost KSA.	Significantly impacts ability to meet planned milestones and/or other key dates. Established acquisition decision points or milestones will be delayed, impacting APB schedule objectives by less than 6 months. Slip puts funding at risk; <5% float to major milestones or program completion.	Significant degradation impairs ability to meet a KSA. Technical design or supportability margin exhausted in key areas; able to meet one or more mission tasks (defined in mission threads, ConOps, OMS/MP); work-arounds required to meet mission objectives.
3	Moderate impact. 3% -<5% increase over APB threshold; or $B-≤ $C; manageable with reserves; inability to meet key cost metrics.	Moderate impact. Costs that drive unit production cost (e.g., APUC) increase of $B - ≤ $C; or $ZZ-YY in programmed dollars (POM); inability to meet key cost metrics.	Costs drive increase of y-z% over program's life cycle cost estimate or within 2% of life cycle ownership cost KSA; inability to meet key cost metrics.	Minor schedule slip, able to meet key milestones. Total program float decreased by X-Y% with float remaining positive, but nearly consumed; <10% float to major milestones or program completion; inability to meet key schedule metrics.	Moderate reduction in technical performance or supportability; unable to meet lower tier attributes (e.g., PAs); planned design or supportability margins reduced; inability to meet key TPMs, CTPs. Work-arounds required to achieve mission tasks (defined in mission threads, ConOps, OMS/MP).
2	Minor impact. 1%-<3% increase over APB threshold; or $A- ≤ $B; exceeding cost metrics tripwires.	Minor impact. Costs that drive unit production cost (e.g., APUC) increase of $A-≤ $B; or $AA-ZZ in programmed dollars (POM); exceeding cost metrics tripwires.	Costs drive increase of x-y% over program's life cycle cost estimate; exceeding cost metrics tripwires.	Able to meet key dates. Total program float decreased by less than X%, with 10% or greater positive float remaining; exceeding schedule metrics tripwires.	Minor reduction in technical performance or supportability; can be tolerated with little or no impact on program objectives. Design margins will be reduced, but within limits/ trade space; exceeding tripwires for TPMs and CTPs.
1	Minimal impact. <1% increase over APB threshold; or <$A. Costs expected to meet approved funding levels, not projected to increase above thresholds.	Minimal. Costs that drive APUC increase of ≤ $A ; or less than $AA in programmed dollars (POM). Costs expected to meet approved funding levels, not projected to increase above thresholds.	Costs drive increase of ≤x% over program's life cycle cost estimate.	Minimal or no schedule impact.	Minimal or no consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires.

*This chart reflects costs broken out by funding category. Programs can break out cost consequences in this manner or consolidate in one column.

For each risk, the program should conduct adequate programmatic and engineering analysis to allow qualitative assessment on the established scale (1 to 5). The assessment should capture the greatest anticipated impact in any area as if the risk were fully realized, that is, without further risk reduction or handling opportunities. For instance, if program analysis of a risk results in a cost consequence rating of "2," a schedule consequence of "3," and a performance consequence of "2," the risk should be characterized as a "3." Note: Programs should attempt to use fully burdened costs in a risk assessment. For example, the "cost" of a potential schedule risk should consider not only the physical resources required to recover, but also some reasonable fraction of the overhead or monthly program "burn rate" required should a program extension be required.

3.3.2 Likelihood

Risk likelihood is the evaluated probability an event will occur given existing conditions. It is important that the estimated likelihood of the risk be tied to a specific well-defined risk event or condition, and risk statement. Table 3-2 provides recommended criteria for establishing the likelihood of a risk occurring. Again, the probability of occurrence should be established based on quantitative programmatic and engineering analyses to the extent practical.

Table 3-2. Recommended Likelihood Criteria

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%

Programs should also consider the effect of aggregate risk on a program. While dealing with individual risks, it is important to understand the overall risk exposure of a program and the threat to successfully satisfying program objectives related to the cumulative effects of multiple risks. Multiple risks may expose the program to a greater risk than any individual risk due to complexity, stretched handling resources, risk interactions, or the aggregate likelihood of risk realization. Monte Carlo methods, for example in an SRA or CRA, can be used in simulation models to find the cumulative effect of multiple risks on total project schedule duration or total project cost, respectively.

Note: The consequence and likelihood level values given in Tables 3-1 and 3-2 are ordinal (1 through 5). Programs should avoid fractional consequence and likelihood scoring (e.g., a likelihood score of 3.4), which incorrectly implies increased fidelity in the assessment and comparisons.

➢ ***Expectations***

- Risk statements and descriptions fully document events that could adversely affect a program's ability to meet cost, schedule, and performance objectives or baselines.
- Risk statements are clearly written using an "if–then" or similar construct.
- Programs use established criteria, tailored only as necessary, to provide a consistent means for evaluating risks.
- Resulting likelihood and consequence ratings should be supported by data and analysis.
- Programs conduct periodic risk analyses to update risk estimates and to align and support other program activities such as EVM, IMS, and technical reviews.
- If the analyzed likelihood is 100 percent, the program should address the event or condition as an issue rather than a risk (see Section 5).

3.3.3 Risk Reporting Matrix

The primary goal of risk reporting is to provide the PM and other decision makers with an effective method for managing and communicating risk. This is achieved through a consistent, disciplined approach that allows for timely and effective data-driven decisions. The risk matrix is an effective tool used to relay risk estimates in a visual display. This characterization also aids in prioritizing risks for risk handling (see Section 3.4).

Once the analysis of likelihood and consequence is complete, program teams should then use the risk matrix shown in the upper right corner of Figure 3-6. This matrix converts the combination of likelihood and the maximum of the cost, schedule, and performance consequence scores to form a risk level for each risk: low (green); moderate (yellow); or high (red). Programs can then use this rating level to effectively communicate a top-level risk analysis and prioritization.

While these values are used to define the risk level (e.g., low, moderate, high), additional factors should be considered to prioritize risks. Cost-effectiveness of perceived risk handling options is obviously a primary consideration in establishing priorities for the allocation of a program's scarce resources among competing risks. Other considerations include the frequency of occurrence, time frame, and interrelationship with other risks.

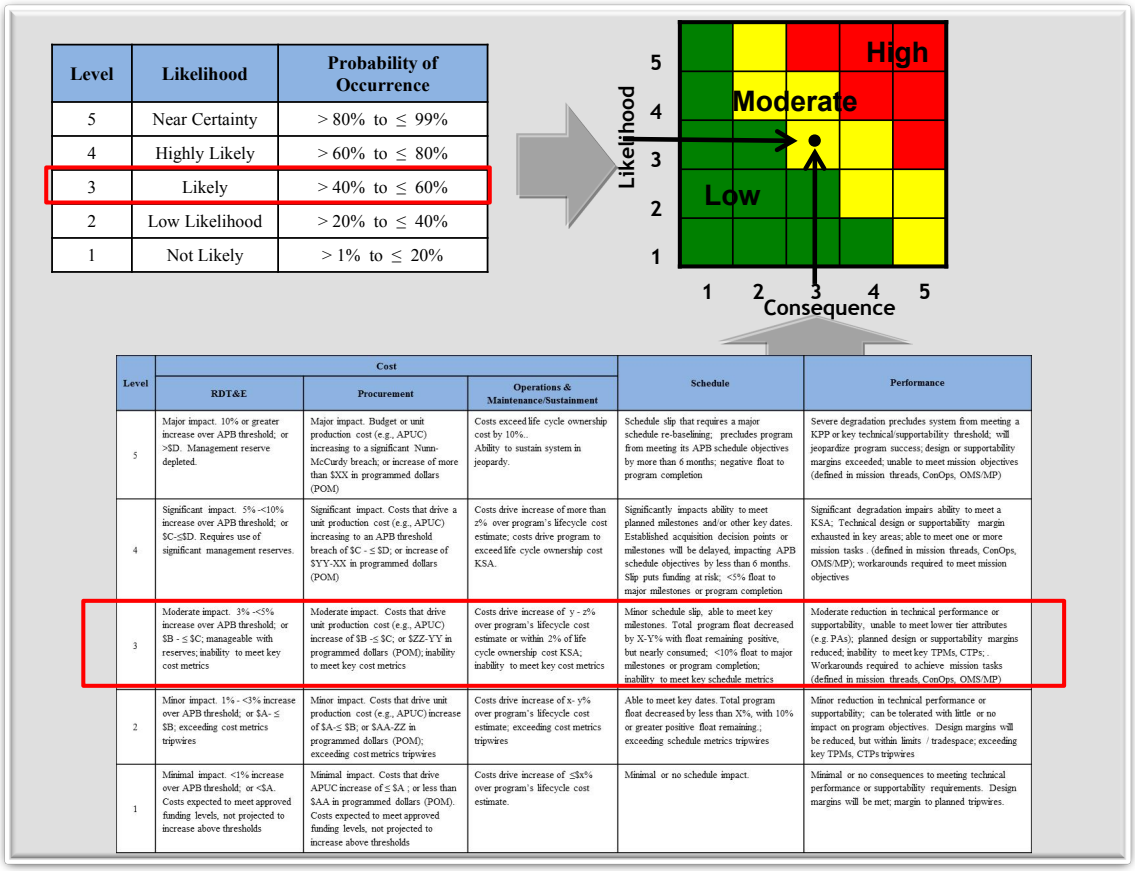


Figure 3-6. Risk Reporting Matrix and Criteria

From a cost consideration standpoint, programs should compare cost-burdened risk and handling strategies to inform decisions. For example, programs could use the expected monetary value (EMV) method as one factor in prioritizing risks based on anticipated returns from applying limited handling resources. The cost exposure of a risk can be expressed as its EMV, which is the likelihood of the risk multiplied by the cost consequence of the risk if realized. The cost of the risk handling effort is then subtracted from the risk exposure to determine the "likely" return on investment (ROI). Note, however, that this simple example uses point estimates rather than distributions for each factor.

For the example in Table 3-3, a program may decide to apply resources to risks 2 and 3 ahead of applying resources for risks 1 and 4.

Table 3-3. Risk Mitigation Expected Monetary Value

Risk	Likelihood	Consequence Cost	Exposure	Cost to Handle	Return on Investment
Risk 1:	20%	$10M	$2M	$1M	$1M
Risk 2:	70%	$10M	$7M	$1M	$6M
Risk 3:	40%	$36M	$14.4M	$2M	$12.4M
Risk 4:	60%	$5M	$3M	$.5M	$2.5M
Total		**$61M**	**$21M**	**$4.5M**	

Again, the ROI is but one factor to consider among the entirety of cost, schedule, and performance considerations. And while EMV may work well for cost and schedule risks, performance risks may require additional engineering or operationally based evaluations. For example, a risk that affects the ability to meet a KPP or other identified critical criteria should be prioritized over other risks even if it has a lower ROI. Effectiveness of the handling strategy might be another consideration.

In summary, the prioritization approach should consider the following:

1. The likelihood and maximum of the cost, schedule, and performance consequence.
2. The cost and expected return on investment of risk handling strategies.
3. Real or expected impact on military utility.
4. Time frame, frequency of occurrence, and interrelationship with other risks.
5. Expected monetary value comparisons.

Programs can then plot prioritized risks in a risk matrix, as shown in Figure 3-7.

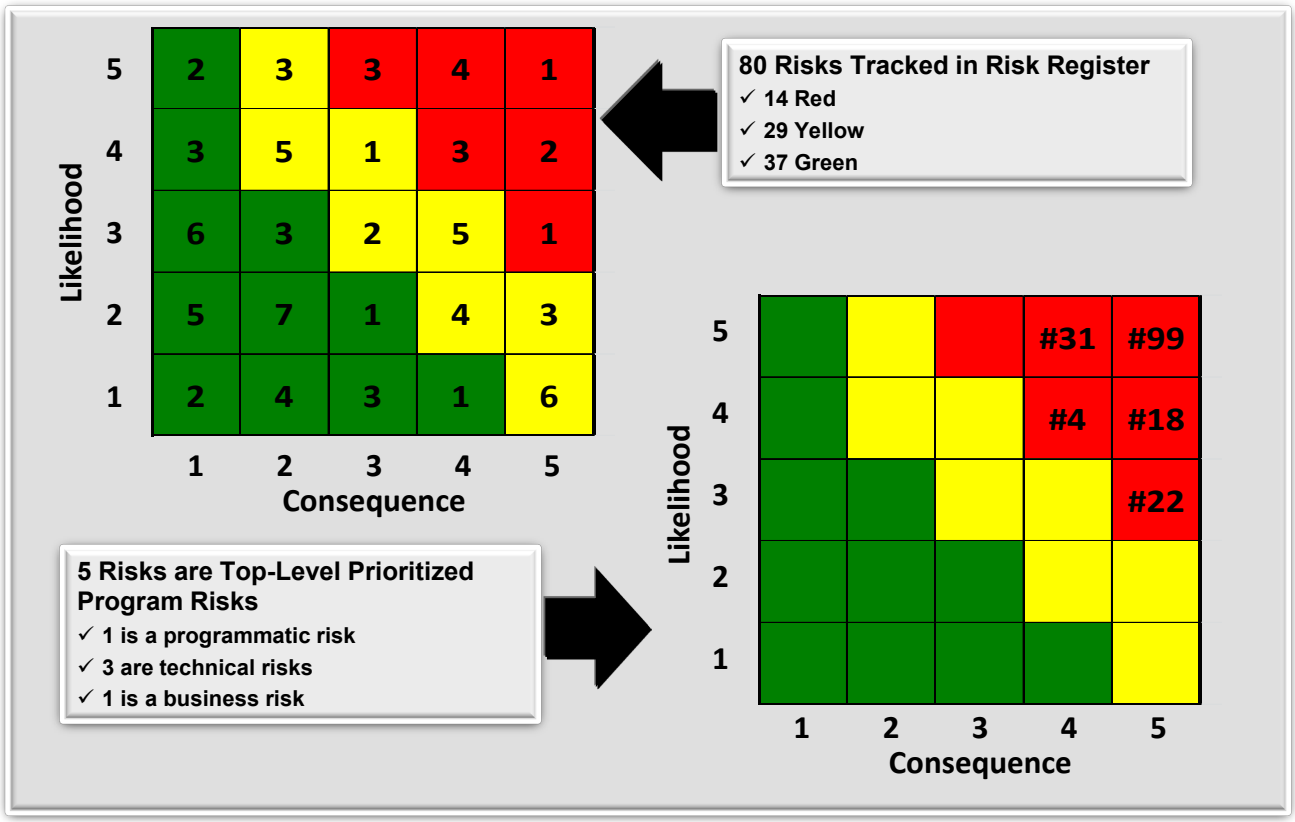


Figure 3-7. Risk Matrix Showing Prioritized Results

Since safety and system hazard risks typically have cost, schedule, and performance impacts for the program, they should be addressed in the context of overall risk management. As a best practice, programs should include current high system hazard/ESOH risks together with other program risks

on the prioritized risk matrix presented at key program decision points. Programs should use a Service-developed method to map these risks to the risk matrix and register, as appropriate.

➢ ***Expectations***

- Risks are characterized as low, moderate, or high based on placement of the likelihood and the maximum of the three consequence values on the risk matrix.

3.3.4 Risk Register

Programs commonly use a risk register as a central repository for all risks identified by the program team and records details as well as actions approved by the RMB. A program should develop a risk register as early as possible in the program's life cycle. It includes information for each risk such as risk category, risk statement, likelihood, consequence, planned handling measures, the risk owner, WBS/IMS linkage and, where applicable, expected closure dates and documentation of changes. Programs may consider combining the risk, issue, and opportunity registers into a single register.

Table 3-4 shows a sample format for a risk register. Government and contractor risk registers should contain much more information than this simple graphic allows. For example, programs should consider capturing the rationale for the selection of risk handling options. Programs should regularly update and maintain the risk register as the status of risks change due to actual versus planned progress for implemented risk handling strategies. The register should be a source for valuable management metrics such as the numbers and types of risks and risk management program efficiency.

Table 3-4. Risk Register

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence Rating	Risk Handling Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status
8231	3.2.2	Name	Technical	Open	II	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	L=3, C=4	Mitigation - Program will apply management reserve to retain adequate software engineers to burn-down SW defects	8/23/2013	1/14/2014	2/12/2014	L=1, C=4	On schedule

The risk register can serve as an important document that provides traceability of program risks and could be a source for lessons learned during or at the end of key program events. The register, along with the program RMP, could provide valuable insight for future program development.

3.4 Risk Handling

The risk handling strategy includes the handling options or combination of options and the specific implementation approach. It answers the question, *What is the plan to address the risk?* or *Should the risk be accepted, avoided, transferred, or mitigated?* After analyzing the risks, program personnel should develop a strategy to manage risks by evaluating the four risk handling options. The program chooses the best option or hybrid of options based on the risk analysis, prioritization, and potential for risk reduction. The selected handling strategy for program-level risks should be reflected in the program's Acquisition Strategy and other documentation and presented at all relevant decision points and milestones. It should include the specifics of *what* should be done; *when* it should be accomplished; *who* is responsible; the resulting cost, schedule, and performance impact; and the *resources* required to implement the risk handling plan. Figure 3-8 highlights key aspects of risk handling.

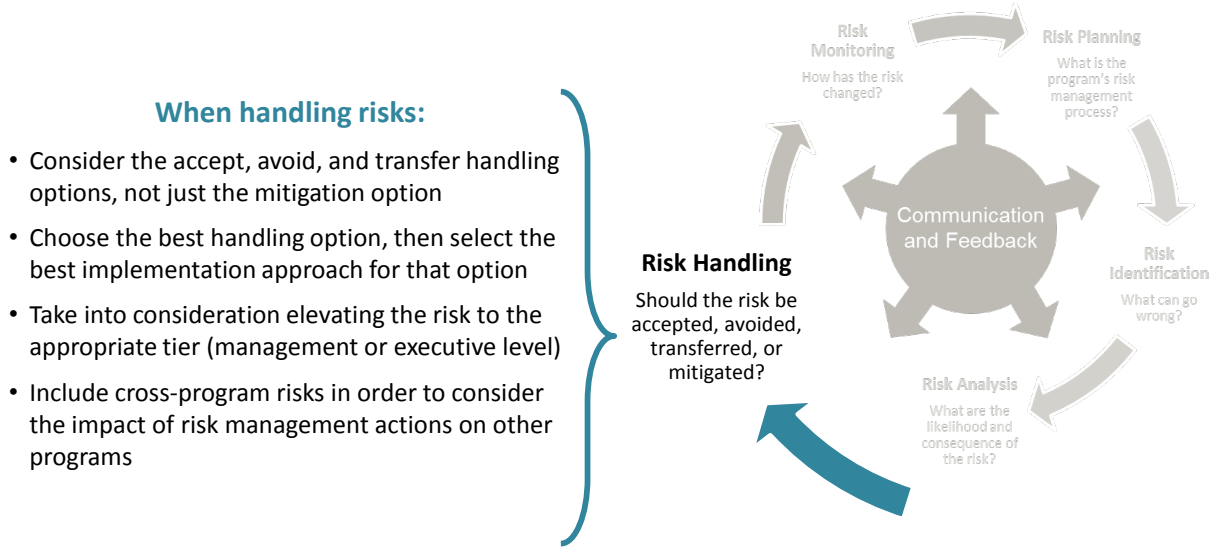


Figure 3-8. Risk Handling

Some risk handling activities may be implemented as "contingency plans" when a specific triggering event occurs. The level of detail in risk handling 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.

When selecting the handling option(s) and formulating the implementation approach, the risk owner and RMB should address questions such as:

- Is the risk handling strategy (option[s] and implementation approach) feasible?
- Is the risk handling strategy affordable in terms of funding and any needed additional resources (e.g., personnel, equipment, facilities)?
- Is adequate time available to develop and implement the risk handling strategy?
- What impact does the risk handling strategy have on the overall program schedule?

- What impact will the risk handling strategy have on the technical performance of the system?
- Are the expectations realistic given program circumstances, constraints, and objectives?

Programs often fall into the trap of identifying ongoing baseline program activities as risk handling activities, without the requisite changes to the planning, requirements, or program budget/resource allocation. This approach is typically insufficient. In most situations, relying on previously planned program activities results in the program's de facto acceptance of the risk.

3.4.1 Risk Acceptance

By risk acceptance, the program acknowledges that the risk event or condition may be realized. Accepting a risk does not mean it should be ignored. It should continue to be tracked through continuous monitoring to ensure the accepted consequences do not change for the worse. The monitoring process should establish knowledge points that provide reevaluation opportunities. Before accepting the risk, the program should identify the resources and schedule that would be needed should the risk be realized. Occasionally, executives and managers must seek relief from the next higher headquarters. Undoubtedly in constrained environments, programs and executive managers occasionally must accept risk due to competing priorities. However, programs should make every attempt to understand the risk so future efforts are fully informed and strategically planned.

3.4.2 Risk Avoidance

Through risk avoidance, the program reduces or eliminates the risk event or condition by taking an alternate path. Simply stated, it eliminates the source of the risk and replaces it with a lower risk solution. Analyzing and reviewing the proposed system in detail provides insight into the drivers for each technical requirement. Examples might be changing operating procedures or using a low-risk mature technology. Risk avoidance may provide the PM with an understanding of what the real needs are and ways of circumventing the risks that are not critical to program cost, schedule, and/or performance. This may require changes to the allocation of program resources, or requirements and specifications that reduce risk to an acceptable level. The avoidance handling option should be used only if the selected implementation approach truly results in the desired effect and reduced risk likelihood and/or consequence.

3.4.3 Risk Transfer

Risk transfer includes reassigning the risk responsibility to another entity. This approach may involve reallocating a risk from one program to another, between the government and the prime contractor, within government agencies, or even across two sides of an interface managed by the same organization. However, programs should recognize transference of risk does not eliminate all responsibility and risks must be monitored for potential consequences. A prerequisite for transferring 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 that is managing the external side of an

interface, to potentially meet the required performance of that subsystem. Transference requires active management to track progress at established knowledge points to ensure expectations are achieved. The transfer option may be viable only if it results in an acceptable risk likelihood and/or consequence posture.

3.4.4 Risk Mitigation

The risk mitigation option seeks to actively reduce risk to an acceptable level. Mitigation generally entails taking action to reduce the likelihood, and on occasion the consequence, of a risk to as low as possible in order to minimize potential program impacts. Programs should avoid the tendency to readily select mitigation as the risk handling option without seriously evaluating the acceptance, avoidance, and transfer options. The approaches listed below are potential aspects of program activities that can be considered for risk mitigation. They include but are not limited to:

- Multiple Development Efforts: Create competing systems in parallel that meet the same performance requirements.
- Alternative Design: Create an off-ramp design option that uses a lower risk approach.
- Trade Studies: Arrive at a balance of engineering requirements in the design of a system.
- Early Prototyping: Build and test prototypes early in the system development.
- Incremental Development: Defer capability to a follow-on increment.
- Technology Maturation: Use when a desired technology will replace an existing technology.
- Robust Design: Use advanced design and manufacturing techniques that promote quality through design; may be more costly than other approaches to design.
- Reviews, Walk-throughs, and Inspections: Reduce the probability/likelihood and potential consequences/impacts of risks through timely assessment of actual or planned events.
- Design of Experiments: Identify critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.
- Open Systems, Standard Items, or Software Reuse: Select commercial specifications and standards, or use existing and proven hardware and software, where applicable.
- Mockups: Explore design options using mockups, especially for man-machine interface.
- Models and Simulation: Investigate various design options and system requirement levels.
- Key Parameter Control Boards: Establish a control board for a parameter when a particular feature (such as system weight) is crucial to achieving the overall program requirements.
- Test, Analyze, and Fix: Plan a period of dedicated testing to identify and correct deficiencies.
- Demonstration Events: Establish knowledge points that demonstrate whether risks are being abated.

- Process Proofing: Simulate actual production environments and conditions to ensure repeatedly conforming hardware and software.

Effective mitigation options should result in acceptably reduced risk likelihood and/or consequence. Typically, risk mitigation activities reduce the likelihood of the risk event occurring. In rare occasions, it is possible to reduce the consequences associated with a risk if the program changes the design architecture or addresses binding constraints, such as budget limitations, inflexible schedule, or requirements, as part of the risk mitigation activities. If actions are taken to reduce consequences, consideration should be given to a complete re-characterization of the risk statement, description, prioritization, and handling. The result is most likely a new risk rather than management of the existing risk.

3.4.5 Risk Burn-Down

The risk handling plan (for all handling options) should include a risk burn-down plan; this should be a consideration for all high, moderate, and selected low risks. For most risks, the burn-down plan consists of time-phased handling activities with specific success criteria. This detail allows the program to track progress to plan to reduce the risk to an acceptable level or to closure. A burn-down plan generally consists of six steps:

1. Identify and lay out the risk handling activities in a sequential manner, using realistic and logical schedule precedence, typically a finish-to-start.
2. Ensure all risk handling activities (1) are clearly defined and jargon free, (2) are objective and not subjective, and (3) have specific, measurable outcomes. For example, the statement "performing a test" fails each of the three criteria, whereas "brassboard throughput test results met or exceeded all performance thresholds requirements, and the results are approved by the user" passes all three criteria.
3. Assign a planned likelihood and consequence value to each risk handling activity. Not all handling activities will result in a score change or burn-down of the risk but are necessary to track the progress of the burn-down plan (e.g., meetings do not mitigate risks, results do).
4. Estimate the start and finish dates for each risk handling activity.
5. Include the risk handling activities or a subset of these activities in the program IMS. Tasks identified in the IMS should describe an activity, a specific measurable outcome, and a point of contact responsible for the completion of each task.
6. Chart the relationship of risk handling activities, plotting risk level versus time to estimate their relative risk burn-down/reduction contribution.

Burn-down charts should be used to track actual progress against the planned reduction of risk levels as part of risk monitoring. Figure 3-9 shows a simple risk burn-down chart. It includes a snapshot of the progress of handling the risk over time and the effectiveness of previous risk handling activity.

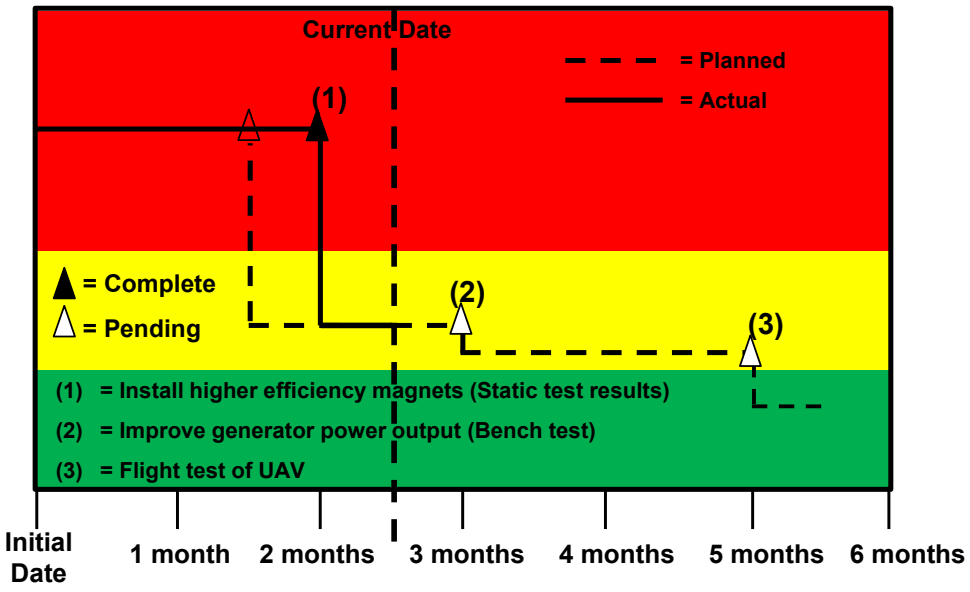


Figure 3-9. Risk Burn-Down

➢ ***Expectations***

- The risk register captures the handling option and associated activities for each risk.
- Risks can be accepted, avoided, transferred, or mitigated.
- Risk mitigation activities typically reduce the likelihood of the risk event occurring.
- Changes in consequence level are generally associated with program-level changes (e.g., architecture, budget, schedule, or requirements) and may necessitate a complete re-characterization of the risk and its handling plan.
- Risks are managed at the appropriate organizational level (executive, management, or working). The program tracks the development and implementation of the risk handling plan.
- The program allocates appropriate budget and other resources to implement the handling plan and enters mitigation activities into the IMS.
- Risks that are assessed as high have resourced risk handling plans. Moderate risks should also typically have resourced risk handling plans, as appropriate.
  - PMs should consider contingency plans for high risks.
- Risk burn-down plans should be time-phased and include specific measurable handling activities; meetings do not burn down risks.

3.5 Risk Monitoring

Risk monitoring answers the question, *How has the risk changed* or *How are the risk handling plans working?* Risk monitoring includes a continuous process to systematically track and evaluate the performance of risk handling plans against established metrics throughout the acquisition process. Not all risk handling will be successful. The program office should reevaluate the risk handling implementation approach and associated activities to determine effectiveness and whether or not changes are needed.

Risk monitoring includes recording, maintaining, and reporting of risks, risk analyses, risk handling, and tracking results. It is performed as part of technical reviews, RMB and RWG meetings, and program reviews, using a risk management tool. Documentation includes all plans and reports for the PM and decision authorities. Risk burn-down charts are also one method to monitor risks.

If a risk changes significantly, the program team should adjust the risk handling strategy accordingly. If the risk is lower than previously analyzed, the program team may reduce or cancel risk handling activity and consider freeing resources for other uses. If risk severity increases, appropriate risk handling efforts should be developed and implemented. The rationale for the changes to the risk handling strategy should be documented and archived for historical and lessons learned purposes.

Successful risk monitoring includes timely, specific reporting procedures as part of effective communication among the program office, contractor, and stakeholders. Risk monitoring documents may include: EVM status, IMS status and reports for associated risk handling plan activities, TPM status, other program metrics, risk register reports/updates, technical reports, watch lists, technical review minutes/reports, test results, and operational feedback. Figure 3-10 highlights selected components of risk monitoring. Risk monitoring allows timely actions to address potential problems.

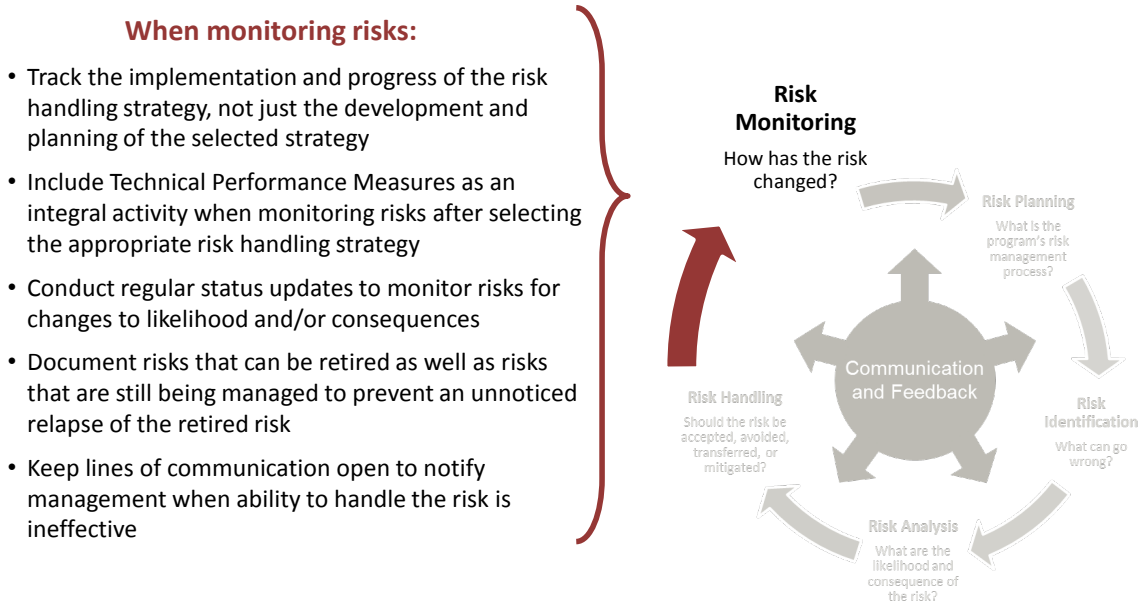


Figure 3-10. Risk Monitoring

Program offices and contractors should establish regular intervals for reviewing risks. Periodic program management and technical reviews provide useful information to identify cost, schedule, or performance barriers to program objectives and milestones. Therefore, periodically throughout the life cycle, programs should reevaluate risks by:

- Monitoring risks for changes to likelihood or consequence as a result of program progress.
- Tracking risk status in the risk register reports/updates and the risk reporting matrix to communicate risk status.
- Alerting management when risk handling plans need to be adjusted.
- Citing those risks that can be retired.
- Reviewing retired risks on a periodic basis to ensure they have not relapsed.

Figure 3-11 illustrates the results of risk handling actions and provides an example of changed risk status following successful completion of risk handling. The plotted position on the risk reporting matrix should show the current assessment of the risk's likelihood and the maximum of the cost, schedule, and performance consequence on the program if the handling strategy is not implemented or fails. Therefore, the program office should feed the risk monitoring results back to reexamine the risk handling strategies and risk analysis levels, as well as the risk identification and risk management planning as warranted.

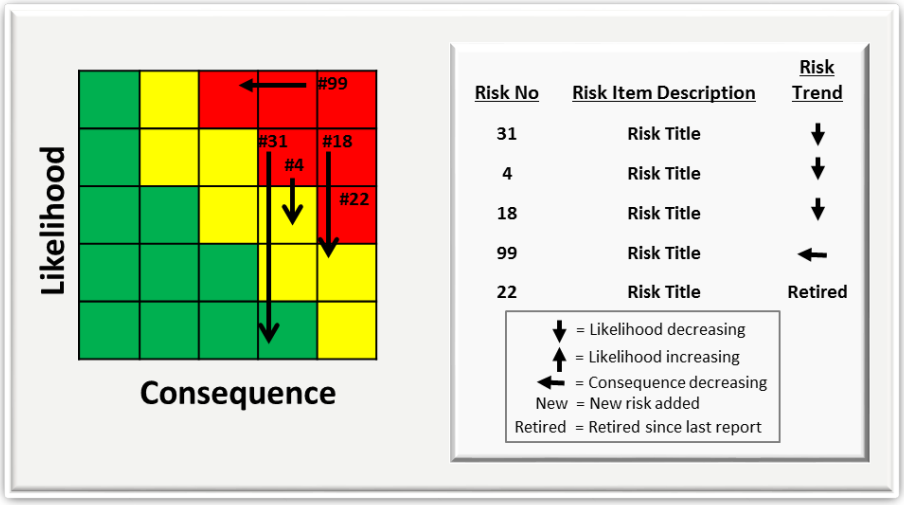


Figure 3-11. Example Risk Monitoring and Trend Matrix

One key to risk monitoring is to establish an effective means to display the current risk status and burn-down progress for the program. Figure 3-12 provides a risk reporting format used to summarize key program risks at Program Management Reviews or other meetings with stakeholders or senior leaders. The PM should use similar indicator systems to quickly evaluate and communicate risk status and trends throughout the life cycle. Program teams should develop more detailed indicators to provide an early warning when the likelihood or consequence exceeds preestablished thresholds/limits, is trending negatively, or has evolved into an issue.

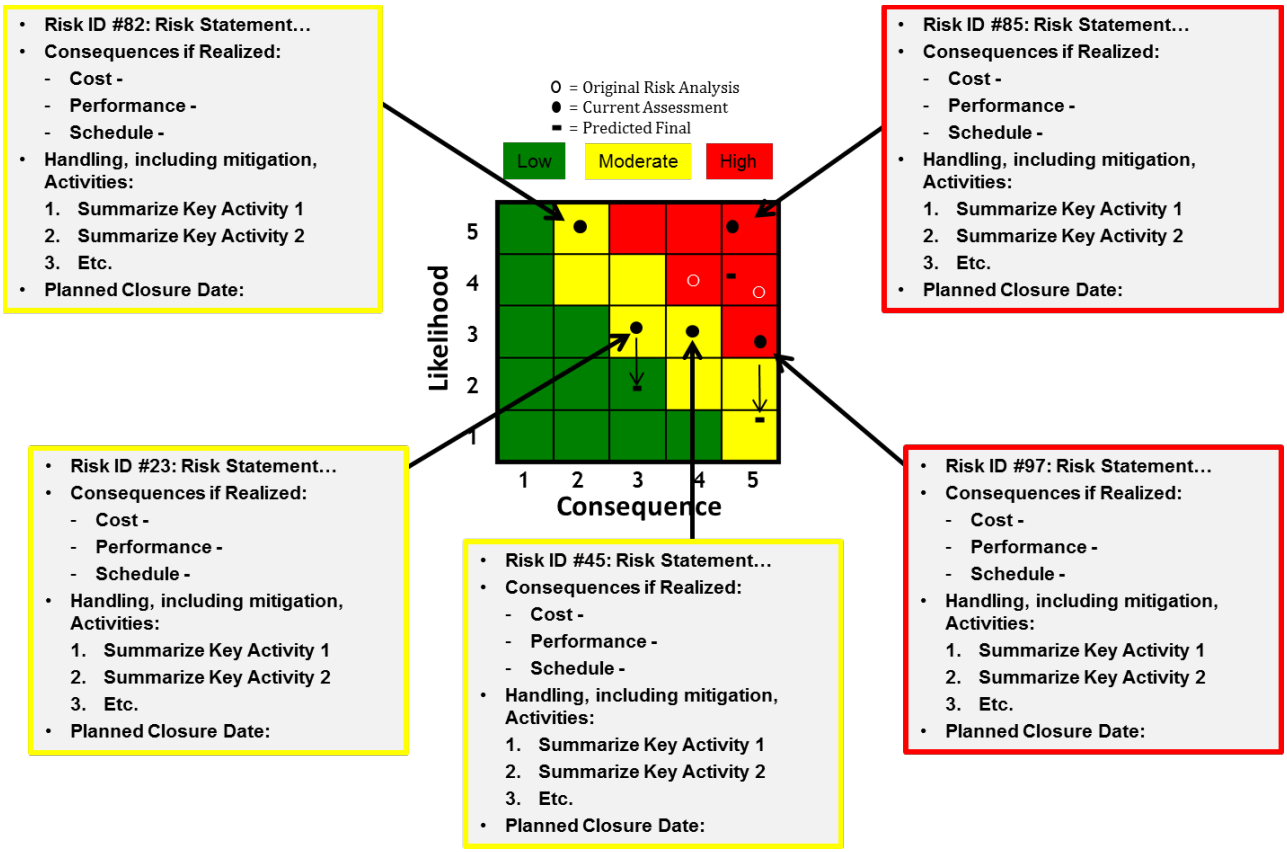


Figure 3-12. Suggested Risk Reporting Format

➢ ***Expectations***

- The program team conducts regularly scheduled status updates to monitor risks for any changes to likelihood or consequence, and to monitor earned value (cost variance), TPMs, and variation in schedule as a result of program progress.
- The team alerts management when risk handling plans should be implemented or adjusted.
- Managers alert the next level of management when the ability to handle a risk exceeds authority or resources.
- The team tracks actual versus planned progress against the risk handling plan.
- The program establishes a management indicator to monitor risk activity.
- The program periodically reviews closed risks to ensure risks have not redeveloped.

4 RISK MANAGEMENT IN RELATION TO OTHER PROGRAM MANAGEMENT AND SYSTEMS ENGINEERING TOOLS

The risk management process should be integrated with other program management and systems engineering functions and associated tools during all phases of the program. Examples of program management tools discussed in this section are the WBS, IMP, IMS, and EVM. TPMs are an example of a relevant systems engineering tool.

The program should use the WBS to ensure comprehensive coverage of all tasks that must be examined for risk during risk identification sessions (see Section 3.2) and periodic reviews of work packages. The program should then enter approved risks into the risk register along with the associated risk analysis results and handling plans and, whenever possible, link the risks to the work packages associated with the handling effort. Similarly, the contract in-scope handling plan activities should be included in the IMS to provide a consistent method of measuring progress toward completion.

For handling efforts that represent new or out-of-scope work, the program may need new resource-loaded work packages to track the effort. The IMP could include major program-level risks. Risk handling efforts should include assigned resources (funded program tasks) reflected in the IMP, IMS, and EVM baselines. Programs should use TPMs and metrics along with EVM and IMS data to assist in identifying and monitoring potential risks and progress to plan.

Collectively, the WBS, IMP, IMS, EVM, and TPM tools help the PM gain insight into balancing program requirements and constraints against cost, schedule, or performance risks.

4.1 Work Breakdown Structure

The WBS (including the WBS dictionary) 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.

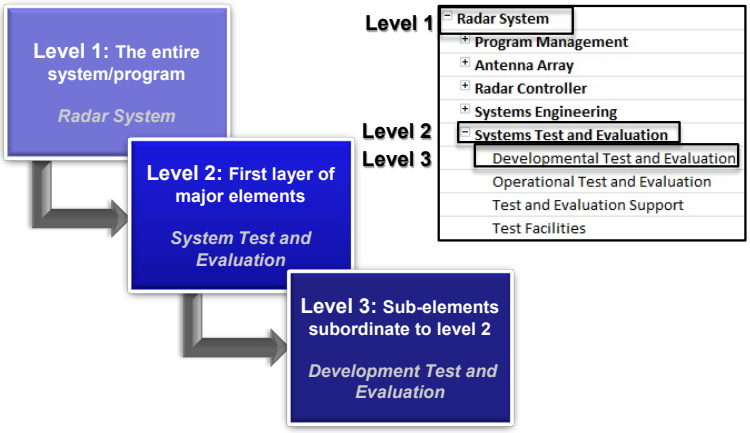


Figure 4-1. Example of WBS Levels

The program should use the WBS as a basis for identifying all the tasks that should be analyzed for risk, for monitoring risks at their respective levels (primarily for impact on cost and schedule performance), and for evaluating the resulting effect of risks on the overall program. Following risk handling planning, the program should update the WBS as needed to reflect selected handling tasks.

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

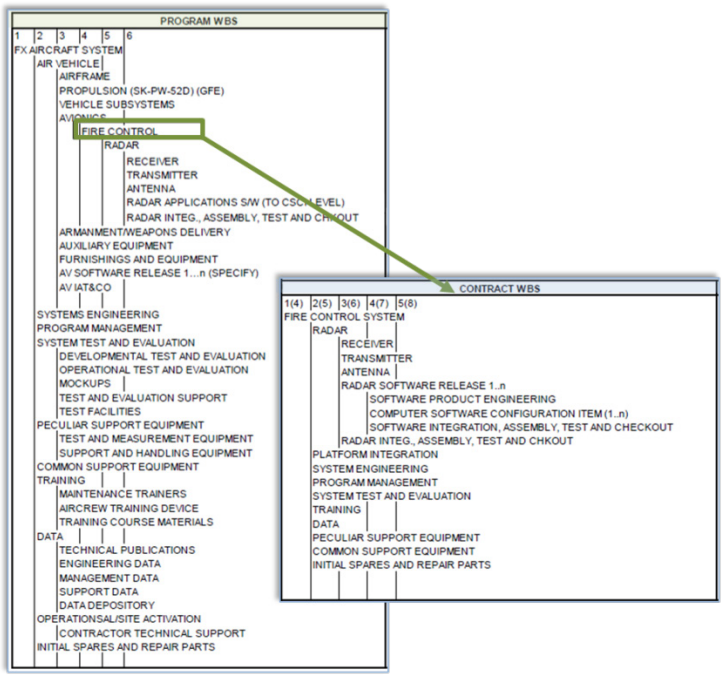


Figure 4-2. Government and Contractor WBS Relationship

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 and facilitate effective planning and forecasting that are critical to project success. The IMP is an overarching event-based plan that displays each milestone and supporting accomplishments needed for program completion. Programs should include risk management tasks and handling activities, as appropriate.

A well-constructed IMS includes distinct tasks that are summarized by WBS identifiers so the program can track progress and measure schedule performance. Risk activities should be included in the program IMP and IMS (Figure 4-3) and resourced appropriately in the IMS. The IMP and IMS should be traceable to the program and contractor WBS and Statement of Work.

The IMP narratives can be a good source to identify risks as they may contain risk-related information. The program should include risk handling activities and associated resources in the IMS to establish an accurate performance measurement baseline and critical path analysis.

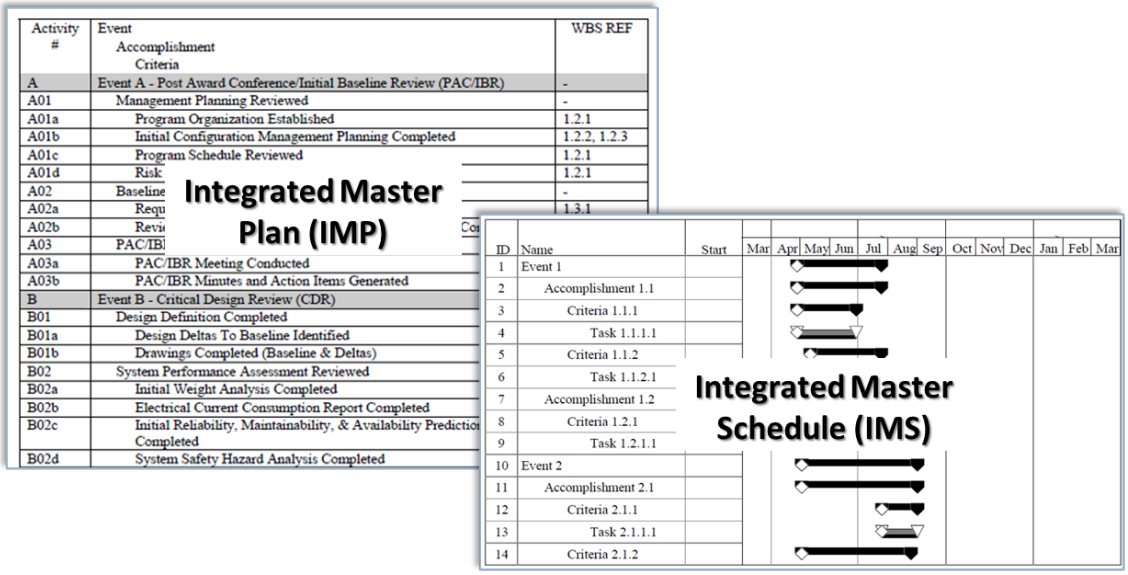


Figure 4-3. IMP/IMS Creation and Implementation

4.2.1 Schedule Health Assessment

Programs should regularly assess the health of the IMS through a schedule health assessment (SHA). The Defense Contract Management Agency (DCMA) uses 14 evaluation criteria to assess the quality and structural integrity of a schedule. Figure 4-4 summarizes the 14 criteria with a notional assessment. Unhealthy indications should be examined for areas to improve. Programs should ask relevant questions and perform follow-up research to improve a schedule in areas that do not meet the DCMA standard. (See DCMA-EA PAM 200.1 for additional information associated with these 14 evaluation criteria.)

Metric	Goal	Status
Logic – incomplete tasks with missing predecessor or successor logic links	<5%	
Leads – number of leads (overlap between tasks with logic dependencies)	0 tasks	
Lags – number of tasks with lags (delay between a predecessor task's completion and successor's start date)	<5%	
Relationship Type – establishes the order in which each task should be completed	<10% non-Finish-Start	
Hard Constraints – fixed task start or finish date that prevents tasks from being moved by their logic-driven dependencies	<5%	
High Duration – unfinished tasks with a baseline duration of greater than 44 working days	<5%	
High Float – incomplete tasks with total float greater than 44 working days	<5%	
Negative Float – less than zero float, forecasted date may be unrealistic	0 tasks	
Invalid Dates – incomplete tasks with actual start /finish date in the future; forecast dates prior to status date	0%	
Resources – allocated resources (hours/dollars)	0 improper	
Missed Tasks – tasks that do not finish as planned	<5%	
Critical Path Test – identifies broken logic, usually missing predecessors and/or successors	0 days	
Critical Path Length Index (CPLI) – measures the efficiency to finish on time	>=.95	
Baseline Execution Index (BEI) – efficiency with which actual work has been accomplished	>=95%	

Figure 4-4. Sample 14-Point Schedule Health Assessment Items and Status

4.2.2 Schedule Risk Analysis

The SRA uses task duration uncertainties and program risks affecting schedule execution in combination with a statistical simulation technique (most often Monte Carlo method) to analyze the level of confidence in meeting selected program dates. As with any analysis, the quality of the analysis results depends on the quality of the input data. Programs should consider conducting an SRA once an approved, well-structured IMS is available, and update the SRA as well as the underlying schedule on a recurring basis over the course of the program. The results of an SRA are most usefully seen not so much as a definitive forecast but as an indicator on the program's likely schedule progression and completion without additional risk handling actions. As such, the analysis can inform management actions, support "what-if" evaluations, and provide inputs for prioritizing risk handling approaches.

Before performing an SRA, the program should assess the IMS using the criteria provided in Section 4.2.1 to ensure the underlying schedule is free of potential errors that could have an adverse impact on the SRA results. For example, even a single hard constraint can potentially lead to erroneous SRA results associated with modeled outputs. Assuming a satisfactory IMS, a probability distribution is established for the duration of each task containing schedule estimating uncertainty and/or various forms of risk (as discussed in Section 3.2.2). The type of distribution selected and its corresponding characteristics may vary within the schedule. Probability distributions are developed for the remaining durations of all tasks/activities consistent with the authorized work.

The results of an SRA are typically displayed as a histogram (an approximation to a probability density function) providing the frequency of schedule outcomes (dates) and an S-Curve (a cumulative distribution function) providing the cumulative probability of achieving dates associated with given milestones or overall program completion.

Other types of outputs include descriptive statistics, a probabilistic critical path, and a probabilistic sensitivity analysis. All of these results should be evaluated for indicators of schedule risk.

4.2.3 Cost Risk Analysis

As in the case of an SRA, a CRA can potentially provide program management with an early estimate of potential cost overruns and the cost elements with probability distributions that most greatly influence these outcomes. The program should consider developing a CRA once a suitable cost representation is available (e.g., WBS, IMP, IMS), and update the underlying cost model and CRA over the course of the program.

Although the CRA can be performed throughout the acquisition phases, it should be used in conjunction with a technical performance analysis, and an SRA as appropriate. CRAs should address both cost-estimating uncertainty and the risk categories present (e.g., technical, schedule). As the program advances through the acquisition life cycle and the WBS and IMS are expanded, additional elements can be identified and added to lower levels of the cost model as appropriate (e.g., WBS levels 4, 5, or lower).

Different approaches exist for performing a CRA depending upon the underlying model structure. As with SRAs, Monte Carlo simulation is a commonly used tool for this purpose. Common CRA outputs include a histogram and an S-curve. Perhaps the most common model structure is a listing of most likely cost elements, typically in a spreadsheet, that subtotal and total to higher levels of program integration. One or more probability distributions can be assigned to each (input) element to represent cost-estimating uncertainty and risk. Another model structure involves the use of a fully resourced IMS. Probability distributions are added to resources in this approach, and the results are generated via a Monte Carlo simulation. Other, more elaborate methods also exist, such as a joint confidence level methodology that yields a joint cost and schedule risk output.

4.2.4 Performance Risk Analysis

A PRA uses statistical techniques to quantify the performance impact of the modeled item. PRAs are used to evaluate a variety of complex performance risks applicable to DoD programs. Examples include: analysis of alternatives involving a variety of systems and technologies, ballistic testing, dynamic stability of control systems, electronic component and system reliability, missile accuracy, satellite gap analysis versus time, statistical tolerance intervals in designed experiments for test and evaluation, timing closure on application-specific integrated circuits, and weapon system probability of kill. Each PRA will typically have a different model structure, application of probability distributions, and resulting outputs, depending upon the engineering discipline and specific application.

Programs may use TPMs to track selected output from PRAs. See Section 4.4 for a discussion on selecting TPMs.

4.3 Earned Value Management

EVM provides a disciplined, structured, objective, and quantitative method to integrate technical work scope, cost, and schedule objectives into a single cohesive contract baseline plan. This performance measurement baseline is used for tracking contract performance.

The baseline can be used to (1) quantify and measure program/contract performance, (2) provide an early warning system for deviation from a baseline, and (3) provide a means to forecast final cost and schedule outcomes. EVM also can provide an input to the project's risk management process for identifying potential risks and issues, and monitoring and adjusting implemented risk handling plans.

EVM provides a rigorous examination of what has already occurred on the project, using quantitative metrics to evaluate project past performance. If variances in cost and schedule appear in Integrated Program Management Reporting, the program team can then use EVM to analyze the data, determine cost and schedule variances, isolate causes of the variances, identify potential risks and issues that may be associated with the variances, forecast future cost and schedule performance, and implement corrective action plans.

The DoD and the federal government at large have adopted the guidelines in ANSI/EIA-748, an industry EVM standard, for use on government programs and contracts. The DoD EVM policy requires contractor management systems to be compliant with ANSI/EIA-748 to ensure the validity of the information whenever EVM is required.

4.4 Technical Performance Measures and Metrics

TPMs and metrics are useful for measuring technical progress and providing insight into program risks. DoDI 5000.02 requires the use of TPMs and metrics to assess program progress.

Well-planned TPMs and metrics are valuable tools used to support evidence-based decisions at selected events and knowledge points throughout the program life cycle, such as technical reviews, audits, or milestone decisions. Programs should carefully select TPMs and metrics to be used during each life cycle phase to measure progress versus planned technical development and design. These TPMs and metrics should be documented in the SEP. Measures to consider include but are not limited to: requirements; design; integration; manufacturing; system performance; computer hardware usage; cost and progress to plan; lethality; reliability, availability, and maintainability; survivability; size, weight, power, and cooling (SWAP-C); system security (e.g., cybersecurity); and software. Each measure should be SMART (**S**pecific/Objective, **M**easurable, **A**chievable/Observable, **R**elevant, and **T**imely).

Programs should identify and track other metrics such as the progress in program management and systems engineering processes (e.g., staffing, budgets, schedule, configuration management, and quality). Once risks are identified, programs should carefully consider appropriate TPMs and metrics to aid in monitoring the progress of risk handling plans. TPMs and metrics are likely to change over the course of the program as risks are retired and new risks are identified.

- ***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, IMS, and TPMs.
  - Programs use appropriate analytical tools (SHA, SRA, CRA, PRA, EVM, etc.) to help identify, analyze, and/or monitor risks.
  - Programs define and use TPMs and metrics throughout the life cycle to help identify risks and monitor risks, issues, and opportunities.
    - TPMs and metrics selected should be SMART – Specific/Objective, Measurable, Achievable/Observable, Relevant, and Timely.

5 ISSUE MANAGEMENT

Through issue management, the program identifies and addresses events or conditions that have already occurred, are occurring, or are certain to occur in the future and have a potential negative impact on the program.

Sometimes programs mischaracterize an issue as a risk by describing it in future, uncertain terms when, in fact, it has occurred or will certainly occur. Risk management applies resources to lessen the likelihood and/or the consequence of a future event of less than certain probability. Issue management, on the other hand, applies resources to address and resolve the consequences associated with a past, present, or certain future event. Programs also should assess whether issues may create additional potential risks, and evaluate them accordingly.

Figure 5-1 displays the issue management process.

Figure 5-1. Issue Management Process

Issue management and opportunity management (Section 6) are complementary to the risk management process (Section 3). Programs should take advantage of the common practices between issue and risk management while recognizing and accounting for the distinctive characteristics of each. Programs should establish a separate Issue Management Board, but may evaluate whether separate boards are necessary. The key is to ensure proper focus on both issues and risks so that attention on current problems will not overtake efforts to manage risks and opportunities. Either way, programs should establish a defined and structured issue management process to ensure issues are identified, analyzed, handled, and monitored to retirement. The process should ensure an effective

strategy is developed for resolving critical and high-priority issues, the strategy has been properly vetted at the program management level or above as appropriate, and resources are made available to ensure execution. Programs should quantify issue urgency so as to prioritize resolution, and document plans of action and milestones (POA&M). Identified issues should be updated periodically until resolved and reviewed during the regularly scheduled program meetings, program reviews, and technical reviews. The Issue Management Board (or RMB equivalent) should assign an owner for each approved issue. Programs should record each approved issue in an issue tracking register and may consider combining the risk, issue, and opportunity registers.

Approved issues should be analyzed using the program's risk management consequence criteria, and the results entered into an issue tracking register. Unlike opportunities and risks, no evaluation of issue likelihood is necessary as the probability = 1. Using the top row from the risk matrix, the issue consequence value is then converted to an issue level using the issue reporting matrix in Figure 5-2, and the results are entered into the program's issue tracking register. The green, yellow, and red regions on the matrix indicate areas of low, moderate, and high issue level, respectively.

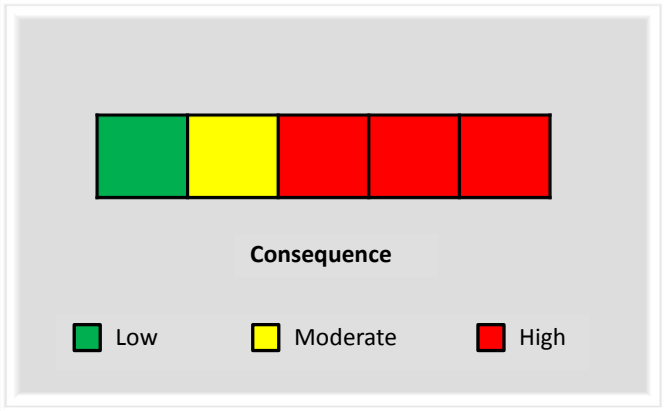


Figure 5-2. Issue Reporting Matrix

Handling (or corrective action) plans should be developed for high issues and moderate issues as appropriate, and the resulting plan documented in the program's issue tracking register. As in the risk and opportunity cases, the program should evaluate the handling options in terms of cost, schedule, performance, and residual risk, and select the best option (or hybrid of options) consistent with program circumstances. The program addresses issues using the following handling options:

- **Accept** – Accept the consequence of the issue based on results of the cost/schedule/ performance business case analysis.
- **Avoid** – Eliminate the consequence of the event or condition by taking an alternate path. Examples may involve changing a requirement, specification, design, or operating procedure.
- **Transfer** – Reassign or reallocate the issue responsibility from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization.

- **Mitigate** – Implement a strategy to reduce the issue consequences and residual risk to as low as possible or minimize its impact on the program.

An implementation approach is then chosen and the resulting handling strategy, along with the necessary resources for implementation, are approved by the RMB (or equivalent) and documented in the issue tracking register. As with risks and opportunities, handling plan activities should be included in the program IMS and the issue tracking register.

The program should track resolution of issues against the issue handling plan (or POA&M, as appropriate). Once the handling plan is in place, the program office should (1) monitor the issue to collect actual versus planned cost, schedule, and performance information; (2) feed this information back to the previous process steps (as shown in Figure 5-1); (3) adjust the handling plan (or POA&M) as warranted; (4) analyze potential changes in the issue level; and (5) examine potential changes in the issue along with potential associated risks. This update information should be included in the program's issue tracking register. Figure 5-3 shows a sample issue tracking register.

Issue	Consequence	Type T/B/P	Plan of Action and 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 or will occur, the type of issue [technical, business, or programmatic], and 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)		
				(P) (A)		
				(P) (A)		
				(P) (A)		

Figure 5-3. Issue Tracking Register

➢ ***Expectations***

- Programs should not confuse issues with risks. Both have consequences, but with issues the probability = 1 as they have already occurred or are certain to occur.
- Issues are assessed for residual risks, and formal risks are established as appropriate.
- Programs document an issue management process. This process may share elements with the risk management process, while respecting differences.
- Programs develop a plan to address, track, and review issues during regular meetings and reviews.
- 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

Opportunities are potential future benefits to the program's cost, schedule, and/or performance baseline, usually achieved through reallocation of resources. Risk and opportunity management support Better Buying Power initiatives to achieve "should-cost" as well as "will-cost" objectives. Figure 6-1 is a simple portrayal of how opportunity management and risk management help realize benefits for a program.

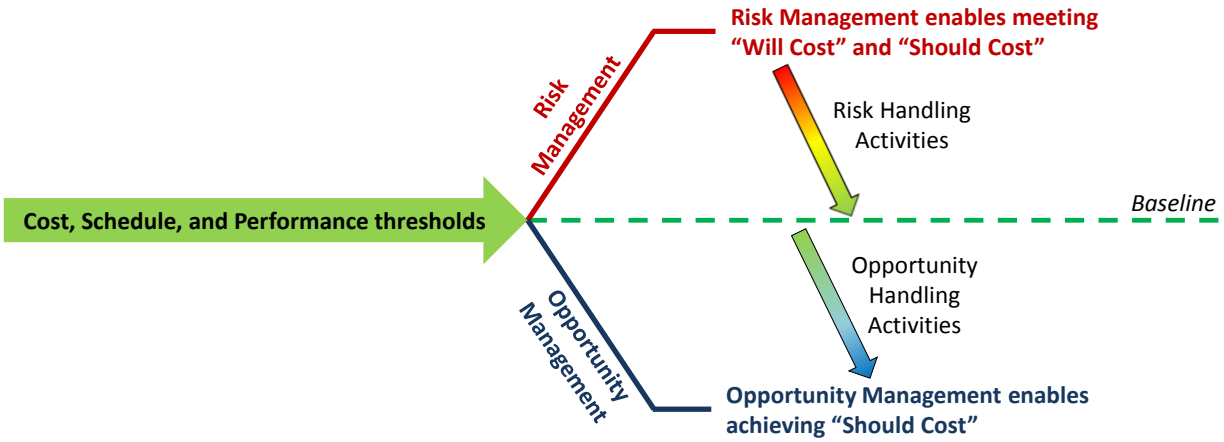


Figure 6-1. Opportunities Help Deliver Should-Cost Objectives

Opportunity management, like issue management, should be considered as complementary to risk management (Section 3). Program personnel should use opportunity management to plan, identify, analyze, handle, and monitor initiatives that yield potential program cost reductions, schedule reductions, and/or performance improvements. Opportunity management, issue management, and risk management all attempt to improve potential program outcomes.

Identifying opportunities starts with forecasting potential enhancements within the program's technical mission and stakeholder objectives. As opportunities emerge, the program can shift focus toward understanding how to take advantage of opportunities while continuing to manage risks and issues. Opportunity management measures potential program improvement in terms of likelihood and benefits. Figure 6-2 shows the opportunity management process.

Opportunities should be evaluated for both advantages and disadvantages. This is important because potential benefits associated with an opportunity may be overstated and corresponding risks may be understated. In addition, all candidate opportunities should be thoroughly screened for potential risks before they are approved, and handling plans should be developed and implemented as appropriate.

Figure 6-2. Opportunity Management Process

Through the opportunity management process, the program identifies potential enhancements to cost, schedule, and/or performance. Opportunities may be identified before program execution and should be sought across the program life cycle. Important sources of opportunities include system and program changes that yield reductions in total ownership cost. For example, adherence to a modular open systems approach or securing appropriate government rights to a technical data package can offer opportunities in sparing and competition for modifications. These cost reductions can be in research, development, test, and evaluation (RDT&E), production, and operations and maintenance (O&M) dollars throughout the life cycle.

During production, the program should continuously analyze opportunities for design and manufacturing 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 yield production or support cost reductions.

During the Operations and Support (O&S) phase, opportunities often may arise from the observation and analysis of actual in-service performance. In addition, the emergence of more efficient production practices or better performing components can provide opportunities for improved reliability, more efficient fuel consumption, improved maintenance practices, other reduced support costs, or economic capability enhancements.

Although there is an upside to pursuing the desired benefits of opportunity management, there are also downsides resulting from changes in the baseline plan and scope of the program, as well as potential unanticipated outcomes and risks. The program should perform an analysis to estimate and

justify the potential added cost and/or schedule needed to achieve the intended benefit, or the decreased performance that may result from implementing the opportunity.

Programs may establish a separate Opportunity Management Board, but this guide assumes the RMB also oversees opportunity management. Once candidate opportunities are identified, the program RMB (or equivalent) should examine the opportunity and, if approved, assign an owner, and track it in the opportunity register (analogous to the risk register). The next step is to perform a cost, schedule, and performance benefit analysis for each approved opportunity and document the results. Opportunities with sufficient potential should be evaluated relative to potential handling options.

The cost, schedule, and performance benefit analysis should justify the handling option selected. Available resources are often a zero-sum situation—applying resources to evaluate and implement opportunities may reduce available risk handling resources, so expenditures must be weighed against program success. In such cases the potential constraints associated with limited resources may still warrant pursuing an opportunity, but this must be balanced against the potential likelihood of achieving the desired benefits, and the degree of value added in meeting existing program requirements.

Programs should not ignore opportunities with small improvements that can be obtained with minor effort and without program disruption. Aggregation of multiple smaller benefits may accrue to a larger program benefit.

Programs should use care to avoid using opportunities as a means of "gold plating" requirements. Even though an opportunity may appear to be a good idea, expenditures need to be justified. Also the government and vendor may see opportunity benefits and associated changes in cost, schedule, and performance differently. For example, a vendor is not likely to propose or facilitate an opportunity that may not benefit itself. When possible, programs should consider ways to create incentives for vendors to recognize and recommend opportunities.

Handling options should be evaluated in terms of cost, schedule, and performance potential benefits and risk, and the best option (or hybrid of options) selected. These handling options include:

- **Pursue** – Fund and implement a plan to realize the opportunity. (Determination of whether to pursue the opportunity will include evaluation of when the opportunity would be realized, the cost, additional resources required, risk, and time to capture.)
- **Reevaluate** – Continuously evaluate the opportunity for changes in circumstances.
- **Reject** – Intentionally ignore an opportunity due to cost, technical readiness, resources, schedule burden, and/or low probability of successful capture.

Given the selected option, the program should then choose a handling implementation approach and develop a handling plan. Determinations of cost, resources, and time to achieve the benefit of the opportunity all weigh into the decision whether to expend resources to pursue and implement the opportunity.

For the "pursue" handling option, the resources needed to implement the handling plan should be approved and documented in the program's opportunity register. Handling plan activities should be included in the opportunity register (or equivalent) and inserted into the program IMS in order to track progress to plan. Risks identified with the opportunity should be included in the risk register.

As an example of handling, 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 given the potential weight reduction. In this case, the program may opt to watch the potential opportunity and reevaluate improving the product after Low-Rate Initial Production.

Once the opportunity handling plan is in place, the program office should monitor the opportunity. It should collect actual versus planned cost, schedule, performance, and benefit information, feed this information back to the prior process steps, adjust the handling plan as warranted, analyze potential changes in the opportunity level, and examine potential risks and additional opportunities that may be identified. This updated information should be included in the program's opportunity register and risk changes identified in the risk register. Figure 6-3 shows a sample opportunity tracking register for use at Program Management Reviews or other reviews.

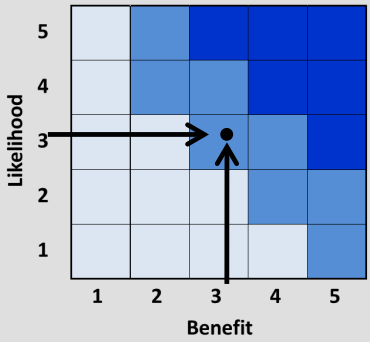
Opportunity	Likeli-hood	Cost to Implement	Benefit					Oppor-tunity Level	Handling Strategy	Expected Closure
			Cost			Schedule	Performance			
			RDT&E	Procurement	O&M					
Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades.	Mod	$3.2M			$4M	3 month margin	4% greater lift	Moder-ate	Reevaluate - Summarize the handling plan	March 2017
Opportunity 2: Summarize the opportunity activity.	Mod	$350K	$25K		$375K			Low	Reject	May 2017
Opportunity 3: Summarize the opportunity activity.	High	$211K		$0.4M	$3.6M	4 months less long-lead time needed		High	Summarize the handling plan to realize the opportunity	January 2017

Figure 6-3. Opportunity Tracking Register

If a program desires to analyze the likelihood and benefits of an opportunity in a similar fashion as with analyzing risks, it could choose to establish likelihood and benefits criteria for opportunities. The program should note, however, that risks and opportunities (and their associated 5x5 matrixes) are not the dual or mirror image of each other. Attempting to develop opportunity likelihood and consequence scales and matrix from equivalent risk scales and 5x5 matrix without sound reasoning and data will likely lead to erroneous results. Simple adjustments to risk likelihood and consequence scales and a 5x5 matrix will not yield meaningful opportunity likelihood and benefit scales and matrix. Figure 6-4 below includes likelihood and benefit scales and a sample 5x5 matrix. This figure

is only an illustration and should not be used "as is," but must be developed using an appropriate, valid value function, and associated decision weights.

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%



Level	Cost			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance		
5	Significant cost benefit of >$W; or reduces costs by >q% of budget	Significant cost benefit of >$D or; reduces production unit cost by >q%	Significant cost benefit for O&M savings	Exceptional benefit in meeting major milestones and improving critical path	Exceptional benefit to design margin, system performance and requirements
4	Major cost benefit $Z - <$W; or reduces costs by p% - <q% of budget	Major cost benefit of $C - <$D or; reduces production unit cost by p% - <q%	Major cost benefit for O&M savings	Major benefit in meeting major milestones and improving critical path	Major benefit to design margin, system performance or requirements
3	Cost benefit of $Y - <$Z; or reduces costs by n%- <p% of budget	Moderate cost benefit of $B - <$C or; reduces production unit cost by n% - <p%	Moderate Cost benefit for O&M savings	Moderate benefit in meeting major milestones	Moderate benefit to design margin, system performance or requirements
2	Minor cost benefit of $X - <$Y; or reduces costs by m%- <n% of budget	Minor cost benefit of $A - <$B or; reduces production unit cost by m%- <n%	Minor cost benefit for O&M savings	Minor benefit in meeting lower level milestones	Minor benefit to design margin, system performance or requirements
1	Minimal cost benefit of <$X; or reduces costs by <m% of budget	Minimal cost benefit of <$A or; reduces production unit cost by <.5%	Minimal cost benefit for O&M savings	Minimal benefit to improving overall schedule	Negligible benefit to design margin, system performance or requirements

Figure 6-4. Opportunity Matrix and Criteria

➢ ***Expectations***

- PMs use opportunity management to plan, identify, analyze, handle, and monitor initiatives that potentially yield improvements in the cost, schedule, and/or performance baseline.
- PMs evaluate and actively pursue selected opportunities to improve the program cost, schedule, and performance baselines.
- PMs review risks, issues, and opportunities during regular program meetings.
- Programs establish or integrate opportunity tracking registers and Opportunity Management Boards.
- Programs establish opportunity likelihood and benefit criteria in line with program "should-cost" objectives.
- Programs evaluate approved opportunities and manage any associated risks.

7 MANAGEMENT OF CROSS-PROGRAM RISKS

Programs should identify and manage internal and external interfaces, which can be a significant source of risk. An integration activity involving mature hardware and software such as non-developmental government-furnished equipment generally progresses more smoothly because it uses established and stable interfaces. However, the design, integration, and test activities associated with new development usually result in technical, programmatic, and business risks.

Interdependent programs may have differing priorities regarding funding levels, hardware and software development schedules, SWAP-C requirements, immature technologies, and testing results. Other differences may include but are not limited to spectrum, bandwidth, threats, mission area, and support concept. To handle cross-program risks, interdependent programs should have strong risk management processes, regularly share risk management information, and foster a mutually supportive environment.

The following activities can aid a program in managing activities when fielding a new system that depends on programs outside the PEO's portfolio or from another Service:

- Seek program champions within the Service(s) and OSD who can:
  - Ensure effective management control over critical interfaces with external programs.
  - Align funding and priorities (schedules, form factor requirements, additional resources, etc.) of external programs.
  - Instill sense of commitment to dependent system's successful development and fielding.
- Ensure interface management is in place to meet cost, schedule, and performance objectives.
  - 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 concerns at the lowest possible level.
  - Develop a time-phased risk and issue management process that elevates risks and issues progressively as necessary to the PM, PEO, Service Acquisition Executive, and Defense Acquisition Executive in order to align priorities and resources. Risks and issues should not be allowed to languish but should be elevated to appropriate management level ahead of key handover dates.
  - Establish collaboration across appropriate joint and international programs to ensure interfaces support interoperability needs of the end-to-end mission capabilities.
- Develop memorandums of agreement (MOA) with external programs to identify and manage critical interfaces. 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, and performance

objectives, 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 variance in cost, schedule, and performance. Tripwires may include changes to dependent programs because of risk, issue, and opportunity management activities.
- The contractors should establish Associate Contractor Agreements to facilitate working relationships as appropriate.
- Table 7-1 is a sample table of required MOAs from the Acquisition Strategy Outline and SEP Outline.

Table 7-1. Sample Table of Required MOAs

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. Also develop agreements for the discrete deliverables that can be tracked to the schedule. Assess schedule performance to plan on a regular basis as a potential input to risk identification activities. Figure 7-1 is an example synchronization schedule from the SEP Outline.
- Develop an integration plan that tracks interdependent program touch points, identifies risks, analyzes risks, and institutes a plan to handle 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 handle integration risks and promote effective 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.

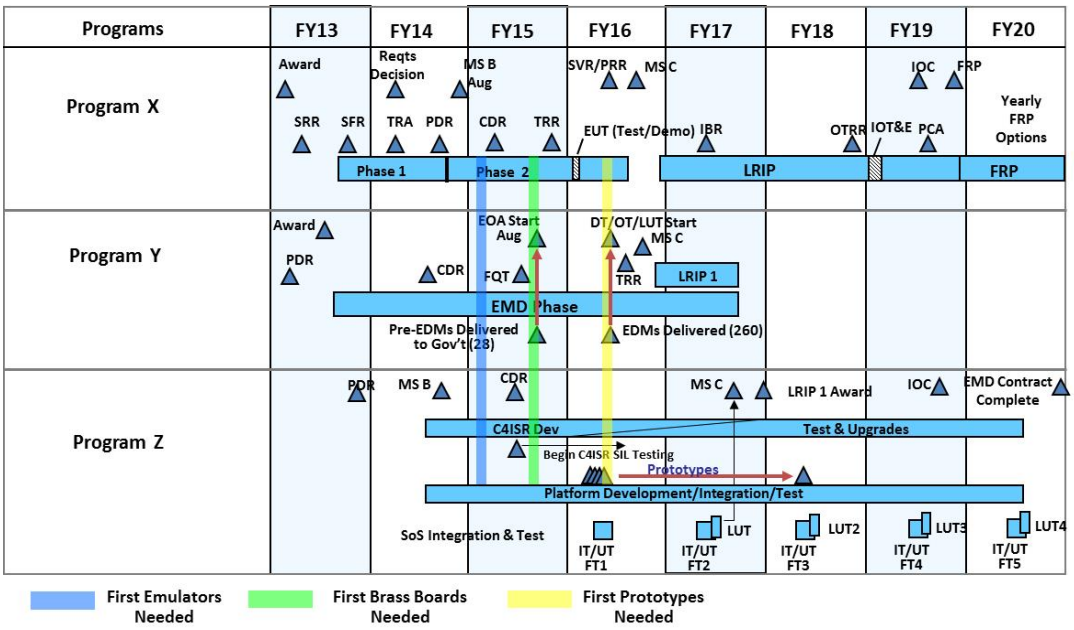


Figure 7-1. Sample Synchronization from the SEP Outline

- 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 corresponding SRAs, 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 to update risk handling plans and associated 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, Defense Acquisition Board, and Defense Acquisition Executive Summary meetings, etc.) as interface concerns warrant.
  - Programs with key external dependencies with other programs in development should consider exchanging liaisons with each other'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, schedule, performance, technology (Technology Readiness Levels are one measure), and system-of-systems management with external programs.
  - Activities required due to interdependencies should be identified early enough so that necessary resources can be secured.

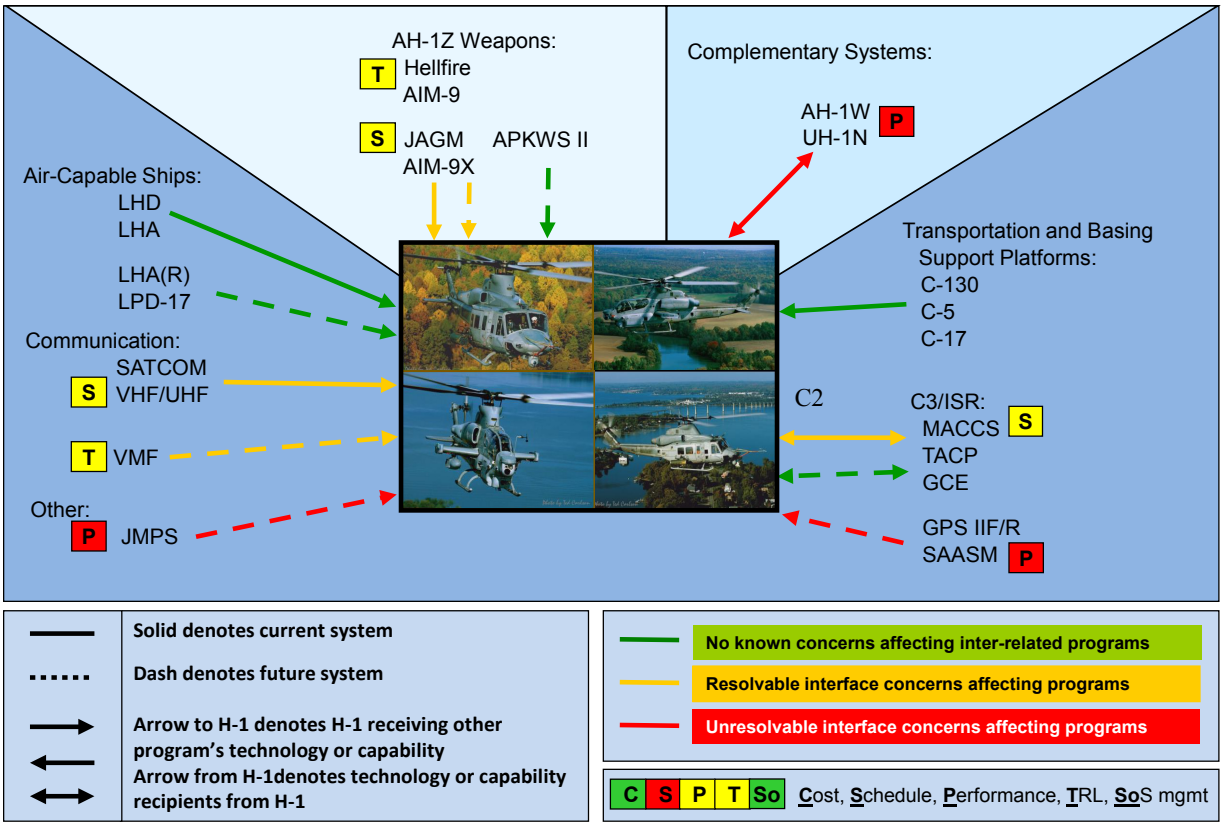


Figure 7-2. Tracking Interdependency Risks

➢ ***Expectations***

- There is collaboration and shared commitment 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 providing systems on which other programs are critically dependent agree to provide early warning to the dependent programs; tripwires for cost, schedule, and/or performance measures are established in the SEP and MOAs.
  - Giver-receiver relationships and deliverables are established and documented; required deliverables are tracked in the IMS.
- The program schedule reflects sufficient time for integration and test, as well as corrective actions.
- Senior managers implement risk management activities recognizing external dependencies to include cross-program risks.
- Interface Control Documents are established and approved.

APPENDIX A. RISK MANAGEMENT CONSIDERATIONS DURING ACQUISITION LIFE CYCLE PHASES

Programs will have many criteria to meet 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) phase entrance and exit criteria. Failure to meet one or more of these criteria can have undesirable consequences for the program, so it is prudent to assess risks to meeting them. Figure A-1 depicts the Department of Defense Instruction (DoDI) 5000.02 acquisition life cycle for hardware-intensive programs.

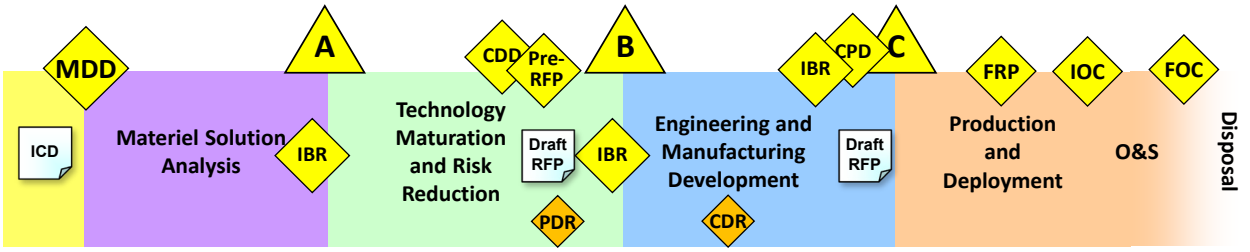


Figure A-1. Acquisition Life Cycle

At the start of each acquisition phase, the program team should assess any risks related to achieving key objectives for that phase. The program team should assess at a minimum, three aspects: (1) the Acquisition Strategy and program framing assumptions, (2) applicable ADM requirements (phase entrance/exit criteria), and (3) entrance/exit criteria for the applicable Systems Engineering Technical Reviews (SETR) consistent with the program's Systems Engineering Plan (SEP).

All of these aspects should be considered in risk identification. SETR checklists should be used continuously during the acquisition phase to identify the source of potential risks to avoid "discovery" just before the technical review. Tailorable checklists for each review are available at the Defense Acquisition University Acquisition Community Connection Practice Center website.

➢ ***Expectations***

- Programs continuously use DoDI 5000.02 acquisition phase entrance criteria, ADM requirements, and entrance/exit criteria for upcoming SETRs as a framework for the program's risk management process.

1. Pre-Materiel Development Decision

Though not an actual life cycle phase, the activities accomplished before the Materiel Development Decision (MDD) are the finalization of the Initial Capabilities Document (ICD), formulation of the Analysis of Alternatives (AoA) guidance for the conduct of the AoA during the Materiel Solution

Analysis (MSA) phase, and initial development of acquisition approaches for the alternatives under consideration.

Because the ICD 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 Office of the Secretary of Defense [OSD] level) to review the ICD. Conducting engineering analysis of the ICD is a key risk management activity early in the program life cycle. 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 and capability gaps? Are the capability gaps and the attributes of the desired capabilities described in terms of desired effects? Does the ICD contain broad descriptions of desired outcomes to 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 a 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?
- Are the ICD parameters for the capability attributes stated in measurable terms with measures and metrics with defined criteria so 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 community helps ensure the AoA identifies risks for each alternative being considered, including relative risks. The AoA guidance should require the AoA team to:

- Provide early evaluation 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.
- Clearly identify cost and schedule drivers for alternative solutions and requirements.
- Consider possible trade-offs among risk, life cycle cost, schedule, and performance objectives (including 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 Milestone Decision Authority (MDA).

Programs draft acquisition approaches for the different alternatives considered in the AoA. These activities also help the program identify risks:

- Develop notional schedules for each alternative based on analogous programs.
- Assess the technical feasibility of each alternative in areas of software development, integration, manufacturing, and reliability.

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, refine the requirements, and conduct planning to support a decision on the acquisition strategy for the product. Key engineering activities include trades between cost, schedule, and performance, affordability analysis, risk analysis, and risk management planning.

To help refine requirements, sponsors should consider providing draft technical requirements to industry and involve industry in funded concept definition to support requirements definition. This enables the acquisition community to receive industry feedback on early 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 AoA conducted after the MDD. Figure A-2 displays the risk management touch points during the MSA phase.

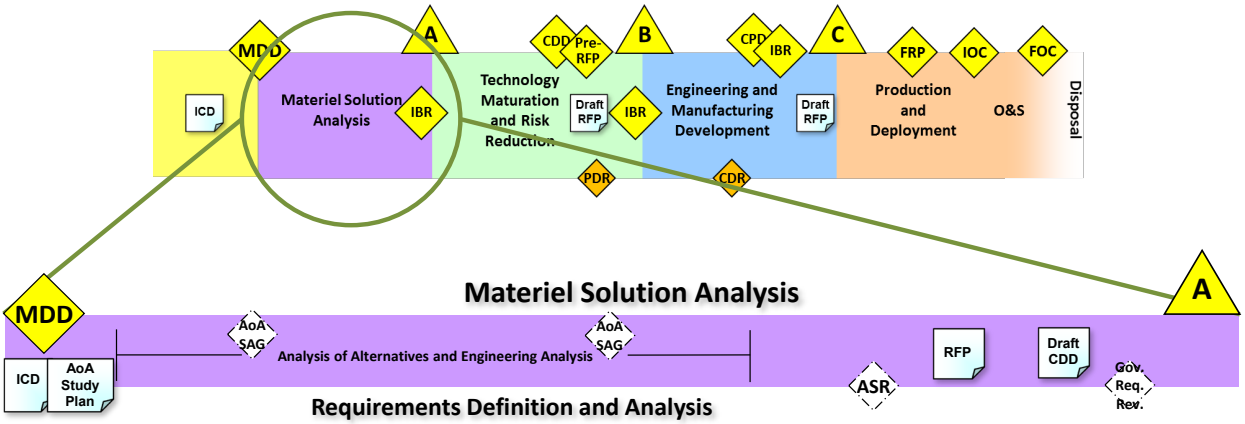


Figure A-2. Materiel Solution Analysis Phase[1] Risk Touch Points

The Service sponsor plans for an AoA to support the selection of a materiel solution. The plans include AoA Guidance and an AoA Study plan. The study team assesses cost, schedule, technical, and programmatic risk as part of any AoA. This is necessary to inform the available trade space and

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

to inform the cost-benefit analysis that is used to shape affordable technical development initiatives. Initial program risks should include those identified as a core element of AoA assessments per DoDI 5000.02. AoA risk assessments should serve as an initial source of potential program risks.

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 are assessed for realism relative to prior analyses and related systems (engineering and schedule risk).
- Interfaces and dependencies that involve other programs. The program should consider 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)?

Following the selection of the preferred materiel solution, the program managers (PM) conduct an Alternative System Review (ASR) to assess and handle risk. One purpose of the ASR is to ensure technical risks are identified and analyzed, and appropriate handling plans are in place. This is an extension of the work begun during the AoA, but it now focuses on a single materiel solution. 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 entrance and exit criteria, should be assessed and identified as part of risk identification.

The program needs to plan for the Technology Maturation and Risk Reduction (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. The program should identify specific risks for risk reduction, with exit criteria to be assessed at the end of TMRR. The program should capture these risks in the Request for Proposal (RFP) and consider them when developing the program cost and schedule, the Acquisition Strategy, and risk-reduction prototyping plans.

➢ ***Expectations***

- Programs assess integration, engineering, schedule, and technology risks related to alternative materiel solutions.
- Programs that depend on products from other programs are aware of the risks posed by changes 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 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 (DoDI 5000.02).

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

- Risk reduction prototyping (at the system level or at the technology, subcomponent, or component level if appropriate) if they materially reduce EMD 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 to 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 management touch points during the TMRR phase. The SETRs conducted during the TMRR phase to assess and handle 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 handling plans, and work with the PM to resource the handling plans.

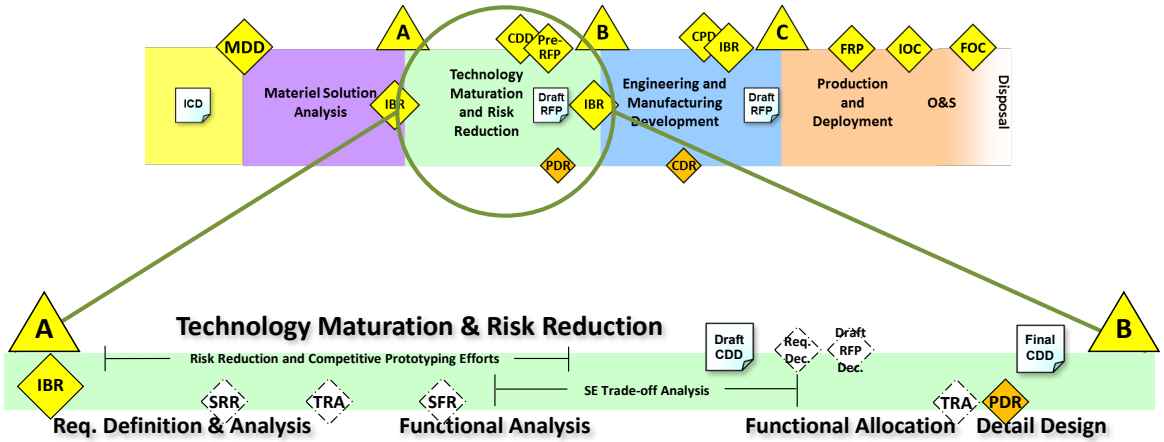


Figure A-3. Technology Maturation and Risk Reduction Phase Touch Points

The program can reduce technology risk by maturing the program critical technologies, conducting demonstrations in a relevant environment, and assessing demonstration results against requirements and stakeholder expectations. DoDI 5000.02 states the following:

> Technology Readiness Levels . . . should be 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.

During competitive and risk reduction prototyping, risks of achieving SRR, SFR, and PDR entrance criteria should be identified as part of risk identification.

The risk-related outputs of the TMRR phase are:

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

Beyond establishing 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 handling 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 handling plans, and works with the PM to resource the handling plans.
- Programs use SETRs to help identify and analyze risks.
- Risks related to completion of each of the artifacts comprising the Functional and Allocated Baselines were addressed.
- 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.
- The technical, programmatic, and business risks of acquiring the product are understood, with handling plans in place.
- Sources of risk in the TMRR phase have been adequately mitigated to the point the PM and MDA can proceed into EMD having ensured adequate mitigation plans and funding are in place.
- Risk management is included in RFP formulations, evaluation criteria, and the offerors' proposed Statements of Work, including tasks and processes to be employed for risk management. Prime contractors flow risk management processes and reporting requirements down to subcontractors and suppliers.
- Based on the TMRR phase reduction of risk, the PM and MDA make a decision to proceed into EMD with requirements that are achievable, a program that is affordable, and an Acquisition Strategy and schedule that are executable.

4. Engineering and Manufacturing Development (EMD) Phase

The purpose of the EMD phase is to develop, build, and test a product to verify that all operational and derived requirements have been met and to support production or deployment decisions (DoDI 5000.02). During this phase the program 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 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 and fielding. It includes the establishment of the product baseline for all configuration items.

Figure A-4 illustrates the risk management touch points during the EMD phase. The SETRs conducted during the EMD phase to assess and handle 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

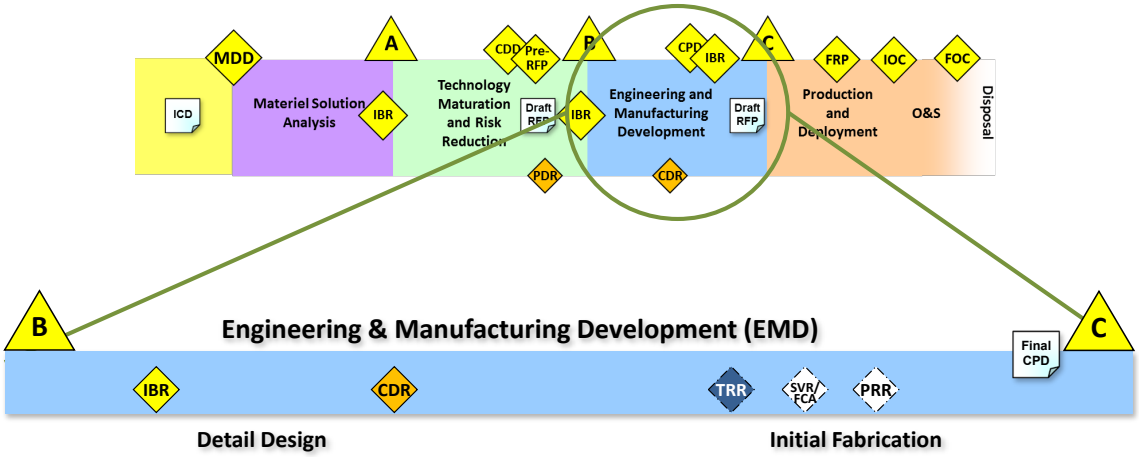


Figure A-4. Engineering and Manufacturing Development Phase Risk Touch Points

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 entrance criteria should be identified.

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

These SETRs have as a single goal, from the risk perspective, to be an assessment of the product and processes to ensure the system can proceed to validation and Low-Rate Initial Production and Full-Rate Production (FRP) 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 to help identify and analyze risks.
- Programs complete 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 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 P&D phase is to produce and deliver requirements-compliant products to receiving military organizations. Figure A-5 displays the risk management touch points of the P&D phase. The program teams develop rigorous P&D risk handling options to plan and resource effective risk handling plans. Specific actions include:

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

Following Milestone C and during production, the risks of successfully completing Initial Operational Test and Evaluation (IOT&E) and 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 (CPD). One exit criterion is the determination of acceptable technical risk for fielding and sustainment.

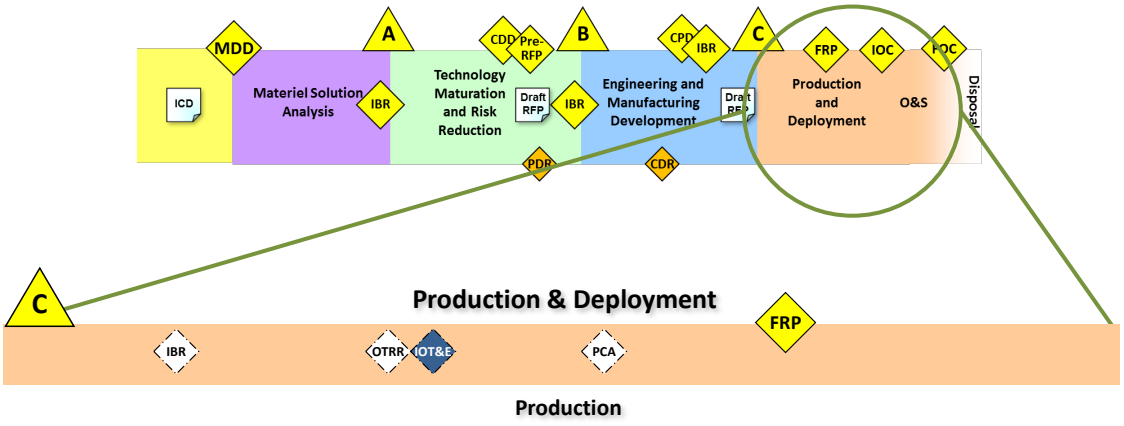


Figure A-5. Production and Deployment Phase Risk Touch Points

➢ ***Expectations***

- The program team conducts rigorous production risk assessments and puts in place plans and resources to effectively handle any unacceptable risks.
- Programs use the PCA to help identify and analyze risks.
- IOC and FOC risks are acceptable.
- The RMP is updated to include 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 control.

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 system deployment, programs should plan for and establish the In-Service Review (ISR) exit criteria. The ISR is a multidisciplined 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, the program team implements plans and resources to effectively handle any identified unacceptable risks.

Appendix B. Proactive Risk Management Activities

This appendix identifies common areas of technical, programmatic, and business risk associated with a program. It also identifies proactive activities a program might conduct during program planning and execution to prevent risks from developing or to better identify, analyze, handle, and monitor risks should they occur. Many of the identified activities are conducted as part of baseline program activities. It is important to note the list of identified risk areas is not all-inclusive.

1. COMMON TECHNICAL RISKS

1.1. Requirements

Proactive program activities contributing to successful risk management:

Materiel Solution Analysis (MSA) Phase

- Establish an affordability goal.
- Develop design concepts to assess the state of the possible and inform requirements, Request for Proposal (RFP), and source selection activities.
- Hold a government-only requirements review to ensure the proper translation of the user requirements into the performance specification.
- Ensure the program is guided by a small set of key requirements (e.g., minimize the number of Key Performance Parameters [KPP] and Key System Attributes [KSA], per the JCIDS Manual, and other attributes, to avoid constraining the contractors' design trade space).
- Ensure 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 Capability Development Document (CDD) in the RFP.
- Where appropriate, 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 battlespace. These architectures contain a 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.
- Be mindful of required modifications that affect size, weight, power, and cooling (SWAP-C) allocations, integration challenges, performance degradations resulting from integration in a

new platform, and support implications when evaluating the potential use of commercial and government off-the-shelf hardware and software.

- Identify system (hardware and software) assurance risks early to ensure system requirements, design, and architecture will produce a secure system in operations.

Technology Maturation and Risk Reduction (TMRR) Phase

- Ensure that contractors are required to identify problematic requirements as well as cost and 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 the requirements' 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 as a function of system requirements (including KPPs, major design parameters, and schedule).
  - Identify affordability drivers to the Milestone Decision Authority 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, develop a defined decision hierarchy to promptly identify, analyze, handle, and monitor technical risks and their potential effect on cost, schedule, and performance.
  - If trade study decisions are not made within 2 weeks after the completion of the trade study, continually escalate them to the next level until a binding decision is made.
  - To ensure timely decisions, the program manager (PM) should be empowered to make decisions on all requirements below the KSA level.
- Ensure prototyping activities conducted during the TMRR phase are representative of the planned end item design in order to have merit in informing trade studies and mitigating integration, technology, and technical and/or engineering risks.
  - Ensure stable requirements to preclude requirements changes that negate the relevance of prototyping and associated investments.
- Prepare a post-Milestone Systems Engineering Plan (SEP) update (Service-approved) that reflects the contractor(s) technical planning (e.g., detailed schedule, Technical Performance Measures (TPM), the contractor's organization, etc.). This establishes the baseline for assessing performance to plan in order to inform risks and required risk handling activities.
  - Develop interim values for TPMs and review them during the normal battle rhythm of program activities to inform areas of potential risk.

Engineering and Manufacturing Development (EMD) Phase

- Minimize requirements creep. New requirements should be evaluated for their cost, schedule, and performance impacts. Some requirements may need to be pushed to a follow-on increment in order to stay within program objectives.
- 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.
    - When required changes to KPPs could jeopardize a program's military utility or affordability, CSBs should coordinate with the Joint Requirements Oversight Council.
- In order to handle potential 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 (CDR) and testing, ensure that the final CDD reflects achievable requirements at an acceptable risk level to reduce performance risks during the operational test and evaluation.

TMRR, EMD, and Production and Deployment (P&D) Phases

- Plan for contingencies and technical risk handling activities by establishing cost, schedule, and performance 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.

1.2. Technology

Proactive program activities contributing to successful risk management:

MSA and TMRR Phase

- Ensure critical technologies (with Technology Readiness Level [TRL] < 6) are achievable and risks are manageable within schedule and resource constrains. Limit the number of critical technologies, as appropriate.
    - 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 Milestone B.
- Ensure 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 than 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. Execute off-ramps as planned to handle cost, schedule, and performance risks.

TMRR, EMD, and P&D Phases

- Conduct a government Technology Readiness Assessment early in the TMRR phase to identify and assess critical technology elements in the contractor's proposal.
  - Develop detailed time-phased maturation plans.
- Keep sponsors/leadership informed of appropriate technology risks and handling plans.

EMD and P&D Phase

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

1.3. Integration, Testing, and Manufacturing

Proactive program activities contributing to successful risk management:

MSA Phase

- Develop a competitive and risk reduction prototyping strategy that is focused on burning down potential technical risks (e.g., technology, engineering, and integration).
- Solicit an integration plan, IMS through prototype delivery, and drawings/models in the TMRR phase RFP to assess the bidding contractors' understanding of the technical risks associated with developing the system and required planning to execute it.

TMRR and EMD Phases

- Be proactive in the early identification, analysis, and handling of risks by planning to conduct an effective developmental test and evaluation program that:
  - Contains risk reduction and competitive prototyping of the system or key subsystems that are representative 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 approach precludes the discovery of substantial design risks and/or 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.
  - Reflects a full set of event-driven developmental test activities across the program's acquisition life cycle (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 effectively planned and conducted to identify potential risks as early as possible, thus reducing, if not eliminating, potential cost and schedule overruns.
    - Is structured to provide program management and technical leadership insights into the technical, technology, and integration risks, which may have an impact on the system's compliance with user and specification requirements. [1]
- 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 failure modes prior to the start of government testing.

EMD Phase

- Burn down integration risks through a combination of component/subsystem hot benches, system integration laboratories, high-value test assets, early prototypes, and full prototypes.
- Use 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 potential subsystem-level interaction risks.
    - Provide evidence of systems integration maturity and risk burn-down through the government checkout 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 CDR.
    - Help handle technical, cost, and schedule risks associated with full prototypes. Examples of potential technical risks 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.
        - Fault thresholds set too tight that contribute to the unnecessary shutdown of boxes or subsystem.
- The EMD phase schedule should reflect the completion of qualification testing prior to the Low-Rate Initial Production decision.

[1] Kendall, Frank. "Perspectives on Developmental Test and Evaluation," *ITEA Journal* 34 (March 2013): 6–10. https://acc.dau.mil/adl/en-US/653463/file/72222/March_2013_ITEA_Journal_Kendall_Dev_Test.pdf.

2. COMMON PROGRAMMATIC RISKS

2.1. Schedule

Proactive program activities contributing to successful risk management:

MSA Phase

- Develop an acceptable risk program schedule early in the program. The schedule should:
  - Reflect consideration of relevant historical schedules as opposed to relying solely on an externally imposed timeline.
  - Reflect the appropriate suite of Systems Engineering Technical Reviews, tailoring as necessary.
  - 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 handled before proceeding to the next phase.
  - Be structured to ensure that system performance is demonstrated before significant financial commitments.
  - Contain an acceptable level of concurrency.
- Include an Integrated Master Plan (IMP), top-level schedule, and risks in the RFP to inform the contractors' proposal.
- Assess the contractors' IMS during source selection to assess the contractors' understanding of the technical effort and required phasing of the work package.

TMRR, EMD, and P&D Phases

- Avoid the urgency of schedule need outweighing good engineering and program management.
- Ensure 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.
- Ensure the program has Tier 2 and below schedules that show technical and integration activities such as:
  - Technical reviews, Program Management Reviews, and technical interchange meetings that address technical and integration efforts reflected.
  - Establishment of system integration laboratories and contractor and/or government facilities.
  - Development, integration, and test activities with external programs.

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

- Ensure program management control efforts include the linkage between the IMP, IMS, TPMs, 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 includes all appropriate integration activities (e.g., models and simulations, hardware and software integration, distributed simulation, component, subsystems, system, family of systems and/or system-of-system-level integration) (see Section 4.2). 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 SRAs on a regular basis to evaluate potential risks and the ability to achieve the next Systems Engineering Technical Review, major test event, and acquisition milestones.

2.2. Communication

Proactive program activities contributing to effective risk management:

MSA, TMRR, EMD, and P&D Phases

- Ensure horizontal communications across Integrated Product Teams and vertical communications up through management (e.g., the lead systems engineer, PM, Program Executive Office (PEO), etc.).
- To handle program management of 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.
    - Make the effort to include all organizations that could support or 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 handling inevitable technical, programmatic, and business risks.

- Ensure transparency with Service, user, Office of the Secretary of Defense (OSD), and congressional stakeholders by regularly providing them with progress of ongoing efforts (e.g., competitive and risk reduction prototyping, systems engineering trade-off analysis, and knowledge point reviews) and the impact of any proposed funding reductions.
- Hold Working Integrated Product Team meetings (e.g., systems engineering, acquisition, test and evaluation, etc.) with the OSD and Service staff engineers on a regular basis to assess system maturation (e.g., performance to plan of TPMs) as well as any associated risks, issues, and/or opportunities.

3. COMMON BUSINESS RISKS

3.1. Dependencies

Proactive program activities contributing to effective risk management:

TMRR, EMD, and P&D Phases

- Seek program champions within the Service(s) and OSD who can:
  - Ensure interface management is in place to meet cost, schedule, performance requirements, and ultimately support program success.
  - 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 until it is resolved.
- Develop memorandums of agreement (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.
- Ensure contractors put Associate Contractor Agreements in place 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.
- Develop an integration plan to track interdependent program touch points, identify and approve risks, and handle and monitor resulting moderate and high risks.
- To assist in handling 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 OSD stakeholders to review cross-program progress, risks, and issues.
- Establish a tiered battle rhythm of meetings with external programs and associated contractors.

3.2. Resources

Proactive program activities contributing to effective risk management:

TMRR, EMD, and P&D Phases

Be prepared to substantiate the impact of any proposed funding reductions, including any resultant technical, technology, integration, and/or engineering risks.

- Understand the impact of "what-if" funding cut scenarios, such as 5%, 10%, 15%, etc. reductions.
- Solicit information from the requirements sponsors who know the capability priorities that cannot be deferred.
- Do not mask the potential impacts of proposed funding reductions. Ensure that leadership fully understands the implications of the funding cut. On the other hand, do not overstate the impact as doing so could diminish risk management and program credibility.

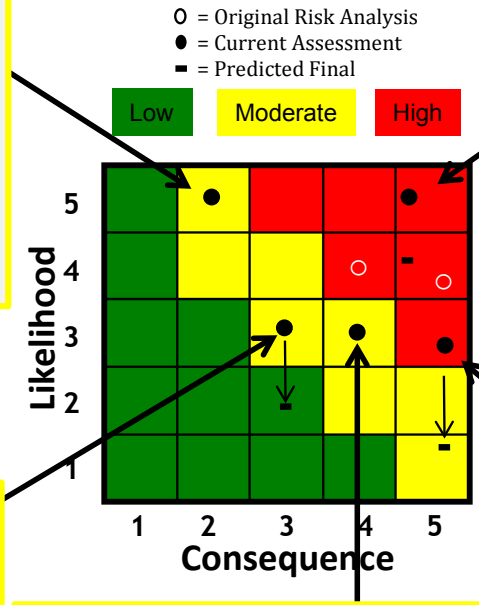
APPENDIX C. SAMPLE TEMPLATES FOR REPORTING RISKS, ISSUES, AND OPPORTUNITIES

1. Risk Register (Table 3-4)

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Tier	Risk Event	Likelihood, Consequence Rating	Risk Handling Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status
8231	3.2.2	Name	Technical	Open	II	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	L=3, C=4	Mitigation - Program will apply management reserve to retain adequate software engineers to burn-down SW defects	8/23/2013	1/14/2014	2/12/2014	L=1, C=4	On schedule

2. Suggested Risk Reporting Format (Figure 3-12)

- Risk ID #82: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Handling Method: (Accept, Avoid, Transfer or Mitigate) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:



- Risk ID #85: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Handling Method: (Accept, Avoid, Transfer or Mitigate) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #23: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Handling Method: (Accept, Avoid, Transfer or Mitigate) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #45: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Handling Method: (Accept, Avoid, Transfer or Mitigate) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

- Risk ID #97: Risk Statement…
- Consequences if Realized:
  - Cost -
  - Performance -
  - Schedule -
- Handling Method: (Accept, Avoid, Transfer or Mitigate) Summarize activities:
  1. Summarize Key Activity 1
  2. Summarize Key Activity 2
  3. Etc.
- Planned Closure Date:

3. Alternative Risk Reporting Format

Risk	Likeli-hood (1-5)	Consequences					Handling Activities	Planned (P) Actual (A)		Closure Date
		Cost			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	(P)	(P) 8/12/15
								(A)	(A)	
							2 –Activity YYY	(P) 10/12/13	(P)	
								(A) 11/1/13	(A)	(A)
							3 – Activity ZZZ	(P) 8/12/15	(P)	
								(A)	(A)	
Risk 2	4		$2.2M		8 months		1 –Activity aaa	(P) 7/13/14	(P)	(P)7/13/14
								(A)	(A)	
							2 -	(P)	(P)	
								(A)	(A)	(A)
							3 -	(P)	(P)	
								(A)	(A)	
Risk 3	2		$520K		2 months		1 -	(P)	(P)	(P)
								(A)	(A)	
							2 -	(P)	(P)	
								(A)	(A)	(A)
							3 -	(P)	(P)	
								(A)	(A)	

Insert risk statement in this column

Insert assessed likelihood rating for the risk

Briefly describe the cost, schedule, and performance consequences of the risk

Summarize the key handling activities

Show the planned and actual completion dates and cost for each activity

List the planned and actual risk closure dates

4. Issue Tracking Register (Figure 5-3)

Issue	Consequence	Type T/B/P	Plan of Action and 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 or will occur, 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)		
				(P) (A)		
				(P) (A)		
				(P) (A)		

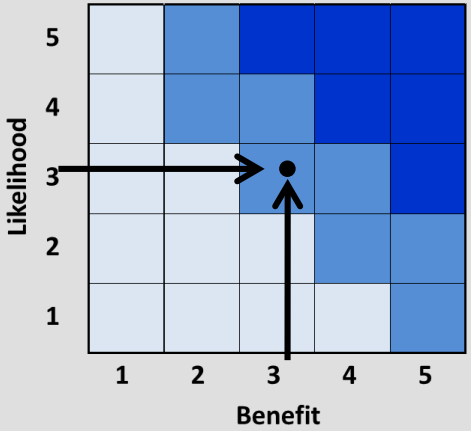
Key

5. Opportunity Tracking Register (Figure 6-3)

Opportunity	Likeli-hood	Cost to Implement	Benefit					Oppor-tunity Level	Handling Strategy	Expected Closure
			Cost			Schedule	Performance			
			RDT&E	Procurement	O&M					
Opportunity 1: Procure Smith rotor blades instead of Jones rotor blades.	Mod	$3.2M			$4M	3 month margin	4% greater lift	Moder-ate	Reevaluate - Summarize the handling plan	March 2017
Opportunity 2: Summarize the opportunity activity.	Mod	$350K	$25K		$375K			Low	Reject	May 2017
Opportunity 3: Summarize the opportunity activity.	High	$211K		$0.4M	$3.6M	4 months less long-lead time needed		High	Summarize the handling plan to realize the opportunity	January 2017

6. Sample Opportunity Matrix and Criteria

Level	Likelihood	Probability of Occurrence
5	Near Certainty	> 80% to ≤ 99%
4	Highly Likely	> 60% to ≤ 80%
3	Likely	> 40% to ≤ 60%
2	Low Likelihood	> 20% to ≤ 40%
1	Not Likely	> 1% to ≤ 20%



Level	Cost			Schedule	Performance
	RDT&E	Procurement	Operations & Maintenance		
5	Significant cost benefit of >$W; or reduces costs by >q% of budget	Significant cost benefit of >$D or; reduces production unit cost by >q%	Significant cost benefit for O&M savings	Exceptional benefit in meeting major milestones and improving critical path	Exceptional benefit to design margin, system performance and requirements
4	Major cost benefit $Z - <$W; or reduces costs by p% - <q% of budget	Major cost benefit of $C - <$D or; reduces production unit cost by p% - <q%	Major cost benefit for O&M savings	Major benefit in meeting major milestones and improving critical path	Major benefit to design margin, system performance or requirements
3	Cost benefit of $Y - <$Z; or reduces costs by n%- <p% of budget	Moderate cost benefit of $B - <$C or; reduces production unit cost by n% - <p%	Moderate Cost benefit for O&M savings	Moderate benefit in meeting major milestones	Moderate benefit to design margin, system performance or requirements
2	Minor cost benefit of $X - <$Y; or reduces costs by m%- <n% of budget	Minor cost benefit of $A - <$B or; reduces production unit cost by m%- <n%	Minor cost benefit for O&M savings	Minor benefit in meeting lower level milestones	Minor benefit to design margin, system performance or requirements
1	Minimal cost benefit of <$X; or reduces costs by <m% of budget	Minimal cost benefit of <$A or; reduces production unit cost by <.5%	Minimal cost benefit for O&M savings	Minimal benefit to improving overall schedule	Negligible benefit to design margin, system performance or requirements

APPENDIX D. ROLES, RESPONSIBILITIES, AND RELATIONSHIPS

1. GOVERNMENT RESPONSIBILITIES

- Develop and execute an effective risk management process to help achieve program objectives and involve the contractor as early as possible.
- Include contract provisions that foster flow of risk management requirements from contractor to subcontractors.
- Recognize that the contractor may treat risk differently from the government because of differences in government and contractor business and program viewpoints.
- Understand how program decisions impact risks for efforts not yet on contract. For example, a development contractor may not identify a production risk. The program should recognize these risks are still valid and need to be captured in the program's risk management process.
- Address any subtleties in contract provisions that could affect the success of the risk management program, including applicable incentives for effective risk management as demonstrated through defined program objectives.
- Conduct thorough risk analyses of proposals in support of source selection activities.
- Ensure systems engineering trade-off analyses consider risk elements along with design performance to establish cost, schedule, and performance trade space.
- Evaluate the results of competitive and risk reduction prototyping to assess the risk related to design maturity and achieving program objectives.
- Reflect the effectiveness of the contractor's risk management effort in the Contractor Performance Assessment Report System evaluation.

2. TYPICAL CONTRACTOR RESPONSIBILITIES

- Strive to align internal risk management processes as much as possible with the program's overall risk management program; include the risk management approach in the proposal.
- Provide all applicable candidate risks to the Risk Management Board (RMB) for consideration. Communicate relevant subcontractor risks to the government in a timely manner.
- Flow risk management requirements to subcontractors; include provisions for consistent risk management processes and definitions; establish means to integrate subcontractor risk management process within the overall program risk management effort.
- Conduct risk identification and analysis during all phases of the program, including proposal development, and apply appropriate risk handling strategies and plans.
- Assess the impact of risks during proposal and baseline development.

- Select and implement risk management tool(s) that are electronically common or compatible with government counterparts.
- Support, as required, government risk management efforts, such as the RMB; reporting to senior management and other stakeholders; and training program 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 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 program phases, including proposal development.
- Incorporate risk handling activities into Integrated Master Schedule (IMS) and program budgets as appropriate.
- Synthesize and correlate new and ongoing risk elements in the IMS, risk handling plans, estimates at completion, technical status documentation, and program updates and reviews.

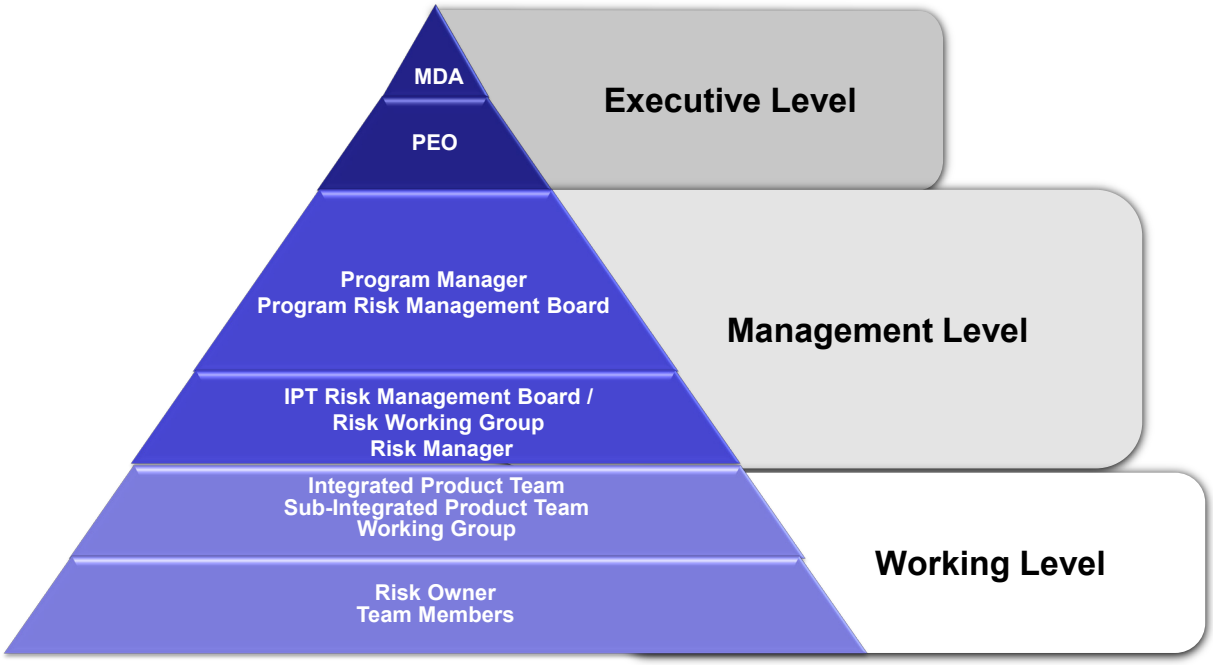


Figure D-1. Risk Management Roles and Responsibilities Tiering

3. SUGGESTED TIERED ROLES AND RESPONSIBILITIES

3.1. Executive Level

Milestone Decision Authority

- Tailors and approves programs proceeding into the next acquisition phase based on the status of the cost, schedule, and performance risks of acquiring the product, the adequacy of the plans, and funding available to address those risks.

Program Executive Officer

- Considers not only individual program risks, but also risks from a portfolio and system-of-systems perspective. Executes program oversight by monitoring and evaluating program-level, senior leader special interest risks, and execution of risk handling plans. Provides direction regarding management of cross-Program Executive Office (PEO) (external), portfolio (internal), program-level, or special interest risks and issues.

3.2. Management Level

Program Manager

- Complies with statutory and regulatory risk management requirements.
- Ensures the program Statement of Objectives, Statement of Work, and Contract Data Requirements List include provisions to support a defined program Risk Management Plan (RMP) and process.
- Establishes and executes an integrated risk management process with the contractor and key subcontractors; ensures the development of and approves the program's RMP.
- Ensures the appropriate disciplines and Integrated Product Teams (IPT) are involved in the program risk management process (program management, engineering, contracting, information assurance, legal, financial management, earned value management [cost account managers and cost schedule analyst], logistics, manufacturing, test and evaluation, quality assurance, and system safety).
- Forms and chairs a program RMB, which should include deputy program managers (PM), chief or lead systems engineer, IPT leads, risk management coordinator, equivalent prime contractor leads, and other members relevant to the program strategy, phase, and risks.
- Ensures risk handling plans are approved at the appropriate level to include acceptance of risk and issue consequences (e.g., environment, safety, and occupational health, and system safety).
- Communicates program-level and special interest risk status, using the program's approved risk reporting format, during stakeholder meetings (Defense Acquisition Board, Overarching

Integrated Product Team, Service Acquisition Executive review, PEO review), program reviews, technical reviews, risk review board meetings, and other appropriate meetings.

- Assigns responsibility and proper authority for risk management activities, monitors progress, and includes stakeholders in the formulation and approval of risk handling plans.
- Provides or allocates resources to effectively manage risks, issues, and opportunities.
- Communicates with the user on potential requirement, funding, and schedule impacts.
- Includes cost, schedule, and performance risk management trade space in all design, development, production, sustainment, and support considerations.
- Actively seeks opportunities for potential cost, schedule, and performance improvements.

Program Risk Management Board

- Ensures the risk management process is executed in accordance with the program's RMP.
- Ensures risk management efforts are integrated and at the appropriate working level.
- Reviews and validates identified program-level risks; approves risk handling plans, including adequacy of resources and any changes to approved plans.
- Monitors the status of risk handling efforts, including resource expenditures and quantitative assessment of risk reduction.
- Continually assesses the program for internal and external risks and for 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/Milestone Decision Authority [MDA]) and other stakeholder personnel.
- Determines which risks are managed at the program or special interest level and which risks are managed at the IPT or working group levels.
- Ensures each risk is assigned an owner to lead handling plan development and execution.
- Periodically reviews risks from lower-level boards.

IPT Risk Management Board/Risk Working Group

- Reviews the risks owned by the IPTs.
- Assesses and recommends whether risks should be elevated to the next level for review.
- Determines whether new or updated risk analyses and handling plans are adequate.
- Approves and tracks the status of IPT-level risk handling plans.
- Approves risk closure for IPT-level risks and notifies the program RMB of closure.

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 and risk register.
- Provides risk management training.
- Facilitates risk identification and analysis evaluations.
- Completes an initial screening of risks.
- Prepares risk briefings, reports, and documents required for program reviews.

3.3. Working Level

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

- Develop and implement the risk planning outlined in the Systems Engineering Plan, Systems Engineering Management Plan, Acquisition Strategy, and/or RMP, and support the 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 IPT RMB, the PM, and the 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 conduct risk analysis to ensure sufficient, relevant, and timely information is provided to decision makers.
- Recommend risk handling options, estimate handling option funding requirements, support implementation of the selected risk handling plan, and track progress of risk handling efforts.
- Monitor risk burn-down effectiveness and report program-level 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 analysis results are 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

- Estimates the initial risk likelihood and consequence values.
- Leads development of proposed handling plan and options for assigned risks to include required cost and resource estimates and fallback plans for high-level risks.
- Briefs the risk handling plan to the program or IPT RMBs, as appropriate, for approval.
- Implements and reports on the progress of the handling plan.
- Delegates risk events to other individuals or teams, by expertise, as required.

Team Members

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

Appendix E. Risk Management Process Vignette

The following example illustrates the application of a risk management process to the development of a hypothetical Unmanned Aerial Vehicle (UAV) Jammer. The example follows the steps outlined in Section 3.

Scenario: A UAV Jammer payload was demonstrated in the Technology Maturation and Risk Reduction (TMRR) phase. The UAV uses an air scoop to route ram air into a turbine, which drives a generator supplying the jammer energy. The program finished the technology demonstration phase with several risks, which are planned to be resolved during the early part of the Engineering and Manufacturing Development (EMD) phase. Among the several risks outstanding at this point, only one risk was rated as high, and the handling of that high risk will be discussed for the purposes of this example.

Risk Identification: During TMRR wind tunnel and limited flight testing, the turbine power was demonstrated at only 90 percent of what was needed/allocated to accomplish full jammer effectiveness. It was not clear whether 100 percent could be achieved in a production version and especially under more comprehensive flight conditions (full flight envelope). The program prepared an initial risk statement:

> *If the 90 percent of target power level achieved by the existing ram air turbine design during the TMRR phase cannot be improved, then reduced jammer effectiveness may result.*

Risk Analysis: Subject matter experts (SME) analyzed the power uncertainty and determined that if, in fact, only 90 percent could be achieved, the result would be a reduction of overall jamming effectiveness by 8 percent. The SME analysis was significant when combined with the knowledge that jammer effectiveness was a Key Performance Parameter (KPP) for the program. At this point in the analysis, the program updated the risk statement:

> *If the ram air turbine generator performance cannot be improved from the 90 percent demonstrated during TMRR to the full target power level, then an 8 percent reduction in jammer effectiveness, which is marginally below the KPP value, may result.*

On a scale of 1 to 5, the likelihood that the existing generator design could not produce power to the full target level was rated 4 because, based on demonstration and analysis, the SME and associated engineering team assessed there was a 60-80 percent probability of not achieving the KPP with the current design. The consequence was rated 5, since the KPP on jammer effectiveness was threatened unless increased generator output could be provided. This risk was high priority because of the combination of the high likelihood and the potential consequence of not meeting a KPP. The initial risk is depicted on the risk matrix in Figure E-1.

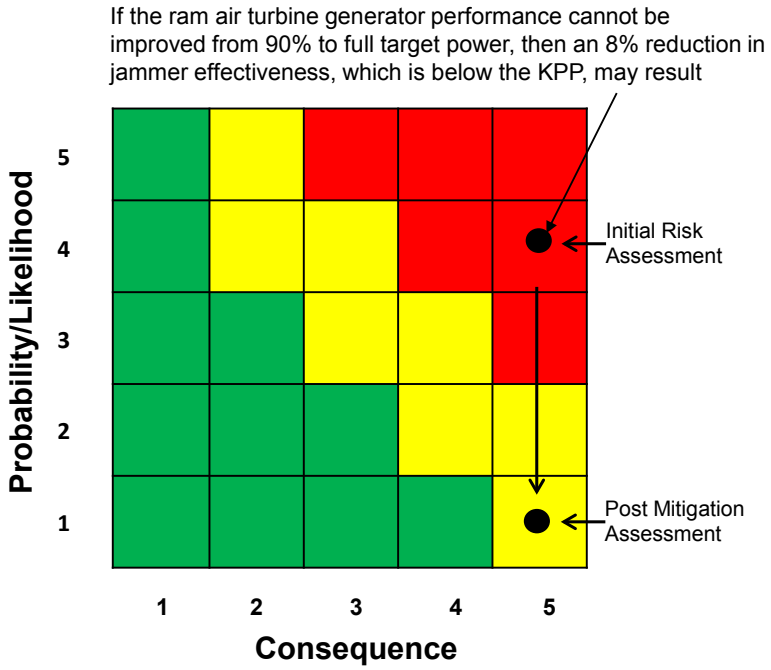


Figure E-1. Risk Matrix for Ram Air Turbine Generator

Risk Handling: The program manager (PM) examined handling options. Because of the significance of the potential performance shortfall, the PM adopted a handling plan to mitigate the risk:

A. Initiate a parallel development effort over a 5-month period in EMD, employing higher efficiency but within state-of-the-art generator magnets in the turbine stator. There was no adverse schedule impact since integration testing was planned at the completion of the parallel development. A slight increase of the UAV drag was computed to result from use of the higher efficiency generator, but the increase was computed to be well within performance margins.

Before adopting this handling plan, because of the critical need to achieve as close to full jammer effectiveness as possible while also minimizing any degradation to vehicle range, endurance, or payload performance, the PM examined three other alternatives, as follows:

B. Increase the inlet scoop area. This would reduce the UAV range by introducing higher vehicle drag and cost $3 million plus an 8-month slip. Probability of success was assessed as 70 percent.

C. Use more advanced set of radar components that required less power. This option would cause a year slip and $5 million and possibly reduce reliability. Probability of success was assessed as 65 percent.

D. Work with the user to reduce requirements. The user stated that reduction could not be accepted unless there was no other way, and any reductions would have to be evaluated in terms of continued program viability.

For the preferred alternative, Option A, a parallel development effort using an enhanced magnet, the SMEs conducting the analysis assessed the probability of success as 95 percent, the risk of failure thus 5 percent. The mitigation cost was estimated as $1 million, less than 0.5 percent of EMD cost. Recurring system cost impact was very small, within estimating error.

The preferred alternative was assessed by a consensus of SMEs to be 95 percent likely to regain full target power. At a minimum, it was assessed that even if the mitigation was not fully effective in regaining 100 percent target power, a substantial level of improvement in power output was expected to be achieved, narrowing any residual performance gap to a marginal level, posing a lesser threat of not realizing the KPP power level. The risk handling plan included projected consequences and likelihood at each risk mitigation step based on expected performance against the quantitative metrics established for each risk mitigation step. Thus, the post-mitigation risk was projected to move in several steps from (4,5) (likelihood, consequence) to (1,5), since there was high confidence the mitigation would be effective in regaining full target power (see Figure E-1.)

To closely track and evaluate the progress of the mitigation plan, the PM monitored the risk burn-down plan for the enhanced ram air turbine generator design. The activity was entered in the Integrated Master Schedule and risk register.

Technical Performance Measures in this case included design parameters form, fit, and weight, and power performance. But since the design was virtually identical to that of the TMRR phase, except for the magnets, metrics were emphasized in power delivery. Power delivery metrics were established along with key events. If the new generator did not meet any of the metrics at any time during the planned 5-month development/demonstration period, its effort would be terminated and discussions pursued with the user relative to alternatives, discussed earlier.

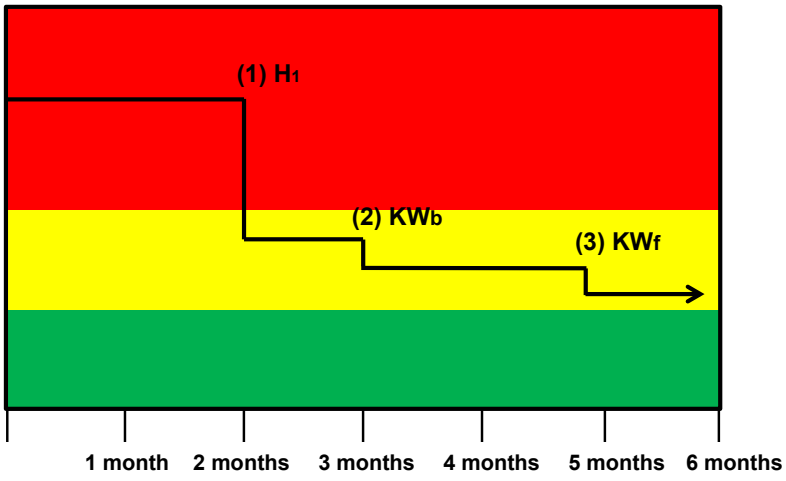
Metric measurement periods were set over the 5-month development. First the magnetic intensity was to be measured at the desired configuration; second the power generated at the prototype configuration “bench test” or simulation; and finally the power generated in actual flight testing.

There were three key event dates to evaluate progress of burning down the risk with quantitative thresholds established for the success of each step: Step (1) Test to measure the configured magnetic strength, with the required magnetic field strength using the enhanced magnets calculated to be H_1 amperes/meter established as the threshold for the static magnetic strength. If successful, this step was assessed to reduce the likelihood from 4 to 2. Step (2) Measure the prototype bench test power output using a motor driver to simulate turbine effects to demonstrate that the power output satisfies the established threshold value, designated KW_b (measured in watts). Finally, step (3) Conduct a flight test of the UAV with the reconfigured generator installed to confirm that the in-flight generator power output, over a range of conditions, satisfies the final in-flight power level (KW_f) required for the jammer.

The last two activities were assessed to lower the likelihood from a 2 to 1. The tests were set for 2 months, 3 months, and 5 months respectively after EMD contract award. The Program Risk

Management Team updated the risk burn-down plan chart with updated evaluations of consequence and likelihood at each step based on the demonstrated power delivery metrics.

The results of the static test of magnet strength were of the greatest significance. The program created a risk burn-down diagram (Figure E-2) for the improved generator. The vertical axis of the burn-down diagram spanned high, moderate, and low risks.



(1) Enhanced magnet demonstrates field strength equal to or greater than H_1 A/m
(2) Prototype generator demonstrates power output equal to or greater than KW_b in bench test
(3) Prototype generator demonstrates in-flight power output equal to or greater than KW_f over required envelope

Figure E-2. Risk Burn-Down Diagram for Option A

Risk Monitoring and Closure: The Integrated Product Team (IPT) team accomplished continuous monitoring and reported directly to the chief engineer/lead systems engineer. The team was augmented by three SMEs from government labs/engineering centers and academia who were invited to the key meetings and to important weekly teleconferences with industry counterparts. The IPT was co-chaired by government and prime contractor representatives and included the generator vendor. The IPT team was responsible for maintaining the risk charts and graphics, reporting the activity schedule status, and ensuring that test events were properly planned. Status reports to the PM were updated during the staff meetings and during the risk and opportunity review board meetings, and they were formally documented in the risk register, which included other program risks.

The efforts were also captured in the Earned Value Management process. Closure would be achieved when tests demonstrated the preferred design (or other design, if necessary) satisfied the established threshold success criteria and the design was established as the final configuration with the attendant specification. During program updates, the program might depict this and other program-level risks on a risk chart as displayed in Figure E-3. Note the generator risk is displayed at the top right of the figure.

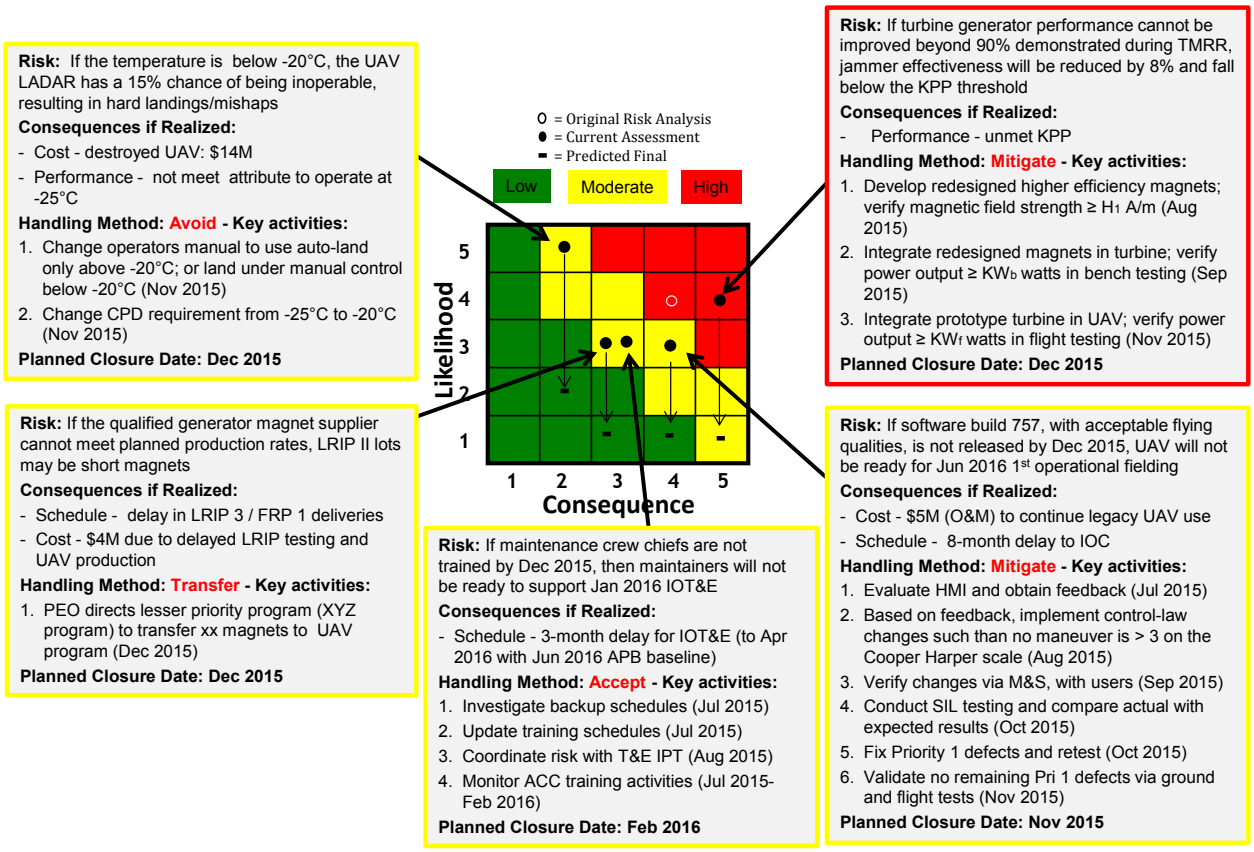


Figure E-3. Risk Reporting Chart

Outcome: The modified generator design was a success based upon demonstrated test performance and analysis of results. Once the flight test was concluded, the program closed the risk and finalized the generator configuration status while maintaining scrutiny of the additional prototype test articles and following limited production units to ensure the performance was sustained.

Glossary

accept (risk): acknowledge that a risk event or condition may be realized and have sufficient resources in place to deal with the risk when it occurs. **(issue):** accept the consequence of the issue based on results of the cost/schedule/performance business case analysis.

avoid (risk): reduce or eliminate a risk event or condition by taking an alternate path. **(issue):** eliminate the consequence of the event or condition by taking an alternate path. Examples may involve changing a requirement, specification, design, or operating procedure.

Baseline Execution Index (BEI) (schedule): the efficiency with which actual work has been accomplished when measured against the baseline plan.

Better Buying Power: the implementation of best practices to strengthen the Defense Department's buying power, improve industry productivity, and provide an affordable, value-added military capability to the Warfighter (source: http://bbp.dau.mil).

business risks: non-technical risks that generally originate outside the program office, or are not within the control or influence of the program manager. 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.

cost risk analysis (CRA): methodology to estimate the distribution of potential outcomes for selected cost elements.

critical path: the longest sequence of activities through the project, which represents the shortest duration possible.

Critical Path Length Index (CPLI) (schedule): tool to measure a schedule's efficiency to finish on time.

float (schedule): the amount of time a task can be delayed without causing a delay to subsequent tasks.

handle (risk): develop and implement a plan to address the risk by examining the four handling options (accept, avoid, transfer, mitigate), choosing the best option (or hybrid of options), obtaining suitable resources associated with the plan, and implementing the plan.

hard constraint (schedule): constraints that fix a task's start date or finish date and may prevent tasks from being moved by their dependencies. Hard constraints are undesirable because they prevent the schedule from being logic driven.

high duration (schedule): a baseline duration of greater than 44 working days (2 months) for an unfinished task.

high float (schedule): float (or slack) of more than 44 working days, which may indicate that the critical path is unstable and the schedule is not logic driven.

identify (risk): examine the aspects of a program to determine risk events and associated cause(s) that may have negative cost, schedule, and/or performance impacts.

invalid date (schedule): actual start/finish date that reflects a future date beyond the current status date.

issue: current problem that has occurred (such as a realized risk) or is certain to occur (probability = 1) in the future.

Key Performance Parameter (KPP): performance attribute of a system considered critical or essential to the development of an effective military capability. KPPs are contained in the Capability Development Document and the Capability Production Document and are included verbatim in the Acquisition Program Baseline. KPPs are expressed in term of parameters that reflect Measures of Performance using a threshold/objective format. KPPs must be measurable, testable, and support efficient and effective test and evaluation (source: JCIDS Manual).

Key System Attribute (KSA): performance attribute of a system considered important to achieving a balanced solution/approach to a system, but not critical enough to be designated a Key Performance Parameter. KSAs must be measurable, testable, and support efficient and effective test and evaluation. KSAs are expressed in terms of Measures of Performance (source: JCIDS Manual).

lag (schedule): duration between a task's completion and its successor's start date. Lags can contribute to an artificially restrained schedule.

lead (schedule): overlap between tasks that have a dependency. The use of leads to alter total float will artificially restrain the schedule and may result in resource conflicts.

likelihood (risk): the assessed probability that an event will occur given existing conditions.

logic (schedule): in a schedule, logic links all work package elements in the order they should be executed using predecessors and/or successors. Without logic the schedule is static and not useful for program management (e.g., the critical path is unknown).

missed task (schedule): tasks that do not finish as planned. An excessive number of missed tasks may indicate poor schedule execution performance, inadequate resources, and/or an unrealistic baseline plan.

mitigate (risk): implement a strategy to reduce the risk to an acceptable level. **(issue):** implement a strategy to reduce the consequence to an acceptable level.

negative float (schedule): less than zero float, which may indicate that the forecasted date (start-to-finish) is unrealistic and will affect a schedule's overall realism.

opportunity: potential future benefits to the program's cost, schedule, and/or performance baseline, usually achieved through reallocation of resources.

performance risk analysis (PRA): process that uses statistical techniques to quantify the performance of the modeled item. Each PRA will typically have a different model structure, application of probability distributions, and resulting outputs, depending on the engineering discipline and specific application.

program-level risk: risk that needs the attention and resources of the program manager.

Program Protection Plan (PPP): a defense acquisition program's integrated system security engineering document. It describes the program's critical program information and mission-critical functions and components, the threats to and vulnerabilities of these items, the plan to apply countermeasures to mitigate associated risks, and planning for exportability and potential foreign involvement.

programmatic risks: non-technical risks that are generally within the control or influence of the program manager or Program Executive Office. 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.

pursue (opportunity): fund and implement a plan to realize the opportunity. (Determination of whether to pursue the opportunity will include evaluation of when the opportunity would be realized, the cost, additional resources required, risk, and time to capture.)

reevaluate (opportunity): continuously evaluate the opportunity for changes in circumstances.

reject (opportunity): intentionally ignore an opportunity due to cost, technical readiness, resources, schedule burden, and/or low probability of successful capture.

relationship (schedule): the order in which each task should be completed. The finish-to-start relationship is the preferred schedule hierarchy method.

resources (schedule): hours or dollars. In a schedule, tasks that have durations of one or more days should have an allocation of resources (hours/dollars) to complete the assigned work.

risk: future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance. Risks are defined by (1) the probability (greater than 0, less than 1) of an undesired event or condition and (2) the consequences, impact, or severity of the undesired event, were it to occur.

risk management approach: the organization, tools, and methods a program chooses to carry out its risk management process.

Risk Management Board (RMB): a board chartered as the senior program group, usually chaired by the program manager or deputy program manager, that approves candidate risks and their causes. The board reviews and/or approves risk analysis results, risk handling plans and associated resources, and actual versus planned progress associated with implemented risk handling plans. It is an advisory board to the program manager and provides a forum for all stakeholders and affected parties to discuss their concerns.

Risk Management Framework: the unified information security framework for the federal government that is replacing the legacy certification and accreditation processes within federal government departments and agencies, the Department of Defense, and the Intelligence Community (source: http://www.rmf.org/).

Risk Management Plan (RMP): program document describing the program's risk management process and associated methodologies and products, potential risk categories, ground rules and assumptions, organizational roles and responsibilities, and other risk management resources. The plan should address how often the document will be reviewed and updated. It should outline risk management training for program personnel in order to establish an appropriate risk management culture and to provide personnel with an understanding of the program's risk management processes and how to use the program's risk management tools.

risk manager: program team member responsible for implementing the risk management process, updating the RMP, and assisting team members to (1) identify and document candidate risks, (2) develop risk analysis results, (3) develop draft risk handling plans, (4) include risk information in the risk register, (5) develop risk reports, and (6) update this information versus time.

risk register: a tool commonly used as a central repository for all risks identified by the program team and approved by the Risk Management Board. The register records details of all risks identified throughout the life of the project. It includes information for each risk such as category, likelihood, consequence, risk level, risk handling plans, and resources required to implement them, actual versus planned progress versus time, and, where applicable, expected closure dates.

schedule health assessment (SHA): assessment using the DCMA 14 Point Schedule Metrics to identify potential problem areas with a contractor's Integrated Master Schedule. These metrics provide the analyst with a framework for asking educated questions and performing follow-up research.

schedule risk analysis (SRA): a methodology to estimate the distribution of potential schedule outcomes for selected milestones and activities, taking into account a specified level of schedule-estimating uncertainty and risks associated with tasks contained in the schedule.

should-cost: the concept that [DoD] managers should set cost targets below independent cost estimates and manage with the intent to achieve them (source: http://bbp.dau.mil/bbp2focus.html).

stakeholder: a person, group, or organization that has responsibility and influence over the success of a program or system. Stakeholders include the program manager, the Milestone Decision

Authority, acquisition commands, contractors, contract managers, suppliers, test communities, and others (source: http://acqnotes.com/acqnote/careerfields/stakeholders).

Systems Engineering Management Plan (SEMP): documents multiple aspects of a supplier's applied systems engineering approach (may also be called the "contractor's System Engineering Plan" or an Offeror's Plan in response to a solicitation). This document, if written in response to a government Systems Engineering Plan, provides insight regarding application of the contractor's standards, capability models, and tool sets to the acquisition program at hand (source: DAG).

Systems Engineering Plan (SEP): a defense acquisition program's functional technical planning document. It describes the program's overall technical approach, including organization, major systems engineering activities, processes, resources, metrics, products, risks, event-driven schedules, and design considerations.

Technical Performance Measure (TPM): a graphical depiction of a product design assessment. It displays values derived from tests and future estimates of essential performance parameters of the current design. It forecasts the values to be achieved through the planned technical program effort, measures differences between achieved values and those allocated to the product element by systems engineering processes, and determines the impact of those differences on system effectiveness. TPMs are typically related to Key Performance Parameters and Measures of Effectiveness (source: https://dap.dau.mil/glossary/).

technical risks: risks that may prevent the end item from performing as intended or from meeting 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, system security/cybersecurity, and training.

transfer (risk): reassign or reallocate the risk responsibility to another entity. This approach may involve reallocating a risk from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization. **(issue):** reassign or reallocate the issue responsibility from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization.

will-cost: cost estimate established following DoD and Service memos, instructions, regulations, and guides; that represents the official Service position for budgeting, programming, and reporting; sets the threshold for budgeting Acquisition Program Baseline, [Selected Acquisition Report], and Nunn-McCurdy; and is continually updated with current available information (source: USD(AT&L)/DAU, January 12, 2012).

Work Breakdown Structure (WBS): a product-oriented family tree composed of hardware, software, services, data, and facilities. Produced from systems engineering efforts, it breaks down authorized program work into appropriate elements for planning, budgeting, scheduling, and cost accounting.

Acronyms

AoA	Analysis of Alternatives
APB	Acquisition Program Baseline
ASR	Alternative System Review
CDD	Capability Development Document
CDR	Critical Design Review
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CPD	Capability Production Document
CRA	cost risk analysis
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DAG	Defense Acquisition Guidebook
DAU	Defense Acquisition University
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EMD	Engineering and Manufacturing Development (phase)
EMV	expected monetary value
ESOH	environment, safety, and occupational health
EVM	earned value management
FOC	Full Operational Capability
FRP	Full-Rate Production
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
IDE	Integrated Data Environment
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOC	Initial Operational Capability
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
LRIP	Low-Rate Initial Production

MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
MSA	Materiel Solution Analysis (phase)
O&M	operations and maintenance
O&S	Operations and Support (phase)
OIPT	Overarching Integrated Product Team
OSD	Office of the Secretary of Defense
P&D	Production and Deployment (phase)
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PEO	Program Executive Office or Program Executive Officer
PM	program manager
PMR	Program Management Review
PRA	performance risk analysis
RFP	Request for Proposal
RMB	Risk Management Board
RMP	Risk Management Plan
ROI	return on investment
ROMB	Risk and Opportunity Management Board
SAG	Senior Advisory Group
SE	systems engineering
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SHA	schedule health assessment
SME	subject matter expert
SOW	Statement of Work
SRA	schedule risk analysis
SWAP-C	size, weight, power, and cooling
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction (phase)
TPM	Technical Performance Measure
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
WBS	Work Breakdown Structure

REFERENCES

Works Cited

Acquisition Strategy Outline. Attachment to "Document Streamlining –Document Streamlining–Program Strategies and Systems Engineering Plan (SEP)." Memorandum. Washington, D.C.: Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics, April 20, 2011. 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-TDS_AS_Outline-04-20-2011.pdf

ANSI/EIA-748. Earned Value Management Systems. New York: American National Standards Institute/Electronic Industries Alliance, June 2007.

CJCSI 3170.01I. Joint Capabilities Integration and Development System (JCIDS). Washington, D.C.: Chairman of the Joint Chiefs of Staff, January 23, 2015. https://dap.dau.mil/policy/Documents/2015/CJCSI_3170_01I.pdf

Defense Acquisition Guidebook. Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics, n.d. https://dag.dau.mil/Pages/Default.aspx

DCMA-EA PAM 200.1. Earned Value Management System Program Analysis Pamphlet. Washington, D.C.: Defense Contract Management Agency, October 2012, pp. 28–32. http://www.dcma.mil/policy/200-1/PAM-200-1.pdf

Department of Defense Instruction (DoDI) 5000.02. Operation of the Defense Acquisition System. Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics, January 7, 2015. http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

Department of Defense Instruction (DoDI) 8510.01. Risk Management Framework (RMF) for DoD Information Technology (IT). Washington, D.C.: Department of Defense Chief Information Officer, March 12, 2014. http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). "Systems Engineering." Chapter 4 in *Defense Acquisition Guidebook.* Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics, May 15, 2013. https://acc.dau.mil/docs/dag_pdf/dag_ch4.pdf

Kendall, Frank. "Perspectives on Developmental Test and Evaluation," *ITEA Journal* 34 (2013): 6–10. https://acc.dau.mil/adl/en-US/653463/file/72222/March_2013_ITEA_Journal_Kendall_Dev_Test.pdf

Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS). Washington, D.C.: Joint Requirements Oversight Council, February 12, 2015. https://acc.dau.mil/jcids

MIL-STD-881C. 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, October 3, 2011. https://acc.dau.mil/CommunityBrowser.aspx?id=482538

MIL-STD-882E. Standard Practice for System Safety. Wright-Patterson Air Force Base, Ohio: Headquarters Air Force Materiel Command/SES (System Safety Office), May 11, 2012. http://acqnotes.com/acqnote/tasks/mil-std-882e-system-safety

Systems Engineering Plan (SEP) Outline. Attachment to "Document Streamlining –Document Streamlining–Program Strategies and Systems Engineering Plan (SEP)." Memorandum. Washington, D.C.: Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics, April 20, 2011. 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

Risk Identification, Integration, and Ilities (RI3) Guidebook. Version 1.2. Washington, D.C.: Department of the Air Force, December 15, 2008. https://acc.dau.mil/CommunityBrowser.aspx?id=318289

Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). "Implementation Directive for Better Buying Power 3.0–Achieving Dominant Capabilities through Technical Excellence and Innovation." Memorandum, Attachment 2: "Better Buying Power 3.0 Implementation Guidance." Washington, D.C.: USD(AT&L), April 9, 2015, pp. 31-32. http://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf

Weapon Systems Acquisition Reform Act of 2009. Public Law 111-23, 111th Cong., May 22, 2009. http://www.gpo.gov/fdsys/pkg/PLAW-111publ23/html/PLAW-111publ23.htm

Other Sources

Air Force Instruction 63-101/20-101. Integrated Life Cycle Management. Sections 3.10 (Risk-Based Program Management and Decision Making); 4.13 (Risk Management Plans and Risk Planning); 7.7 (Information Assurance); 7.8 (Certification and Accreditation). Washington, D.C.: Department of the Air Force, March 7, 2013 (incorporating through Change 2, Feb. 23, 2015). http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101_20-101/afi63-101_20-101.pdf

Air Force Pamphlet 63-128. Integrated Life Cycle Management. Section 12 (Life Cycle Risk Management). Washington, D.C.: Department of the Air Force, July 10, 2014. http://static.e-publishing.af.mil/production/1/saf_aq/publication/afpam63-128/afpam63-128.pdf

BKCASE (Body of Knowledge and Curriculum to Advance Systems Engineering) Editorial Board. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, version 1.4. R.D. Adcock (EIC). Hoboken, N.J.: The Trustees of the Stevens Institute of Technology, 2014. http://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)

Department of Defense Earned Value Management Implementation Guide (EVMIG). Alexandria, Va.: Defense Contract Management Agency, October 2006. https://acc.dau.mil/CommunityBrowser.aspx?id=386074

Department of Defense Directive (DoDD) 5000.01. The Defense Acquisition System. Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics, May 12, 2003, certified current as of November 20, 2007. http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf

Department of Defense Directive (DoDD) 5250.01. Management of Intelligence Mission Data (IMD) in DoD Acquisition. Washington, D.C.: Under Secretary of Defense for Intelligence, January 13, 2013. http://www.dtic.mil/whs/directives/corres/pdf/525001p.pdf

Department of Defense Instruction (DoDI) 5200.01. DoD Information Security Program and Protection of Sensitive Compartmented Information. Washington, D.C.: Under Secretary of Defense for Intelligence, October 9, 2008, incorporating Change 1, June 13, 2011. http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

Department of Defense Instruction (DoDI) 5200.39. Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation. Washington, D.C.: Under Secretary of Defense for Intelligence/Under Secretary of Defense for Acquisition, Technology, and Logistics, May 28, 2015. ,http://www.dtic.mil/whs/directives/corres/pdf/520039p.pdf

Doran, George T. "There's a S.M.A.R.T. Way to Write Management's Goals and Objectives." *Management Review* (American Management Association Forum) 70 (11): 35–36, 1981.

Earned Value Management (EVM) Frequently Asked Questions (FAQs). Washington, D.C.: Department of Defense, Performance Assessments and Root Cause Analyses http://www.acq.osd.mil/evm/faqs.shtml [accessed April 7, 2015].

Joint Agency Cost Schedule Risk and Uncertainty Handbook (JA CSRUH). Washington, D.C.: Naval Center for Cost Analysis, March 12, 2014. https://www.ncca.navy.mil/tools/csruh/JA_CSRUH_16Sep2014.pdf

OMB Circular No. A–11, Part 7. Planning, Budgeting, Acquisition, and Management of Capital Assets. Washington, D.C.: Office of Management and Budget, July 25, 2014. https://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc

Program Managers' Guide to the Integrated Baseline Review Process. Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, April 2003. https://acc.dau.mil/CommunityBrowser.aspx?id=37635

Space and Missile Systems Center Risk Management Process Guide. Version 2. Los Angeles, Calif.: Department of the Air Force, Space and Missile Systems Center, September 5, 2014. https://acc.dau.mil/adl/en-US/715033/file/78621/Risk%20Management%20Process%20Guidance%20_Version_2_09052014_Final_S.pdf

Standard Process for Risk and Issue Management in Acquisition Programs. Version 1.1. Wright-Patterson Air Force Base, Ohio: Air Force Life Cycle Management Center, May 28, 2014.

U.S. Air Force Cost Risk and Uncertainty Analysis Handbook (CRUH). Washington, D.C.: Air Force Cost Analysis Agency, April 2007. https://acc.dau.mil/adl/en-US/316093/file/46243/AF_Cost_Risk_and_Uncertainty_Handbook_Jul07.pdf

Websites

Better Buying Power
http://bbp.dau.mil/

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

Defense Acquisition University–Acquisition Community Connection Practice Center
https://acc.dau.mil/

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

Department of Defense Earned Value Management
http://www.acq.osd.mil/evm/

International Council on Systems Engineering
https://www.incose.org/

Life-Cycle Mission Data Plan (LMDP) Guidebook
https://acc.dau.mil/CommunityBrowser.aspx?id=289687&lang=en-US

NASA Risk Management Page
http://www.hq.nasa.gov/office/codeq/risk/

Risk Management Community of Practice, Acquisition Community Connection
https://acc.dau.mil/rm

Systems Engineering Technical Review Checklists
https://acc.dau.mil/CommunityBrowser.aspx?id=639996

Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs

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

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