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

January 2017

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

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION,
TECHNOLOGY,
AND LOGISTICS

JAN - 9 2017

MEMORANDUM FOR: DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
COMPONENT ACQUISITION EXECUTIVES
PRESIDENT, DEFENSE ACQUISITION UNIVERSITY
DIRECTORS, ACQUISITION CAREER MANAGEMENT

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

In Better Buying Power 3.0, I highlighted the need to improve the Department's ability to understand, anticipate, and mitigate technical risks before they become issues, and to recognize and pursue opportunities that may significantly benefit program outcomes.

In support of this effort, the Deputy Assistant Secretary of Defense for Systems Engineering revised and renamed the *Department of Defense (DoD) Risk Management Guide* as the *DoD Risk, Issue, and Opportunity Management Guide.* The electronic version is available through the DoD Systems Engineering website at http://www.acq.osd.mil/se/pg/guidance.html.

The guide provides practical advice to programs as they work to identify, analyze, and manage risks, issues, and opportunities. Program Managers and engineers need to understand the technical risks they face and structure programs and acquisition strategies in a manner that best mitigates those risks to deliver a product to our Warfighters. While processes help, the quality and effectiveness of risk mitigation planning, judgement, and the decisions made by program managers matter the most for achieving objectives. Please disseminate this guide across your organization.

Frank Kendall

This page is intentionally blank.

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. It builds from and supersedes the *DoD Risk Management Guide* but reflects revisions to emphasize managing not only program risks but also issues and opportunities. Readers should assume that general references to managing risk would be tailorable to complementary activities addressing issues and opportunities.

A range of policy, regulatory, or statutory directives call out risk management for its recognized positive relationship to program outcomes. However, the value of risk management is not tied to a formal adherence to policy. Rather the value lies in the Program Manager's (PM) ability to apply critical thinking and adopt a culture of risk management that influences program decisions and execution of technical fundamentals. This approach aims to manage uncertainty and increase predictable outcomes in delivering capability to the warfighter.

Risk management is an integral part of program management and systems engineering. A PM must align risk appetite with organizational capacity to manage risks and allocate limited resources to the best effect. Risk management principles addressed in this document echo the time-proven 1986 Packard Commission recommendations and reflect recent DoD Better Buying Power initiatives. In 2015, the Under Secretary of Defense for Acquisition, Technology, and Logistics emphasized risk management as a focus of Better Buying Power:

> 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.

This guide describes strategies and processes for risk, issue, and opportunity (RIO) management that programs should begin early in program development and apply continuously throughout the acquisition life cycle. Each program should tailor the practices and not get bogged down in unnecessary or excess process formality that doesn't add value. Early identification of the program's key uncertainties and challenges can inform decisions on the basic program structure and the activities needed to enable successful and efficient delivery of the intended product.

Although this guide focuses primarily on the government program office, industry plays a central role in executing the management necessary for delivery of acquisition products. Government and

industry may differ in the prioritization of risks, driven in part by differing perspectives or incentives. Certainly the type of contract, cost or fixed price and associated incentives, can affect the nature of the actions taken by government and industry in their respective roles. Nevertheless, close collaboration and a shared commitment to realism, even when inconvenient, are essential to effective risk management.

The guide is organized as follows:

Section 1: Introduces the scope and overview of the guide.

Section 2: Describes how risk informs the decisions shaping a program acquisition strategy and structure, and the most important activities to manage risk by life cycle phase.

Section 3: Describes how a program manages risks and issues by developing plans to reduce the consequences and/or the likelihood of the risks or issues.

Section 4: Describes opportunity management, including the similarities and differences between opportunity and risk management.

Section 5: Highlights considerations to manage risks related to internal and external interfaces with interdependent programs. Discusses the different priorities of interdependent programs and techniques to manage and mitigate cross-program risks.

Appendixes: Appendix A provides additional information on establishing and documenting a Program Risk Process (PRP). Appendix B discusses integrating risk management with other program management and systems engineering tools, and Appendix C provides a vignette illustrating how a program might address a particular risk.

Some sections contain text boxes with expectations/take-aways that programs 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 advance the ability of DoD programs to plan for and manage risks, issues, and opportunities. The quality of thinking and judgment applied to these areas often will determine whether a program meets its objectives throughout the life cycle. Managing these areas requires strategic thinking and begins with early decisions on program structure that take into account the program's unique uncertainties and risks. The analysis and informed judgment needed to identify and control risk are fundamental to effective program planning and management.

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

- **Risks** are potential 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) that should be addressed.
- **Opportunities** have potential future benefits to the program's cost, schedule, and/or performance baseline.

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.

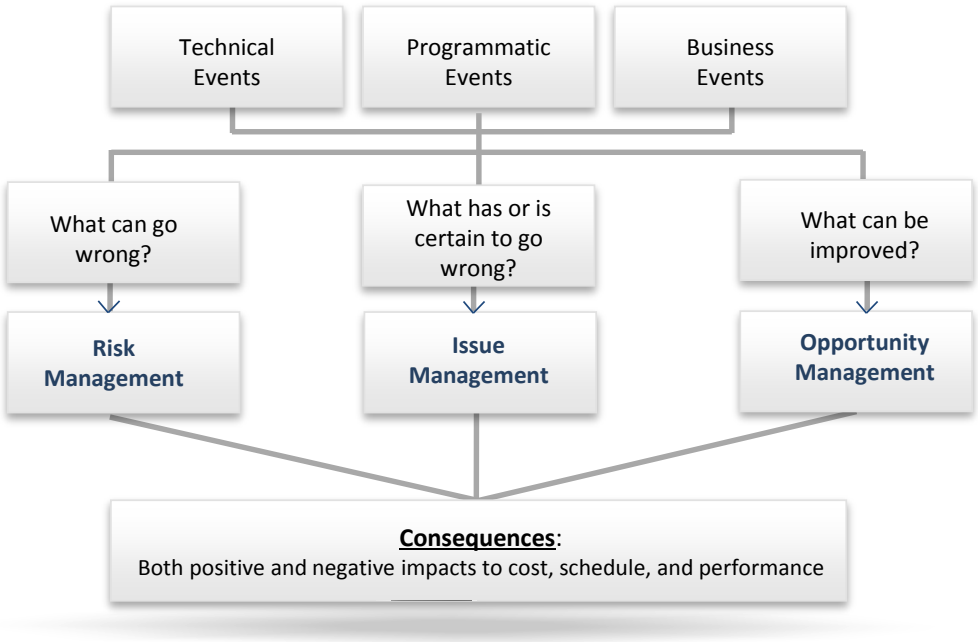


Figure 1-1. Overview of Potential Sources of Program Risks, Issues, and Opportunities

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 (DAG); Military Department guidance; and other instructions, policy memorandums, and regulations.

1.2 Scope

DoD distinguishes mandatory policy from recommended guidance. This document serves solely as guidance for risk management approaches for DoD acquisition programs. It is to be used as appropriate reference material and not as a checklist. This guide reflects experience drawn from numerous DoD programs and suggests risk considerations programs should keep in mind when developing an Acquisition Strategy and program structure, including activities bearing on risk by phase and considerations relating to contract type.

This guide includes a strategic consideration of how risk shapes program structure and content, as well as a suggested process to manage discrete risks by phase. The process is designed to produce risk mitigation plans, which provide the substantive steps a program will take to mitigate its actual risks. This guide uses the term “risk mitigation plan” to refer to the plans that are initially summarized in the program’s Acquisition Strategy and updated as risks are identified and managed. It also suggests the term Program Risk Process (PRP) to refer to the documented process a program uses to execute its tailored risk, issue, and opportunity processes. The term PRP is not mandatory but is a suggestion to distinguish process documentation from descriptions of risk mitigation plans.

This guide focuses centrally on risk. Analogous discussions, with some distinctions, could apply to issues and opportunities as well. This guide does not attempt to address, in detail, 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 risks such as cybersecurity. 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. Using the forthcoming Directive-Type Memorandum (DTM) 17-001, Cybersecurity in the Defense Acquisition System, programs should consider cybersecurity in technical risk management activities to address risk identification, analysis, mitigation planning, mitigation implementation, and tracking. They should use evolving program and system threats to inform operational impacts.

1.3 Risk Management Overview

The PM is responsible for implementing effective risk management within program constraints. Successful risk management requires planning and resourcing, and should be implemented early in the life cycle beginning with the Materiel Solution Analysis (MSA) phase or earlier based on early

collaboration among the operational, acquisition, and technology communities. The goal is to identify risks to inform decisions on structure and content, and develop mitigation strategies for the risks that must be addressed to deliver intended capabilities.

The practice of risk management constitutes a significant aspect of program management and draws from all disciplines, including systems engineering, use of models and simulation, requirements definition, developmental and operational test, earned value management (EVM), production planning, quality assurance, and logistics. Risk management needs to be both top-down (program leadership) and bottom-up (from working-level staff members) 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, mitigation, and monitoring activities.

Making risk management work depends on process, but more importantly on people with knowledge and experience in the disciplines relevant to the product, and with the resolve to identify and address the risks that could influence program objectives. An organizational climate, open to external perspectives, that seeks independent board members for design reviews can strengthen the effectiveness of a program's risk management. Well-understood requirements flowed to the product, an integrated schedule coupled to earned value management (EVM), an independent cost estimate, and the tenacity to pull on the threads that reveal problems all contribute to prospects for success.[1]

While the processes described in the guide enable risk management, the risk mitigation plans for individual risks (the output of the processes) are significantly more important. In the end, what matters most are the quality and effectiveness of the program's risk mitigation plans and their implementation in reducing the risks to realizing program objectives, not the process itself.

The steps of the risk management process are generally applicable to the management of risks and issues in multiple phases of the life cycle. At the same time, the nature of the specific actions taken for each step typically will be different depending on the program phase. The differences in the specific actions are driven by the changing types of individual risk, the information and tools available, the outcomes that need to be achieved, the degree of maturity and stability that must be demonstrated, and the residual risks that are tolerable following mitigation efforts.

Programs should define, implement, and document an appropriate, tailored risk process. The process should address planning, identification, analysis, mitigation, and monitoring of risks and issues. See Section 3 for more detail.

[1] Drawn from personal communication with VADM Joseph Dyer, June 1993.

This page is intentionally blank.

2 MANAGING RISK BY ACQUISITION PHASE

2.1 Planning Considerations

2.1.1 Strategy Development

The most important decisions to control risk are made early in a program life cycle (Figure 2-1). PMs and teams[1] must understand the capabilities under development and perform a detailed analysis to identify the key risks. During the early phases, the program works with the requirements community to help shape the product concept and requirements. Once the concept and requirements are in place, the team determines the basic program structure, the acquisition strategy, and what acquisition phase to enter based on the type and level of key risks. Risk steers planning and tailoring.

If technology maturity or requirements stability risks exist, the PM should structure a program to enter the life cycle at Milestone A. For example, if there is some doubt as to whether the program can achieve the requirements, the PM should consider a risk reduction phase with competitors building and testing prototypes in order to validate achievability of the requirements. Programs also may use prototypes to quantify the impact of technology on performance, demonstrate the ability to integrate new technologies into mature architectures, and to reduce risk and cost.

If the technologies are mature, the integration of components is at acceptable risk, and the requirements are stable and achievable, the PM can consider entering directly at Milestone B to begin Engineering and Manufacturing Development (EMD).

If a materiel solution already exists and requires only military modification or orientation, the PM can structure the program enter at Milestone C with a small research and development (R&D) effort to militarize the product.

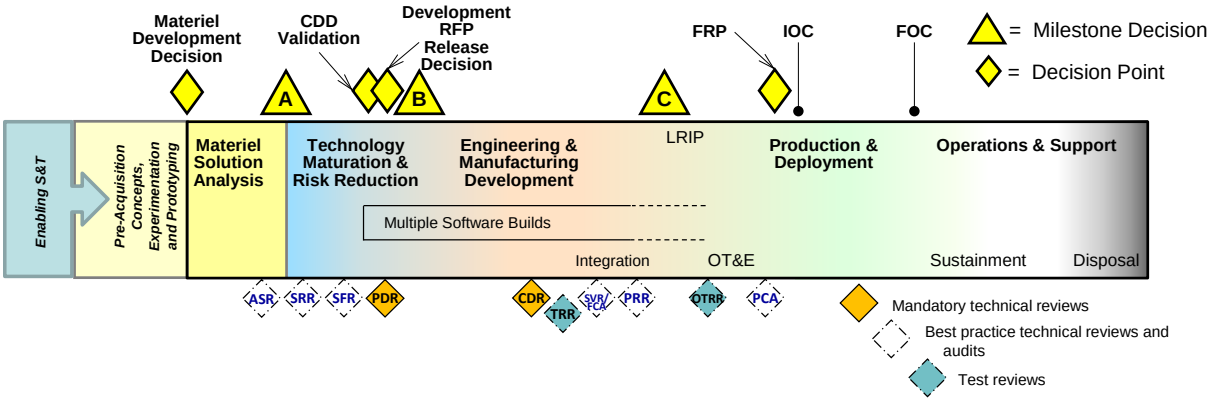


Figure 2-1. DoD Acquisition Life Cycle

[1] Early in a program life cycle, a PM may not yet be designated. However, there is usually a responsible acquisition organization overseeing development planning efforts.

Statute requires PMs to document a comprehensive approach for managing and mitigating risk (including technical, cost, and schedule risk) in the Acquisition Strategy. Likewise, DoD policy requires programs to summarize the top program risks and associated risk mitigation plans in the Acquisition Strategy. Policy also requires programs to describe their technical approach, including key technical risks, and management and execution of risk mitigation activities, in the Systems Engineering Plan (SEP).

2.1.2 Framing Assumptions

When developing the acquisition strategy and program framework, programs make assumptions. Programs sometimes make assumptions without realizing it, but these framing assumptions need to be identified and validated because they can put the entire program at risk if they turn out to be incorrect. Examples of framing assumptions include priority or achievability of requirements, schedule dependencies, procurement quantities, threats, availability of specialty metals or technology, or accuracy of models and simulations.

2.1.3 Integration with Contractor's Processes

Risk management is not a stand-alone process. It is integral to other program processes, such as requirements development, systems engineering, design, integration, cost estimating, schedule tracking, test and evaluation, EVM, issue management, sustainment, and so on. The government program office, the prime contractor(s), and associated subcontractors should employ a compatible risk management process to facilitate the alignment of risk registers and transfer of data between parties.

The Request for Proposal (RFP) should address risk management by requiring that the offeror include in the proposal the nature of tasks, processes, and tools planned for collaborative government and industry risk management to ensure mutual understanding of risk efforts. The PM determines contract incentives and contract type to align government and contractor interests and risk management objectives.

The program's risk profile is the dominant consideration in deciding which contract type to pursue. Things to consider include firmness of the requirements and maturity of the technology required; the experience level of potential offerors; and the capacity of industry to absorb potential overruns and the business case for industry to do so. The type of contract, cost-plus or fixed-price, fundamentally will affect the roles and actions of the government and industry in managing risk.

Cost type contracts: Cost type contracts are best suited to situations in which the inherent technical risks are greater (typically during development). Consequently, these programs will need to allocate sufficient resources to manage emerging risks and should reevaluate sufficiency of funds during budget cycle reviews, before acquisition milestones, and with the award of follow-on contracts. Government retains control in a cost type environment and should make (with the prime contractor)

final decisions on risk mitigation plans. Although a contractor may have responsibility for managing a risk, the government still has ownership and responsibility for the efforts and outcomes.

Fixed-price contracts: Fixed-price development is most appropriate when the requirements are stable and expected to remain unchanged, where technical and technology risks are understood and minimal, and the contractor has demonstrated a capability to perform work of the type required. PMs and their contracting officers should reach an agreement with industry contractors during contract negotiations on how key risks must be mitigated, when progress will be measured, and any appropriate contract incentives and options. Although a contractor may have financial responsibility for mitigating a risk on a fixed-price contract, the government needs the product and bears the risk if the contractor fails to deliver it in a timely manner so the risk is never fully transferred to industry.

Appendix A includes a list of typical government and contractor responsibilities regarding risk management.

2.2 Pre-Materiel Development Decision Phase

This period is the best opportunity for the acquisition community to provide a balanced view to the users of what is realistically possible to achieve. Collaborative planning between the operational user and the technology/acquisition communities informs the translation of capability needs to initial requirements, and can guide technology investments or transition opportunities for candidate solutions. Early systems engineering provides trade space analysis for alternative candidate concepts. Therefore, the requirements community and the project manager/organization should establish a close dialogue and relationship in this phase to account for the key risks in program planning. Industry can also help. Development Planning (DP) organizations, working the concept prior to the Materiel Development Decision (MDD), can solicit ideas from industry through carefully crafted Requests for Information that seek insight into concepts, technologies, materials, and research investments. Industry feedback can help bound the realm of the possible.

Products of the pre-Materiel Development Decision (MDD) period include the formulation of the Initial Capabilities Document (ICD) and the Analysis of Alternatives (AoA) guidance for the conduct of the AoA during the MSA phase. The PM and acquisition community should participate in these activities and the initial development of acquisition approaches for the alternatives under consideration.

2.3 Materiel Solution Analysis Phase

In the MSA phase, the program conducts the analyses and other activities needed to finalize the concept of operations for the program product, refine the requirements, and conduct planning to support a decision on the acquisition strategy for the product. A key risk management activity during this phase is an engineering analysis of the ICD to better identify risks during the AoA. The program should evaluate requirements for technical feasibility, quantify gaps, and focus on contributing

technology components. Engineering analyses should focus on the affordability analysis, risk analysis, risk management planning, and trades among cost, schedule, and performance.

Acquisition sponsors should consider providing industry with draft technical requirements. Funded competitive concept definition studies (e.g., early design trade studies and operations research) can also inform decisions about requirements and are valuable to help refine and support requirements definition. Early industry feedback provides critical insight into the trade-offs among requirements, risks, and costs. Figure 2-2 displays the MSA phase activities.

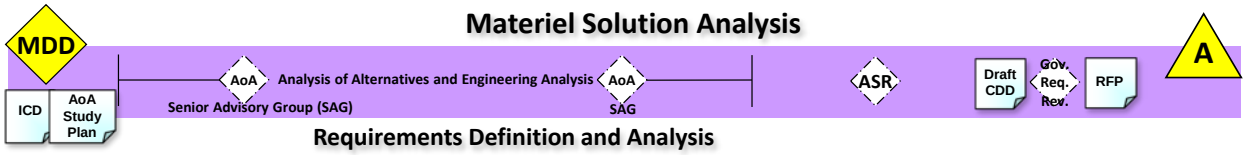


Figure 2-2. Materiel Solution Analysis Phase Activities

The Service sponsor plans for an AoA to support the selection of a materiel solution. This planning includes both the AoA Guidance and an AoA Study plan. These guide the study team to assess cost, schedule, technical, and programmatic risk to inform the available trade space and cost-benefit analysis to shape affordable technical development. AoA focus areas should include uncertainty (or confidence level) associated with each alternative's schedule estimate, proposed performance, and technical risks. The AoA study team should assess each of the following for realism relative to prior analyses and related systems:

- Interfaces and dependencies that involve other programs and the 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)?
- Framing assumptions: Are these assumptions still valid? What are the risks and impacts of an incorrect assumption?

Following the selection of the preferred materiel solution, the PM should conduct an Alternative System Review (ASR) to support a dialogue between the end user and acquisition community, leading to a draft performance specification for the preferred materiel solution. The PM should also establish the program risk register to ensure the program has identified, analyzed, and established mitigation plans for all relevant risks.

By the end of the MSA phase, the program has focused on a single materiel solution and needs to plan for the next phase of activity. The maturity of the design and the nature of remaining risks will drive the decision about which phase will come next (i.e., Technology Maturation and Risk Reduction (TMRR), EMD, or Production and Deployment (P&D) phase). The program should address these risks in the RFP and program plans.

2.3.1 Suggested Activities in the MSA Phase[2] to Reduce Risk

Significant risk management activities of the MSA phase include the following:

- Establish an affordability goal and schedule and performance margins.
- Develop design concepts to assess the state of the possible and inform the requirements, the draft RFP and Request for Information (RFI), and source selection activities.
- Avoid constraining the design trade space (e.g., minimize the number of Key Performance Parameters (KPP) and Key System Attributes (KSA), per the Joint Capabilities Integration and Development System (JCIDS) Manual).
- Ensure the government and bidders have a complete and common understanding of the requirements
- Solicit industry feedback regarding the feasibility of requirements, unit costs, and maturity of technologies via industry days, meetings with prospective bidders, and RFIs.
- Hold a government-only requirements review to ensure the proper translation of the user requirements into the performance specification.
- Where appropriate, define the requirement in the performance specification for open systems architectures and interfaces, which can reduce the costs and time for changes or upgrades.
- Identify system (hardware and software) assurance risks early to ensure system requirements, design, and architecture will produce a secure system in operations.
- Ensure critical technologies are achievable. Risks should be manageable within schedule and resource constraints. Limit the number of critical technologies, as appropriate.
    - Structure TMRR phase activities to validate performance during build, integration, and test to ensure requisite performance can be demonstrated by EMD.
    - Ensure TMRR phase proposals include assessments of the maturity of proposed technologies. Validate with independent subject matter expert (SME) risk assessment.
    - Collaborate with the S&T community to develop relevant technology, and request S&T dollars to mature key technologies.
- Focus the competitive prototyping strategy (if selected) on burning down the most critical technical risks (e.g., technology, engineering, and integration).
- Ensure the next phase RFP requires the contractors' proposals to include:
    - Contractor testing with defined success criteria before the start of government testing

[2] MSA activities in the areas of requirements, technology, integration, test, and manufacturing may apply across multiple acquisition phases. Although they may not be repeated in the following sections, programs should consider the full range of activities when tailoring plans for a particular program and risk area.

  - A requirement for contractors to identify problematic requirements as well as the cost and schedule associated with the requirements in their proposals to support the early maturation of the Capability Development Document (CDD) requirements.

- Ensure the TMRR phase RFP requires bidding contractors to identify risks and to provide an integration plan, an Integrated Master Schedule (IMS) through prototype delivery, and drawings/models so the government can assess (1) the contractors' understanding of the technical risks and (2) the required planning to execute the plans.
  - Develop a realistic program schedule, with appropriate phasing, which reflects consideration of relevant historical schedules as opposed to relying solely on an externally imposed timeline.
  - Be event-driven versus schedule-driven to ensure risks are mitigated before the program proceeds to the next phase; ensure the schedule reflects an acceptable level of concurrency.
- Establish communication: horizontal, across Integrated Product Teams (IPT) and joint risk boards; and vertical, up through management on both the government and contractor sides. Continue through all life cycle phases.
- Engage senior leadership from within the acquiring command, sponsor, and user community to manage program risks.
  - Build an external senior leader stakeholder group and working groups.
  - Ensure stakeholders understand the basis for the technical requirements so they feel ownership for appropriate risk reduction activities.

2.4 Technology Maturation and Risk Reduction Phase

If a TMRR phase is necessary, it should focus on reducing risks in technology, engineering, integration, and life cycle cost to the point that the Milestone Decision Authority (MDA) can make an EMD decision with confidence that the cost and schedule objectives carry understood and manageable risk. If the requirements community has clear and stable requirements and the supporting technology is mature, it may be possible to skip this phase and go directly to EMD or beyond.

Key risk areas include system performance and affordability. The PM decides what risk reduction activities to conduct in the TMRR phase but should prioritize starting with elements that represent the highest risk that can be reduced during this period of lower financial commitment. The PM should consider including special contract incentives for the high-risk areas. Typically, these activities include risk-reduction prototyping (which may be competitive) of the system, critical subsystems, technology, subcomponent, or component level. Prototyping of immature technologies can help inform decisions on how and whether to proceed. Another TMRR phase risk reduction activity is to identify and assess the materials and manufacturing processes the program will require.

Figure 2-3 displays the TMRR phase activities, including the following Systems Engineering Technical Reviews (SETR) to assess and manage risk: System Requirements Review (SRR), System

Functional Review (SFR), and Preliminary Design Review (PDR). Throughout the TMRR phase, the program team should conduct a rigorous assessment of technical risk, develop risk mitigation options, and execute and monitor risk mitigation plans.

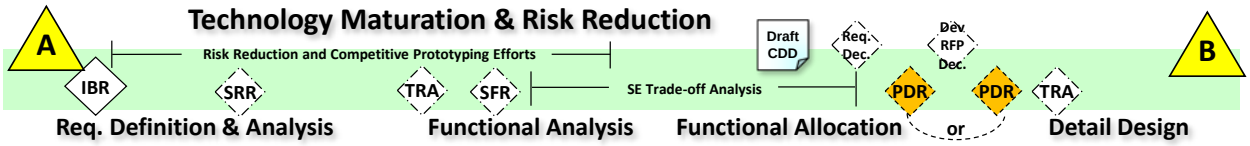


Figure 2-3. Technology Maturation and Risk Reduction Phase Activities

2.4.1 Suggested Activities and Practices in the TMRR Phase[3] to Reduce Risk

Significant risk management activities of the TMRR phase include the following:

- Assess TMRR risks mitigation effectiveness, and evidence that the program has demonstrated critical technologies in a relevant environment and end-item design context.
- Develop an EMD schedule that includes time for integration, interdependency linkages, and mitigation of manufacturing risks.
- Conduct system or subsystem risk reduction prototyping validation and competition.
- Assess the preliminary design and allocated baseline to identify problematic requirements and risks to meeting operational requirements, technical achievability, and cost/affordability targets. Ensure derived requirements do not contribute to requirements creep.
- Conduct systems engineering trade-off and preliminary design activities to support the assessment of final requirements in the CDD.
- Incorporate decisions from Configuration Steering Board (CSB) meetings and/or knowledge point review (includes requirements and intelligence communities).
- Track program interdependencies, interfaces, and associated memorandums of agreement (MOA) in periodic meetings with external programs and associated contractors/stakeholders.
- Verify validity of program framing assumptions.
- Plan for contingencies and technical risk mitigation activities by establishing reasoned cost, schedule, and performance margins.
    - Ensure risk mitigation plans are reflected in the Integrated Master Plan (IMP), IMS, Technical Performance Measures (TPM), and the EVM baseline. This may or may not require a change to the contractor work packages or resources. (Continue in subsequent phases.)

[3] These practices may apply to the EMD phase as well. Programs should consider the range of activities when tailoring their risk mitigation plans.

  - Identify resourced off-ramps for any critical technologies in the IMS.
  - Avoid allowing the urgency of the schedule to outweigh good engineering and management.
- Conduct a government Technology Readiness Assessment (TRA) and risk assessment early in the TMRR phase. Ensure prototyping activities are relevant to the planned end item design and include plans to demonstrate technologies that present uncertainty.
  - Identify applicable commercial technologies and develop an integration plan.
  - Consider directed options (directed subcontractors) as opposed to industry teaming.
  - Enable early evaluation of risks by planning an effective developmental test and evaluation program with adequate test articles and schedule duration for regression testing.
- Conduct a government TRA before MS B to identify and assess critical technology elements in the contractor's EMD proposal.
- Conduct schedule risk analyses (SRA) on a regular basis to evaluate the likelihood to achieve the planned schedule.
- For trade studies affecting KPP/KSAs, develop a decision hierarchy to promptly identify and mitigate technical risks and their impact on cost, schedule, and performance.
- Consider S&T investments to support EMD and beyond.
- Develop MOAs with all external interdependent programs.

2.5 Engineering and Manufacturing Development Phase

The decision to enter EMD should be made when the design is mature, the requirements are stable, and the risks are acceptable. By entering this phase, a program commits to a product. It initiates the Department's efforts for full-scale development and testing of a product to support verification of all operational and derived requirements so the program can begin production and deployment.

During the EMD phase, the program manages the remaining risk, builds and tests production-representative 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 2-4 displays the EMD phase activities. The program should conduct a Critical Design Review (CDR), a System Verification Review (SVR), a Functional Configuration Audit (FCA), and a Production Readiness Review (PRR) as part of its ongoing systems engineering and risk management efforts to assess and manage risk. These SETRs are technical milestones to assess the product and processes to ensure the system can perform as desired and proceed into the next phase within cost and schedule constraints at an acceptable level of risk.

Figure 2-4. Engineering and Manufacturing Development Phase Activities

The PM should focus the risk management activities on the transition from development to production. The program should consider conducting a manufacturing readiness assessment before Low-Rate Initial Production (LRIP) and again before Full-Rate Production (FRP) to identify risks related to critical manufacturing processes and product characteristics. Examples of specific risk areas include requirements/design stability, integration and interdependency risks, and manufacturing/supply chain quality.

2.5.1 Suggested Activities in the EMD Phase to Reduce Risk

Additional risk management activities to reduce risk exposure in this phase include the following:

- Continue knowledge point reviews, CSB meetings, and assessment of framing assumptions as in the TMRR phase. When not making a change to KPPs could jeopardize a program's utility or affordability, coordinate with the Joint Requirements Oversight Council.
- Update requirements trace and risk assessment for the draft Capability Production Document (CPD).
- Conduct early risk-focused developmental testing with adequate time for necessary regression tests.
- Work with the operational test and evaluation community for early participation, requirements trace, and assessment.
- Require contractor testing with predefined success criteria to facilitate resolving integration activities and failure modes before the start of government testing.
- Establish and manage size, weight, power, and cooling (SWAP-C) performance and R&M allocations for all subsystems.
- Align logistics analysis, training, and support systems with system development.
- Plan technology refresh cycles to be implemented in the P&D and O&S phases to address technology obsolescence risks.

2.6 Production and Deployment Phase

The purpose of the P&D phase is to produce and deliver requirements-compliant products to receiving military organizations. The design must be stable enough to commit to production prior to entering this phase.

Figure 2-5 displays the P&D phase activities. Specific actions include implementing mitigation plans for achieving Initial Operational Capability (IOC) and Full Operational Capability (FOC), which entails updating risk mitigation plans to address production and sustainment risks.

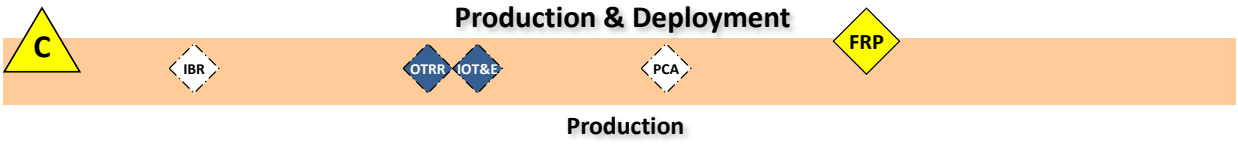


Figure 2-5. Production and Deployment Phase Activities

Following Milestone C, the program continues to mitigate risks to successful completion of Initial Operational Test and Evaluation (IOT&E) and the Physical Configuration Audit (PCA). The PCA verifies and validates that the product built is compliant with the design and meets the CPD. It also identifies technical risks for fielding and sustainment.

2.6.1 Suggested Activities in the P&D Phase to Reduce Risk

Additional activities to reduce risk exposure in the P&D phase include the following:

- Conduct a thorough PCA to verify production does not introduce new risks.
- Address risk associated with new requirements, follow-on increments, or deferred activities.
- Work with the Defense Contract Management Agency (DCMA) to assess production schedule risks.
  - Identify and assess delivery schedule dependencies with external programs/users.
- Identify sustaining engineering needs and fund as appropriate.

2.7 Operations and Support Phase

In the Operations and Support (O&S) phase, the risk activities include monitoring in-service usage, problem reports, parts availability/obsolescence, engineering modifications, technology insertions, and operational hazard risks. The Service support organizations often work with the program offices.

During this phase, programs should plan for and establish In-Service Reviews (ISR). The ISR is a multi-disciplined assessment to characterize the in-service health of the deployed system and the 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.

3 RISK AND ISSUE MANAGEMENT

Risk and issue management are closely related and use similar processes. All defense programs encounter risks and issues and must anticipate and address them on a continuing basis.

Risks are characterized by probability of occurrence and consequence. Through risk management, programs apply resources to lessen the likelihood of a future event occurring or the consequence should it occur. As risks increase in probability, programs should anticipate that the events will occur (i.e., become issues) and should put plans in place early to mitigate the consequences.

An issue differs from a risk in that its occurrence is certain, not probabilistic. An issue is characterized by its consequence, and issue management applies resources to address and reduce the potential negative consequences associated with a past, present, or certain future event. Issues may occur when a previously identified risk is realized, or they may occur without prior recognition of a risk. In addition, issues may spawn new risks.

Figure 3-1 depicts a suggested five-step management process that may be applied to a discrete risk or issue. The steps are broadly applicable to multiple phases in the program life cycle, but the details of particular actions will vary depending on program phase. This process for managing individual risks and issues operates within a broader framework in which consideration of risk shapes the basic program structure and content. Sections 3.1–3.5 further discuss risks. Selected aspects of the discussion may also apply to issues, discussed specifically in Section 3.6.

Figure 3-1. Risk and Issue Management Process Overview

3.1 Risk Process Planning

Risk process planning consists of the program's activities to develop, implement, and document steps the program will take to mitigate individual risks. The SEP should summarize the process. If a program develops a PRP (Program Risk Process) document that describes the process in more detail, the program can refer to the PRP in the SEP. For example, the PRP should describe the program's risk management expectations, risk management organization (e.g., Risk Management Boards (RMB), frequency of meetings and members), ground rules and assumptions, candidate risk categories, use of risk management tools, and training of program personnel. The PRP should mention how often the document will be reviewed and updated.

Figure 3-2 summarizes the aspects of risk process planning. The planning should outline each of the risk management steps described in the succeeding sections.

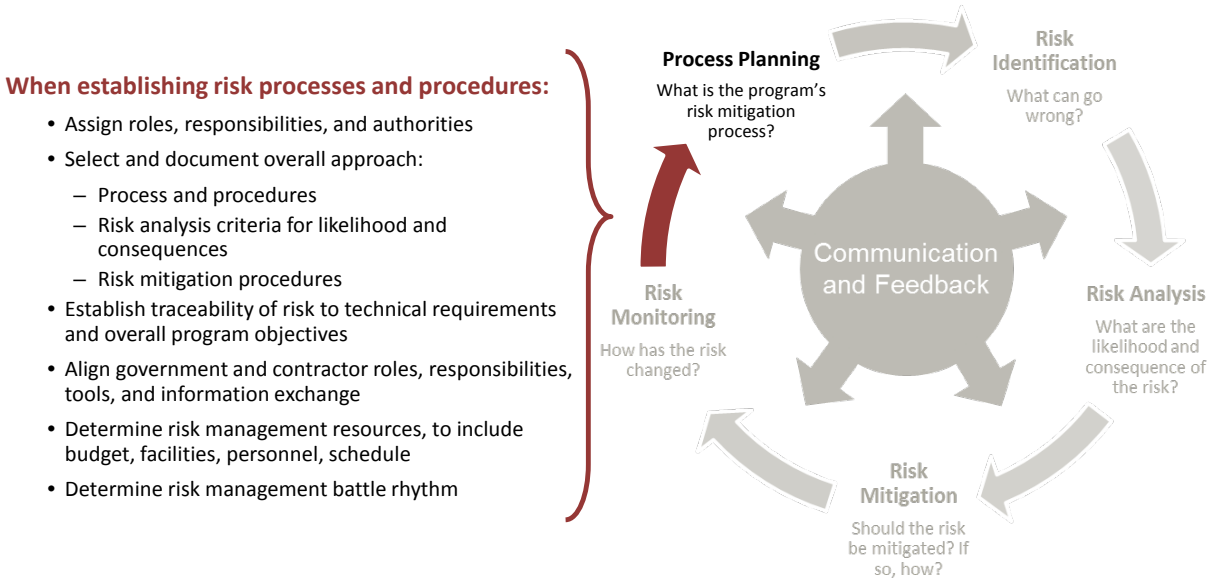


Figure 3-2. Risk Process Planning

The process for managing individual risks applies to all program phases, but as uncertainties and risks change with each program phase, the plans for specific actions to manage risk will change as well. Early in the acquisition cycle, the program focuses on shaping the program structure and content needed to produce a desired capability. In the TMRR phase, the focus shifts to gaining a thorough understanding of risks and to mitigating the actual risks in the context of designing the specific product to be delivered. As the program approaches entry to the production phase, the emphasis is on whether the product design meets requirements and is stable, producible, and affordable. The focus on the central risks in each phase is on achieving the necessary levels of assurance to proceed.

Appendix A provides additional information on establishing a risk planning process.

3.2 Risk Identification

A program identifies risks by answering such questions as *What can go wrong?* or *What is particularly difficult in this program development?* This step involves examining the program to determine risk events and associated cause(s) that may have negative cost, schedule, and/or performance impacts. The program should attempt to drill down far enough to understand underlying root cause(s) to the level required to inform risk analysis and the development of mitigation strategies discussed in Section 3.4.

All government and contractor program personnel are encouraged to identify candidate risks at any time. The government has a special need and responsibility to thoroughly understand and independently assess technical risks, which may be significant in source selection and in planning a program's structure and resourcing.

The risk manager, in a supportive role, is responsible for examining and compiling the identified risks in a risk register (see Section 3.3.4) and summarizing them at a manageable level of detail.

3.2.1 Risk Identification Methodologies

The program should begin identifying risks early and should continue as the program progresses, particularly as it enters a new phase or range of activities. Risk identification starts with understanding the nature of the specific product to be created and the requirements shaping the product. The program Acquisition Strategy is then structured to mitigate identified key risks.

This guide recommends an approach that incorporates reviewing source documents, analyzing a reference design and mission profile, and engaging subject matter expertise through standard methods of inquiry (e.g., brainstorming, interviews, and lessons). Program personnel should understand the program's requirements, goals, plans, and supporting analyses. Particularly relevant sources for identifying the risks include JCIDS documents, government technical requirements and specifications documents, AoA products, constraints, and assumptions.

In addition to risks that are inherent to the planned product, some risks may arise from inadequate estimating or planning of program activities. If not properly developed, planning documents may fail to address intrinsic risks or may inadvertently introduce new risks. For example, if a program fails to plan for needed test range time, this oversight could result in an unforeseen schedule risk in a later phase. Programs should review the planning documents (e.g., AS, SEP, TEMP, IMS) from their earliest formulation to look for inconsistencies or inadequacies in content, scope, or sequence of planned activities that pose risks.

User and acquisition communities should communicate regularly to identify high-risk requirements and inform potential systems engineering trade-offs during the development of JCIDS documents. For example, the program should analyze changes to requirements, especially changes to KPPs and KSAs, to determine what risks may be introduced that could jeopardize affordability, schedule, and performance. Programs should also assess requirements allocation to specifications to ensure they

are not excessively conservative and that specifications provide value commensurate with cost and schedule.

The program should consider the following approaches to inquiry, examination, or analysis to identify technical, programmatic, and business risks:

- Interviews with program team leads, SMEs, and/or program stakeholders, review of lessons learned, including risks or issues on similar programs, and systematic review of Work Breakdown Structure (WBS) elements against known process or other risks
- Examination of RFPs and proposals during source selection
- Systems engineering activities over the life cycle:
  - Development planning trade studies to identify sources and relative scale of risks related to closure of capability gaps, achievability of formative requirements; identification of cost, schedule, and performance drivers in AoA and subsequent analyses; and selection of a preferred materiel solution
  - Identifying dependencies and interoperability requirements
  - Planning for technical content for each phase, including staffing and facility plans
  - Systems Engineering Technical Reviews (SETR) during TMRR and EMD: to identify problematic requirements, immature technologies, design shortfalls, and difficulty of closing gaps to intended capabilities
  - Assessment of the maturity of critical technologies
  - Checklists/trigger questions on development, production, and/or support activities
  - Evaluation of results from prototyping or integration and test activities
  - Review of design changes, such as Class I Engineering Change Proposals
  - 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
- Analysis of metric trends (KPPs, KSAs, TPMs, schedules, budgets, the program's Earned Value Management System, the rate of Class I and II design changes, 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 requirements)
  - 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, single source suppliers, access to raw materials, export control, etc.

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

Figure 3-3 cites a few methods to use when identifying program risks (see also Section 2 for additional information on identifying risks throughout the life cycle).

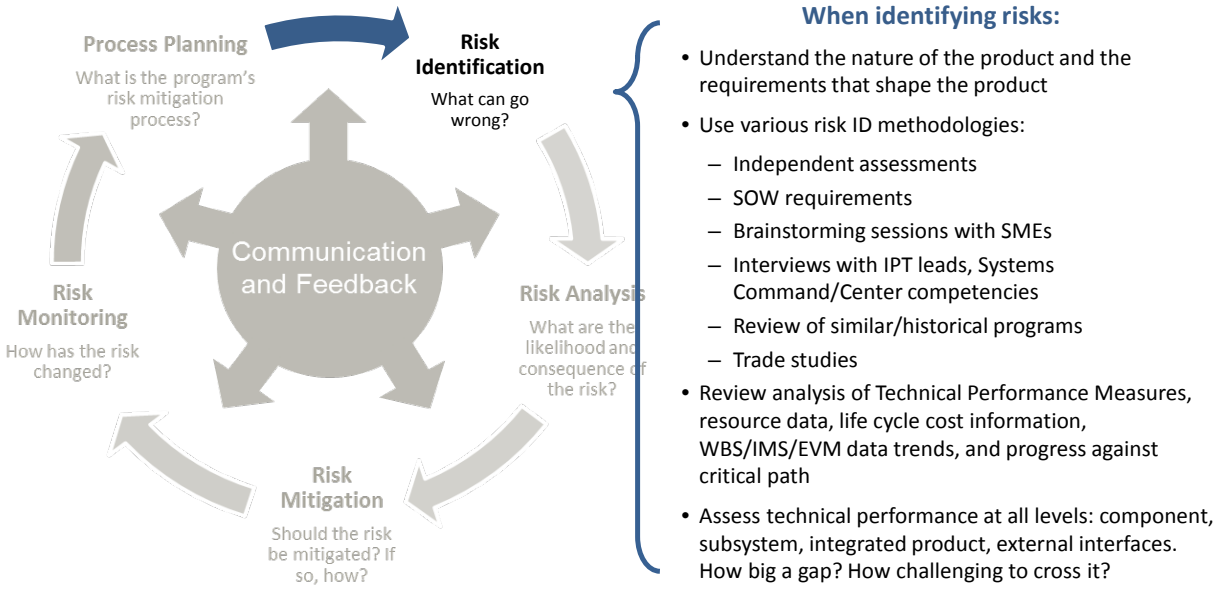


Figure 3-3. Risk Identification

3.2.2 Risk Categories

Acquisition risks with cost, schedule, and performance impacts can be grouped broadly into three categories: technical, programmatic, and business:

- **Technical** – 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. Programs sometimes confuse technology, engineering, and integration risks. All three are a type of technical risk described as follows:

- Technology – 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 – 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 – 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. Integration can be associated with hardware or software from component through system-of-systems level.

- **Programmatic** – 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)** – Non-technical risks that generally originate outside the program office, or are not within the control or influence of the PM. As appropriate, business risks should be escalated up the chain to the appropriate level. Business risks can come from areas such as program dependencies; resources (funding, schedule delivery requirements, people, facilities, suppliers, tools, etc.); priorities; regulations; stakeholders (user community, acquisition officials, etc.); market factors; and weather.

PMs should focus government and contractor efforts on risks over which they have or can influence control and also work within the acquisition chain of command to manage external risks arising outside their immediate control. Programs cannot ignore these risks and should have contingency plans in place for external risks that are outside their immediate control. Some risks may need to be raised higher in the chain of command.

3.2.3 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 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 helps prevent vague or inconsistent risk statements.

Multiple approaches exist in writing a risk statement. As an example, an **"if–then"** format presents the possible risk event or condition ("if") and the potential outcome or consequence(s) ("then"). When possible, programs should use a single approach for consistency and should present each risk in a clear, concise statement. The risk statement should not include a potential risk mitigation strategy, other solution, or other extraneous information. More information and examples for writing risk statements can be found on the DASD(SE) website (http://www.acq.osd.mil/se).

3.2.4 Evaluation of Candidate Risks

Program staff at the working level and SMEs should analyze candidate risks and present the resulting data to the RMB (or equivalent) for evaluation. Potential outcomes include the following: approved, rejected, need more information (deferred), management action, or engineering process/practice item.

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). This approach assumes 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 high 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 for mitigation.

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 mitigation efforts. Consistent predefined likelihood and consequence criteria provide a structured means for evaluating risks so decision makers and program office staff can make objective comparisons. 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 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 where practical. To efficiently

accomplish this step, the team may consider working from the impact or consequence first. Figure 3-4 depicts how risks should be analyzed and what impact areas to quantify.

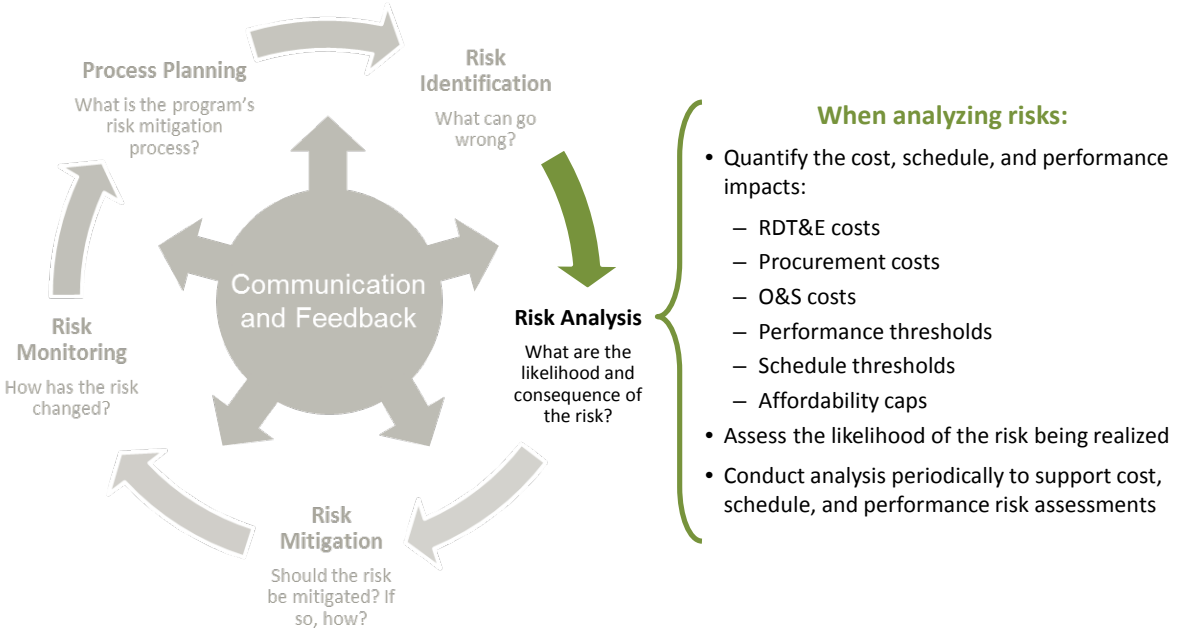


Figure 3-4. Risk Analysis

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.

3.3.1 Consequence

During analysis, 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.

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 of breaching a 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 PRP.

Table 3-1 lists multiple criteria for programs to consider. Programs should develop tailored, simplified criteria to assess cost, schedule, and performance consequences.

Table 3-1. Sample Consequence Criteria

Level	Cost	Schedule	Performance
5 Critical Impact	10% or greater increase over APB objective values for RDT&E, PAUC, or APUC Cost increase causes program to exceed affordability caps	Schedule slip will require a major schedule rebaselining Precludes program from meeting its APB schedule threshold dates	Degradation precludes system from meeting a KPP or key technical/supportability threshold; will jeopardize program success [2] Unable to meet mission objectives (defined in mission threads, ConOps, OMS/MP)
4 Significant Impact	5% - <10% increase over APB objective values for RDT&E, PAUC, or APUC Costs exceed life cycle ownership cost KSA	Schedule deviations will slip program to within 2 months of approved APB threshold schedule date Schedule slip puts funding at risk Fielding of capability to operational units delayed by more than 6 months[1]	Degradation impairs ability to meet a KSA. [2] Technical design or supportability margin exhausted in key areas Significant performance impact affecting System-of System interdependencies. Work-arounds required to meet mission objectives
3 Moderate Impact	1% - <5% increase over APB objective values for RDT&E, PAUC, or APUC Manageable with PEO or Service assistance	Can meet APB objective schedule dates, but other non-APB key events (e.g., SETRs or other Tier 1 Schedule events) may slip Schedule slip impacts synchronization with interdependent programs by greater than 2 months	Unable to meet lower tier attributes, TPMs, or CTPs Design or supportability margins reduced Minor performance impact affecting System-of System interdependencies. Work-arounds required to achieve mission tasks
2 Minor Impact	Costs that drive unit production cost (e.g., APUC) increase of <1% over budget Cost increase, but can be managed internally	Some schedule slip, but can meet APB objective dates and non-APB key event dates	Reduced technical performance or supportability; can be tolerated with little impact on program objectives Design margins reduced, within trade space [2]
1 Minimal Impact	Minimal impact. Costs expected to meet approved funding levels	Minimal schedule impact	Minimal consequences to meeting technical performance or supportability requirements. Design margins will be met; margin to planned tripwires

Notes:
[1] Consider fielding of capability to interdependent programs as well.
[2] Failure to meet TPMs or CTPs directly derived from KPPs or KSAs are indicators of potentially not meeting a KPP or KSA

APB: Acquisition Program Baseline; APUC: Average Procurement Unit Cost; ConOps: Concept of Operations; CTP: Critical Technical Parameter; PAUC: Program Acquisition Unit Cost; PEO: Program Executive Officer; KPP: Key Performance Parameter; KSA: Key System Attribute; OMS/MP: Operational Mode Summary/Mission Profile; RDT&E: Research, Development Test & Evaluation; TPM: Technical Performance Measure

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 mitigation 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. The estimated likelihood of the risk should be tied to a specific well-defined risk event or condition and risk statement. Table 3-2 provides typical criteria for establishing the initial assessment of 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. Typical 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%

The initial assessment of probability of occurrence needs to be considered in combination with consequences, should the event be realized, and also the projected effectiveness of mitigation actions when making decisions on whether a given probability level is too high and would preclude proceeding on a planned course of action. Depending on the circumstances, there may be cases in which a risk (probability and consequence) is high enough to change course, in the absence of assured mitigation.

Programs should also consider the effect of aggregate risk on a program. While dealing with individual risks, leaders and engineers should understand the overall risk exposure of a program and the threat that cumulative or compounding effects of multiple risks pose to successfully satisfying program objectives. Multiple risks may expose the program to a greater risk than any individual risk due to complexity, stretched resources, risk interactions, or the aggregate likelihood of risk realization. Monte Carlo methods such as those used in an SRA or cost risk analysis (CRA) may 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 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 are 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 (or approaching 100%), the program addresses the event or condition as an issue rather than a risk (see Section 3-6).

3.3.3 Risk Reporting Matrix

The primary goal of risk reporting is to provide the PM and other decision makers with a consistent method for managing and communicating risk to make data-driven decisions. The risk matrix is an effective tool to relay risk estimates in a visual display. This characterization also aids in prioritizing risks for risk mitigation (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 3-5. 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 communicate a top-level risk analysis.

While these values are used to define the risk level (e.g., low, moderate, high), additional factors should be considered to prioritize risks. The cost-effectiveness of perceived risk mitigation options is 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.

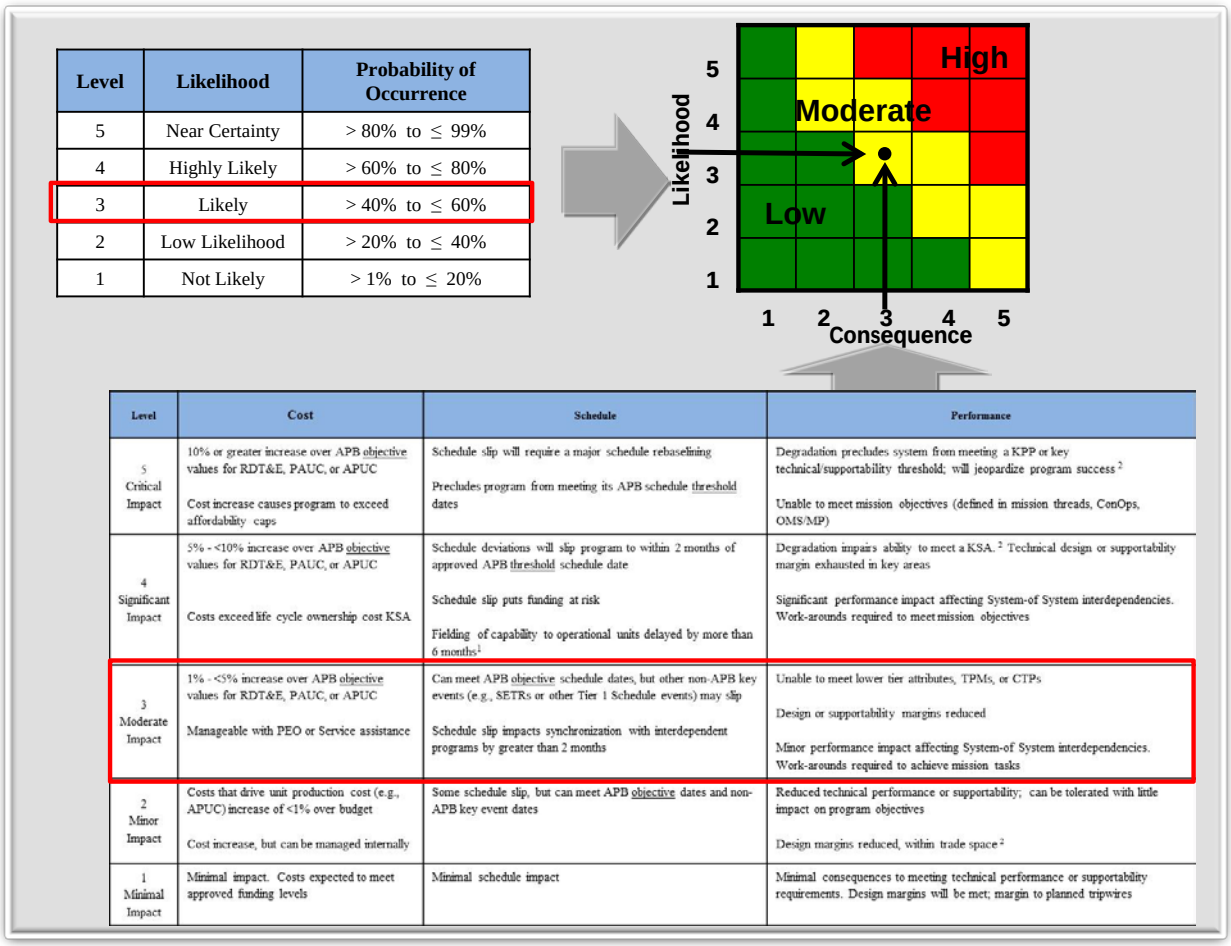


Figure 3-5. Risk Reporting Matrix and Criteria

Programs should compare cost-burdened risk and mitigation 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 resources. The cost exposure or risk-weighted consequence 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 mitigation effort is then subtracted from the risk-weighted consequence to determine the likely return on investment (ROI), including life cycle ROI.

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. (Note, however, that this simple example uses point estimates rather than distributions for each factor.)

If resources are available, taking into account all other considerations, the program may choose to invest as much as practical (considering the risk-weighted consequence) to mitigate high-consequence risks. With limited resources, the program must compare the weighted expected returns when deciding where to invest.

Table 3-3. Weighted Consequence Risk Mitigation

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

Again, the expected return 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 normally be prioritized over other risks even if it has a lower ROI. Expected effectiveness of the mitigation 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 ROI of risk mitigation strategies
3. Actual or expected impact on military utility
4. Time frame, frequency of occurrence, and interrelationship with other risks
5. Weighted expected return

Programs can then plot prioritized risks in a risk matrix, as shown in Figure 3-6.

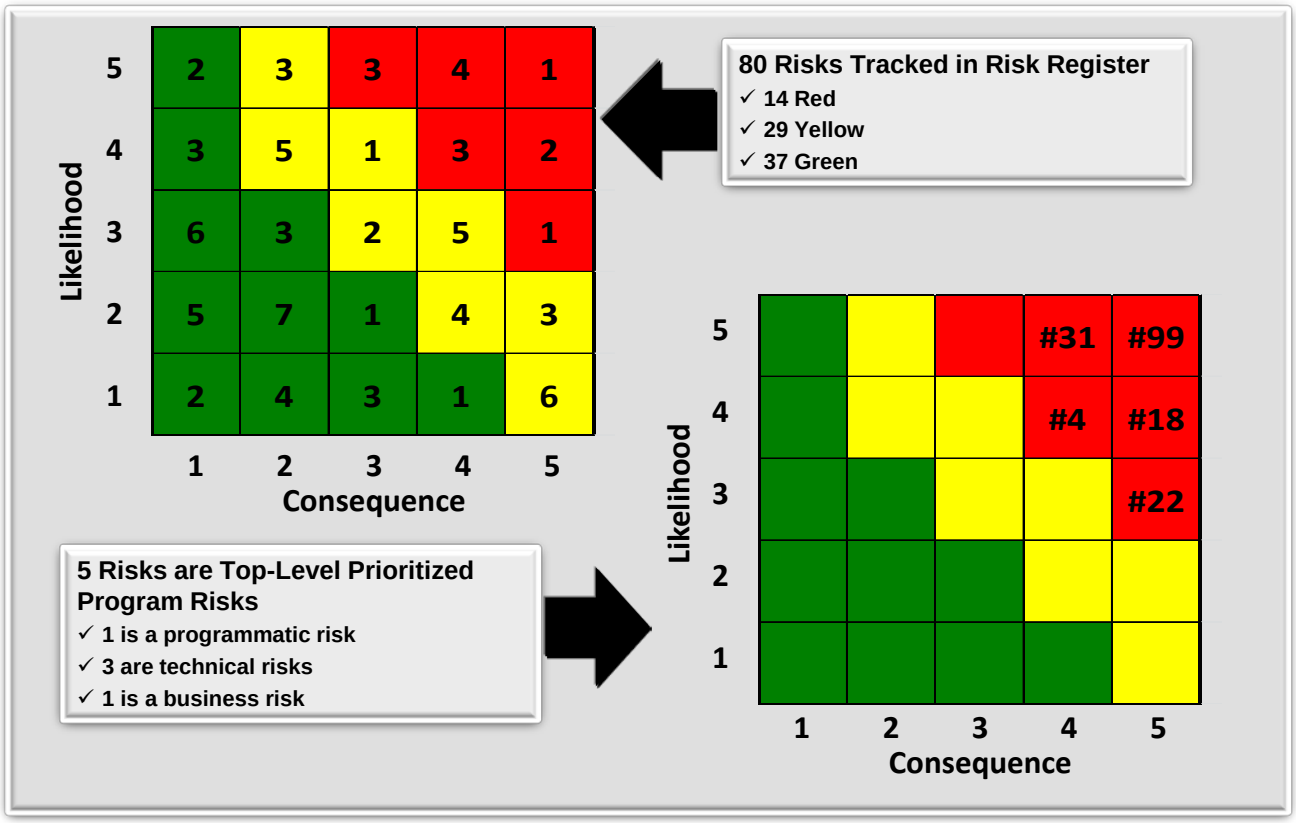


Figure 3-6. Risk Matrix Showing Prioritized Results

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 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 to describe and track risks and to record 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 mitigation 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, a program should consider capturing the rationale for the selection of risk mitigation options and should regularly update the risk register as the risk status changes.

Table 3-4. Risk Register Excerpt

Risk Number	Linked WBS/IMS ID#	Owner	Type of Risk	Status	Risk Event	Likelihood, Consequence Rating	Risk Mitigation Strategy	Risk Identified Date	Risk Approval Date	Planned Closure Date	Target Risk Rating	Plan Status
8231	3.2.2	Name	Technical	Open	Excessive number of priority 1 and 2 software defects may cause a delay to the start of IOT&E	L=3, C=4	Control - Program will apply mitigation reserve to retain adequate software engineers to burn-down SW defects	8/23/2015	1/14/2016	2/12/2016	L=1, C=4	On schedule

The risk register can provide traceability of program risks and can be a source for lessons learned during or at the end of key program events. The register, along with the program PRP, can provide valuable insight for future program development.

3.4 Risk Mitigation

The risk mitigation strategy includes the 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 controlled?* After analyzing the risks, program personnel should develop a strategy to manage risks by evaluating the four risk mitigation options. The program chooses the best option or hybrid of options based on the risk analysis, prioritization, and potential for risk reduction. The selected strategy for program-level risks should be reflected in the program's Acquisition Strategy and other documentation and should be 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 individual risk mitigation plan. Figure 3-7 highlights key aspects of risk mitigation.

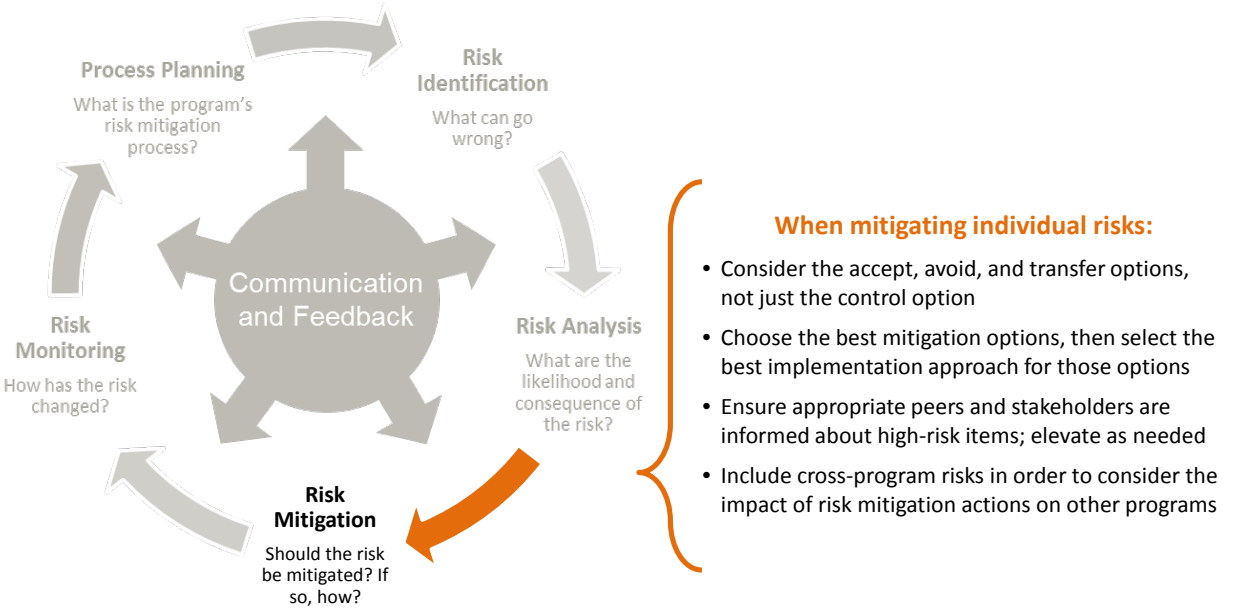


Figure 3-7. Risk Mitigation

The system design should incorporate features that provide resiliency, such as safety margins, growth provisions, modularity, cybersecurity, graceful or predictable degradation, and avoiding single-point-of-failure designs. Such provisions should be based on analysis to establish reasonable levels of risk avoidance without adding unnecessary cost or capability.

Some risk mitigation activities may be implemented as contingency plans when a specific triggering event occurs. The level of detail in risk mitigation 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 mitigation option(s) and formulating the implementation approach, the risk owner and RMB should address questions such as:

- Is the risk mitigation plan **feasible** (options and implementation approach)**?**
- Is the risk mitigation plan **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 mitigation plan?
- What **impact** does the risk mitigation plan have on the overall program schedule and on the technical performance of the system?
- Are the **expectations** realistic given program circumstances, constraints, and objectives?

Programs can fall into a trap of identifying ongoing baseline activities as risk mitigation activities. Programs should analyze the baseline contract activities to ensure plans are adequate to effectively address mitigation of risks. For emergent risks, programs should avoid identifying ongoing baseline

activities as risk mitigation without requisite analysis of the adequacy of planned actions or resources.

3.4.1 Risk Acceptance (and Monitoring)

By accepting the risk, the program acknowledges that the risk event or condition may be realized and the program is prepared to accept the consequences. Accepting a risk does not mean it should be ignored. The program should continue to track the risk to ensure the accepted consequences do not change for the worse or the likelihood increase. Monitoring implies the program establishes knowledge points that provide opportunities to reevaluate the risk. Before accepting the risk, the program should identify the resources and schedule that would be needed should the risk be realized. Occasionally, managers must seek relief from the next higher headquarters. Undoubtedly in constrained environments, programs occasionally must accept risk. However, they should make every attempt to understand the risk so future efforts are fully informed.

3.4.2 Risk Avoidance

Through risk avoidance, a program reduces or eliminates the risk event or condition by taking an alternate path. It eliminates the source of the risk and replaces it with another solution. Analyzing and reviewing the proposed system in detail provides insight into the drivers for each technical requirement.

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. One type of avoidance is deferral of a selected capability to a subsequent upgrade or release. A program should choose this option only if the system would be fielded without the additional capability anyway. In general, needed performance that might be difficult to achieve should be addressed earlier rather than be deferred. Another example might be changing operating procedures or using a low-risk mature technology.

3.4.3 Risk Transfer

Risk transfer includes reassigning or delegating responsibility for tasks to mitigate a risk to another entity. This might include transferring the financial responsibility as well. This approach may involve reallocating risk management tasks from one program to another, between government organizations, or across two sides of an interface managed by the same organization. The same risk may be carried (shared) by multiple government organizations. However, programs should recognize transference of risk does not eliminate all responsibility and risks must be monitored for potential consequences.

While financial risk may be substantially transferred by certain contractual arrangements or inter-program agreements, the schedule and performance risk cannot be fully transferred because the government needs the product. For example, if a radio is built to be used by multiple platforms but is

modified for use on one platform program, it may be a risk to that program, but it also can be a risk to the radio program office. Development of government-furnished equipment for application to multiple programs typifies this type of risk.

3.4.4 Risk Control

The risk control option seeks to actively reduce risk to an acceptable level. Control generally entails taking action to reduce the likelihood, or the consequence, of a risk to as low as practical in order to minimize potential impacts. Section 2 discussed activities to reduce risk exposure by phase. Following are additional examples of activities a program might consider for risk control:

- Multiple Development Efforts: Create competing systems in parallel that meet the same performance requirements.
- Early Prototyping: Build and test system representative prototypes focused on the highest risk elements.
- Incremental Development: Defer capability to a follow-on increment. (This may be combined with risk reduction S&T efforts.)
- Reviews, Walk-throughs, and Inspections: Reduce the probability/likelihood and potential consequences/impacts of risks through early assessment of actual or planned events, allowing earlier adjustments to planned work.
- Design of Experiments: Identify critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.
- Models and Simulation: Evaluate various design options and system requirement levels to increase knowledge earlier.
- Key Parameter Tracking Systems and 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.
- Demonstration Events: Establish events that increase knowledge of whether risks are being abated or not.
- Process Proofing: Simulate actual production environments and conditions to ensure repeatedly conforming hardware and software.

Control options should result in reduced risk likelihood and/or consequence. Risk control activities often reduce the likelihood of the risk event occurring or accelerate knowledge affecting the likelihood. It is possible to reduce the consequences associated with a risk if the program takes steps to sequence work to accelerate risk realization (do the hard things first), and/or limit impact or prepare for alternative approaches, such as redesign, if risks are realized. If actions are taken to reduce consequences, the program may consider whether to update the risk statement. The result may be a new risk description with revised consequences and an updated prioritization and mitigation strategy.

Appendix B explains how to integrate risk mitigation activities with other program management tools such as the WBS, IMS, and EVM.

3.4.5 Risk Burn-Down

A program should develop a risk burn-down plan for all high and moderate risks and for selected low risks. For most risks, the burn-down plan consists of time-phased 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. Developing a burn-down plan generally consists of six steps:

1. Identify and organize the risk mitigation activities in sequence manner, using realistic and logical schedule precedence, typically a finish-to-start.
2. Ensure all risk mitigation activities (1) are clearly defined, (2) are objective, 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 mitigation activity. Some activities may not 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 mitigation activity.
5. Include the risk mitigation activities or a subset of these activities in the program IMS. Programs should update the IMS for mitigation of emergent risks not accommodated in the existing work plans. 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 mitigation activities, plotting risk level versus time to estimate their relative risk burn-down/reduction contribution.

Risk monitoring should include the use of burn-down charts to track actual progress against the plan. Figure 3-8 shows a simple risk burn-down chart. It includes a snapshot of the progress of mitigating the risk over time and the effectiveness of previous risk mitigation activity.

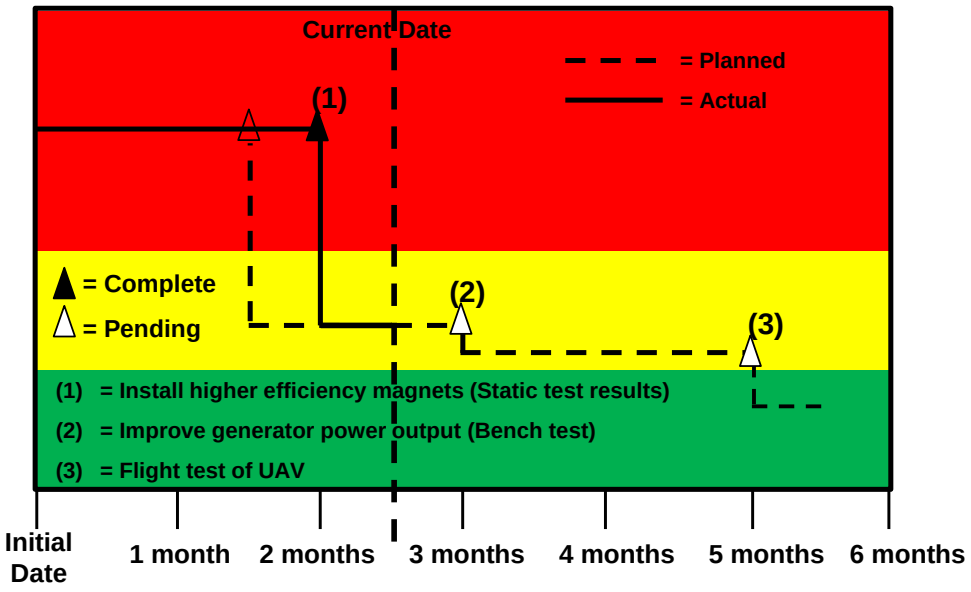


Figure 3-8. Risk Burn-Down

➢ ***Expectations***

- The risk register captures the mitigation option and associated activities for each risk.
- Risks can be accepted and monitored, avoided, transferred, or controlled.
- Risk control activities typically reduce the likelihood of the risk event occurring.
- Programs burn down high-consequence risks early to minimize late program-level changes or to provide early recognition of need for change.
- Risks are managed at the appropriate organizational level (executive, management, or working). The program tracks the development and implementation of the risk mitigation plan.
- The program allocates appropriate budget and other resources to implement the mitigation plan and enters mitigation activities into the IMS.
- The program has resourced mitigation plans for high risks and has resourced plans for moderate risks as appropriate.
  - o PMs should consider contingency plans for high risks.
- Risk burn-down plans should be time-phased and include specific measurable mitigation 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 mitigation plans working? Based on results, should additional actions be taken to mitigate or control the risk?*

Risk monitoring includes a continuous process to systematically track and evaluate the performance of risk mitigation plans against established metrics throughout the acquisition process. Not all risk mitigation will be successful. The program office should reevaluate the risk mitigation approach and associated activities to determine effectiveness and whether action is needed. Potential decision points and actions should be identified as part of risk management planning.

Risk monitoring includes recording, maintaining, and reporting risks, risk analyses, risk mitigation, and tracking results. It is performed as part of technical reviews, RMB and Risk Working Group (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, as in Figure 3-8, are also one method to monitor risks.

If a risk changes significantly, the program team should adjust the risk mitigation strategy accordingly. If the risk is lower than previously analyzed, the program team may reduce or cancel risk mitigation activity and consider freeing resources for other uses. If risk severity increases, appropriate risk mitigation efforts should be developed and implemented. The rationale for the changes to the risk mitigation strategy should be documented and archived for historical 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 mitigation 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 3-9 highlights selected components of risk monitoring. Risk monitoring allows timely actions to address potential problems.

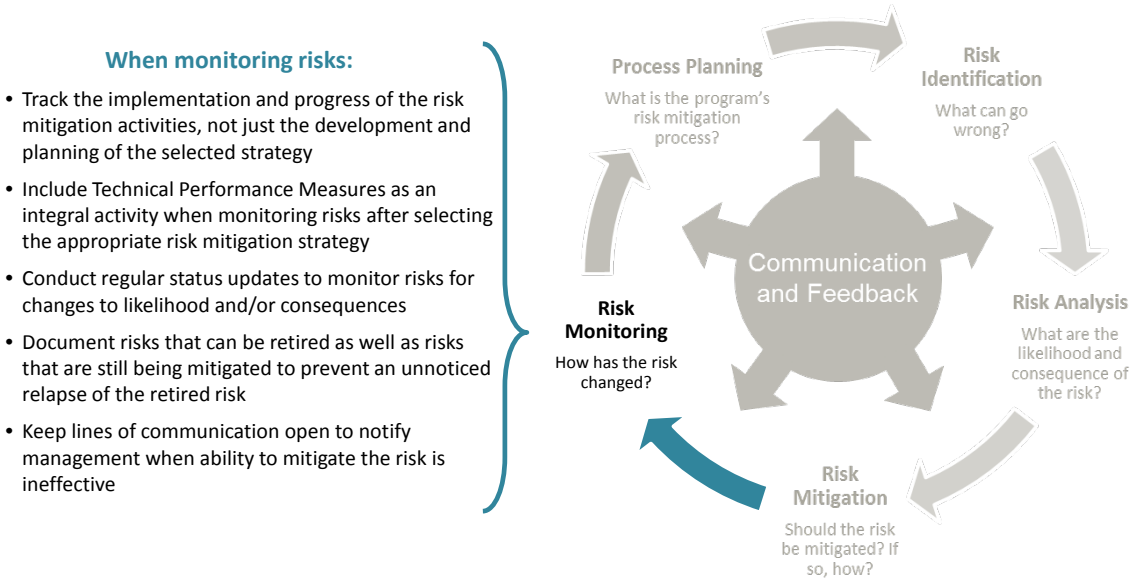


Figure 3-9. Risk Monitoring

Program offices and contractors should establish regular intervals for reviewing risks; however, events in the burn-down plans should serve as automatic triggers to action. 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 mitigation 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 3-10 illustrates the results of risk mitigation actions and provides an example of changed risk status following successful completion of risk mitigation. 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 mitigation strategy is not implemented or fails.

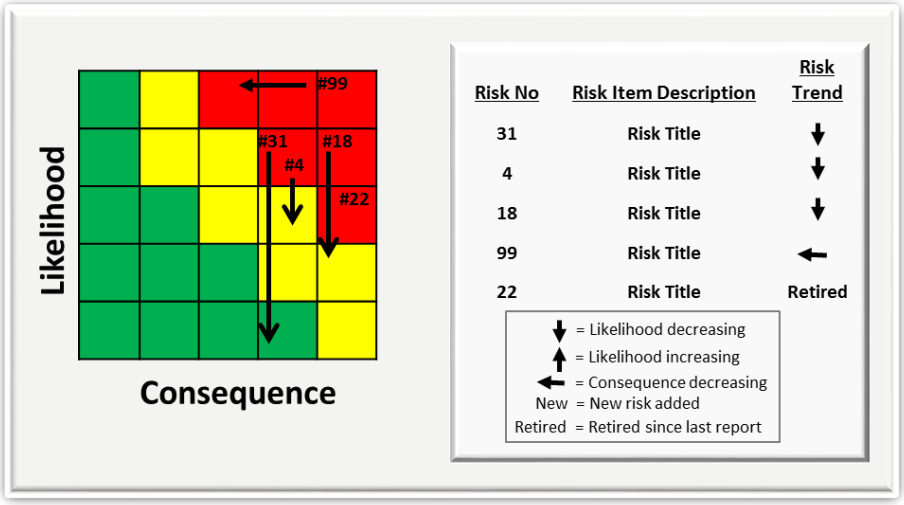


Figure 3-10. Example Risk Monitoring and Trend Matrix

The program should establish an effective means to display the current risk status and burn-down progress. Figure 3-11 provides a risk reporting format used to summarize the top 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 pre-established thresholds/limits, is trending negatively, or has evolved into an issue.

Appendix C contains a vignette of a hypothetical risk that applies the risk management processes discussed in this chapter.

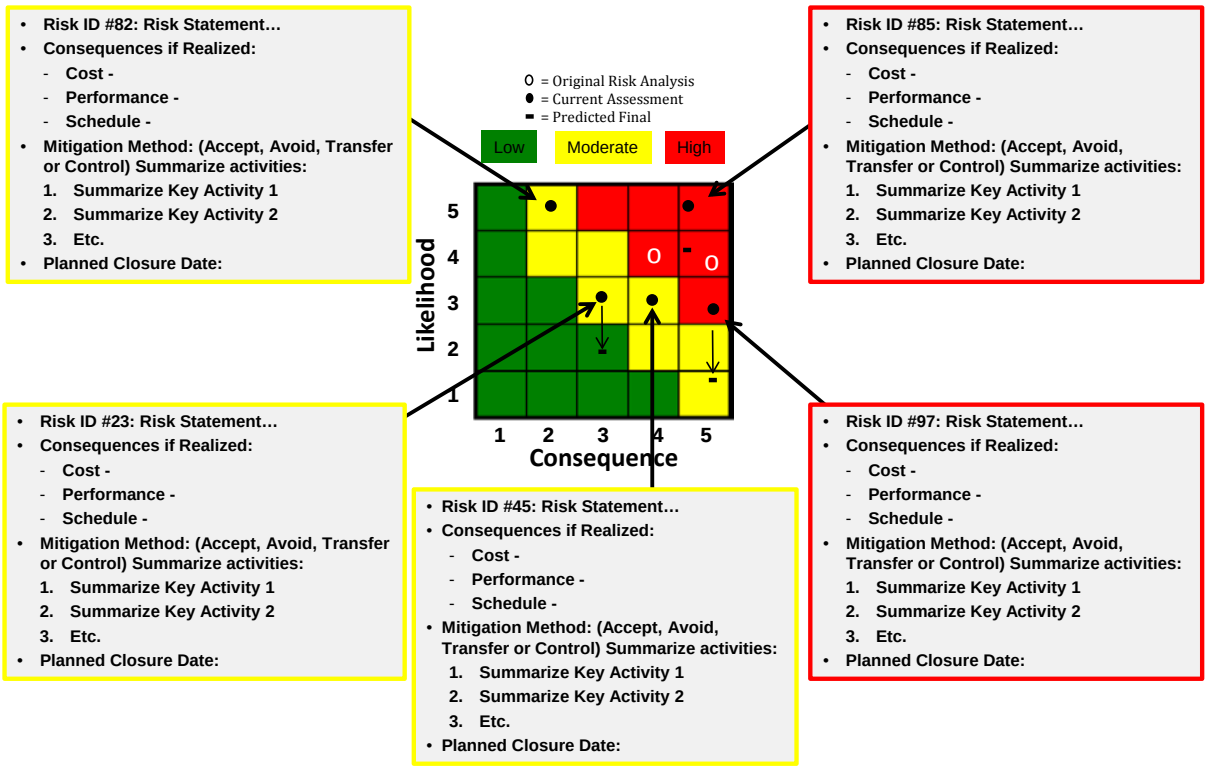


Figure 3-11. Suggested Risk Reporting Format

➢ ***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 leadership when risk mitigation plans should be implemented or adjusted or immediately when an event of consequence in the risk mitigation plan occurs. Similarly, the team should notify peers.
- Managers alert the next level of management when the ability to mitigate a risk exceeds authority or resources.
- The team tracks actual versus planned progress against the risk mitigation plan.
- The program establishes a management indicator to monitor risk activity.
- The program periodically reviews closed risks to ensure risks have not redeveloped.

3.6 Issue Management

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

Issues may occur when a previously identified risk is realized, or issues may emerge without prior recognition of an antecedent risk. In either case, the consequence of an issue needs to be addressed to avoid impeding program progress. As identified risks increase in probability, programs should anticipate their realization as issues and develop early plans to limit the consequences. If an issue emerges from a previously unrecognized risk, the program needs to quickly determine the consequences and timing for resolution to enable the development of plans. Programs also should assess whether issues may create additional potential risks, and should evaluate them accordingly.

Figure 3-12 displays the issue management process.

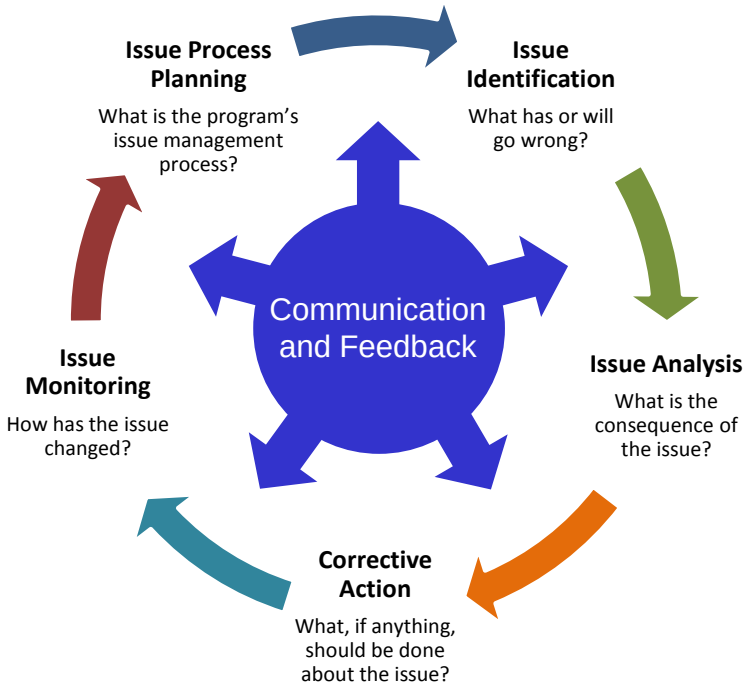


Figure 3-12. Issue Management Process

Issue management is complementary to the risk management process. Programs should take advantage of the common practices between issue and risk management while recognizing the distinctive characteristics of each. Programs may evaluate whether a separate issue-specific board is necessary or may be able to operate as efficiently with the RMB. The key is to focus on both issues and risks so the attention on current problems will not overtake efforts to manage risks (and opportunities). Programs should establish an issue management process to ensure issues are identified, analyzed, addressed, and tracked to retirement. The process should enable the program to

develop an effective approach for resolving any critical or high-priority issues, to vet the approach at the program management level or above as appropriate, and ensure resources are made available for execution.

Programs should determine the urgency of the issue in order to prioritize its resolution, and should document corrective action plans (sometimes referred to as plans of action and milestones (POA&M)), and include an Estimate at Completion (EAC) and the IMS. The program should update identified issues periodically and review them during regularly scheduled program meetings, program reviews, and technical reviews until the issues are resolved. The program leadership (RMB or equivalent) should assign an owner for each approved issue. Programs may consider combining the risk, issue, and opportunity registers into a single register for ease of management, and should record each approved issue in a register.

Issues should be analyzed using the program's risk management consequence criteria, and the results entered into the 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 converted to an issue level using an issue reporting matrix like the one in Figure 3-13, and the results are entered into the program's register. The green, yellow, and red regions on the matrix indicate areas of low, moderate, and high issue level, respectively.

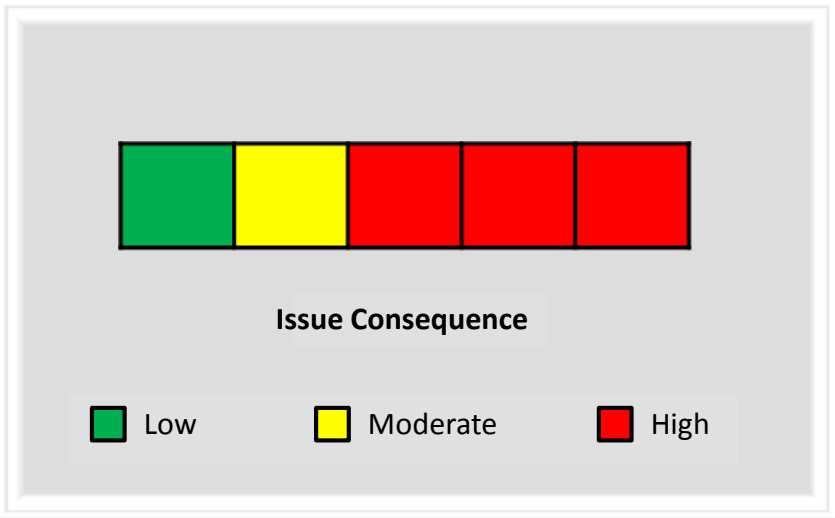


Figure 3-13. Issue Consequence Reporting Matrix

The program should evaluate the options for correction in terms of cost, schedule, performance, and residual risk, and select the best option (or hybrid of options) consistent with program circumstances. The primary options for issues are:

- **Ignore:** Accept the consequences without further action based on results of a cost/schedule/performance business case analysis; or

- **Control:** Implement a plan to reduce issue consequences and residual risk to as low a level as practical or minimize impact on the program. This option typically applies to high and

moderate consequence issues. If an issue arose from a previously recognized risk, some steps to reduce consequences may, or should have already been taken and a plan should be in place before the issue occurs. This is particularly the expectation for an antecedent risk with a high probability of occurrence and is consistent with the recognized continuum of risk to issue as probability increases.

Less common options include Avoid and Transfer, which carry the same definitions for issues as they do for risks (see sections 3.4.2 and 3.4.3). Avoid is sometimes considered one version of Control and subsumed in that option.

The program identifies an implementation approach, along with the necessary resources for implementation, obtains approval by the program leadership (RMB or equivalent), and documents the approach in the register. As with risks and opportunities, corrective activities for issues should be included in the IMS.

The program should track resolution of issues against the corrective action plan. Once the 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 (see Figure 3-12); (3) adjust the plan as warranted; and (4) analyze potential changes in the issue, its level, and potential associated risks. This information should be included in the program's risk/issue register.

➢ ***Expectations***

- As the probability of occurrence of a risk increases, the program should anticipate the realization of the risk and put plans in place to address the consequences.
- Issues are assessed for residual risks, and formal risks are established as appropriate.
- Programs document an issue management process in the PRP. This process may share elements with the risk management process.
- 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.

4 OPPORTUNITY MANAGEMENT

Opportunities are potential future benefits to the program's cost, schedule, and/or performance baseline, usually achieved through proactive steps that include allocation of resources. Risk and opportunity management support Better Buying Power initiatives to achieve should-cost objectives. Figure 4-1 is a simple portrayal of how opportunity management and risk management help realize benefits for a program.

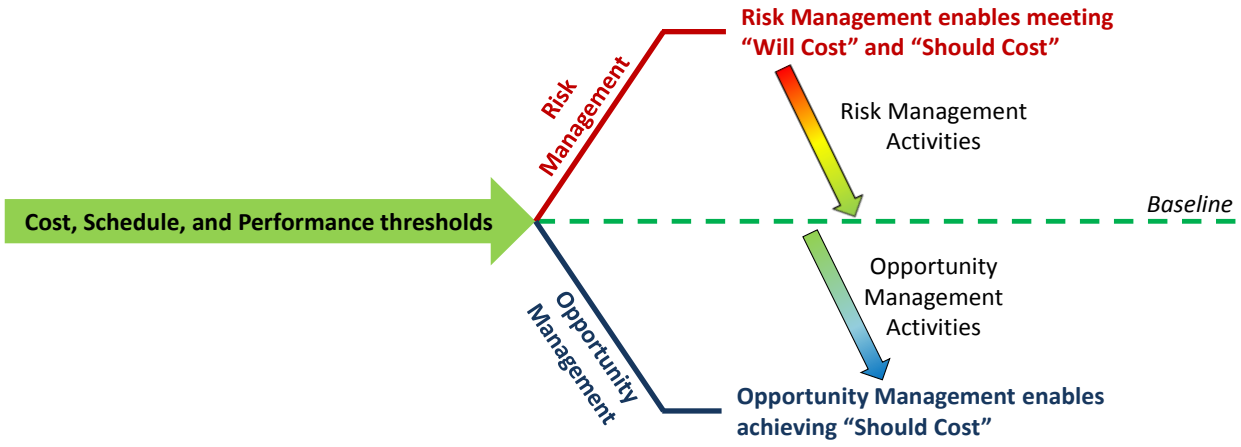


Figure 4-1. Opportunities Help Deliver Should-Cost Objectives

Opportunity management, like issue management, is complementary to risk management (Section 3). Program personnel should implement an opportunity identification and evaluation process to plan, identify, analyze, manage, and monitor initiatives that yield potential program cost reductions, schedule reductions, and/or performance improvements. As with risk and issue management, the program uses opportunity management to attempt to improve potential program outcomes. Opportunities can also help offset cost or schedule impacts from realized risks. Programs should document their opportunity management processes and may choose to incorporate these processes in the PRP.

Identifying opportunities starts with an active search for potential enhancements within the program's technical mission and stakeholder objectives. As opportunities are found or identified, the program evaluates the likelihood and potential benefits as well as the risks involved.

Candidate opportunities should be evaluated for costs, benefits, and potential risks before they are approved. If approved, the program should develop an opportunity management plan outlining how it will take advantage of the opportunity while continuing to manage risks and issues. Figure 4-2 shows the opportunity management process.

Figure 4-2. Opportunity Management Process

Opportunities may be identified before program execution and should be sought across the program life cycle. 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. Short-term gains with long-term negative consequences are usually not opportunities or appropriate should-cost initiatives.

During R&D and production, the program should continuously analyze opportunities for design and manufacturing changes that yield reductions in production and support R&D and 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 O&S phase, opportunities 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.

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 management options.

Programs should consider contracting for value management (e.g., Value Engineering Change Proposals) and incentives to encourage pursuit of opportunities. Programs should also encourage 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 consider ways to create incentives for vendors to recognize and pursue or recommend opportunities.

Management 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 options include:

- **Pursue now** – Fund and implement a plan to realize the opportunity. (Determination of whether to pursue the opportunity will include evaluation of the return of any investment when the opportunity would be realized, the cost, additional resources required, risk, and time to capture.)
- **Defer –** Pursue/cut-in later; for example, request funds for the next budget and request the S&T community mature the concept.
- **Reevaluate** – Continuously evaluate the opportunity for changes in circumstances.
- **Reject** – Intentionally ignore an opportunity because of cost, technical readiness, resources, schedule burden, and/or low probability of successful capture.

Given the selected option, the program should then choose an implementation approach.

For the “pursue” option, the resources needed to implement the plan should be approved and documented in the program’s opportunity register. Management 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, 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 during early production.

Once the opportunity management 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 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 4-3 shows a sample opportunity register for use at Program Management Reviews or other reviews.

Opportunity	Likeli-hood	Cost to Implement	Return on Investment					Program Priority	Management Strategy	Owner	Expected Closure
			Monetary			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	#2	Reevaluate - Summarize the mitigation plan	Mr. Bill Smith	March 2017
Opportunity 2: Summarize the opportunity activity.	Mod	$350K	$25K		$375K			#3	Reject	Ms Dana Jones	May 2017
Opportunity 3: Summarize the opportunity activity.	High	$211K		$0.4M	$3.6M	4 months less long-lead time needed		#1	Summarize the mitigation plan to realize the opportunity	Ms. Kim Johnson	January 2017

Figure 4-3. Opportunity Register

Opportunity Management Vignette. During early production of a hypothetical UAV, a government program office identified a new technology battery that could replace the existing one at lower unit cost and with a greater life span, while satisfying the F3 requirements. The UAV was designed to be modular and the battery is a Line Replaceable Unit (LRU) to the system. The battery costs $1,200 each when bought at quantities, and it would replace the existing one that costs $2,000. Thus there would be an $800 savings per unit. Since 500 units would be bought, the total savings in production would come to 800 x 500 = $400,000. However, since it would cost more than $500,000 to perform non-recurring work, which includes a regression test of the whole system, initial indications pointed to a loss of $100,000.

The PM directed a more thorough analysis, which included reliability comparisons and supportability costs. The reliability of the new battery was determined to be much higher than that of the existing one, and because it would not have to be replaced as often, the inventory spares requirements would be reduced along with maintenance cost. The new analysis calculated that LCC savings came to approximately $3.8 million. The PM decided to replace the unit. The government funded an Engineering Change Proposal with the contractor covering the cost of retrofit plus forward fit. The risk of failure for this effort was minimal (1-2%) against the $500,000 initial cost, compared with millions in savings.

Similar to the battery initiative, the contractor identified an opportunity to save $3,000 per unit by changing parts of the Guidance Electronics Unit (GEU) to a newer, more reliable and lower cost unit. Since the government and contractor negotiated that 80% of the production savings would go to the contractor, they agreed that the non-recurring qualification cost would be borne by the contractor. The government did not perform a cost-benefit analysis since it would not have to pay for the

change. Once again, the contractor's analysis showed that the replacement GEU not only would result in lower unit production cost to the government (by $600), but also would provide higher reliability, resulting in greater system effectiveness and reduced field support cost. The contractor submitted and implemented a Value Engineering Change Proposal reflecting an 80/20 benefit split in unit cost.

In both of the above cases, the government was in control of the configuration of these two prime items, with the attendant benefits. The cost risk to the government in the second case was zero since it was transferred to the contractor who also stood to benefit, making the risk worthwhile.

➢ ***Expectations***

- Programs implement an active opportunity identification and evaluation process to plan, identify, analyze, manage, and monitor initiatives that potentially yield improvements in the cost, schedule, and/or performance baseline.
- Programs evaluate and actively pursue high-return opportunities to improve the program life cycle cost, schedule, and performance baselines.
- Programs review risks, issues, and opportunities during regular program meetings.
- Programs establish or integrate opportunity tracking and management mechanisms.
- Programs establish opportunity likelihood and benefit criteria in line with program "should-cost" objectives.
- Programs evaluate approved opportunities and manage any associated risks.

This page is intentionally blank.

5 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 that incorporates or hosts products from other programs usually result in technical, programmatic, and business risks.

Interdependent programs may need to reconcile differences in 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. Successful interdependent programs have strong risk management processes, regularly communicate and share risk information, and maintain close collaboration to mitigate cross-program risks.

The acquisition chain of command should act as or appoint a technical authority to control interfaces and interdependencies and to adjudicate differences among participating programs, as necessary. Matters concerning requirements should be referred to the CSB.

Programs should consider the following activities when fielding a new system that depends on programs outside the PM's or PEO's portfolio or from another Service:

- Ensure effective control over critical interfaces with external programs.
- Align funding and priorities (schedules, form factor requirements, additional resources, etc.) of external programs. This may require verifying mechanisms, such as contract vehicles, are available for the needed work.
- Ensure the dependent system's successful development and fielding.
- Ensure interface management is in place to meet cost, schedule, and performance objectives.
- 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. These should not be allowed to languish but should be elevated to an appropriate management level as early as possible.
- Establish collaboration across appropriate joint and international programs to ensure interfaces support interoperability needs of the end-to-end mission capabilities.
- 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.

- PMs and PEOs should develop MOAs 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.
  - PMs should ensure contractors establish Associate Contractor Agreements to facilitate working relationships as appropriate.
  - Table 5-1 is a sample table of required MOAs from the Acquisition Strategy Outline and SEP Outline (see References).

Table 5-1. Sample Table of Required MOAs

REQUIRED MEMORANDUMS 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 5-1 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 mitigate them. The integration plan should:
  - Document the approach to identify interface requirements.
  - Define the interface products.
  - Describe the candidate integration sequences.
  - Show a coordinated delivery of verified configuration items.
  - Describe the integration test approach and facilities.

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

- Hold periodic meetings with all program, contractor, Service, and/or Office of the Secretary of Defense (OSD) stakeholders to review cross-program progress, risks, and issues. Build alliances to garner support in the event of unforeseen risks and issues.

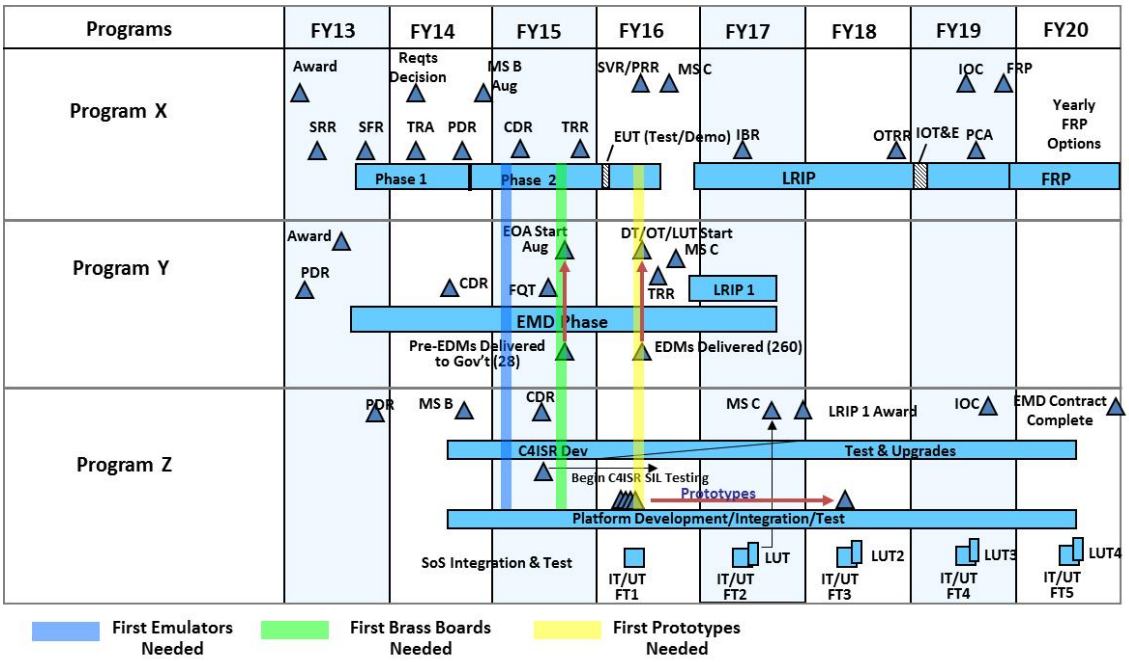


Figure 5-1. Sample Synchronization from the SEP Outline

- 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 of planned maturation activities, as well as any deviations from plans to update risk mitigation 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, RMBs, and meetings with Service and OSD leadership (Overarching Integrated Product Team (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 5-2 shows an example of a program's tracking of the cost, schedule, performance, technology maturity/readiness, and system-of-systems management with external programs.
  - Activities required due to interdependencies should be identified early enough that necessary resources can be secured.

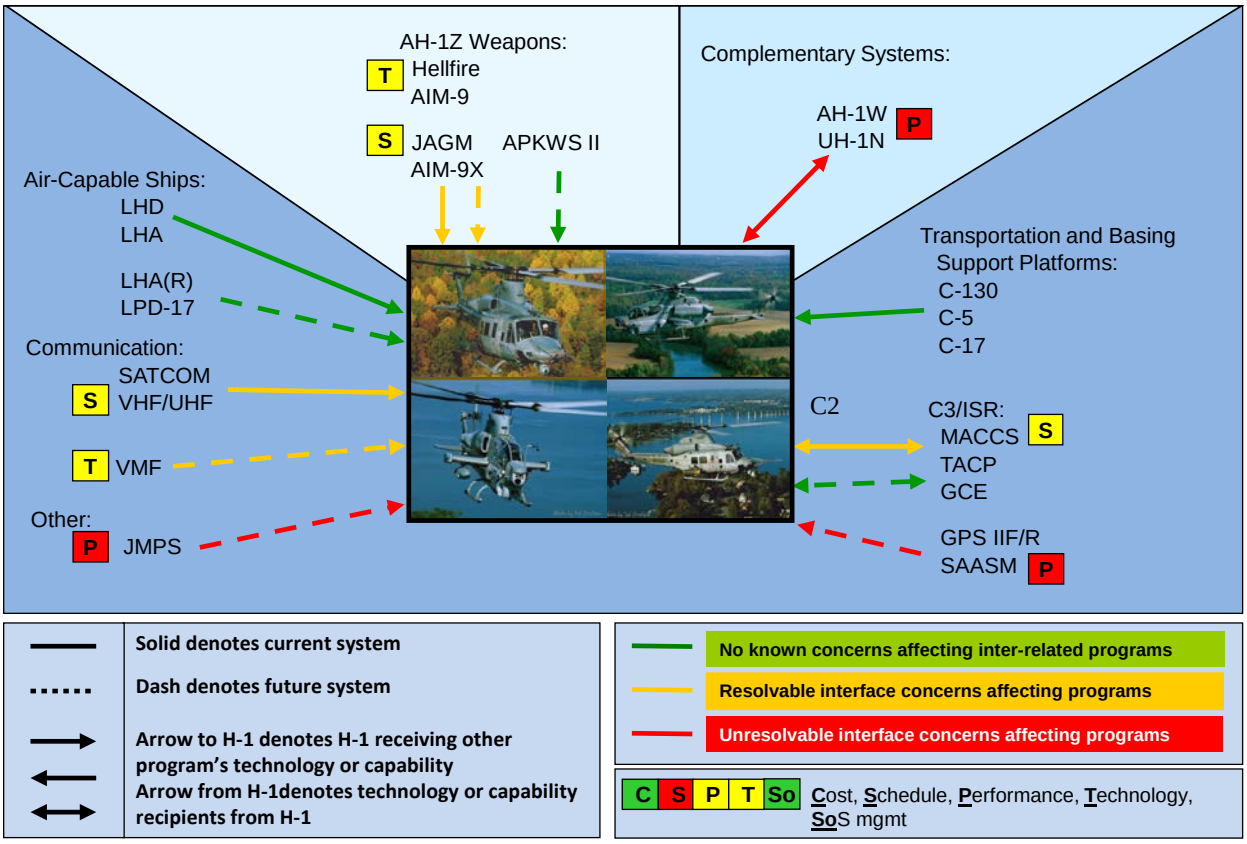


Figure 5-2. Tracking Interdependency Risks

➢ ***Expectations***

- There is a designated technical authority responsible for interface control between affected programs.
- There is collaboration and shared commitment between programs with critical dependencies.
- Programs are bound by the agreements documented in MOAs.
  - o External programs know and accept their SWAP-C allocations.
  - o 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.
  - o Giver-receiver relationships and deliverables are established and documented; required deliverables are tracked in the IMS.
- The schedule reflects sufficient time for integration, test, and 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. PROGRAM RISK PROCESS AND ROLES

Programs should establish processes to develop risk mitigation plans with specific actions and steps to address technology, engineering, programmatic, and business risks as the program progresses. Issues and opportunities are managed similarly as described in this document. The risk management concepts should be incorporated or adapted to issue and opportunity management, as applicable.

A.1 Program Risk Process

Some programs describe their processes in a combined RIO Process document; others describe their plans in separate documents. Programs should make a decision whether to combine the plans so as to best manage all three areas. This section provides guidance for developing a PRP document, but the same principles apply for issues and opportunities, which programs should likewise develop and document, combining into the PRP, if desired.

The PRP should:

- Define and tailor the program's processes to identify, analyze, mitigate and monitor risks.
- Establish the risk management working structure and responsibilities.
- 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 program should create the PRP at the program's initial formulation and update it at intervals during the acquisition life cycle (e.g., when a program is rebaselined, program phase changes, developmental and operational testing, and sustainment). Programs may include aspects of issue and opportunity management planning, as appropriate. Following is an example of a PRP outline:

- **Introduction** – Overview of the purpose and objective of the PRP, the strategy to implement continuous risk management, to include communication between stakeholders and training of the program team in the risk process.
- **Program Summary** – Brief description of the program, including the connection among the Acquisition Strategy and technical strategy outlined in the SEP.
- **Definitions** – Definitions specific to the program to be used in the plan.
- **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 mitigate risks
- Developing criteria to determine whether a candidate risk is accepted
- Changing likelihood and consequence of a risk
- Closing/retiring a risk

- **Risk Process** – Description of the risk management process, methodology, meeting schedule, and guidance for implementing the plan, according to the tailorable five-step DoD process:
  - Risk planning
  - Risk identification
  - Risk analysis
  - Risk mitigation
  - Risk monitoring
- **Risk Process in Relation to Other Program Management Tools –** List of the risk tools the program (program office and contractor(s)) uses to manage risk. 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 process planning before contract award and add to or modify the PRP after contract award. Events that may drive updates include acquisition milestones, contract award, system-level technical reviews, a change to the Acquisition Strategy, program rebaselining, or realization of a major risk.

➢ ***Expectations***

- The government should inform the program's risk management approach through 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 risk management planning, IMP, IMS, and SEMP.
- Programs establish and document a risk, issue, and opportunity management structure appropriate for implementation and oversight (RMB, RWG, etc.).

A.2 Risk Management Board and Risk Working Group

The PM establishes and typically chairs the government RMB as a senior group supporting the PM in risk management. RMB activities will vary consistent with the government and industry contractor roles in a cost or fixed-price contract environment. A cost environment generally provides greater flexibility for government RMB participation with the contractor in a broad range of risk management actions and investment decisions across the program scope. In a fixed-price environment, the government RMB supports the PM in tracking the progress of prime contractor risk-related actions and their implications for overall program status, and also supports PM responsibilities in areas such as GFE and government testing. The government can still provide direction, but a contract modification or claim may result.

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, RWG lead, contracting officer as warranted, a user representative, and others depending on the agenda. The RMB should document actions and decisions in meeting minutes and/or the risk register as necessary. Ultimately the RMB structure should define decision-making responsibilities and accountability.

Both the government and contractor will generally be engaged in managing risks of mutual interest and responsibility. Programs should consider integrating government-contractor RMBs where practical. Often joint RMBs are co-chaired by the two PMs and promote communication in areas of mutual risk. The contract type will have a bearing on the decision-making authority, and therefore the contracting officer representatives will be engaged. On fixed-price contracts, the contractor usually has the decision authority.

Figure A-1. Government and Contractor Joint Risk Management Boards

On large programs, a tiered structure is often implemented to manage lower-level risks. If used, these lower-level boards should have the authority and resources required to fully implement mitigation strategies within their responsibility. The program should ensure recurring visibility into these lower-level risks, issues, or opportunities. 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. All program meetings are candidates for discussing risk status.

Program offices may create one or more RWGs led by a member of the Systems Engineering IPT or Program Management IPT, with representatives 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.

A.3 Selecting a Risk Management Tool

Risk management tools support the implementation and execution of risk management. The PM needs to select the appropriate tool(s) early and document details in the SEP. The Services have developed or endorsed specific risk management tools. The Army-developed tool, Project Recon, is available for DoD-wide use, while the Air Force directed the use of a preferred commercial tool, Active Risk Manager. The Navy-developed tool, Risk Exchange, is hosted on the Naval Systems

Engineering Resource Center website. While these tools differ in operator interface functionality, they all have similar features. These include:

- Traceability and embedded reporting
- Supporting qualitative and quantitative assessment of risks and management activities
- Providing a risk management audit trail

➢ ***Expectations***

- The government program offices and contractors select a common or electronically compatible risk management tool to collectively identify, analyze, mitigate, and monitor risks, issues, and opportunities.
- Access to the risk management tool is available through an Integrated Data Environment. When practical, key subcontractors and external programs employ the same risk management tool and processes. All parties establish appropriate firewalls and take care to protect sensitive government or contractor proprietary risk and technical data.

A.4 Risk Management Roles and Responsibilities

Budget constraints require PMs and contractors to balance program priorities with high-value risk mitigation activities. Given these constraints, an effective risk management process requires the support and commitment of the entire acquisition team. The program and contractor should clearly define the roles and responsibilities in the Acquisition Strategy, SEP, Systems Engineering Management Plan (SEMP), and PRP.

Organizing and training the team to follow a disciplined risk process will enable better informed program decisions. 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 SMEs is often beneficial.

Figure A-2 displays the hierarchy typically involved in risk management. These groups and individuals perform vital roles in the risk process and in helping to identify, analyze, report, and mitigate risks at the appropriate level. These groups provide an array of expertise in areas such as systems engineering, various engineering specialties, logistics, manufacturing, testing, schedule analysis, contracting, cost control/estimating, EVM, and software development. Some of the levels depicted in Figure A-2 below may be eliminated for specific programs or risks.

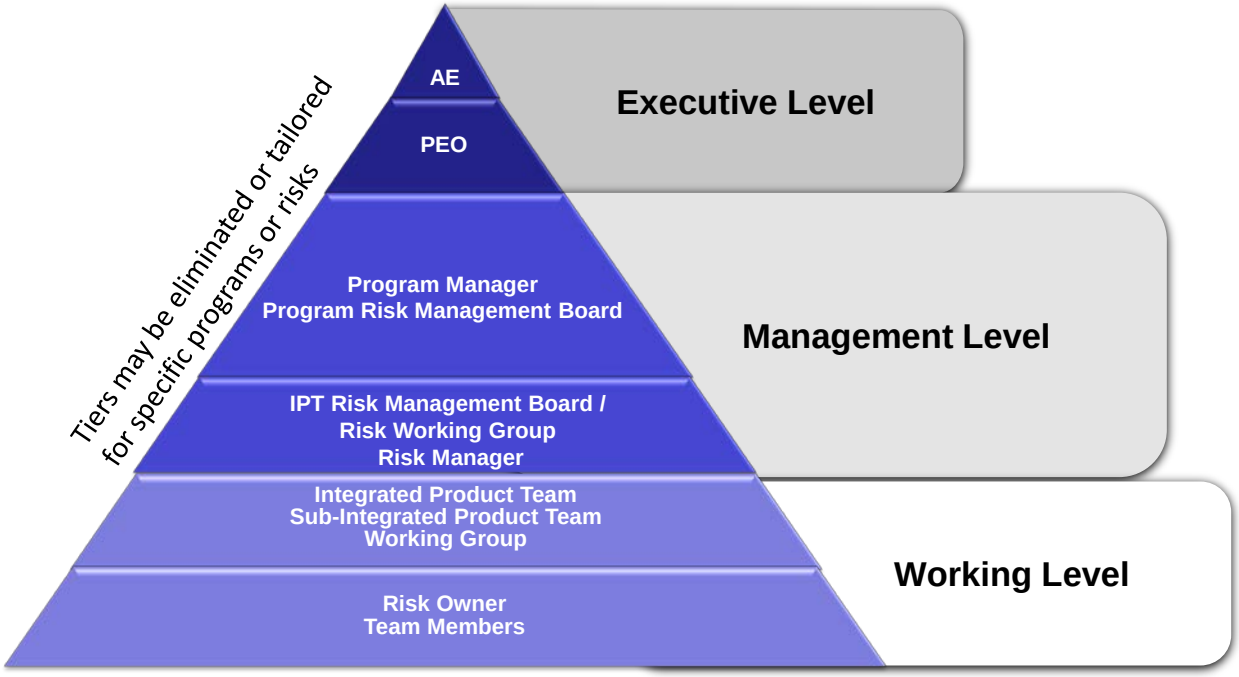


Figure A-2. Roles and Responsibilities Tiering

A.4.1 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 improve the risk management program, including applicable incentives for effective risk mitigation 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.

A.4.2 Typical Contractor Responsibilities

- Strive to align internal risk 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 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 processes and definitions; establish means to integrate subcontractor risk process within the overall program risk mitigation effort.
- Conduct risk identification and analysis during all phases of the program, including proposal development, and apply appropriate risk mitigation strategies and plans.
- Assess the impact of risks during proposal and baseline development.
- 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 mitigation activities into the IMS and program budgets as appropriate.
- Synthesize and correlate new and ongoing risk elements in the IMS, risk mitigation plans, estimates at completion, technical status documentation, and program updates and reviews.

A.4.3 Suggested Tiered Roles and Responsibilities

A.4.3.1 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 mitigation plans. Provides direction regarding management of cross-PEO (external), portfolio (internal), program-level, or special interest risks and issues.

A.4.3.2 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 PRP.
- Establishes and executes an integrated risk management process with the contractor and key subcontractors; ensures the development of and approves the program's PRP.
- Ensures the appropriate disciplines and IPTs are involved in the risk process (program management, engineering, contracting, information assurance, legal, financial management, EVM (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 PMs, 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 mitigation plans are approved at the appropriate level to include acceptance of consequences (e.g., ESOH 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, OIPT, 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 mitigation 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 PRP.
- Ensures risk management efforts are integrated and at the appropriate working level.
- Reviews and validates identified program-level risks; approves risk mitigation plans, including adequacy of resources and any changes to approved plans.
- Monitors the status of risk mitigation 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 (PEO/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 mitigation 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 mitigation plans are adequate.
- Approves and tracks the status of IPT-level risk mitigation 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 PRP 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.

A.4.3.3 Working Level

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

- Develop and implement the risk planning outlined in the SEP, SEMP, Acquisition Strategy, and/or PRP, and support the PM and RMB as required.
- Identify internal and external risks in accordance with the procedures documented in the program's approved PRP. 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 mitigation options, estimate funding requirements, support implementation of the selected mitigation plan, and track progress of 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 PRP.
- 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 mitigation plan and options for assigned risks to include required cost and resource estimates and fallback plans for high-level risks.
- Briefs the risk mitigation plan to the program or IPT RMBs, as appropriate, for approval.
- Implements and reports on the progress of the mitigation 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 B. 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. Collectively, these tools, along with schedule, cost, and performance risk analysis, help the PM gain insight into balancing program requirements and constraints against cost, schedule, or performance risks.

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 mitigation plans and, whenever possible, link the risks to the work packages associated with the mitigation effort. Similarly, the contract in-scope risk mitigation activities should be included in the IMS to provide a consistent method of measuring progress toward completion.

For risk mitigation 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 mitigation 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.

B.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 B-1 depicts a simplified WBS decomposed to Level 3.

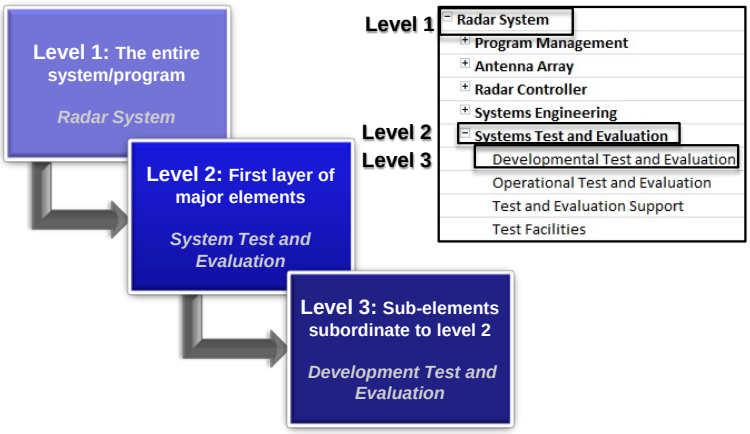


Figure B-1. Example of WBS Levels

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. If needed, the program should update the WBS to reflect selected mitigation tasks.

Figure B-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.

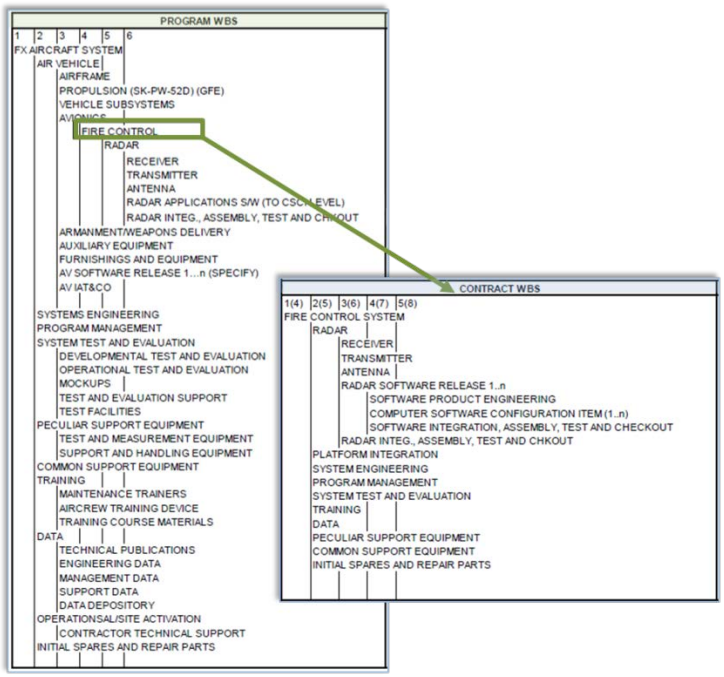


Figure B-2. Government and Contractor WBS Relationship

B.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 mitigation tasks, 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 B-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 mitigation activities and associated resources in the IMS to establish an accurate performance measurement baseline and critical path analysis.

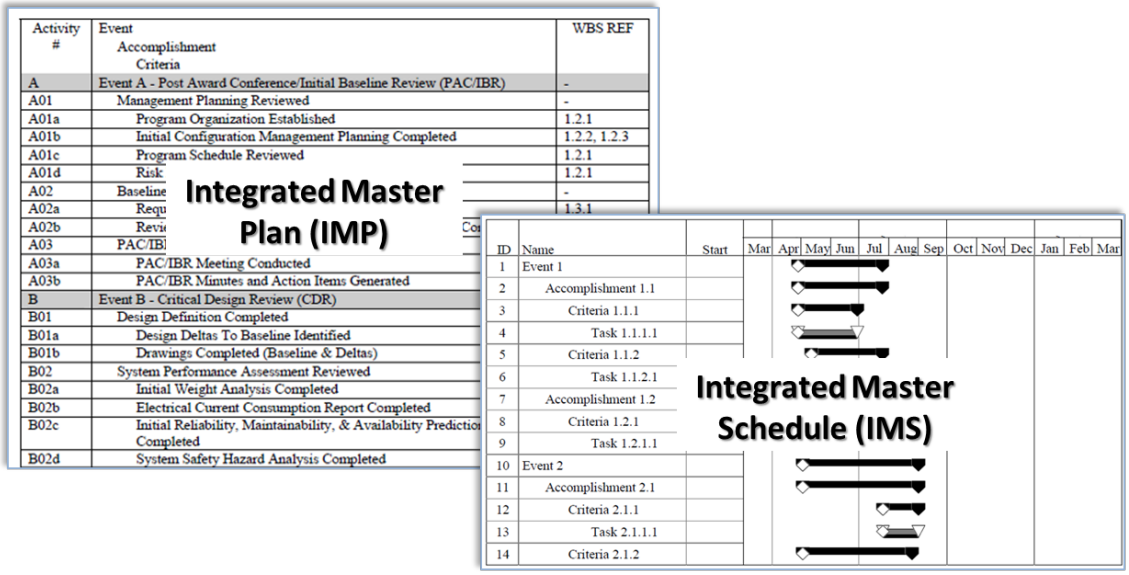


Figure B-3. IMP/IMS Creation and Implementation

Programs should regularly assess the health of the IMS through a schedule health assessment (SHA). The Defense Contract Management Agency (DCMA) 14-point schedule metrics are an excellent tool to assess schedule quality, structural integrity, and overall health. Figure B-4 summarizes the 14 metrics and shows 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.)

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 B-4. Sample 14-Point Schedule Health Assessment Metrics and Status

B.3 Earned Value Management

EVM provides a disciplined, 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, (3) alert management to specific problem areas at the cost account manager level in the EVM system, and (4) provide a means to forecast final cost and schedule outcomes. EVM also can provide information to the project's risk management process for identifying potential risks and issues, and monitoring and adjusting implemented risk mitigation 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.

B.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 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; 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 consider appropriate TPMs and metrics to aid in

monitoring the progress of risk mitigation plans. TPMs and metrics are likely to change over the course of the program as risks are retired and new risks are identified.

B.5 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 of the program's likely schedule progression and completion without additional risk-mitigation actions. As such, the analysis can inform management actions, support "what-if" evaluations, and provide inputs for prioritizing risk mitigation approaches and control activities.

Before performing an SRA, the program should assess the IMS using the criteria provided in paragraph B.2 to ensure the underlying schedule is free of potential errors that could have an adverse impact on the SRA results. For example, 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.

B.6 Cost Risk Analysis

A CRA can 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).

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.

B.7 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: AoA 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 paragraph B.4 of this appendix for a discussion on selecting TPMs.

➢ ***Expectations***

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

APPENDIX C. 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 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 TMRR phase with several risks, which are planned to be resolved during the early part of the EMD phase. Among the several risks outstanding at this point, only one risk was rated as high, and the mitigation 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: SMEs 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 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 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 C-1.

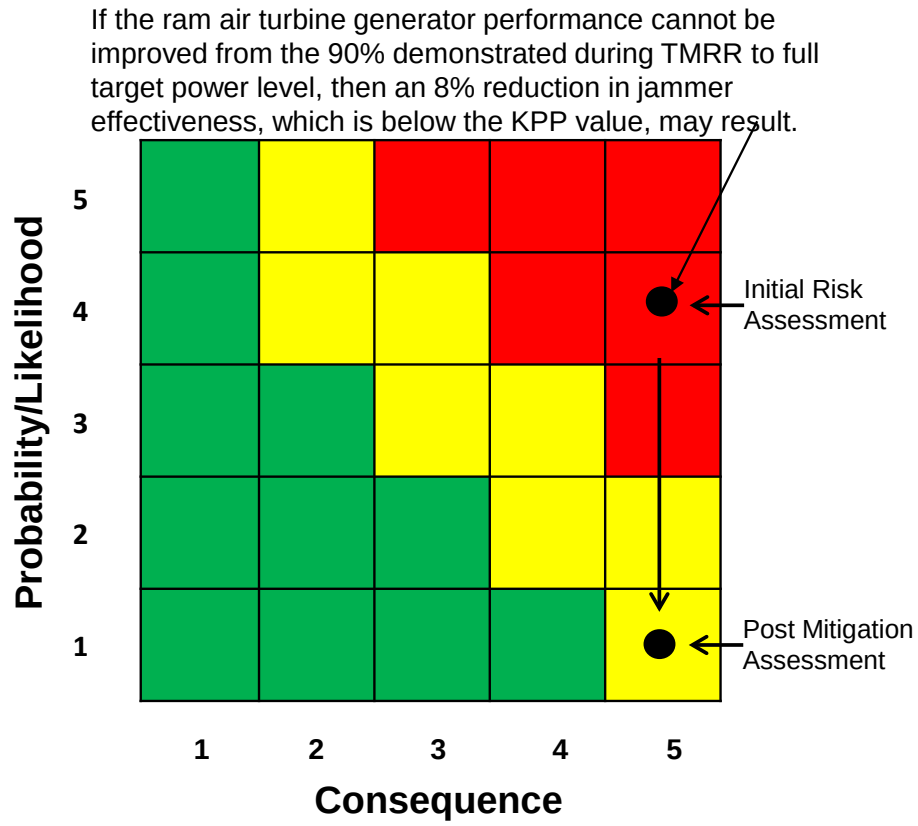


Figure C-1. Risk Matrix for Ram Air Turbine Generator

Risk Mitigation: The PM examined mitigation options. Because of the significance of the potential performance shortfall, the PM opted to control 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 mitigation 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 delay in the schedule. Probability of success was assessed as 70 percent.

C. Use a more advanced set of radar components that required less power. This option would cause a year delay 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 cost to control the risk was estimated as $1 million, less than 0.5 percent of EMD cost. Recurring system cost impact was very small, within estimating error.

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 mitigation plan included projected consequences and likelihood at each risk control step based on expected performance against the quantitative metrics established for each risk control 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 C-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 risk manager entered the activity in the IMS and risk register.

TPMs 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, the program emphasized metrics in power delivery and established the metrics 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, the program would terminate the new generator effort and pursue discussions with the user regarding alternatives, discussed earlier.

The program established three events to evaluate metrics for burning down the risk over the 5-month period:

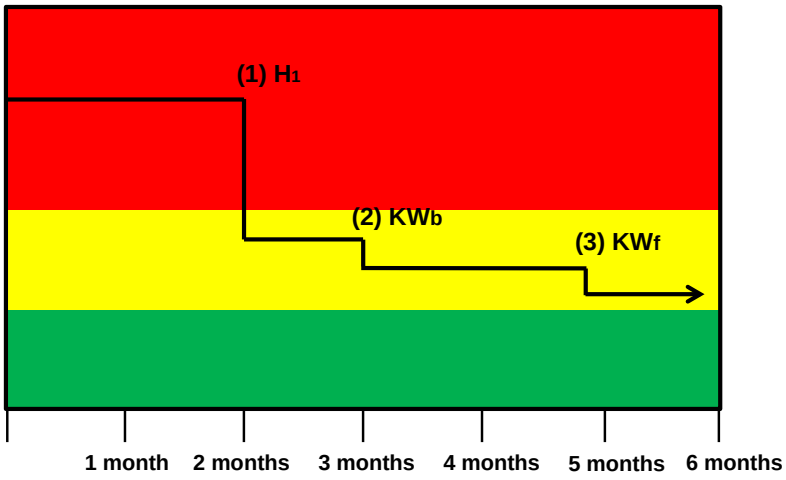
Step 1: Test to measure the configured magnetic field strength. The threshold for static magnetic strength using the enhanced magnets was calculated to be H_1 amperes/meter. The program assessed that meeting this threshold would reduce the risk likelihood from 4 to 2.

Step 2: Measure the prototype bench test power output using a motor driver to simulate turbine effects to demonstrate whether the power output satisfied the established threshold value, designated KW_b (measured in watts).

Step 3: Conduct a flight test of the UAV with the reconfigured generator installed to confirm whether the in-flight generator power output, over a range of conditions, satisfied the final in-flight power level (KW_f) required for the jammer.

The last two activities, if successfully demonstrated, 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 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 C-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 C-2. Risk Burn-Down Diagram for Option A

Risk Monitoring and Closure: The IPT 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.

In this case, the efforts were also captured in the EVM process. (Some short duration mitigation activities may not always be fully captured in EVM) Closure would be achieved when tests demonstrated that 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 C-3. The generator risk is displayed at the top right of the figure.

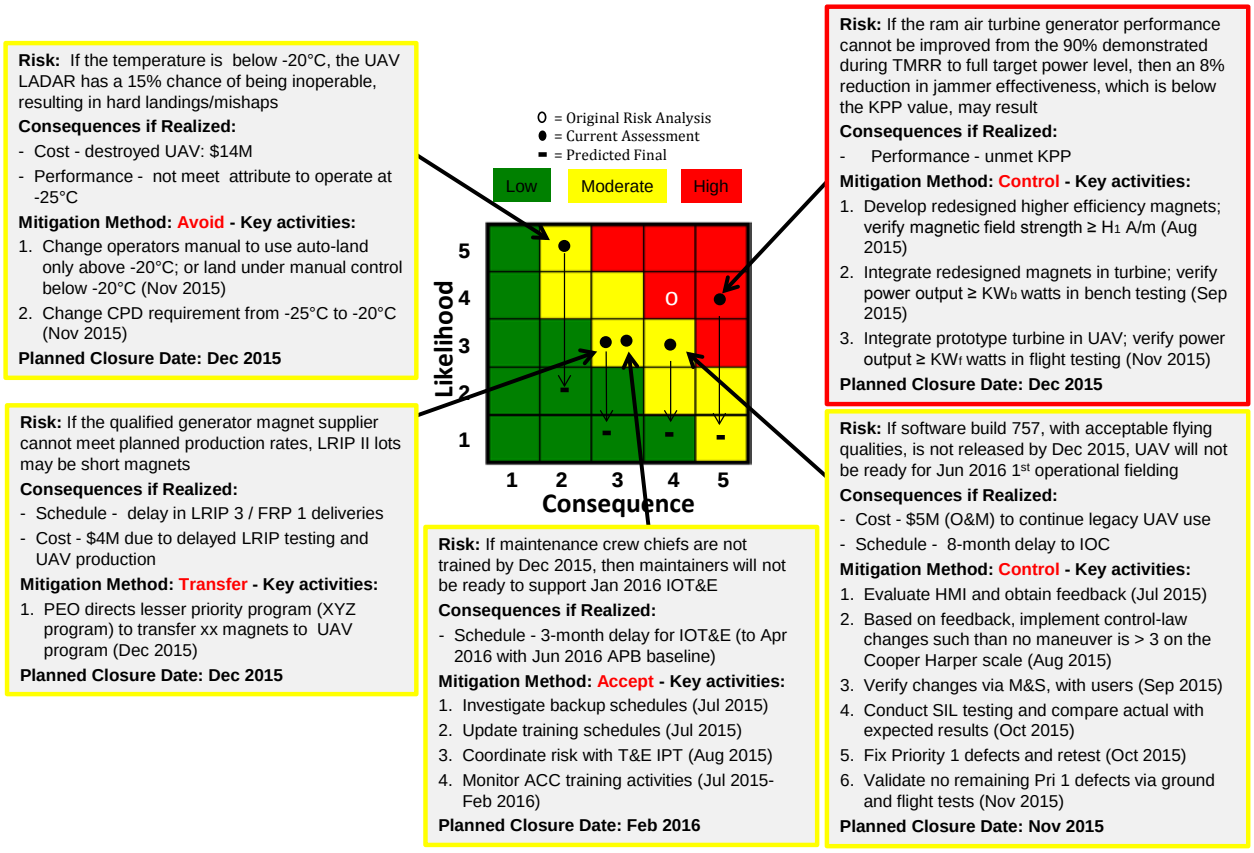


Figure C-3. Risk Reporting Chart

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.

This page is intentionally blank.

Glossary

accept (risk): acknowledge that a risk event or condition may be realized and the program may be willing to accept the consequences. **(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 PM. Business risks can come from areas such as program dependencies; resources (funding, people, facilities, suppliers, tools, etc.); priorities; regulations; stakeholders (user community, acquisition officials, etc.); market; and weather.

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

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.

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: event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (probability = 1).

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

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.

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 PM.

Program Protection Plan (PPP): a defense 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.

Program Risk Process (PRP): 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 document should address how often the PRP 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.

programmatic risks: non-technical risks that are generally within the control or influence of the PM 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: potential future event or condition 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 Board (RMB): a board chartered as the senior program group, usually chaired by the PM or deputy PM, that approves candidate risks and their causes. The board reviews and/or approves risk analysis results, risk mitigation plans and associated resources, and actual versus planned progress associated with implemented risk mitigation plans. It is an advisory board to the PM and provides a forum for all stakeholders and affected parties to discuss their concerns.

Risk Management Framework: the unified information and cybersecurity 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 mitigation plan: program's plan to mitigate an individual risk.

risk manager: program team member responsible for implementing the risk management process, updating the Program Risk Process (PRP), and assisting team members to identify and document candidate risks, develop risk analysis results, develop draft risk mitigation plans, include risk information in the risk register, develop risk reports, and 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 risk category, risk statement, likelihood, consequence, planned mitigation measures, the risk owner, WBS/IMS linkage, and, where applicable, expected closure dates and documentation of changes.

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, influence, or oversight over the success of a program or system. Stakeholders include the PM, 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.

This page is intentionally blank.

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
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

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
PRP	Program Risk Process
RFP	Request for Proposal
RMB	Risk Management Board
RDT&E	research, development, test, and evaluation
RIO	risk, issue, and opportunity
ROI	return on investment
ROMB	Risk and Opportunity Management Board
RWG	Risk Working Group
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
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/Portals/31/Documents/Policy/DCMA-PAM-200-1.pdf?ver=2016-12-28-125801-627

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

Directive-Type Memorandum (DTM) 17-001. Cybersecurity in the Defense Acquisition System. Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics, January 11, 2017. http://www.dtic.mil/whs/directives/corres/pdf/DTM-17-001.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].

IEEE 15288.2. IEEE Standard for Technical Reviews and Audits on Defense Programs, December 10, 2014. https://standards.ieee.org/findstds/standard/15288.2-2014.html

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/

International Organization for Standardization
http://www.iso.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

Risk Management Tools

Active Risk Manager. A commercial risk management tool adapted by the Department of the Air Force for use in the U.S. Air Force Enterprise Risk Management System.
http://www.activerisk.com/usaf

Project Recon. A software suite of tools that enables DoD organizations to capture, manage, and link program risks, issues, and opportunities, owned and maintained by TARDEC Systems Engineering.
https://projectrecon.army.mil/tardec/

Risk Exchange. A tool developed jointly by the Navy and a commercial entity, hosted and maintained by the Naval Systems Engineering Resource Center.
https://nserc.nswc.navy.mil/Pages/Welcome.aspx

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