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

September 2023

Office of the Executive Director for
Systems Engineering and Architecture

Office of the Under Secretary of Defense
for Research and Engineering

Washington, D.C.

Distribution Statement A. Approved for public release. Distribution is unlimited.

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

Office of the Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301-3030
osd-sea@mail.mil
https://www.cto.mil/sea/

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 23-S-3231

Approved by

Principal Deputy Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
September 2023

Risk, Issue, and Opportunity (RIO) Management Guide Change Record

Date	Version	Remarks
January 2017	1	Approved for public release.
September 2023	2	Included a new section on Adaptive Acquisition Framework (AAF) pathways (Section 5). Added Appendix A information on: • Other risk management methods • Software engineering considerations in RIO management • Digital engineering considerations in RIO management • Independent Technical Risk Assessment (ITRA) considerations in RIO management Updated references.
October 2023	2.1	Administrative change: Revised change record table and Section 2 footer.

This page is intentionally blank.

CONTENTS

Preface 1
1 Introduction 3
1.1 Purpose 3
1.2 Scope 4
1.3 Risk Management Overview 5
2 Risk and Issue Management 7
2.1 Risk Management Process Planning 8
2.2 Risk Identification 9
2.2.1 Risk Identification Methodologies 9
2.2.2 Risk Categories 12
2.2.3 Risk Statement 13
2.3 Risk Analysis 14
2.3.1 Consequence 15
2.3.2 Likelihood 17
2.3.3 Risk Reporting and Prioritization 18
2.3.4 Risk Register 21
2.4 Risk Mitigation 24
2.4.1 Risk Acceptance 25
2.4.2 Risk Avoidance 26
2.4.3 Risk Transfer 26
2.4.4 Risk Control 27
2.4.5 Risk Burn-Down 28
2.5 Risk Monitoring 30
2.6 Issue Management 34
3 Opportunity Management 37
4 Management of Cross-Program Risks 43
5 Managing Risk by Adaptive Acquisition Framework Pathway 48
5.1 Overview of Adaptive Acquisition Framework 48
5.2 Managing Risk for Urgent Capability Acquisition (UCA) Pathway 49
5.2.1 UCA Pre-Development Phase 49
5.2.2 UCA Development Phase 50
5.2.3 UCA Production and Deployment Phase 51
5.2.4 UCA Operations and Support Phase 52
5.3 Managing Risk for Middle Tier of Acquisition (MTA) Pathway 54
5.3.1 MTA Rapid Prototyping Path 54
5.3.2 MTA Rapid Fielding Path 56
5.4 Managing Risk for Major Capability Acquisition (MCA) Pathway 57
5.4.1 MCA Planning Considerations 57

5.4.2 MCA Pre-Materiel Development Decision Phase 60
5.4.3 MCA Materiel Solution Analysis Phase 60
5.4.4 MCA Technology Maturation and Risk Reduction Phase 63
5.4.5 MCA Engineering and Manufacturing Development Phase 66
5.4.6 MCA Production and Deployment Phase 67
5.4.7 MCA Operations and Support Phase 68

5.5 Managing Risk for Operation of Software Acquisition Pathway 68

5.5.1 Software Planning Phase 69
5.5.2 Software Execution Phase 74
5.5.3 Software Risk Reduction 78

5.6 Managing Risk for Defense Business Systems (DBS) Acquisition Pathway 80

5.6.1 DBS Capability Need Identification Phase 81
5.6.2 DBS Solution Analysis Phase 82
5.6.3 DBS Functional Requirements and Acquisition Planning Phase 82
5.6.4 DBS Acquisition, Testing, and Deployment Phase 83
5.6.5 DBS Capability Support Phase 84

5.7 Managing Risk for Acquisition of Services Pathway 85

5.7.1 Acquisition of Services Planning Phase 85
5.7.2 Acquisition of Services Development Phase 86
5.7.3 Acquisition of Services Execution Phase 88

Appendix A. Additional Methods and Considerations for Managing Risk in Defense Programs 90

Appendix B. Program Risk Management Process and Roles 106

Appendix C. Risk Management in Relation to Other Program Management and Systems Engineering Tools 117

Appendix D. Risk Management Process Implementation Example 125

Glossary 130

Acronyms 136

References 141

TABLES

Table 2-1. Sample Consequence Criteria for Major Capability Acquisition (MCA) Pathway 16

Table 2-2. Typical Likelihood Criteria 17

Table 2-3. Weighted Consequence Risk Mitigation 20

Table 2-4. Risk Register Excerpt 23

Table 3-1. Sample Opportunity Register 41

Table 4-1. Sample Table of Required MOAs 44

Table A-1. Comparison of Traditional and Agile Approaches on Vignette Risks 97

Table C-1. Sample 14-Point Schedule Health Assessment Metrics and Status 120

FIGURES

Figure 1-1. Overview of Potential Sources of Program Risks, Issues, and Opportunities 3
Figure 2-1. Risk and Issue Management Process Overview 7
Figure 2-2. Risk Management Process Planning 8
Figure 2-3. Risk Identification 12
Figure 2-4. Risk Analysis 15
Figure 2-5. Risk Reporting Matrix and Criteria 19
Figure 2-6. Risk Matrix Showing Prioritized Results 21
Figure 2-7. Risk Mitigation 24
Figure 2-8. Risk Burn-Down 29
Figure 2-9. Risk Monitoring 31
Figure 2-10. Example Risk Monitoring and Trend Matrix 32
Figure 2-11. Suggested Risk Reporting Format 33
Figure 2-12. Issue Management Process 34
Figure 2-13. Issue Consequence Reporting Matrix 35
Figure 3-1. Opportunities Help Deliver Should-Cost Objectives 37
Figure 3-2. Opportunity Management Process 38
Figure 4-1. Sample Synchronization from the SEP Outline 45
Figure 4-2. Tracking Interdependency Risks 46
Figure 5-1. Adaptive Acquisition Framework (AAF) 48
Figure 5-2. Urgent Capability Acquisition Pathway 49
Figure 5-3. Middle Tier of Acquisition Pathway 54
Figure 5-4. DoD MCA Life Cycle 58
Figure 5-5. MCA Materiel Solution Analysis Phase Activities 61
Figure 5-6. MCA Technology Maturation and Risk Reduction Phase Activities 64
Figure 5-7. MCA Engineering and Manufacturing Development Phase Activities 66
Figure 5-8. MCA Production and Deployment Phase Activities 67
Figure 5-9. Life Cycle View of Software Acquisition Pathway 69
Figure 5-10. Business Capability Acquisition Life Cycle 81
Figure 5-11. Seven Steps to the Services Acquisition Process 85
Figure A-1. DevSecOps Life Cycle and Generic Agile Process 93
Figure A-2. Integrating RIO Management with Agile and DevSecOps 95
Figure A-3. Unwanted Technology Transfer Mechanisms 104
Figure B-1. Government and Contractor Joint Risk Management Boards 109
Figure B-2. Roles and Responsibilities Tiering 111

Figure C-1. Example of WBS Levels 118
Figure C-2. Government and Contractor WBS Relationship..... 118
Figure C-3. IMP/IMS Creation and Implementation 119
Figure D-1. Risk Matrix for Ram Air Turbine Generator..... 126
Figure D-2. Risk Burn-Down Diagram for Option A 128
Figure D-3. Risk Reporting Chart..... 129

Preface

This guide is one of several Department of Defense (DoD) policy and guidance documents that address the Department's focus on risk management. This guide builds from and supersedes the *DoD Risk, Issue, and Opportunity (RIO) Management Guide* of 2017 but includes revisions to emphasize RIO management for the DoD Adaptive Acquisition Framework (AAF) pathways (see DoD Instruction (DoDI) 5000.02).

DoD policy, regulation, and statute identify 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 solutions. This approach aims to manage uncertainty and increase predictable outcomes in delivering capability to the warfighter.

Risk management is an integral part of program planning and execution regardless of the acquisition pathway the program uses to acquire a system, product, or service. The PM and Lead Systems Engineer (LSE) are the program members primarily responsible for leading risk management. A PM must align risk tolerance with organizational capacity to manage risks and must allocate resources to the best effect. Risk management principles addressed in this document echo the time-proven 1986 Packard Commission recommendations.

This guide describes strategies and processes for RIO management that a program should begin early in development and reevaluate, revise, and reapply throughout the acquisition life cycle. Each program should tailor the practices and avoid adding a process that does not add value. Identifying the program's key uncertainties and challenges early can help inform decisions on the basic program structure and the activities needed to enable the program to deliver the intended product or services successfully and efficiently.

Although this guide focuses primarily on the Government program office, industry plays a central role in the management necessary to deliver acquisition products and services. Government and industry may differ in the prioritization of risks, in part because of differing perspectives or incentives. For example, 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 performance objectives, 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 a program manages risks and issues by developing plans to reduce the consequences and/or the likelihood of the risks or issues.

Section 3: Describes opportunity management, including the similarities and differences between opportunity and risk management.

Section 4: 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.

Section 5: Describes how risk informs the decisions shaping a program Acquisition Strategy and structure, and the most important activities to manage risk by AAF acquisition pathway.

The appendices provide information on additional methods and considerations for managing risk, roles and responsibilities, integrating risk management with other roles and tools, and illustrative vignettes.

Text boxes highlight expectations 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. Managing these areas requires strategic thinking and begins with early decisions about 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 purpose of this guide, the terms *risk, issue,* and *opportunity* are defined as follows:

- A **risk** is a potential future event or condition that may have a negative effect on achieving program objectives for cost, schedule, and performance. A risk is defined by (1) the likelihood that an undesired event or condition will occur and (2) the consequences, impact, or severity of the undesired event, were it to occur.
- An **issue** is an event or condition with negative effect that has occurred (such as a realized risk) or is certain to occur (likelihood of 5) that should be addressed.
- An **opportunity** offers potential future benefits to the program's cost, schedule, 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.

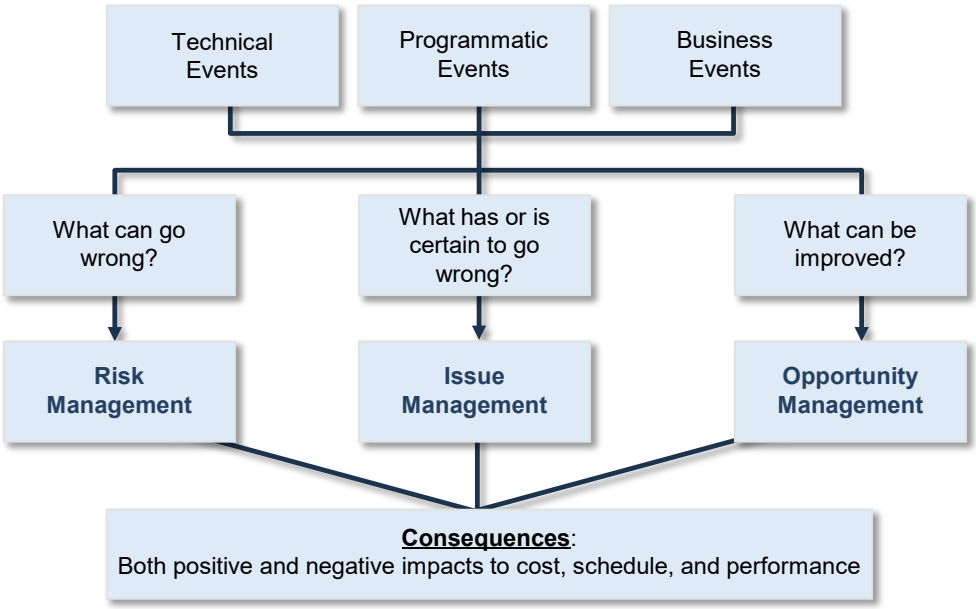


Figure 1-1. Overview of Potential Sources of Program Risks, Issues, and Opportunities

This guide should be used in conjunction with DoDI 5000.02, "Operation of the Adaptive Acquisition Framework"; Military Department guidance; and related direction.

1.2 Scope

DoD distinguishes statute and mandatory policy from recommended guidance. This document serves solely as guidance and not as a mandatory checklist. It reflects experience from numerous DoD programs and suggests risk considerations and mitigation that programs should keep in mind when developing an Acquisition Strategy and program structure.

This guidance is intended primarily for PMs and their staff. This guide includes a strategic consideration of how risk shapes program structure and content, as well as a suggested process to manage risks by phase. The process is designed to produce risk mitigation plans, which provide the substantive steps a program will take to mitigate its individual risks. This guide uses the term "risk mitigation plan" to refer to the plans a program initially summarizes in the Acquisition Strategy and updates as the program continues to identify and manage risks.

This guide uses the term "Program Risk Management Process (PRMP)" to refer to how the program will describe and execute its RIO processes. The term PRMP is not mandatory but is a suggestion to distinguish process documentation from descriptions of risk mitigation plans.

This guide does not attempt to address, in detail, specific requirements to prevent and manage risks related to any functional areas such as system safety or system hazards, including environment, safety, and occupational health (ESOH) hazards and ESOH domain hazards, or risks identified in their respective plans. The reader should refer to guidance including the following for specific areas: DoDI 5000.88, "Engineering of Defense Systems"; MIL-STD-882, "Standard Practice for System Safety"; DoDI 5000.95, "Human Systems Integration in Defense Acquisition"; and the Human Systems Integration (HSI) Guidebook (2022). Note that all HSI domain processes and results help identify risks, issues, and opportunities from legacy systems associated with mishaps, near-misses, safety investigations, and accidents.

Programs should refer to DoDI 8500.01, "Cybersecurity" and DoDI 8510.01, "Risk Management Framework (RMF) for DoD Systems," for policy and procedures regarding the enterprise-wide structure for cybersecurity risk management. Appendix A of this guide presents an overview of the RMF for DoD Systems and Cyber Table Top (CTT) risk assessment as examples of specialized cybersecurity risk management methods.

Programs should develop a method to map specialized cybersecurity risks and issues into their management processes and should evaluate cost, schedule, and performance risks associated with implementing cybersecurity requirements and testing. CTTs can help identify cybersecurity risks in support of engineering and test. Those CTT findings can inform the program evaluation of risk in implementing cyber within the system.

Using the DoD Instructions 5000.83, "Technology and Program Protection to Maintain Technological Advantage," and 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," programs should consider program protection and cybersecurity in technical risk management activities to address risk identification, analysis, mitigation planning, mitigation implementation, and tracking. Many programs apply processes, tasks, and activities intended to avoid, reduce, and mitigate risks as part of risk management. Programs must ensure that the applied processes, tasks, and activities reduce uncertainty through rigor or achieve intended outcomes despite uncertainty.

For the specialized risk induced by electromagnetic spectrum (EMS) supportability and compatibility (EMC), programs should refer to DoDI 4650.01, "Policy and Procedures for Management and Use of the Electromagnetic Spectrum" for information regarding the creation and maintenance of a spectrum supportability risk assessment (SSRA) EMS-dependent systems; and DoDI 3222.03, "DoD Electromagnetic Environmental Effects (E3) Program," for the policy and procedures for conducting an E3 assessment to ensure EMS-dependent system, subsystem, and platform EMC. SSRA and E3 assessments can be conducted in parallel and should be included in a program's overall risk assessment. SSRAs are required to identify a system, subsystem, or platform's spectrum supportability requirement to ensure sufficient spectrum access to support its operation throughout its life cycle. E3 assessments are mandated to ensure EMS-dependent platforms, systems, subsystems, and equipment will be compatible in their intended electromagnetic environments (EMEs) without causing or suffering unacceptable mission degradation due to E3, and will comply with applicable EMS requirements.

1.3 Risk Management Overview

The PM is ultimately responsible for implementing risk management within program constraints. Successful risk management requires planning and resourcing, and should be implemented early in the life cycle based on 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 multiple disciplines, including systems engineering, 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.

A successful risk management program relies on a disciplined process executed by people with relevant product knowledge, experience and resolve to identify and address the risks that may 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 EVM, independent technical risk assessments, an independent cost estimate, and the tenacity to pull on the threads that reveal problems all contribute to prospects for success.

Although the processes described in this 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 risks and issues in all phases of the life cycle, and across all adaptive acquisition framework pathways. The specific actions for each step typically will differ depending on the program phase and on 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, document, and implement an appropriate, tailored risk management process. The process should address planning, identification, analysis, mitigation, and monitoring of risks and issues. Section 2 provides more detail regarding establishing the process.

2 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 commonly characterized by likelihood 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., will become issues) and should put plans and resources in place early to mitigate the consequences. The program should consider modifying the existing baseline program plan, planning for alternate solutions or approaches, providing backup capabilities or future upgrades to address the consequences of pending issues.

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 future certain 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 2-1 illustrates a suggested five-step management process that may be applied to a discrete risk or issue.

Figure 2-1. Risk and Issue Management Process Overview

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 2.1–2.5 further discuss risks. Selected aspects of the discussion also may apply to issues, discussed specifically in Section 2.6.

2.1 Risk Management Process Planning

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

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

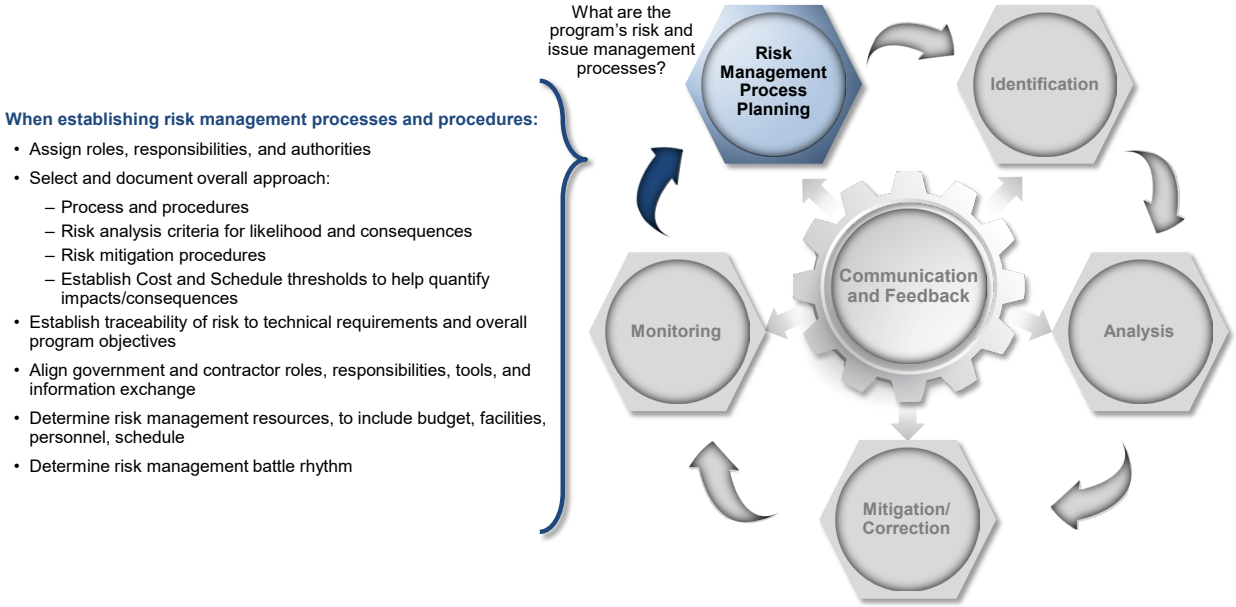


Figure 2-2. Risk Management Process Planning

Appendix B provides additional information on establishing a risk management planning process.

2.2 Risk Identification

A program identifies risks by answering such questions as *What can go wrong?* or *What is particularly difficult in this program development? What information is lacking?* 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 2.4.

Government and contractor program personnel should identify candidate risks at any time and throughout a program's life cycle. For example, a common source of risk is insufficient margin against failure in the nominal (combat or use) environment. Government personnel have a responsibility to thoroughly understand and independently assess technical risks to inform the program's structure and resourcing.

The PM should appoint a trained risk manager to oversee the risk management process. The risk manager, in a supportive role, is responsible for examining and compiling the identified risks in a risk register (see Section 2.3.4) and summarizing them at a manageable level of detail.

2.2.1 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 or service to be created or delivered and the requirements shaping the product or service. The program should then structure the Acquisition Strategy to mitigate identified key risks (those the program deems to present the greatest likelihood and impact).

One approach is to review source documents, analyze a reference design and mission profile, and engage 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 Joint Capabilities Integration and Development System (JCIDS) documents, Government technical requirements and specification documents, SSRA, Analysis of Alternatives (AoA) products, Technology Readiness Assessments (TRAs), evaluation frameworks, test and evaluation results, 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 impact in a later phase. Programs should review the planning documents

(e.g., Acquisition Strategy (AS), SEP, Test and Evaluation Master Plan (TEMP), Integrated Master Schedule (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 Key Performance Parameters (KPPs) and Key System Attributes (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 and tactics to inquiry, examination, or analysis to identify technical, programmatic, and business risks:

- Interviews with program team leads, subject matter experts (SMEs), and 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 Request for Proposals (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 (SETRs) during Technology Maturation and Risk Reduction (TMRR) and Engineering and Manufacturing Development (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, 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 (HSI), reliability, supportability/sustainment, and security
- Use of other leading indicators that may provide earlier indications of risks.
- Independent assessments such as Red Teams, Non-Advocate Reviews, Independent Technical Risk Assessment (ITRAs), Nunn-McCurdy Reviews, Critical Change Reviews, and Independent Cost Estimates.
- Analysis of metric trends (KPPs, KSAs, Technical Performance Measures (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
  - Availability of industrial base, labor market, and supply/material
- Mitigating unwanted technology transfer to competitors or adversaries
- 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 Ilities (RI3) (2008) is one example of a top-level risk identification approach combined with a lower-level approach. The approach combines top-level key processes with topics (e.g., design maturity and stability) and associated trigger questions (a lower-level approach of structured inquiry).

Figure 2-3 cites a few methods for identifying program risks. See also Sections 5 and Appendix A for additional considerations in identifying risks throughout the life cycle.

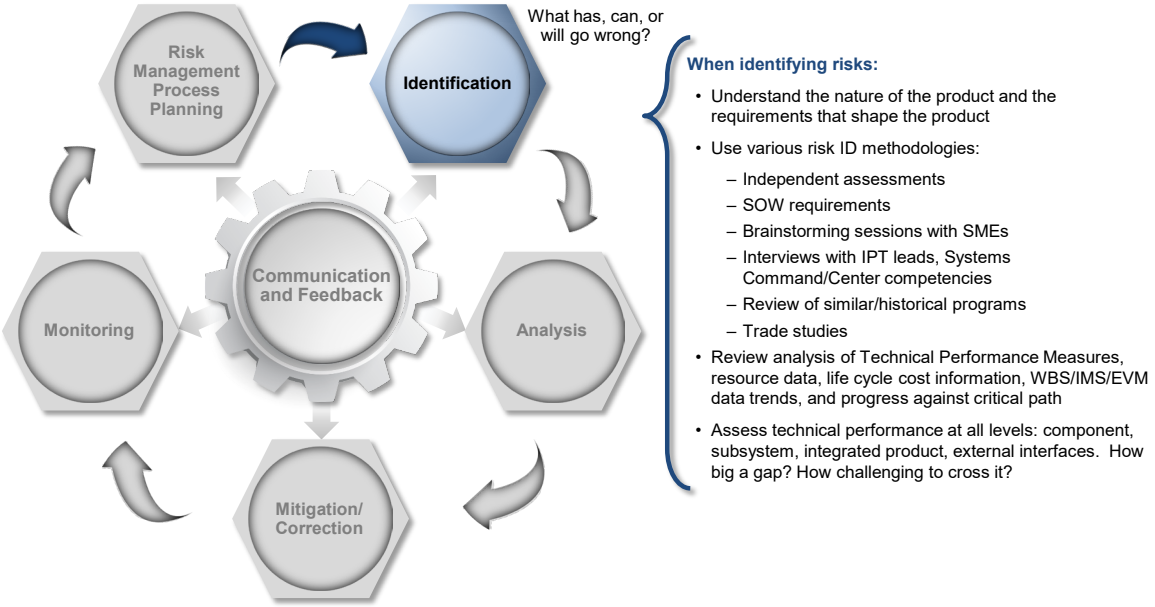


Figure 2-3. Risk Identification

2.2.2 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, 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 or 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.

  - 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.

Often a risk may span multiple categories. For example, the underlying cause of the risk may be of a technical nature, and the program's technical deficiencies can create cost and schedule risks. PMs should focus Government and contractor efforts on risks over which they have or can influence control and also should 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.

2.2.3 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 for 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.

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.

The program should use management actions and the engineering process to address candidate risks that can be handled without raising them to the risk management process (e.g., add a paragraph to an RFP). 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.

2.3 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 for each risk.
- Once all identified risks have risk levels, prioritize risks for mitigation.

Risk analysis provides an estimate of each risk's likelihood and consequence, and the resulting risk level, to allow the program 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 to analyze and estimate the impact of risks.

Although 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. If quantitative risk data such as dollars for cost, time for schedule, or mission loss for performance is available, it can be used in place of qualitative scoring. To efficiently accomplish this step, the team may consider working from the impact or consequence first. Figure 2-4 depicts how risks should be analyzed and what impact areas to quantify.

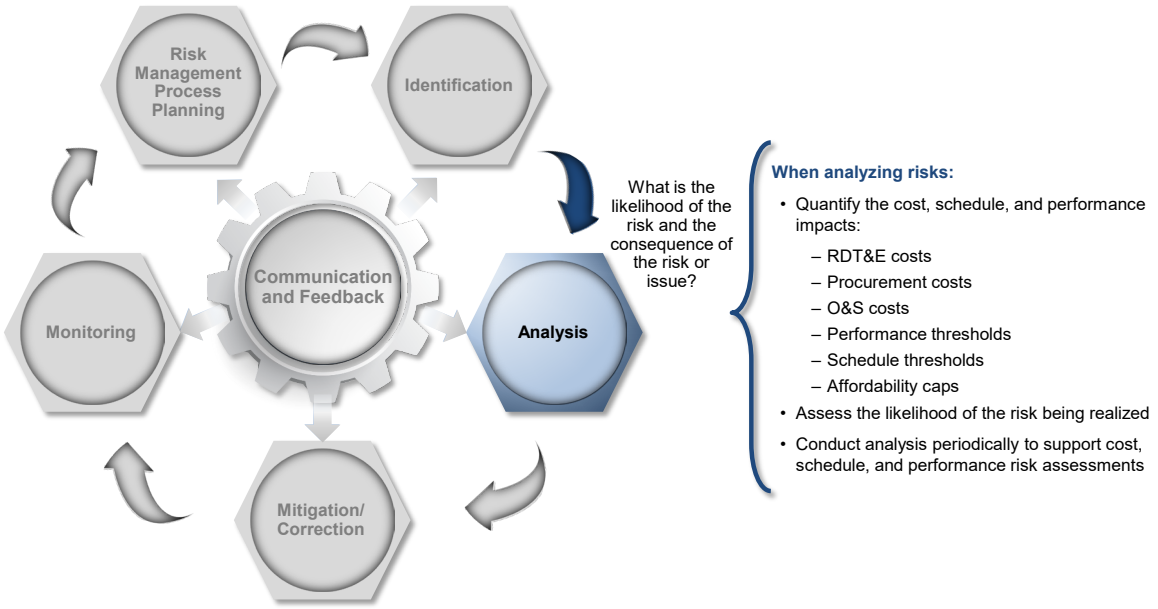


Figure 2-4. Risk Analysis

The following subsections address risk analysis using qualitative consequence (Section 2.3.1) and likelihood (Section 2.3.2) scales plus a standard risk matrix (Section 2.3.3) to convert likelihood and consequence values to relative risk levels.

2.3.1 Consequence

During analysis, each risk should be evaluated in terms of impact to the program (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 at times will have different perspectives on risks and priorities, they should seek a common framework for consequence and likelihood criteria.

Programs may need to tailor criteria based on program-specific circumstances; however, they 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 or Acquisition Program Baseline (APB) threshold should trigger a Level 5 performance consequence rating (see Table 2-1). 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, including program-specific dollar and schedule thresholds, in program planning documents such as the SEP and PRMP document.

Table 2-1 lists sample multiple criteria for programs to consider when assessing cost, schedule, and performance consequences for the Major Capability Acquisition (MCA) pathway. Programs should develop tailored, simplified criteria to assess cost, schedule, and performance consequences for other AAF pathways described in Section 5 of this guide as needed.

Table 2-1. Sample Consequence Criteria for Major Capability Acquisition (MCA) Pathway

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 rebaseline. 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 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-systems 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 has an impact on 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-systems 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.

[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 no meeting a KPP or KSA.

Acronyms: 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, and Evaluation; SETR: Systems Engineering Technical Review; 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). By formulating the technical risk as design margin against failure in environments, the solution becomes restoration of margin by way of more robust design or recognition of excessive conditions and defining acceptable losses as part of a system solution. 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 activities. 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 should a program extension be required.

2.3.2 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 2-2 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. Some programs may determine the likelihood is more accurately represented with a greater or lesser percentage range for the probability of occurrence.

Table 2-2. 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 likelihood 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 likelihood level is too high and would preclude proceeding on a planned course of action (COA). Depending on the circumstances, there may be cases in which a risk (likelihood and consequence) is high enough to change course, in the absence of assured mitigation. Quantification of risk should include the design margins and redundancy

intended for reliability. All systems will fail eventually when they age out, so the risks are for failures before end of life.

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. Having multiple risks may jeopardize the program more than one individual risk because of increased complexity, extended resources, risk interactions, or the aggregate likelihood of realizing risk. Monte Carlo methods such as those used in a schedule risk analysis (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. Likelihood assessment should consider the life cycle phase of the program and future planned program activities. Where available, historical data should be used to determine expected risk reduction or performance improvements from planned engineering, test, or other activities.

Note: The consequence and likelihood level values given in Tables 2-1 and 2-2 are ordinal (1 through 5). Programs should avoid fractional consequence and likelihood scoring (e.g., a likelihood score of 2.4), which incorrectly implies increased fidelity in the assessment and comparisons.

➢ ***Expectations***

- 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 probability = 1 (or approaching 1), the program addresses the event or condition as an issue rather than a risk (see Section 2-6).

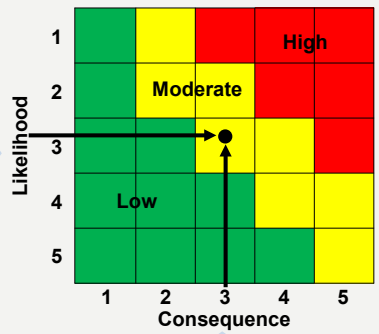
2.3.3 Risk Reporting and Prioritization

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 (many tools are commercially available that may be used by programs for integrating risk management, risk prioritization, and risk reporting). This characterization also aids in prioritizing risks for risk mitigation (see Section 2.4).

Once the analysis of likelihood and consequence is complete, program teams could then use the risk matrix shown in the upper right corner of Figure 2-5. 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.

Although these values are used to define the risk level (e.g., low, moderate, high), programs should consider additional factors 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.

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



Level	Cost	Schedule	Performance
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

Figure 2-5. 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 2-3, 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. ROI may be expressed as a percentage or ratio.)

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 2-3. 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**	**$26.4M**	**$ 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 2-6.

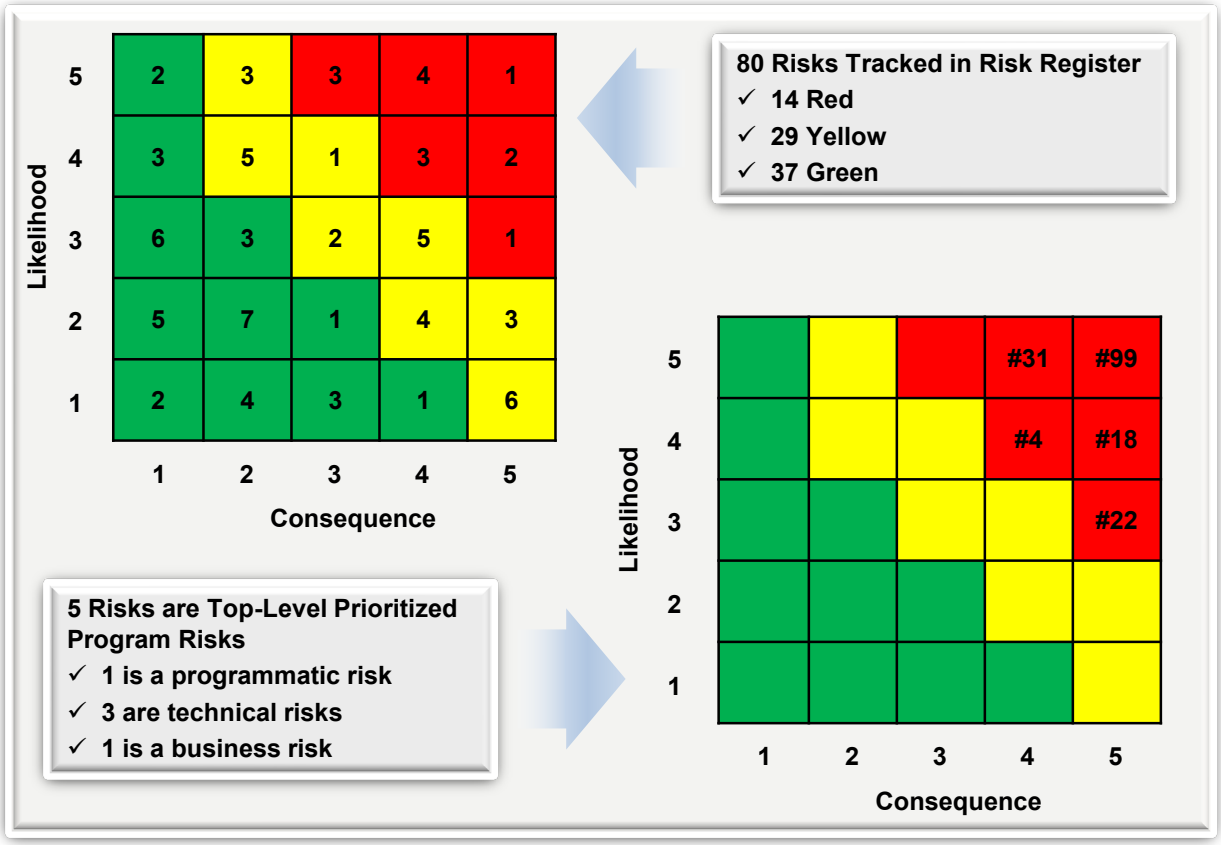


Figure 2-6. Risk Matrix Showing Prioritized Results

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.

2.3.4 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 2-4 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. The risk event may be described as an If-Then statement and the register may also include root cause information.

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 PRMP document, can provide valuable insight for future program development.

Table 2-4. 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

2.4 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?* After analyzing the risks, program personnel should develop a strategy to manage risks by evaluating the four risk mitigation options: *accept, avoid, transfer,* or *control.* 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 details 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 2-7 highlights key aspects of risk mitigation.

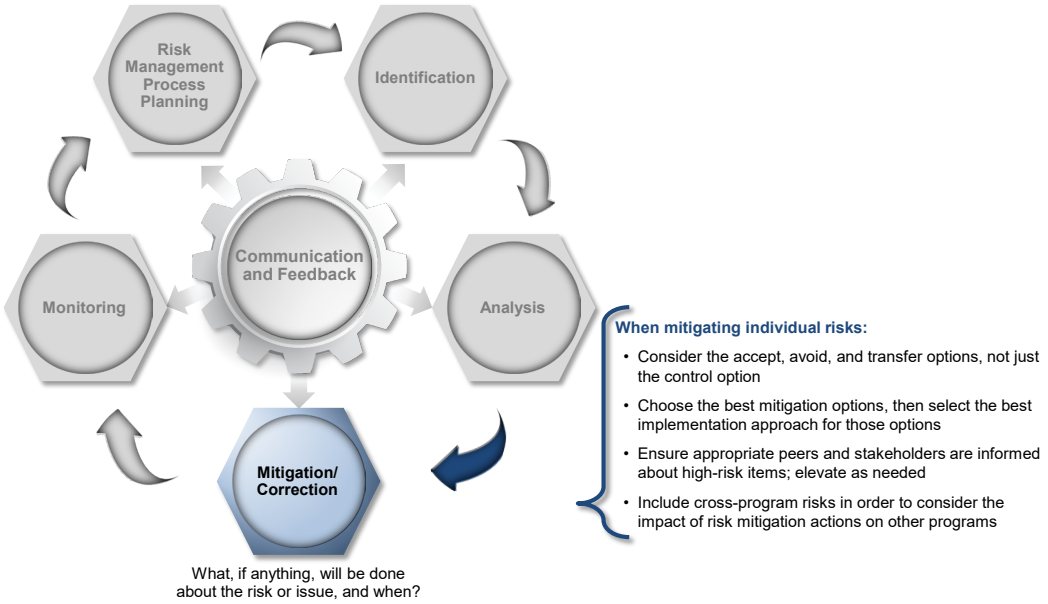


Figure 2-7. Risk Mitigation

The system design should incorporate features that provide resiliency, such as safety margins, growth provisions, modularity, cybersecurity, electromagnetic protection (EP), 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. The feasibility and commitment of resources to the mitigation plan should be objectively assessed when determining likelihood. In some cases, a mitigation plan may not be fully resourced and may not be feasible to complete by the time needed. Best practices for successful mitigation include development of an executable set of activities with technically feasible objectives, incorporating risk reduction activities into the baseline IMS, proofs of concept or early prototype demonstrations, contingency planning (alternate designs or alternate suppliers), and full commitment of funding and staff resources.

2.4.1 Risk Acceptance

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, so many programs call this a “Watch Item.”

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.

2.4.2 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, 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; however, “simple” changes need to be examined to determine why they were not incorporated into the original design solution.

2.4.3 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. This mitigation option is the most difficult to implement because it requires an entity outside the control of the program team to accept that risk and work it independently. Teams should consider a formal agreement (i.e., Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU)), when doing this to ensure both organizations understand their responsibilities and obligations.

While financial risk may be substantially transferred by certain contractual arrangements or interprogram 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.

2.4.4 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 5 discusses activities to reduce risk exposure by acquisition pathway. 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 science and technology (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 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), 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 C explains how to integrate risk mitigation activities with other program management tools such as the WBS, IMS, and EVM.

2.4.5 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, using realistic and logical schedule precedence, typically 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 threshold 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 2-8 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.

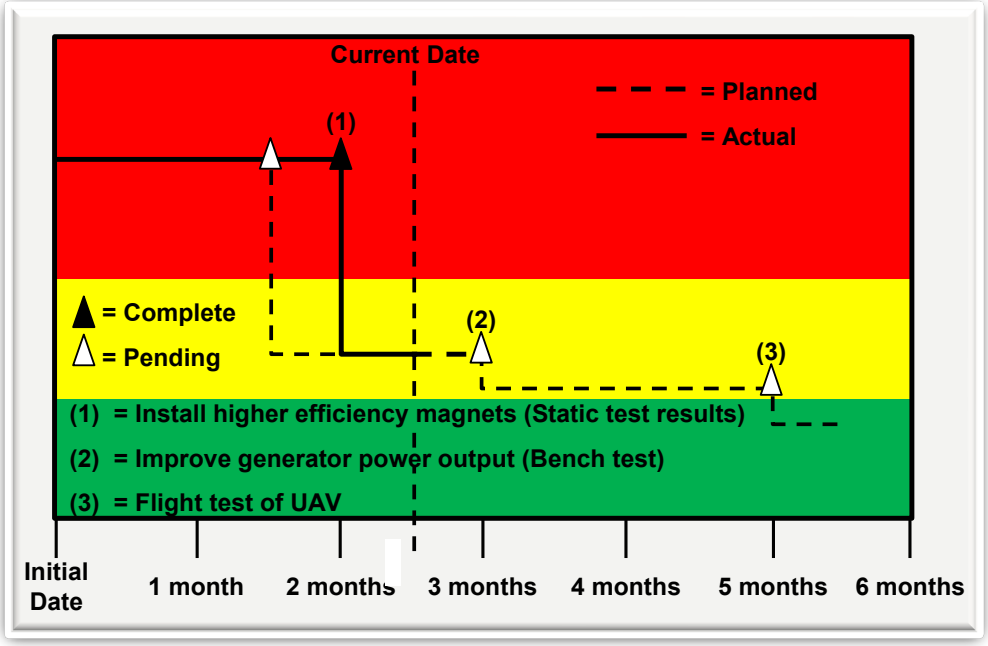


Figure 2-8. Risk Burn-Down

➢ ***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.
    - 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.

2.5 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 2-8, 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 and analysis report, 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 2-9 highlights selected components of risk monitoring. Risk monitoring allows timely actions to address potential problems.

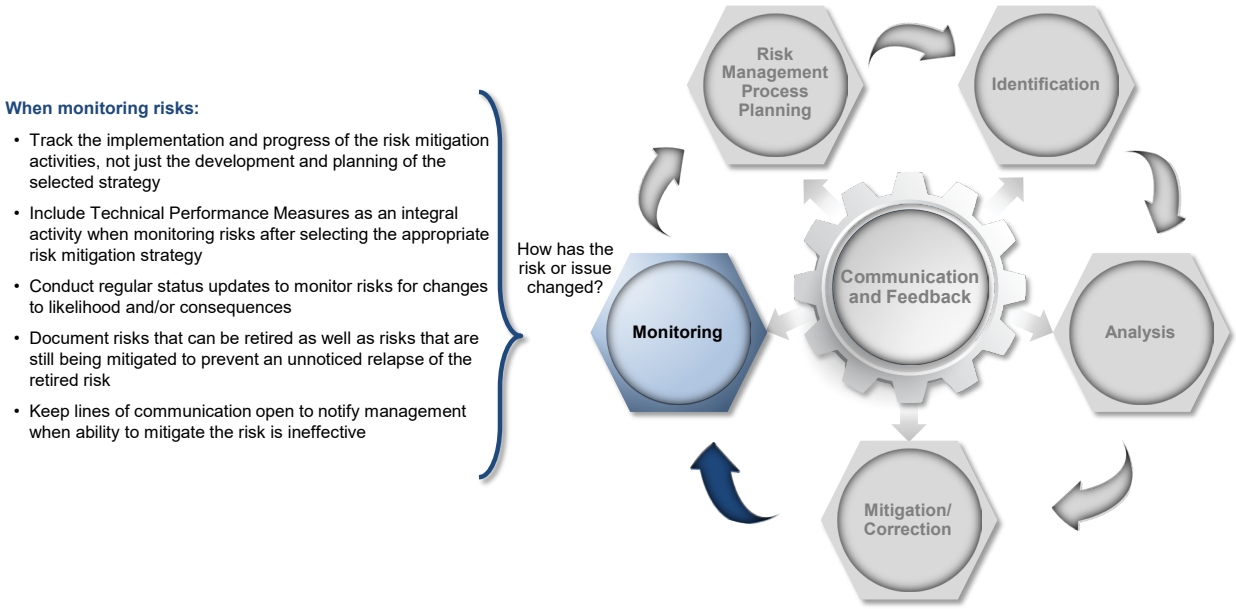


Figure 2-9. Risk Monitoring

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 and 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 2-10 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.

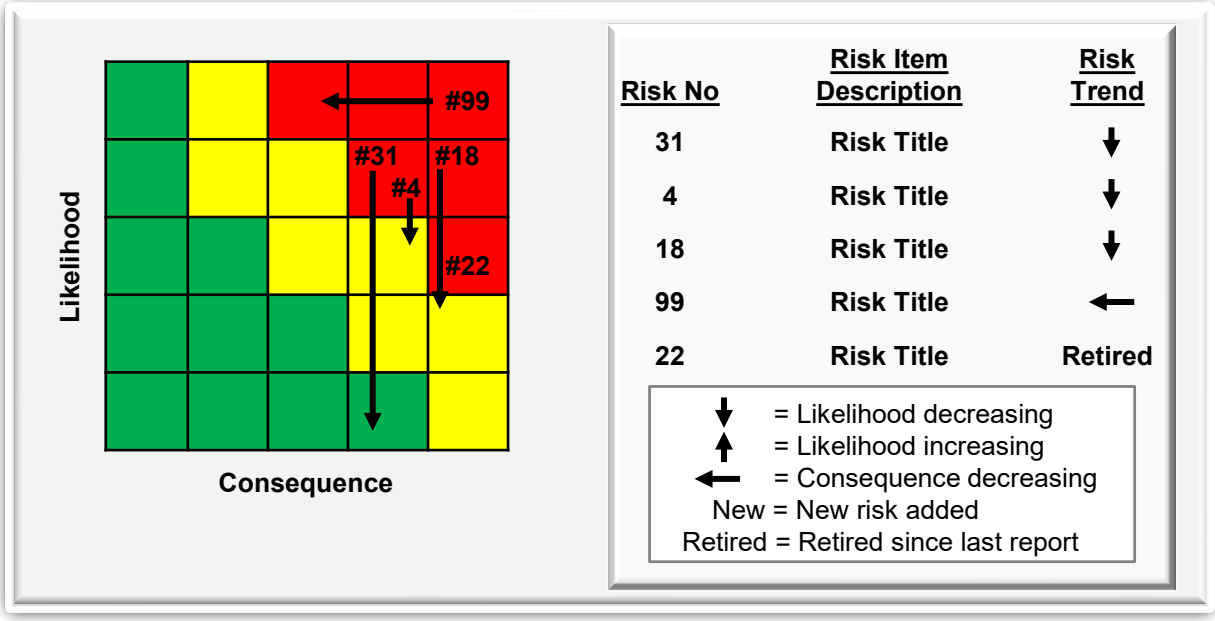


Figure 2-10. Example Risk Monitoring and Trend Matrix

The program should establish an effective means to display the current risk status and burn-down progress. Figure 2-11 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, is trending negatively, or has evolved into an issue.

Appendix D contains an example of a hypothetical risk that applies the risk management processes discussed in this chapter.

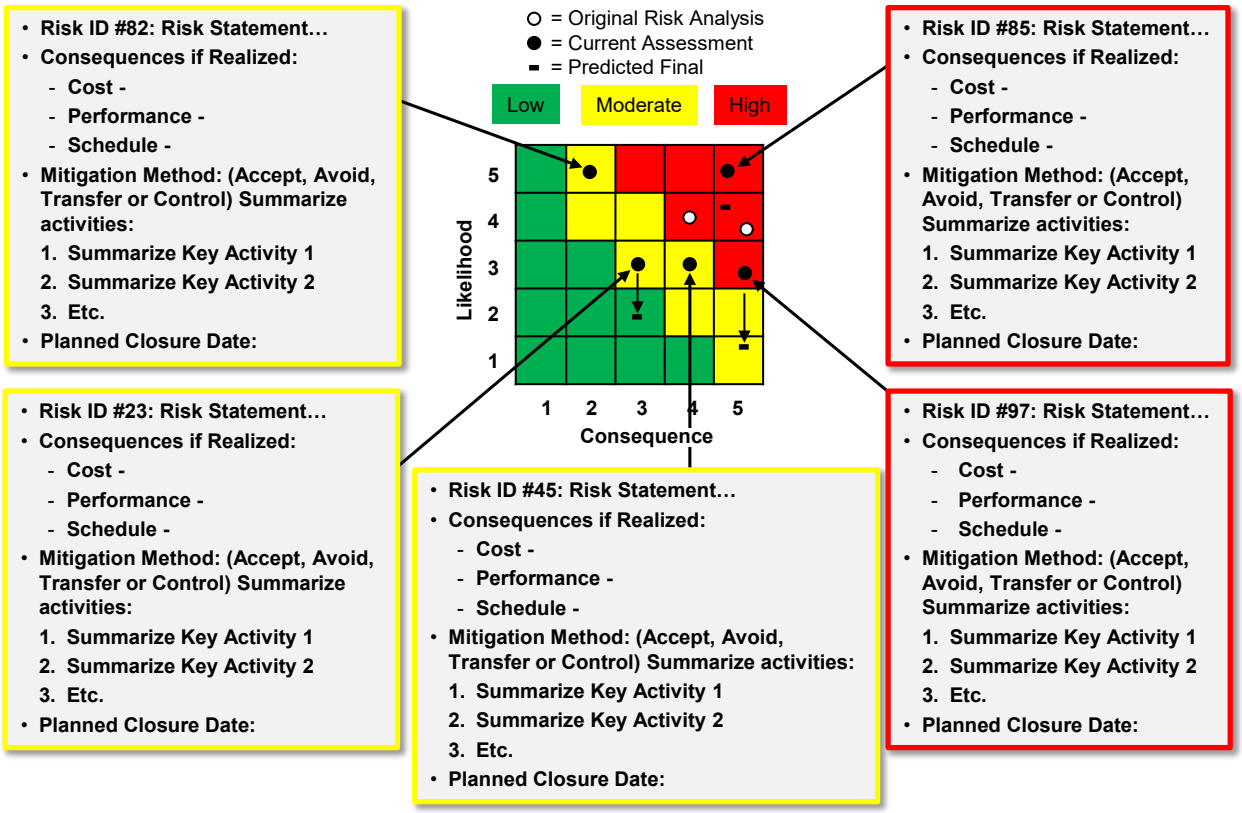


Figure 2-11. Suggested Risk Reporting Format

➢ ***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.

2.6 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 likelihood, 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 2-12 displays the issue management process.

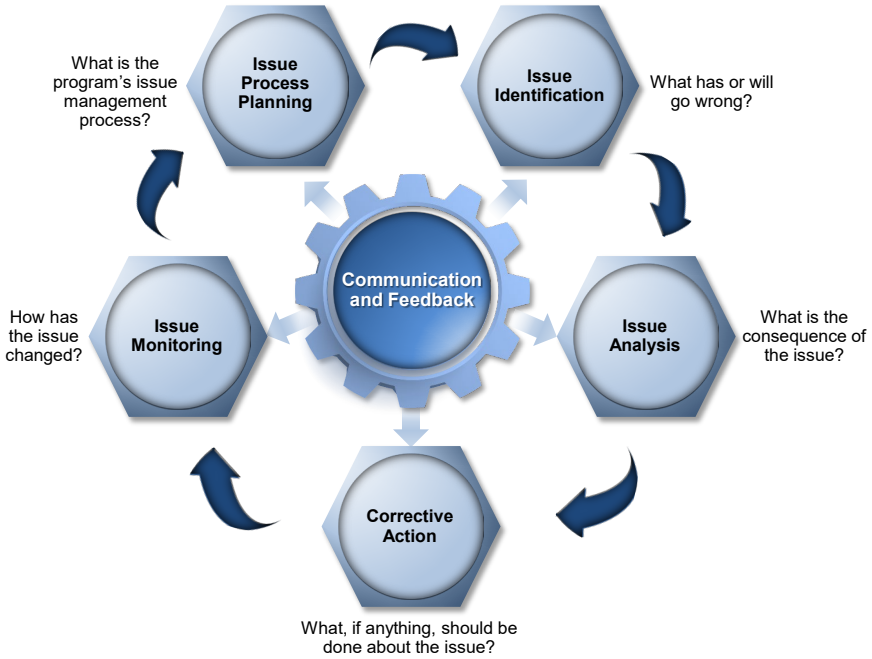


Figure 2-12. Issue Management Process

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 to 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&Ms)) 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 in Figure 2-5, the issue consequence value is converted to an issue level using an issue reporting matrix like the one in Figure 2-13, 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.

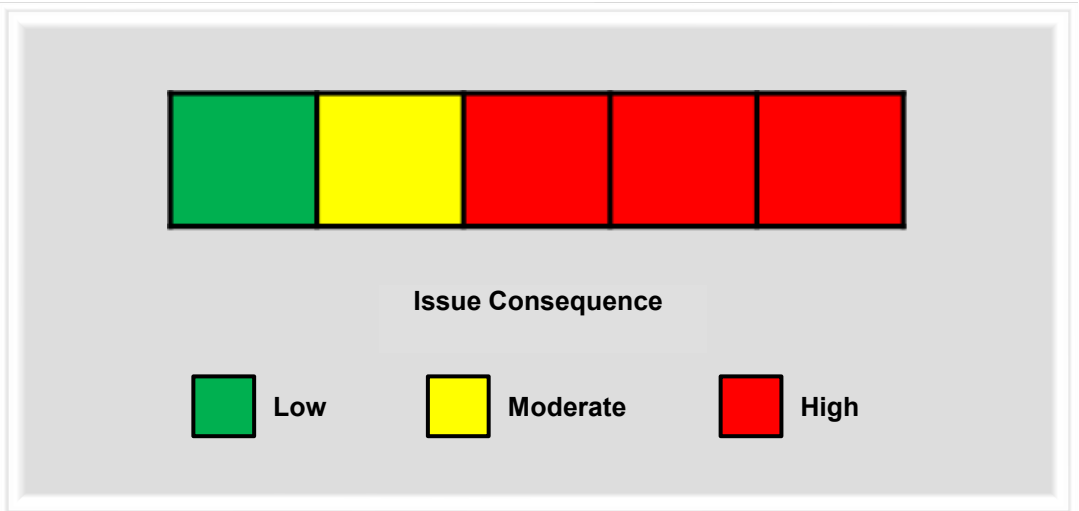


Figure 2-13. Issue Consequence Reporting Matrix

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 have or should have already been taken, so a plan would be in place before the issue occurs. This is particularly the expectation for an antecedent risk with a high likelihood and is consistent with the recognized continuum of risk to issue as likelihood increases.

Less common options include Avoid and Transfer, which carry the same definitions for issues as they do for risks (see sections 2.4.2 and 2.4.3). 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 2-12); (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 or issue register.

➢ ***Expectations***

- As the likelihood 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 PRMP. 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.

3 OPPORTUNITY MANAGEMENT

Opportunities are potential future benefits to the program's cost, schedule, or performance baseline, usually achieved through proactive steps that include allocation of resources. Risk and opportunity management support achieving should-cost objectives. Figure 3-1 is a simple portrayal of how opportunity management and risk management help realize benefits for a program.

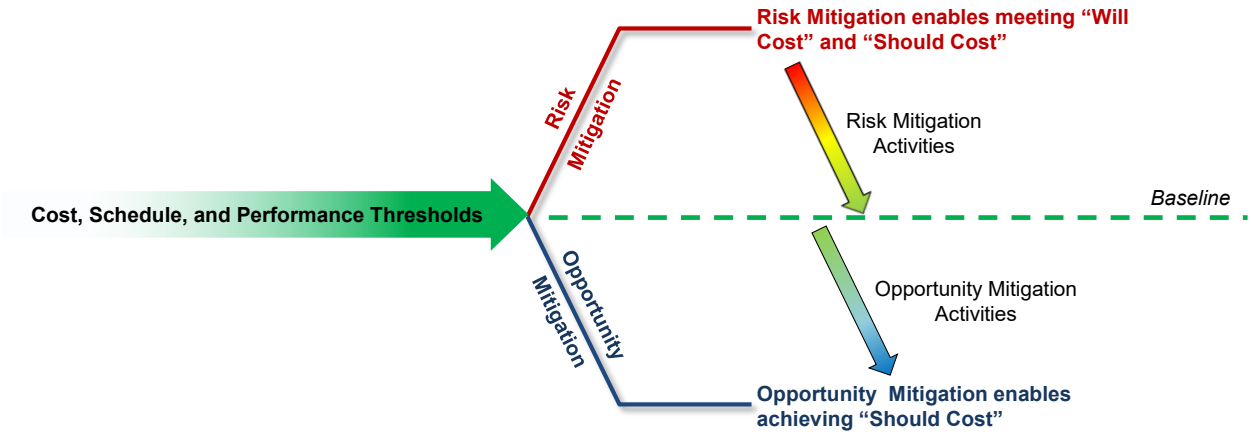


Figure 3-1. Opportunities Help Deliver Should-Cost Objectives

As adversaries create a dynamic threat environment, assessments of system strengths and weaknesses can reveal opportunities to improve mission engineering. These evolving external threat factors create the need for continuous threat modeling and will shape opportunities in requirements, design, development, testing, and sustainment.

Opportunities will take advantage of disruptive technologies, leveraging digital product development to bring new technologies, approaches, tools, and methods to the product development process. They may use advanced digital technologies, such as artificial intelligence, machine learning, and virtual reality in real time and connect processes and data across every level to rapidly build trust and confidence in technical issue management. Opportunities must be traceable through the thread of the mission context.

Opportunities will be dependent on flexible integration of innovative capabilities in a family of systems or systems of systems to respond to the dynamic threat environment. The program personnel must be knowledgeable of the mission context and well-informed in digital engineering and model-based systems engineering.

Complexity and speed-to-need must be overcome through opportunities to apply new techniques and methodologies to develop system capabilities. Opportunity management, like issue management, is complementary to risk management (Section 2). 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, 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 PRMP document.

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. Likelihood for an opportunity depends upon the effort and resources expended to achieve the opportunity.

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 3-2 shows the opportunity management process.

Figure 3-2. Opportunity Management Process

Persons involved in the effort may identify opportunities before program execution and throughout the program life cycle. Sources of opportunities include system and program changes that yield reductions in total ownership cost. For example, adhering to a modular open systems approach or securing appropriate Government rights to a technical data package could offer opportunities in sparing and competition for modifications. These cost reductions could 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 research and development (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 Operation and Support (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, 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. Table 3-1 shows a sample opportunity register for use at Program Management Reviews or other reviews.

➢ ***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.

Table 3-1. Sample Opportunity Register

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 opportunity activity.	Mod	$350K	$25K		$375K			#3	Reject	Ms. Dana Jones	May 2017
Opportunity 3: Summarize 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

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 requirements. The UAV was designed to be modular, and the battery is a Line Replaceable Unit 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 life cycle cost 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 to a newer, more reliable and lower cost unit. Since the Government and contractor negotiated that 80 percent 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 Guidance Electronics Unit 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.

4 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; size, weight, power, and cooling (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 Configuration Steering Board (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 that 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 Memorandums of Agreement (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 4-1 is a sample table of required MOAs from the Acquisition Strategy Outline.

Table 4-1. 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 4-1 is an example synchronization schedule from the SEP Outline.

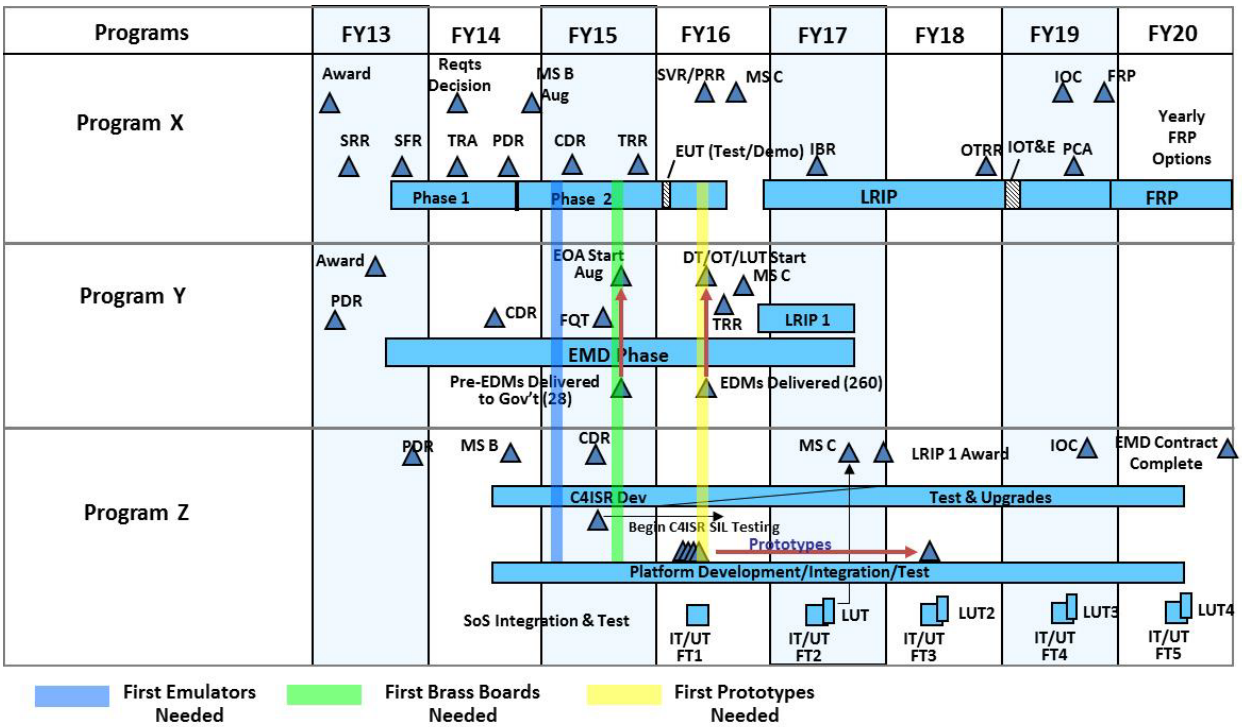


Figure 4-1. Sample Synchronization from the SEP Outline

- 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.
- 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 one another'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 4-2 shows an example of a program's tracking of cost, schedule, performance, technology maturity/readiness, and system-of-systems management.
- Activities required due to interdependencies should be identified early enough that necessary resources can be secured.

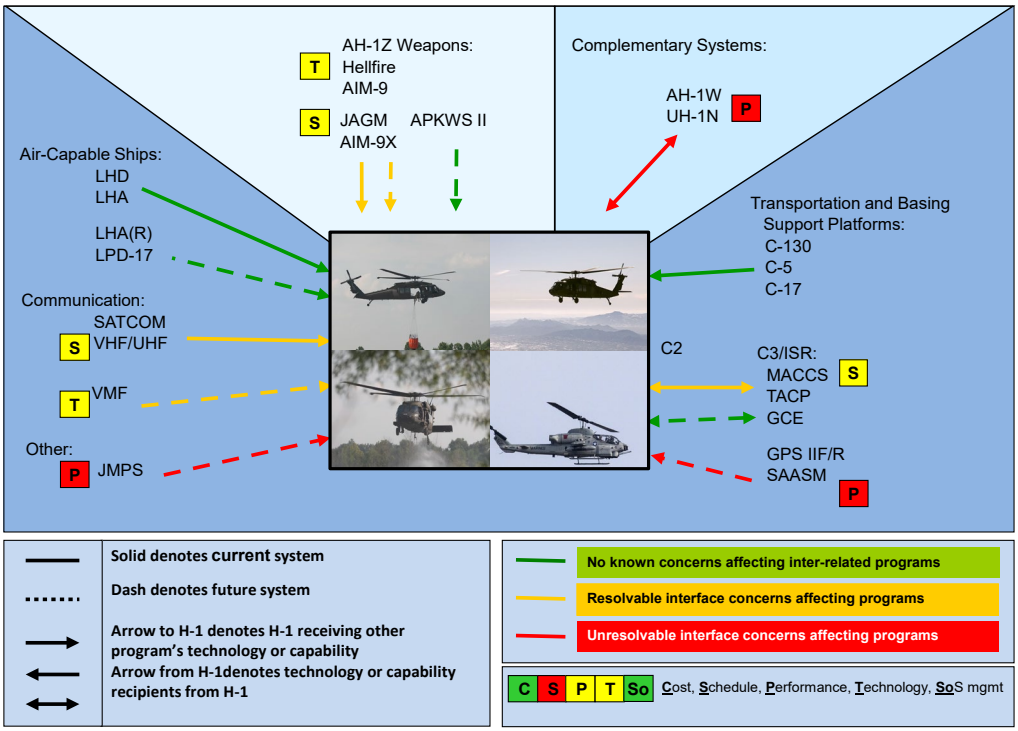


Photo source: DVIDS.

Figure 4-2. Tracking Interdependency Risks

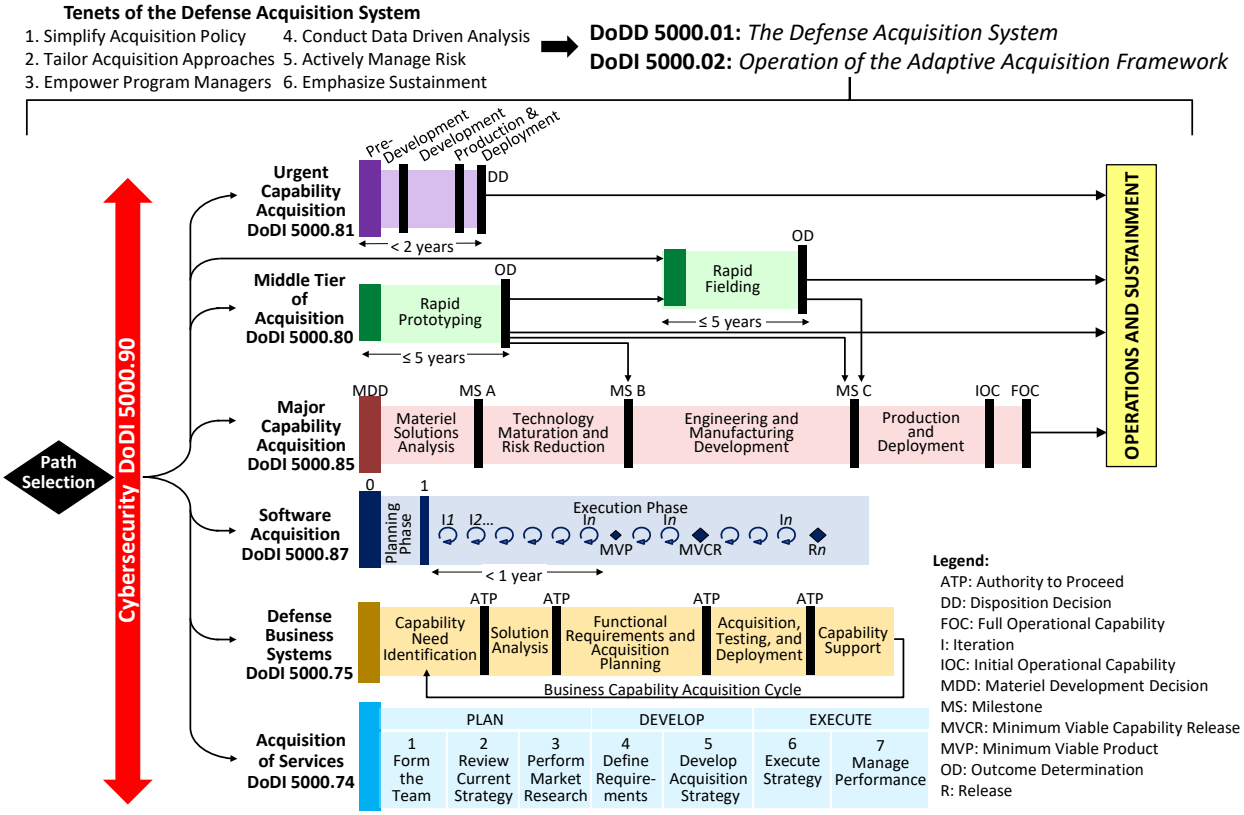
➢ ***Expectations***

- A designated technical authority is 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.
  - External programs know and accept their SWAP-C allocations.
  - Programs providing systems on which other programs are critically dependent agree to provide early warning to the dependent programs; tripwires for cost, schedule, and/or performance measures are established in the SEP and MOAs.
  - Giver-receiver relationships and deliverables are established and documented; required deliverables are tracked in the IMS.
- The schedule reflects sufficient time for integration, test, and corrective actions.
- Senior managers implement risk management activities recognizing external dependencies including cross-program risks.
- Interface Control Documents are established and approved.

5 Managing Risk by Adaptive Acquisition Framework Pathway

5.1 Overview of Adaptive Acquisition Framework

DoD Directive (DoDD) 5000.01, "The Defense Acquisition System," establishes policy and assigns responsibilities. DoDI 5000.02 describes the AAF, which consists of six acquisition pathways designed to promote the efficient delivery of effective, suitable, survivable, sustainable, and affordable solutions to end users. The pathways are Urgent Capability Acquisition (UCA), Middle Tier of Acquisition (MTA), Major Capability Acquisition (MCA), Software Acquisition, Defense Business Systems (DBS) Acquisition, and Acquisition of Services. The PM tailors the program's Acquisition Strategy depending on the pathway(s) the program chooses for the development, and any of the pathways may be tailored to the specific capability being acquired. Figure 5-1 illustrates the AAF pathways and associated key events.



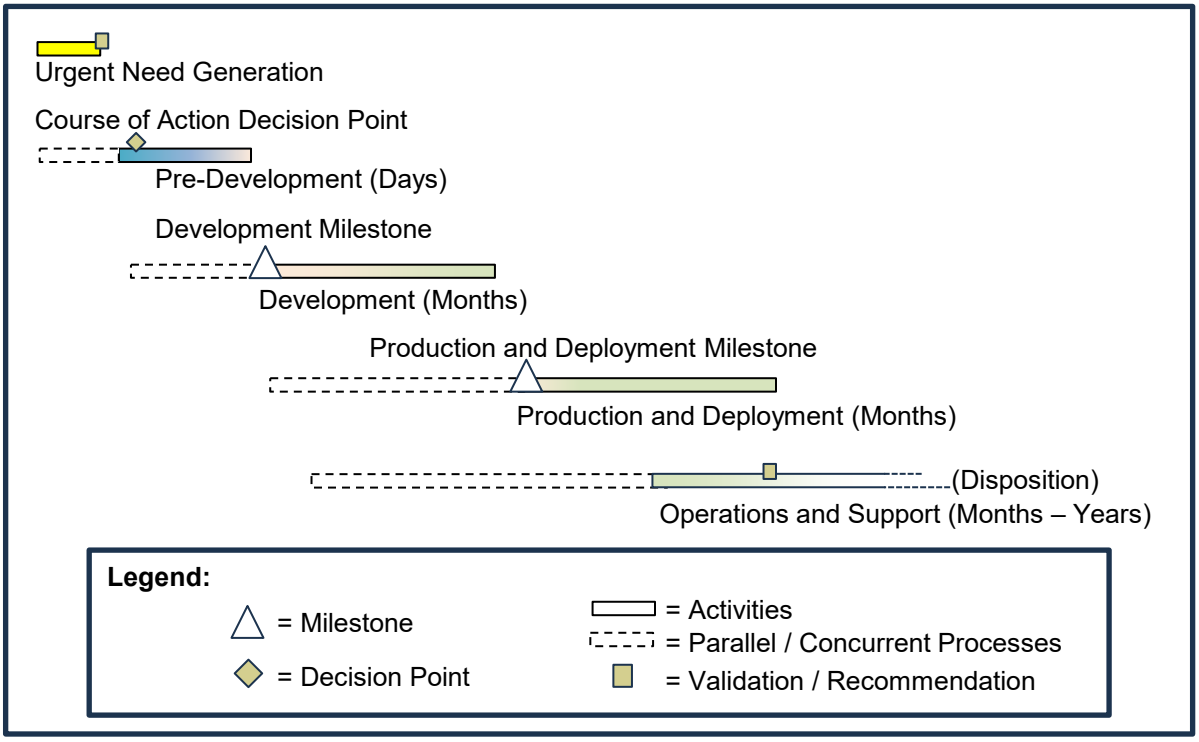
Source: Adapted from DoDI 5000.02.

Figure 5-1. Adaptive Acquisition Framework (AAF)

The following sections describe managing risk for the AAF pathways.

5.2 Managing Risk for Urgent Capability Acquisition (UCA) Pathway

The purpose of the UCA pathway is to field capabilities to fulfill urgent existing or emerging operational needs or quick reactions in less than 2 years. DoDD 5000.71, "Rapid Fulfillment of Combatant Commander Urgent Operational Needs and Other Quick Action Requirements," and DoDI 5000.81, "Urgent Capability Acquisition," establish policies and procedures for acquisition to satisfy urgent operational needs and other quick-reaction capabilities. Figure 5-2 illustrates the UCA pathway. Because of operational urgency, the normal acquisition processes are aggressively streamlined. The goal is to plan for the capability in a few weeks and measure development and production in months.



Source: DoDI 5000.81.

Figure 5-2. Urgent Capability Acquisition Pathway

5.2.1 UCA Pre-Development Phase

The purpose of the UCA Pre-Development phase is to assess and select a COA or COAs to field a quick-reaction capability and develop an acquisition approach.

5.2.1.1 Suggested Best Practice Activities in the Pre-Development Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider for the UCA pathway Pre-Development phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

The PM and the intended user community and requirements validation authority should perform the following activities:

- Assess the required capability and any recommended non-materiel options and, if not adequately stated, determine performance thresholds so they can be testable to assess the minimal set of performance parameters required to adequately reduce the capability gap.
- Analyze potential COAs, if they have not already done so, to consider:
  - The range of feasible capabilities, near, mid, and long term, including consideration of an existing domestic or foreign-made capability.
  - The acquisition risk (cost, schedule, and performance) and the operational risk of each solution.
  - The operational risk to the requesting commander if an effective solution is not deployed in the time specified by the commander.
- Recommend a COA to the Decision Authority (DA) and requirements validation authority.
- Assess and document the safety and supportability risks of the potential COA.
- Include a risk-based life cycle management approach to address supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and by developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain throughout the entire life cycle of the potential COA.
- Notify the DA if unable to identify an effective solution that could be executed under the UCA pathway. The DA will in turn notify the requirements validation authority. If it is a Joint Urgent Operational Need (JUON) or Joint Emergent Operational Need (JEON), a critical warfighter issue identified by the Warfighter Senior Integration Group (SIG), or a SecDef or DepSecDef Rapid Acquisition Authority (RAA) determination, the DA will notify the Defense Acquisition Executive (DAE) and the requirements validation authority through the Executive Director, Joint Rapid Acquisition Cell (JRAC) and the Deputy Director for Requirements and Capability Development in the Joint Staff Force Structure, Resources, and Assessment Directorate (J-8).

5.2.2 UCA Development Phase

The UCA Development phase includes an assessment of the capability's performance, safety, suitability, survivability, supportability including software, and lethality, if appropriate. Assessing these items does not require that all identified deficiencies, including those related to safety, be resolved before production or deployment. The DA, in consultation with the user and

the requirements validation authority, will determine which deficiencies must be resolved and what risks can be accepted.

5.2.2.1 Suggested Best Practice Activities in the Development Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the UCA pathway Development phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Assess the capability's performance, safety, suitability, survivability, supportability, including software, and lethality, if appropriate.
- The DA, in consultation with the user community and the requirements validation authority, determine which deficiencies the program must resolve, and which risks the program can accept. The accepted risks will allow the user community to develop tactics, techniques, and procedures to help minimize the operational risks.
- DoD Component chief information officers establish processes consistent with DoDI 8510.01 for designated approval authorities to make certification determinations expeditiously and issue interim authorization to test or authorization to operate. Information technology (IT) including National Security Systems fielded under the UCA pathway require an authorization to operate in accordance with DoDI 8510.01. DoD Component chief information officers establish processes consistent with DoDI 4650.01 and DoDI 3222.03 to ensure the timely conduct, management, and approval for national EMS certification and departmental SSRA and E3 assessments to identify and document all risk resulting from lack of EMS supportability, EP, and EM.

5.2.3 UCA Production and Deployment Phase

During the Production and Deployment (P&D) phase, the acquiring organization provides the warfighter with the needed capability, including any required training, spares, technical data, including known hazards and accepted mishap risks, computer software, temporary or permanent facilities or infrastructure, support equipment, maintenance, or other logistics support necessary for operation.

5.2.3.1 Suggested Best Practice Activities in the Production and Deployment Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the UCA pathway P&D phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- The PM will summarize the results of development activities, pre-deployment performance, and the program assessment to date. The PM will present plans to transport, deploy, and sustain the capability; to conduct post-deployment assessments; and to train maintenance and operating personnel. The PM will provide this information to the DA for approval.
- The DA, in consultation with the supporting developmental and operational and/or live fire test organization, and with the concurrence of DOT&E for programs under DOT&E oversight, will determine:
  - Whether the capability has been adequately reviewed, performs satisfactorily, is supportable, and is ready for P&D.
  - When assessments of fielded capabilities are required.
- The DA will decide whether to produce and, in coordination with the requester/user, field the capability; approve the updated Acquisition Strategy, which will include the sustainment plan and program baseline; and document the production decision in an Acquisition Decision Memorandum.
- The DoD Components will ensure that the capability and required support (e.g., field service representatives, training) are deployed by the most expeditious means possible and tracked through to their actual delivery to the user.
- The DoD Components will coordinate with each other and the requiring activity to verify the total number of items required, considering necessary support and spares and training assets for deployed or pre-deployment training.
- Upon deployment, the capability will enter O&S.

5.2.4 UCA Operations and Support Phase

In the O&S phase, the PM executes a supportability strategy that meets materiel readiness and operational support performance requirements, is safe, and sustains the capability in the most cost-effective manner over its anticipated total life cycle. Planning for O&S, including support funding, will begin during pre-development and will be documented in the Acquisition Strategy.

5.2.4.1 Suggested Best Practice Activities in the Operations and Support Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the UCA pathway O&S phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- The capability is operated and supported consistent with the sustainment plan approved by the DA at the production milestone.

- The PM or the user community may propose urgently needed improvements to the capability. If within the scope of the initial requirements document, procedures in this pathway may be used to acquire the improvements. If improvements are outside the scope of the validated or approved requirements document, the program may need a new or amended requirements document.
- In collaboration with the original requesting DoD Component, the program will conduct a post-deployment assessment. If practical, the PM will conduct the assessment in the field with the supporting operational test organization. If not practical, the PM may use alternate means for this assessment including a PM or operational test agency assessment of user feedback or other DoD Component feedback. For all programs under DOT&E oversight, DOT&E will independently review and approve the post-deployment assessment approaches.
- No later than 1 year after the program enters O&S (or earlier if directed by the DoD Component), the DoD Component will appoint an official to conduct a disposition analysis. The DoD Component will notify the Executive Director, JRAC and the Deputy Director for Requirements and Capability Development in the Joint Staff J-8 when the disposition analyses for JUONs, JEONs, critical warfighter issues identified by the Warfighter SIG, or DepSecDef RAA determinations are to be completed.
    - The disposition analysis will consider the performance of the fielded capability, mishap data, long-term operational needs, and the relationship of the capability to the Component's current and planned inventory of equipment.
    - The analysis also will consider the continuation of non-materiel initiatives, the extension of S&T developments related to the fielded capability, and the completion of DA-approved and funded materiel improvements.
    - The disposition official will recommend one of the following options:
        - Termination: Demilitarization or Disposal
        - Sustainment for Current Contingency
        - Transition to a Program of Record
    - The disposition recommendation will be made to the DoD Component head for UONs, with critical warfighter issues identified by the Warfighter SIG, or SecDef or DepSecDef RAA determinations.
    - The DoD Component head and the Component Acquisition Executive will review the disposition official's recommendation and, within 4 months of receipt of the recommendation, record the DoD Component head's transition decision in a disposition determination. The Component head will provide disposition determinations for JUONs, JEONs, critical warfighter issues identified by the Warfighter SIG, or SecDef or DepSecDef RAA determinations to the Executive

Director, JRAC and the Deputy Director for Requirements and Capability Development in the Joint Staff J-8.

5.3 Managing Risk for Middle Tier of Acquisition (MTA) Pathway

DoD uses the Middle Tier of Acquisition (MTA) pathway to rapidly develop fieldable prototypes within an acquisition program to demonstrate new capabilities, or to rapidly field production quantities of systems with proven technologies that require minimal development in accordance with DoDI 5000.80, "Operation of the MTA." Figure 5-3 depicts the MTA pathway. MTA focuses on delivering capability in a period of 2-5 years with rapid prototypes and rapid fielding with proven technology.

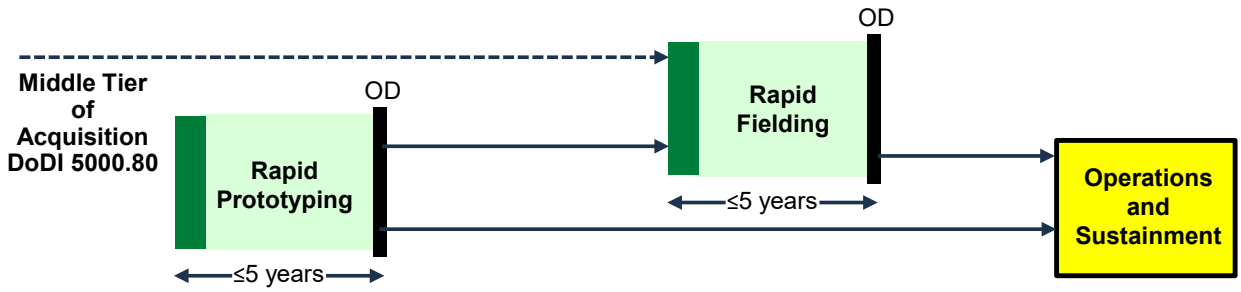


Figure 5-3. Middle Tier of Acquisition Pathway

5.3.1 MTA Rapid Prototyping Path

The Rapid Prototyping path provides for the use of innovative technologies to rapidly develop fieldable prototypes to demonstrate new capabilities and meet emerging military needs. The primary objective for an MTA Rapid Prototyping program is fielding of an operational prototype within 5 years of program start.

5.3.1.1 Suggested Best Practice Activities for Rapid Prototyping Path to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider for the MTA pathway Rapid Prototyping. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Structure the program for successful fielding of operational prototype within 5 years. This is the chief criterion of successful MTA completion.
- Plan operational demonstration for no later than one year before MTA completion, to give schedule margin to mitigate impact of any schedule delays or needed design improvements prior to fielding.

- Avoid complex requirements and be willing to trade off or de-prioritize traditional KPP requirements, remembering the MTA pathway is not subject to the JCIDS process, per statute, except where explicitly defined for the pathway.
- Avoid structuring the program to conduct significant technology development followed by systems integration and test of multiple developmental components.
- Tailor-in SETRs, technical risk assessments, SSRAs and other activities that would most benefit the program outcome and reduce risk.
- Test early to gain knowledge. Test the hard things early. Accept risk of early test failures to enable "go-fast" approach. Use developmental testing to reduce risk early, rather than pushing risk into the operational demonstration.
- Maintain an IMS ensure it is traceable to the Integrated Master Plan (IMP), and conduct regular schedule risk assessment. Continually monitor the critical path to fielding residual operational capability.
- Begin planning for transition as early as possible, including definition of sustainment and technology transition approaches.
- Maintain engagement of key stakeholders in OSD and in operational forces.
- Be willing to descope the planned fielded capability to remove schedule or feasibility risk from the program, as long as residual operational capability is useful to the warfighter.
- Set aside overly complex requirements or high-risk objectives for follow-on or spin-off programs. Adopt an agile approach to requirements.
- Gain as much knowledge as possible during the MTA, to reduce risk in follow-on programs.
- Include a risk-based life cycle management approach to address supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain throughout the entire life cycle.
- Verify with the user and sponsor that required amounts and types of funding will be available to execute the MTA within the 5-year timeline.
- Conduct extensive and thorough market research to determine whether industry can execute the program or develop the technology within the 5-year timeline.
- Ensure required contracting vehicle(s) are in place as soon as possible after program start in order to be able to begin production within the first 6 months.

5.3.2 MTA Rapid Fielding Path

The rapid fielding path provides for the use of proven technologies to field production quantities of new or upgraded systems with minimal development required.

5.3.2.1 Suggested Best Practice Activities for Rapid Fielding Path to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the MTA pathway Rapid Fielding. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Continue knowledge point reviews, CSB meetings, and assessment of framing assumptions as in the Rapid Prototyping phase. When not making a change to KPPs could jeopardize a program's utility or affordability, coordinate with the Joint Requirements Oversight Council.
- Identify potential hardware and software failure modes, then conduct early risk-focused 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 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.
- Update list of microelectronic critical components, including the embedded software, intellectual property, tools, etc., used to program them.
- Revise program/system protection measures, as needed.
- Initiate selective testing for malicious insertions where practicable, including vetting and verification and validation of embedded software, intellectual property, and tools.
- Enforce secure coding practices through code inspection augmented by automated static analysis tools.
- Analyze and track software composition including known vulnerabilities.
- Use dynamic testing tools to identify critical hardware, software, and firmware performance and security risks and issues in the system.
- Detect vulnerabilities, weaknesses, and defects in the software; prioritize; and remediate.

- Assess chain-of-custody from development through sustainment for any known remaining vulnerabilities and weaknesses and planned mitigations.
- Confirm hash checking for delivered products.
- Establish processes for timely remediation of known vulnerabilities (e.g., CVEs) in fielded commercial, commercial off-the-shelf (COTS), and open-source components.
- Confirm planned and automated software testing provides variation in testing parameters and system configurations to maximize coverage.
- Confirm that critical function software and critical components receive rigorous analysis and test coverage.
- Develop a life cycle sustainment plan that clearly articulates the program's plan for logistics support and sustainment activities during the MTA RF phase and in the O&S phase.
- Ensure EMS certification, SSRA, and E3 assessment have been initiated and updated.

5.4 Managing Risk for Major Capability Acquisition (MCA) Pathway

5.4.1 MCA Planning Considerations

5.4.1.1 Strategy Development

The most important decisions to control risk are made early in a program life cycle (Figure 5-4). 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 the concept presents risk in technology maturity or requirements stability, the PM should structure the 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 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 reduce risk and cost.

[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.

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 EMD.

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

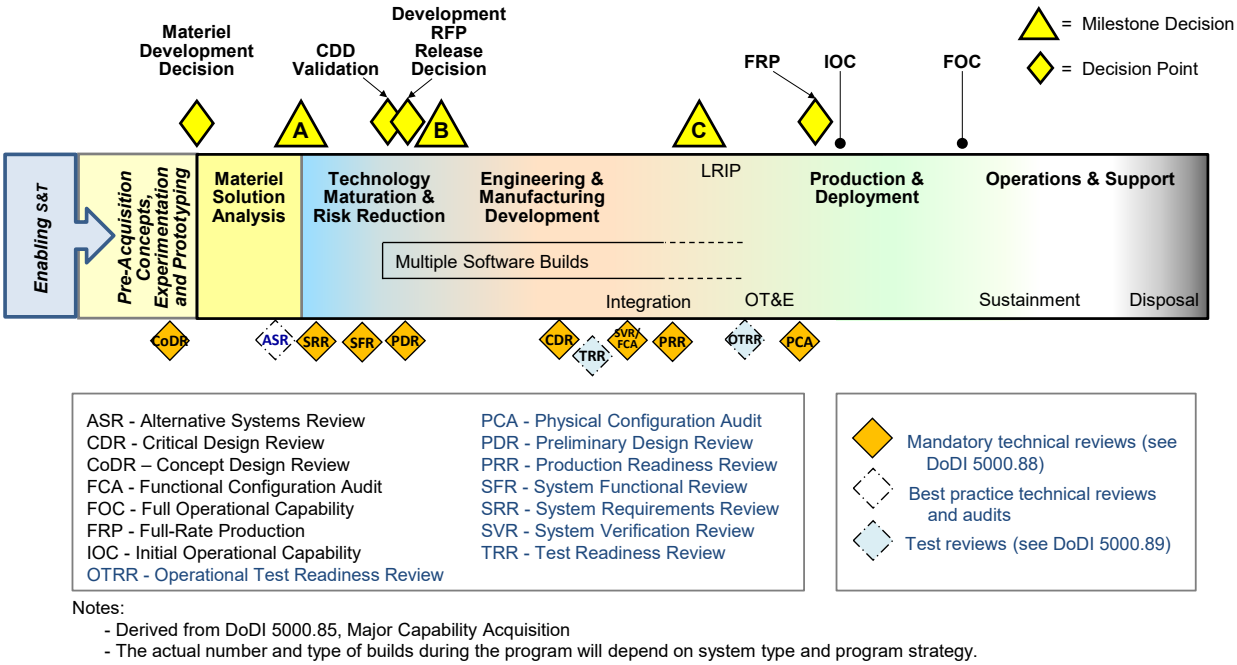


Figure 5-4. DoD MCA Life Cycle

For the MCA pathway, DoDI 5000.85 requires PMs to document a comprehensive approach for managing and mitigating risk (including technical, cost, and schedule risk) in the Acquisition Strategy and to summarize the top program risks and associated risk mitigation plans in the Acquisition Strategy. DoDI 5000.88 requires programs to describe their technical approach, including key technical risks, and management and execution of risk mitigation activities, in the SEP.

5.4.1.2 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.

5.4.1.3 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 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 RFP should include a risk-based life cycle management approach to address supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain throughout the entire life cycle.

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, 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 contracts are 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 regarding 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 B includes a list of typical Government and contractor responsibilities regarding risk management.

5.4.2 MCA Pre-Materiel Development Decision Phase

The MCA Pre-Materiel Development Decision (MDD) phase 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.

Mission engineering and early systems engineering provide trade space analysis for alternative candidate concepts. Mission engineering provides a quantifiable basis to inform technical and budgetary planning decisions on potential solutions to fulfill mission capability gaps and to synergize mission concepts, system requirements, technologies, and budgets. 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 organizations, working the concept before the MDD, can solicit ideas from industry through Requests for Information (RFIs) that seek insight into concepts, technologies, materials, and research investments.

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

5.4.3 MCA 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 5-5 displays the MSA phase activities.

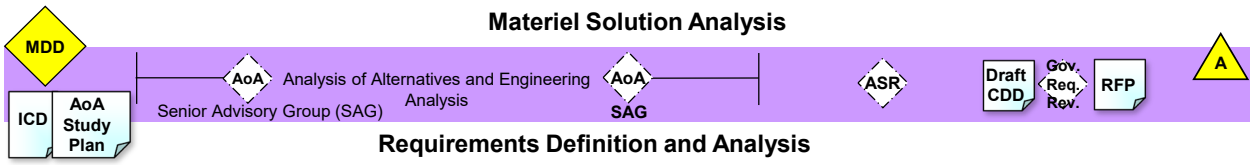


Figure 5-5. MCA Materiel Solution Analysis Phase Activities

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 relative to prior analyses and related systems:

1. Interfaces and dependencies that involve other programs and the maturity and risks associated with the interfaces themselves (integration risk).
2. 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)?
3. Framing assumptions: Are these assumptions still valid? What are the risks and impacts of an incorrect assumption?

After selecting the preferred materiel solution, the PM should conduct an Alternative System Review (ASR) to support a discussion 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 influence the decision about which phase will come next (i.e., TMRR, EMD, or P&D). The program should address these risks in the RFP and program plans.

5.4.3.1 Suggested Best Practice Activities in the MSA Phase[2] to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the MCA pathway MSA phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

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 RFI, and source selection activities.
- Avoid constraining the design trade space (e.g., minimize the number of KPPs and KSAs, per the JCIDS Manual).
- Ensure the Government and bidders have a complete and common understanding of the requirements and mission context.
- Solicit industry feedback regarding the feasibility of requirements, unit costs, and maturity of technologies by holding 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) risks early to ensure system requirements, design, and architecture will produce a secure system in operations.
- Ensure EMS certification, SSRA, and E3 assessment have been initiated and updated.
- 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 SME risk assessment.

[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.

  - 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, including:
  - Contractor testing with defined success criteria before the start of Government testing.
  - 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 IMP and IMS through prototype delivery, drawings, and models so the Government can assess (1) the contractors' understanding of the technical risks and (2) the required planning to execute the identified risks.
  - 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 the program mitigates risks before proceeding to the next phase; ensure the schedule reflects an acceptable level of concurrency.
- Establish communication: horizontal, across Integrated Product Teams (IPTs) 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.

5.4.4 MCA 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 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 the TMRR 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 regarding 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 5-6 displays the TMRR phase activities, including the following SETRs 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.

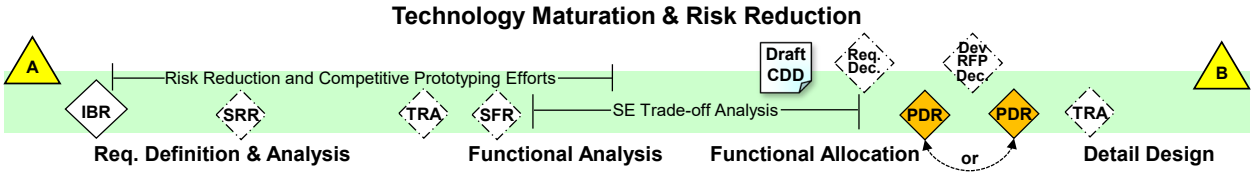


Figure 5-6. MCA Technology Maturation and Risk Reduction Phase Activities

5.4.4.1 Suggested Best Practice Activities and Practices in the TMRR Phase[3] to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the MCA pathway TMRR phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

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

- Assess the effectiveness of TMRR risk mitigation 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 producibility and quality risks.
- Conduct system or subsystem risk reduction prototyping validation and competition.

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

- 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 CSB meetings or knowledge point review (includes requirements and intelligence communities).
- Track program interdependencies, interfaces, and associated MOAs in periodic meetings with external programs and associated contractors and stakeholders.
- Plan for contingencies and technical risk mitigation activities by establishing reasoned cost, schedule, and performance margins.
    - Ensure risk mitigation plans are reflected in the IMP, IMS, TPMs, and the EVM baseline. This may or may not require a change to the contractor work packages or resources. (Continue in subsequent phases.)
    - 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 Milestone B to identify and assess critical technology elements in the contractor's EMD proposal.
- Conduct a Manufacturing Readiness Assessment (MRA) to assess manufacturing maturity risks.
- Conduct an SRA on a regular basis to evaluate the likelihood to achieve the planned schedule.
- For trade studies affecting KPPs and KSAs, develop a decision hierarchy to promptly identify and mitigate technical risks and their impact on cost, schedule, and performance.

- For programs that include EMS-dependent systems, ensure EMS certification, SSRA, and E3 assessment have been initiated and updated.
- Consider S&T investments to support EMD and beyond.
- Develop MOAs with all external interdependent programs.

5.4.5 MCA Engineering and Manufacturing Development Phase

By entering the EMD 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 P&D.

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 5-7 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. 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 5-7. MCA 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 an MRA 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 and design stability, integration and interdependency risks, and manufacturing or supply chain quality.

5.4.5.1 Suggested Best Practice Activities in the EMD Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the MCA pathway EMD phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

Additional activities to reduce risk exposure in the EMD 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).
- For programs that include EMS-dependent systems, ensure EMS certification, SSRA, and E3 assessment have been initiated and updated.
- 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 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.

5.4.6 MCA 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 before entering this phase.

Figure 5-8 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.

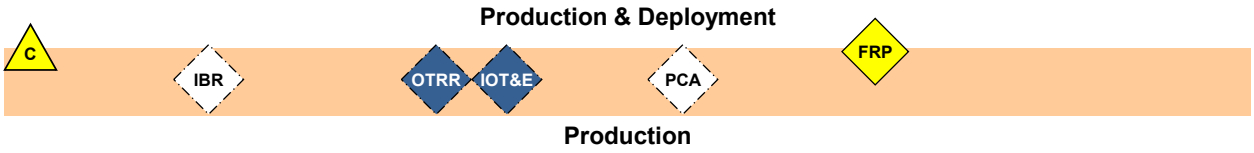


Figure 5-8. MCA Production and Deployment Phase Activities

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.

5.4.6.1 Suggested Best Practice Activities in the P&D Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the MCA pathway P&D phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

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

- Conduct a thorough PCA to verify that 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 and users.
- Identify sustaining engineering needs and fund as appropriate.

5.4.7 MCA Operations and Support Phase

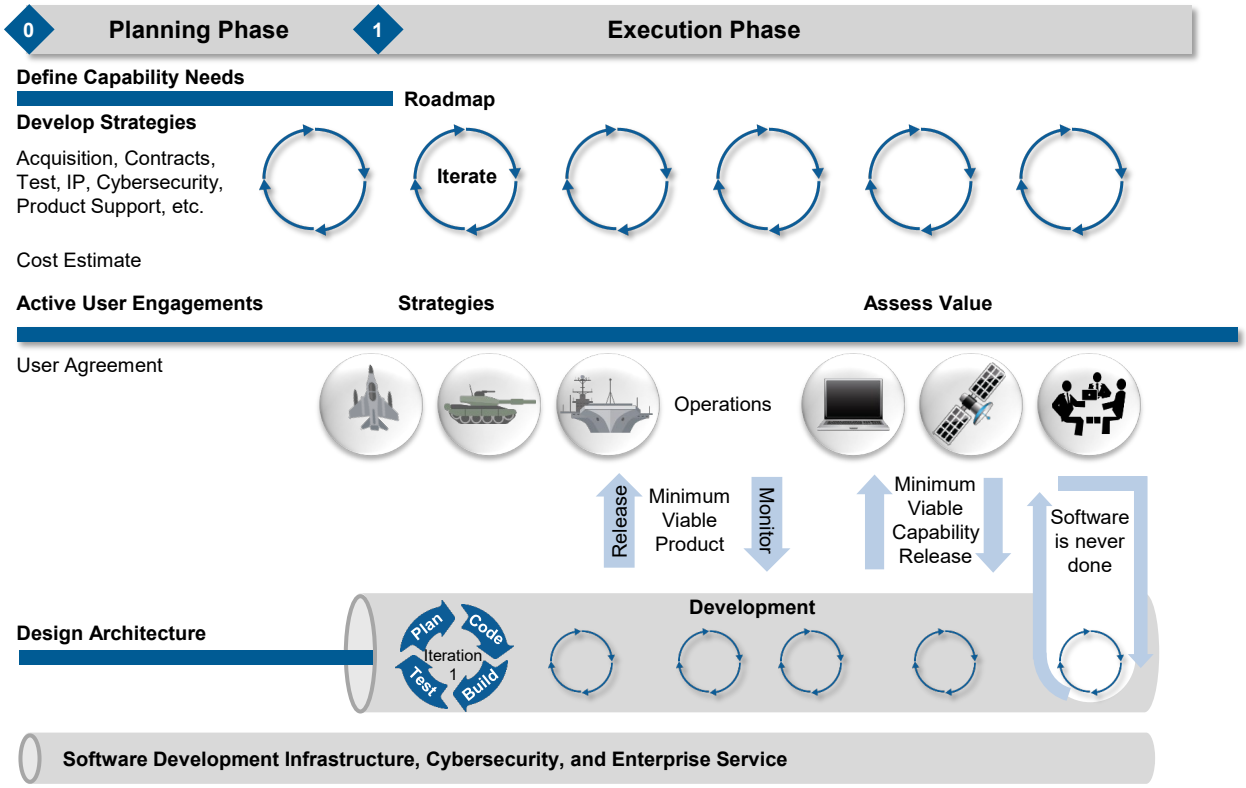
In the O&S phase, the risk activities include monitoring in-service usage, problem reports, parts availability and obsolescence, engineering modifications, technology insertions, and operational hazard risks. The Service support organizations often work with the program offices.

During this phase, programs should plan for and establish Sustainment Reviews (SRs). The SR is a multidisciplined 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 SR include risk assessment of operational hazards, product baseline integrity, supply chain status, determination of acceptable operational hazard risk, and in-service usage or support risk. For more information on SRs, see DoDI 5000.91, “Product Support Management for the Adaptive Acquisition Framework.”

5.5 Managing Risk for Operation of Software Acquisition Pathway

The Software Acquisition pathway is for the timely acquisition of custom software capabilities developed for the Defense Acquisition System in accordance with DoDI 5000.87, “Operation of the Software Acquisition Pathway.” This pathway is designed for software-intensive systems. The pathway objective is to facilitate rapid and iterative delivery of software capability to the

user. This pathway integrates modern software development practice such as Agile software development, DevSecOps, and Lean practices. Capitalizing on active user engagement and leveraging enterprise services, working software is rapidly and iteratively delivered to meet the highest priority user needs. Tightly coupled mission-focused Government-industry software teams leverage automated tools for development, integration, testing, and certification to iteratively deploy software capabilities to the operational environment. Figure 5-9 depicts the operation of the Software Acquisition pathway.



Source: Adapted from DoDI 5000.02.

Figure 5-9. Life Cycle View of Software Acquisition Pathway

5.5.1 Software Planning Phase

The purpose of this phase is to better understand the users' needs and plan the approach to deliver software capabilities to meet those needs. The Planning phase will be guided by a draft Capability Needs Statement (CNS) per DoDI 5000.87 or a Software Initial Capabilities Document (SW ICD) per JCIDS. Programs should consider activities and best practices listed below during the Planning phase to reduce risk. Note: Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.

5.5.1.1 Define Capability Needs

- PM and Program Management Office engage with the sponsor during the CNS or SW ICD development to ensure the capabilities are stated clearly and are operationally feasible, technically feasible, and testable.
- Prioritize required capabilities in the CNS or SW ICD to effectively guide the software development.
- If using the embedded path, align the CNS or SW ICD with the requirements documents of the system(s) in which the software will be embedded.
- Include cyber survivability requirements to address potential threats.

5.5.1.2 Develop Strategies

- Identify software activities across the system life cycle.
- Use the concept of "test and evaluation as a continuum" (see Collins 2023) to enable rapid success in fielding needed capabilities. Choose an iterative software development methodology that incorporates continuous testing and evaluation, resiliency, and cybersecurity, with maximum possible automation, as persistent requirements.
- Include a risk-based life cycle management approach to address software vulnerabilities, supply chain and development environment risk, and intelligence threats throughout the entire life cycle.
- Consider developing prototypes or initial capabilities to explore possible solutions and architecture options and to solicit user and stakeholder feedback.
- Ensure the following artifacts are approved before entering the Execution phase: the CNS or SW ICD, user agreement (UA), Acquisition Strategy, test strategy, and cost estimate.
- Develop a UA before the Execution phase to gain commitment to continuous user involvement and to assign decision-making authority for the development and delivery of software capability releases. Decisions include defining and prioritizing required capabilities, trade-offs of software features and cadence, user acceptances, and readiness for operational deployment. The UA will commit proper resourcing of operational user involvement to provide acquirers, developers, and testers with insights into the operational environment, provide feedback on interim and fielded software, support test and evaluation, and shape future requirement details, e.g., user stories and features.
- Employ a risk-based business and technical management approach to rapidly and iteratively deliver software capabilities balanced against quality, security, intelligence threats, system safety, performance, and other factors.
- If the program is using the embedded software path, align test and integration with the overarching system testing and delivery schedules.

- Incorporate plans to continuously improve or refine software development processes, practices, tools, and program strategies to reflect them.
- Establish effective metrics to monitor and manage the program. Planned metrics should consider recommendations for agile metrics per the DoD Agile Metrics Guide (2020) and needs to provide the program with adequate ability to manage day-to-day Agile software development needs, e.g., rapid root cause analysis of failures, identification of constraints, rapid learning.
- Integrate and automate metrics to support real-time visualization. Make metrics available through a self-service portal for transparency and continuous updates.
- If the program's maturity on executing Agile or DevSecOps is low, then ensure development plans allow for team growth in execution of new methodologies and practices.
- Include training in tools, processes, and practices for all staff in the effort unless they have all worked together before on a similar project.
- Consider contracting for services to perform one-time, highly specialized tasks, e.g., setting up infrastructure and software factory.
- Plan how overall program risk management will integrate with product iterations and daily Agile activities.

5.5.1.3 Roadmap

- Incorporate regular stakeholder feedback to shape the product road map and program backlogs.
- Ensure the product vision and road map establish the Agile architectural transition strategy of new features, e.g., set boundaries, define context.
- Ensure the product vision and road map establish specific planned capabilities if evolving from an existing non-Agile architecture.

5.5.1.4 Active User Engagements

- Actively engage users throughout the software life cycle to understand their mission deficiencies, required enhancements to existing operational capabilities, cybersecurity requirements, features, interoperability needs, legacy interfaces, intelligence needs, threat intelligence, and other desired attributes.
- Conduct user engagements with each iteration to ensure delivered software capabilities address their priority needs.
- Develop and maintain program backlogs that identify detailed user needs in prioritized lists.

- Establish a rapid and iterative feedback loop to evaluate various approaches and decisions.

5.5.1.5 Design Architecture

- Consider modern microservice-based architecture within the overall plan.
- Focus on and understand impacts of abstraction, cohesion, coupling, and complexity throughout the program life cycle.
- Consider cloud, cloud platform, or edge computing within development or operations regardless of program domain.
- Understand how architecture enables automated testing, immutable infrastructure, and immutable containers.
- Establish baseline architecture and review for weaknesses (e.g., Common Weakness Enumeration) and susceptibility to attack (e.g., Common Attack Pattern Enumeration and Classification); refine architecture to reduce potential attack surfaces and mission impacts.
- Review architecture and design against secure software design principles, which include but are not limited to, system element isolation, least common mechanism, least privilege, fault isolation, input checking, validation, and patterns proven for building secure and resilient software.
- Enable a modular open systems approach that is interoperable with required systems.

5.5.1.6 Software Development Infrastructure

- Establish iterative software development infrastructure capabilities to ensure automation is embedded in the development process (e.g., software factory, continuous integration pipeline, automated unit testing, automated static code analysis, automated deployment pipelines) at the beginning of the program, which enables test and evaluation as a continuum. If automation is not embedded at the beginning of the program it can result in a lack of efficiency and constrain the velocity and agile efficacy of the program.
- Stand up initial infrastructure and software factory quickly.
- Establish infrastructure necessary for integration and processes for integration. Consider the risk of integrating software from other organizations, if appropriate.
- Ensure automated collection of metrics of the end-to-end development processes to identify bottlenecks and other opportunities to improve velocity.

5.5.1.7 Cybersecurity

- Contribute to selection of secure design and coding standards for software.

- Identify critical functions that use software.
- Establish requirements to mitigate software vulnerabilities, defects, or failures based on mission risks.
- Develop and document an understanding of how DoD systems may be attacked via software, i.e., attack patterns.
- Develop a plan for a software threat modeling, static analysis, software composition analysis (SCA), and dynamic analysis.
- Determine security requirements for programming languages, architectures, tool deployment and maintenance, development environment, and operational environment.
- Establish assurance requirements for software to deter, detect, react, and recover from faults and attacks.
- Establish tracking processes for completion of software assurance requirements.
- Determine automated software security checks throughout the Software Development Life Cycle and establish verification procedures and tools as a core process.
- Enforce secure coding practices through code inspection augmented by automated static analysis tools.
- Analyze and track software composition including known vulnerabilities.
- Detect vulnerabilities, weaknesses, and defects in the software; prioritize; and remediate.
- Assess chain-of-custody from development through sustainment for any known remaining vulnerabilities and weaknesses and planned mitigations.
- Establish processes for timely remediation of known vulnerabilities in fielded commercial, COTS, and open-source components.
- Continue to enforce secure design and coding practices through inspections and automated scans for vulnerabilities and weaknesses.
- Maintain automated code vulnerability scans, reporting, and prioritization, and execute defect remediation plans.
- Review chain-of-custody across development, from development to sustainment, and during sustainment for the record of remaining weaknesses and vulnerabilities remaining and planned mitigations, as appropriate.
- Conduct Mission-Based Cyber Risk Assessments (MBCRAs) to focus design and testing.

5.5.1.8 Enterprise Services

- Consider the development environment, processes, automated tools, designs, architectures, and implications across the broader portfolio, Component, and joint force.

- Select automated tools and establish toolchains for design, vulnerability scan and analysis, etc.
- Leverage enterprise services that exist within the organization and from parent and peer organizations, e.g., other Services and the Department.
- Ensure the organization performs the appropriate security assessments on enterprise offerings.
- Work with enterprise service management to find ways to increase velocity.

5.5.1.9 Other

- Incorporate software requirements into solicitations.
- Understand skill differences between traditional and Agile software development paradigms.
- Focus on adequate levels of process training, e.g., Agile product owner training, Agile leadership training, and Agile software developer training.
- Develop a plan to correlate and prioritize software findings.
- Develop a plan to address legacy code in the software.
- Be aware of supply chain risks when using COTS or GOTS software.
- Perform software reviews and inspections.
- Identify technical expertise needed to assist with software activities.
- Assess system requirements for inclusion of software.
- Seek out and incorporate best practices from across the Services and the Department.
- Ensure requirements for shared resources (e.g., test environments, interfacing systems) are identified early to reduce risk of unavailability.
- Identify and understand constraints on the development effort. Unidentified and unaddressed constraints will limit velocity.
- Consider best practices identified in the Government Accountability Office (GAO) Agile Assessment Guide: Best Practices for Agile Adoption and Implementation (2020).

5.5.2 Software Execution Phase

The purpose of this phase is to rapidly and iteratively design, develop, integrate, test, deliver, and operate resilient and reliable software capabilities that meet the users' priority needs. Programs should consider activities and best practices listed below to reduce risk during the Execution

phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.

5.5.2.1 Plan Iteration

- Review technical debt from previous iteration for resolution in this iteration.
- Include users in planning of iteration and priorities.
- Consider the program's life cycle objectives and actively manage technical debt.
- Identify the critical path to achieving MVCR within the one-year time constraint. Continue to monitor and revise what is on the critical path for MVCR as iterations are completed.
- Iteratively refactor design and code.
- Reduce cybersecurity vulnerabilities.
- Create effective modular open systems approaches to support future capabilities.

5.5.2.2 Code

- Make use of tools to automate static and dynamic code analysis for quality, e.g., memory leaks, complexity, security.
- Incorporate a peer review before committing code to baseline. Automate the workflow where possible.
- Ensure adequate comments are present to understand code purpose and design.
- Follow the program's established coding style and standard.

5.5.2.3 Build

- Ensure a repeatable build process by employing automation to maintain control over build inputs and build processes.
- Maintain traceability between build and the artifacts (code, scripts, control file, libraries, data, and tools) that produce the build.
- Build frequently and refine the build process over time to increase level of automation, speed up the build process, and improve build reliability.

5.5.2.4 Test

- Confirm that planned and automated software testing provides variation in testing parameters and system configurations to maximize coverage.
- Confirm that critical function software and critical components receive rigorous analysis and test coverage.

- Verify test resources, test cases, test scenarios, and test data.
- Ensure that requirements for shared resources (e.g., test environments, interfacing systems) are identified early to reduce risk of unavailability.
- Ensure the test environment resembles the intended deployment environment as much as feasible, e.g., configuration of software, configuration of platform, hardware used, networks, etc.
- Make use of simulations and other approaches to provide data loads on which the software system will need to operate in the intended environment.
- Ensure testing includes considerations of most stressing and operationally relevant use cases and scalability in the intended deployment.
- Ensure "rainy day" scenarios are included in testing, e.g., reduced communications, disruption of communications, failover situations, and erroneous data transfers from other systems. All resilient operating modes and designed features should be included in mandatory test coverage.
- Maintain and enhance automated regression tests and employ test coverage analyzers to increase test coverage.
- Conduct periodic penetration tests using the enhanced automated test coverage.
- Confirm that software requirements are mapped to module test cases and to the final acceptance test cases.
- Implement recurring cybersecurity assessments of the development environment, processes, and tools.

5.5.2.5 Iterate

- Develop and track a set of metrics to assess and manage the performance, progress, speed, cybersecurity, and quality of the software development, its development teams, and ability to meet users' needs.
- Review and update the risk register and backlog before each iteration. Reprioritize with the user based on feedback from previous iteration(s) and track accumulation of technical debt.
- Use knowledge from previous iterations to review architecture for continuing development without accumulating technical debt, and for future scalability and extensibility.
- Use metrics to improve development processes and track progress.
- Adjust quantity of user stories or use cases allocated to the iteration based on past team performance, if necessary.

- Ensure definition of done is clearly defined for the iteration.

5.5.2.6 Release

- Confirm hash checking for delivered products.
- Develop and maintain a software Bill of Materials (sBOM) for each release. Automate the production of the sBOM.

5.5.2.7 Minimum Viable Product

- Use an iterative, human-centered design process to define the Minimum Viable Product (MVP), recognizing that an MVP's definition may evolve as user needs become better understood.
- Acknowledge development of the MVP as a risk reduction measure.
- Employ the MVP to establish an automated software development pipeline in cases where such a pipeline is not already well established.
- Anticipate refinement of the products and the processes over time and plan accordingly.
- Use insights from the MVP feedback to define the Minimum Viable Capability Release (MVCR).
- Consider deploying the MVP to real user environments for effective assessment and feedback. If the MVP version of the software is determined sufficient to be fielded for operational use, the MVP will become the MVCR.

5.5.2.8 Monitor

- Monitor evolving threats and attacks, respond to incidents and defects, identify and fix vulnerabilities, and incorporate software-enhancing upgrades.
- Maintain trouble reports for released software and prioritize with users.
- Plan to measure Central Processing Unit (CPU) loading, network loading, and storage use. Incorporate feedback from measurements into product improvements.
- Plan and design monitoring features into the software for system health monitoring by user as well as for developer feedback, e.g., uptime, crash data dump, unused features, policy enforcement, data throughput, software inventory, logs, and other performance measures.

5.5.2.9 Minimum Viable Capability Release

- Use an iterative, human-centered design process to define an MVCR.
- Conduct rigorous mission-oriented developmental test and evaluation with actual users to mitigate the risk of failing the subsequent operational test.

- Perform an audit of all previous developmental testing (contractor and Government) to ensure that all requirements have been addressed and verified.
- Ensure there is sufficient time between MVP and MVCR to fix any defects (including cyber vulnerabilities) found during MVP or cyber developmental testing.

5.5.2.10 Operations

- Plan for tools to manage system scaling, load balancing, and backup, if needed in the intended environment.
- Plan and execute how to gather data for feedback into the product backlog for future releases.
- Build in recovery and restoration mechanisms to restore systems to a known verified state.

5.5.3 Software Risk Reduction

5.5.3.1 Suggested Activities for Software Acquisition Pathway to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the Software Acquisition pathway. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Conduct MBCRAs to identify highest mission consequence cyber risks.
- Conduct risk-assessed level of testing to focus Government T&E on highest risk releases and functions.
- Ensure RAM requirements are included in contracts or service-level agreements.
- Contribute to selection of secure design and coding standards for software.
- Identify mission-critical functions that use software.
- Identify software activities across the system life cycle.
- Establish requirements to mitigate software vulnerabilities, defects, or failures based on mission risks.
- Incorporate software requirements into solicitations.
- Plan for software training and education.
- Develop and document an understanding of how DoD systems may be attacked via software (i.e., attack patterns).
- Develop a plan for software threat modeling, static analysis, software composition analysis, and dynamic analysis.

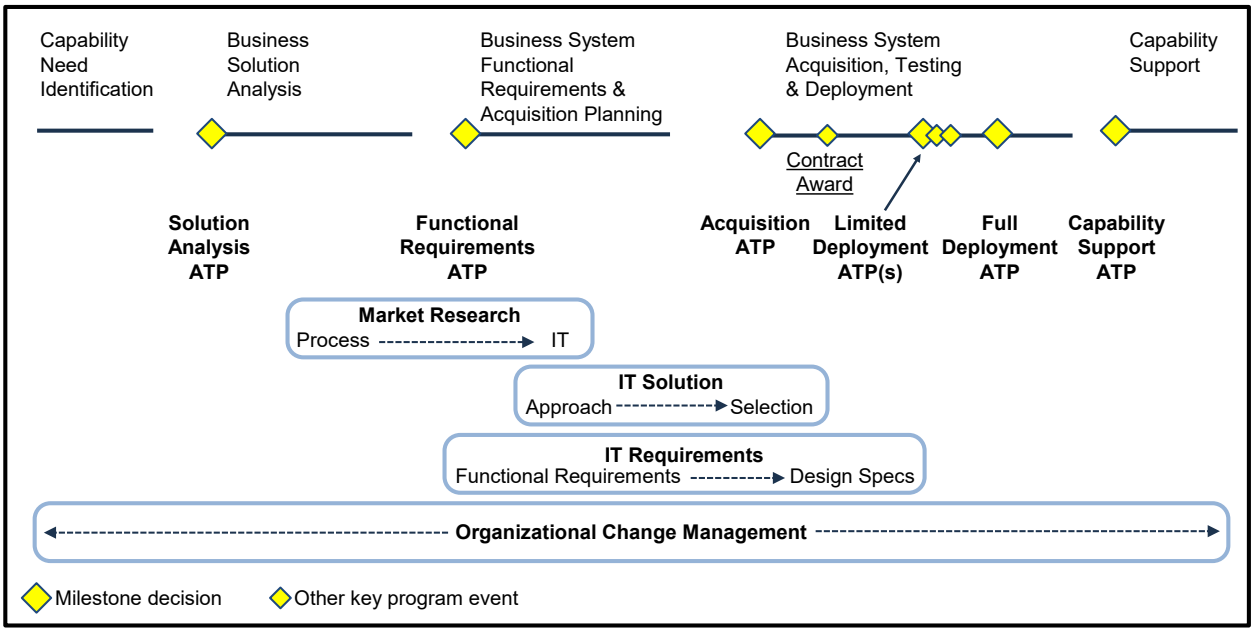
- Select automated tools and establish toolchains for design, vulnerability scan and analysis, etc.
- Determine security requirements for programming languages, architectures, tool deployment and maintenance, development environment, and operational environment.
- Develop a plan to correlate and prioritize software findings.
- Develop a plan to address legacy code in the software.
- Establish assurance requirements for software to deter, detect, react, and recover from faults and attacks.
- Perform initial software reviews and inspections and establish tracking processes for completion of software assurance requirements.
- Identify technical expertise needed to assist with software activities.
- Assess system requirements for inclusion of software.
- Establish baseline architecture and review for weaknesses (e.g., Common Weakness Enumeration) and susceptibility to attack (e.g., Common Attack Pattern Enumeration and Classification); refine architecture to reduce potential attack surfaces and mission impacts.
- Review architecture and design against secure software design principles, which include but are not limited to, system element isolation, least common mechanism, least privilege, fault isolation, input checking, validation, and patterns proven for building secure and resilient software.
- Confirm that software requirements are mapped to module test cases and to the final acceptance test cases.
- Determine automated software security checks throughout the software.
- Establish the software development life cycle, verification procedures, and tools as a core process.
- Enforce secure coding practices through code inspection augmented by automated static and dynamic analysis tools.
- Analyze and track software composition, including known vulnerabilities.
- Detect vulnerabilities, weaknesses, and defects in the software; prioritize; and remediate.
- Assess chain-of-custody from development through sustainment for any known remaining vulnerabilities and weaknesses and planned mitigations.
- Confirm hash checking for delivered products.

- Establish processes for timely remediation of known vulnerabilities in fielded commercial, COTS, and open-source components.
- Confirm that planned and automated software testing provides variation in testing parameters and system configurations to maximize coverage.
- Confirm that critical function software and critical components receive rigorous analysis and test coverage.
- Verify test resources, test cases, test scenarios, and test data.
- Continue to enforce secure design and coding practices through inspections and automated scans for vulnerabilities and weaknesses.
- Maintain automated code vulnerability scans, reporting, and prioritization, and execute defect remediation plans.
- Maintain and enhance automated regression tests and employ test coverage analyzers to increase test coverage.
- Conduct periodic penetration tests using the enhanced automated test coverage.
- Monitor evolving threats and attacks, respond to incidents and defects, identify and address vulnerabilities, and incorporate software-enhancing upgrades.
- Review chain-of-custody across development, from development to sustainment, and during sustainment for the record of remaining weaknesses and vulnerabilities and planned mitigations, as appropriate.
- Review the suggested best practices in the planning and execution sections (5.5.1 and 5.5.2) and pose the following questions:
    - Is the program following the suggested practice or performing the suggested activity?
    - If not, is there a risk to software development and delivery by ignoring that practice or activity?

5.6 Managing Risk for Defense Business Systems (DBS) Acquisition Pathway

The Defense Business Systems (DBS) Acquisition pathway is used to acquire information systems that support DoD business operations. The DBS pathway for the Defense Acquisition System is planned, developed, and executed in accordance with DoDI 5000.75, "Business Systems Requirements and Acquisition." This pathway applies to defense business capabilities and their supporting business systems, including those with "as-a-service" solutions such as financial and financial data feeder; contracting; logistics; planning and budgeting; installations management; human resources management; and training and readiness systems. It also may be used to acquire non-developmental software-intensive programs that are not business systems.

Figure 5-10 provides the framework for acquisition and business decisions in the life cycle and may be tailored as necessary to contribute to successful delivery of business capabilities.



Source: DoDI 5000.75.

Figure 5-10. Business Capability Acquisition Life Cycle

5.6.1 DBS Capability Need Identification Phase

- The capability need is based on the desired end state in a business mission area, the problem(s) preventing it, and the future capabilities required to achieve it.
- Definition of the future capabilities will include analysis of other organizations with similar capability needs.

5.6.1.1 Suggested Best Practice Activities in the Capability Needs Identification Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the DBS pathway Capability Needs Identification phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Identify business and mission need.
- Define capabilities to deliver business and mission need.
- Conduct analysis of performance measures.
- Ensure the program follows and implements applicable laws, regulations, and policies.
- Perform cost analysis to complete next steps.

5.6.2 DBS Solution Analysis Phase

- Future capabilities are based on re-engineering the high-level future business processes that will deliver the capabilities. This includes selecting and tailoring commercial best practices to meet the needs of the end user community.
- Definition of the future capabilities will include market analysis and research of other organizations with similar capabilities to identify processes that can be adopted.
- The functional sponsor must ensure funding is available to support the phase activities and must provide a plan for funding future phases, as appropriate. The availability of funding must be validated by the appropriate resource official before the Functional Requirements Authorization to Proceed (ATP).

5.6.2.1 Suggested Best Practice Activities in the Solution Analysis Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the DBS pathway Solution Analysis phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Build on concept and requirements description.
- Develop "to-be" capability process maps for each business capability.
- Develop initial capability implementation plan.
- Determine rough order of magnitude estimates and cost benefits.

5.6.3 DBS Functional Requirements and Acquisition Planning Phase

Functional requirements describe how the business system will achieve the future business processes.

The PM engages further with industry (e.g., market research, benchmarking, requests for information, industry days) so functional requirements reflect the current state of practice and inform the Acquisition Strategy. Additional information on functional requirements is included in Appendix 4D.

The appropriate cost agency will support development of alternatives and determination of the solution approach that best fits the needs and organizational goals based on economic analysis in accordance with DoDI 7041.03, "Economic Analysis for Decision-Making."

The Acquisition Strategy included in the capability implementation plan reflects the solution approach and describes how the PM will identify and select business system solutions. Additional information on criteria for potential business system solutions is included in Appendix 4D.

The PM may, with the approval of the DA, conduct design specification activities normally conducted after the Acquisition ATP to inform the Acquisition Strategy. As appropriate, the PM will partner with the contracting officer to develop draft RFPs that align with the Acquisition Strategy for the contract actions that follow the Acquisition ATP.

Before the Acquisition ATP is approved, the appropriate Chief Management Office (CMO) decision authority will approve the initial certification based on the chosen approach. Additional information on CMO certification is in Appendix 4C.

5.6.3.1 Suggested Best Practice Activities in the Functional Requirements and Acquisition Planning Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the DBS pathway Functional Requirements and Acquisition Planning phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Identify and define IT functional requirements and information assets.
- Conduct market analysis.
- Establish a process for determining the Acquisition Strategy.
- Establish a process for choosing a solution approach.
- Identify funding.
- Include a risk-based life cycle management approach to address supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and by developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain throughout the entire life cycle.

5.6.4 DBS Acquisition, Testing, and Deployment Phase

After selecting a solution according to the Acquisition Strategy, the program should conduct a fit-gap analysis based on known capabilities of the COTS/government off-the-shelf (GOTS) software in the selected business system solution.

Design specifications will reflect fit-gap analysis and prioritization of features to allow for cost and schedule trades within scope. The implementation plan should describe the baseline for development, delivery, and support activities, expressed in terms of releases and deployments.

- A limited deployment is any deployment before the Full Deployment ATP that provides a set of functionalities to a set of users of the business system. The functional sponsor and PM will recommend the functionality and number of users. Limited deployments will be approved at a Limited Deployment ATP.
- The DA will require sufficient testing before Limited and Full Deployment ATPs. For business systems on the DOT&E Oversight List, DOT&E will approve all operational test plans, and an IOT&E will be conducted before the Full Deployment ATP.
- Full deployment is the delivery of full functionality planned to all planned users of the business system in accordance with the Full Deployment ATP.

The DA will oversee establishment of cost, schedule, and performance parameters for each release before development or delivery.

5.6.4.1 Suggested Best Practice Activities in the Acquisition, Testing, and Deployment Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the DBS pathway Acquisition, Testing, and Deployment phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Establish a process for selecting a solution.
- Perform fit-gap analysis.
- Develop or update design specification.
- Establish a process to conduct continuing cost, schedule, and performance assessments as needed.

5.6.5 DBS Capability Support Phase

The functional lead, with the support of the PM, leads development of capability requirements, business process design and re-engineering, and training for the business system in support of continuous process improvement.

The functional lead and PM jointly develop and execute tailored capability implementation plans for each new set of capability requirements addressed in this phase.

The functional lead and PM will continue periodic assessments of opportunities available in the marketplace to determine changes necessary to reduce costs or improve efficiencies to maintain the relevance of the capability and the business system.

The PM will establish and manage cost, schedule, and performance metrics associated with upgrades to the approved baseline.

5.6.5.1 Suggested Best Practice Activities in the Capability Support Phase to Reduce Risk

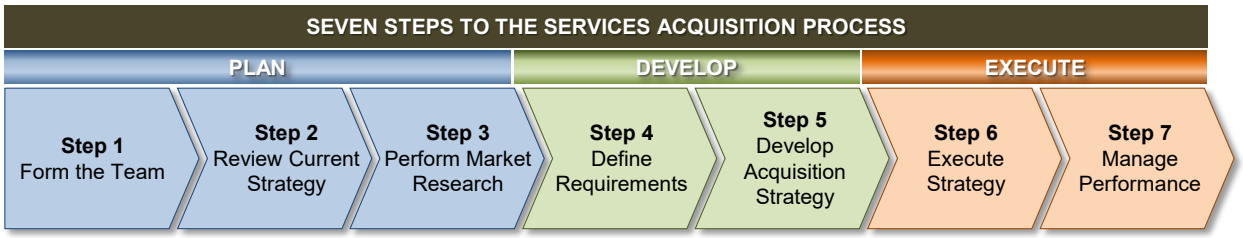
(Note: The activities listed below are suggested best practice for programs to consider during the DBS pathway Capability Support phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Perform limited developmental testing and document the results.
- Perform full operational testing and document the results.
- Conduct frequent assessments to determine software capability maturation.
- Develop or update transition and sustainment plan.

5.7 Managing Risk for Acquisition of Services Pathway

This pathway is for the acquisition of contracted services with a total estimated value at or above the simplified acquisition threshold (SAT). This pathway is intended to assist programs to identify the required services, research the potential contractors, contract for the services, and manage performance. The pathway activities are broken into three phases: Plan, Develop, and Execute.

The Acquisition of Services pathway phases incorporate the "Seven Steps to the Service Acquisition Process" outlined in DoDI 5000.74. Figure 5-11 shows the steps. Additional guidance is available from the DAU Service Acquisition Mall (SAM) website and the Guidebook for Acquiring Engineering Technical Services (ETS), Version 2.0 (2017).



Source: Adapted from DoDI 5000.02.

Figure 5-11. Seven Steps to the Services Acquisition Process

5.7.1 Acquisition of Services Planning Phase

In Step 1, the PM, or Functional Services Manager (FSM), as designated by the decision authority or designee, is the lead responsible for bringing together the appropriate cross-functional individuals for the Multi-Functional Team (MFT). The team members will understand the requirement, understand how the requirement relates to the mission, and be able to put an executable strategy together in support of the mission.

In Step Two, the MFT is responsible for assessing the health of the current service acquisition, if one exists. If this is a new service acquisition, move to Step Three and use the questions below to formulate the strategy. To accomplish this assessment, the MFT will interview the stakeholders and key customers and capture their concerns, priorities, and projected requirements, which will affect how the acquisition is developed.

In Step Three, the program will gather and analyze information about the capabilities within the market to satisfy the agency needs. This step is vital for accomplishing the next two steps, Define Requirements and Develop Acquisition Strategy.

5.7.1.1 Suggested Best Practice Activities in the Planning Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs during the Acquisition of Service pathway Planning phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Understand the services acquisition process.
- Apply and use the Acquisition Requirements Roadmap Tool (ARRT) to define and refine service requirements in order to create an initial draft of the Performance Work Statement (PWS) and Quality Assurance Surveillance Plan (QASP).
- Develop specific acquisition-related documents (i.e., team charter, project plan, stakeholder analysis, PWS, QASP, and an acquisition approach.).
- Find the right people, with the appropriate expertise and skill set, for the team.
- Identify senior leadership and stakeholders who are affected by the outcomes to ensure their involvement and support.
- Develop a Communication Plan to keep stakeholders and others informed of the requirements' status and direction. Conduct an initial risk analysis/assessment (primarily programmatic and business risks)
- Create a project library to maintain the knowledge base.
- Identify and plan for needed training as the team moves through this acquisition.

5.7.2 Acquisition of Services Development Phase

In Step Four, requirements definition is the most important and most difficult part of services acquisition. A good quality requirements document makes procuring and managing the service well organized and efficient. During this phase, the team, with the FSM as the lead, may produce the following:

- A risk analysis

- Performance objectives and standards through the use of a requirements road map concept
- Methods and means of inspection
- PWS, Statement of Work (SOW), or Statement of Objectives (SOO)
- Preliminary QASP
- Independent Government cost estimate
- Stakeholder consensus

In Step Five, the Acquisition Strategy describes the FSM's plan to achieve the execution of goals set within the service acquisition life cycle. The MFT summarizes the overall approach to acquiring services (including the schedule, structure, risks, funding, and business strategy). The Acquisition Strategy documentation should contain sufficient detail to allow senior leadership and the Service Category Decision Authority to assess whether the strategy makes good business sense, effectively implements laws and policies, and reflects management's priorities, including affordability. The strategy could evolve over time and should always reflect the current status and desired mission outcome. The MFT will review Step Five under the Service Acquisition Mall. The following are key outcomes of the Acquisition Strategy:

- Allow for competition.
- Provide opportunity for small business.
- Select the appropriate contract type.
- Determine a performance incentive approach.
- Determine the appropriate source selection approach to achieve the best value contractor .
- Develop appropriate planning documents.
- Nominate a Contracting Officer's Representative (COR)
- Post a draft RFP (recommend posting for industry comments).

5.7.2.1 Suggested Best Practice Activities in the Develop Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the Acquisition of Services pathway Development phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Conduct risk analysis.
- Performance objectives and standards through the use of a requirements road map concept.

- Select the appropriate contract type.
- Determine a performance incentive approach.
- Determine the appropriate source selection approach to achieve the best value contractor .Develop appropriate planning documents.
- Develop methods and means of inspection.
- Prepare an initial draft PWS, SOW, or SOO.
- Prepare and post a draft RFP; respond to industry with Q&A
- Prepare preliminary QASP.
- Perform the independent Government cost estimate.
- Acquire stakeholder consensus and obtain approval from the Service Requirements Review Board.

5.7.3 Acquisition of Services Execution Phase

In Step Six, after the team has completed the required planning in Steps Four and Five, the FSM reads the pre-solicitation documentation one more time before presenting the required documents to the Contracting Officer for execution. The FSM ensures the requirement, the QASP, and the Incentives demonstrate what the outcome should be and how the contractor's performance will be measured. If the documents represent the services acquisition adequately, the documents are transferred, along with the funding document, to the Contracting Officer for contract execution. The MFT will review Step Six under the Service Acquisition Mall.

In Step Seven, the result should be that the acquisition delivers the performance results the stakeholders need to successfully support their mission, but the team may remain engaged with the contractor and stakeholders over several years. There are two key elements to this step: (1) the basic functions of administering the contract such as validating contractor invoices, tracking cost data when required, managing change as it occurs and making sure the contractor is getting paid on a timely basis; and (2) managing the relationship and expectations between three key groups: customers, stakeholders, and the contractor.

Developing an environment of trust and fair play is vital to keeping all parties focused on achieving the intended mission results. This includes assessing performance using the QASP, documenting performance for any incentive arrangement you may have created, and finally making sure performance is documented annually in the Government past performance database with a fair and objective Contractor Performance Assessment Reporting System.

5.7.3.1 Suggested Best Practice Activities in the Execution Phase to Reduce Risk

(Note: The activities listed below are suggested best practice for programs to consider during the Acquisition of Services pathway Execution phase. Programs should tailor the activity lists as appropriate to meet the Acquisition Strategy objectives.)

- Conduct rigorous source selection.
- Adopt methodologies that support test and evaluation as a continuum.
- Ensure pre-award approval documents are complete.
- Finalize QASP.
- Develop post-award implementation/transition plans.
- Transition to performance management.
- Manage performance results in accordance with QASP/Service Delivery Summary (SDS)
- Conduct quarterly supplier and key stakeholders performance reviews.
- Evaluate effectiveness of strategy.
- Develop plan for managing continuous improvement.
- Document contractor performance annually through the Contractor Performance Assessment Reporting System (CPARS)

Appendix A. Additional Methods and Considerations for Managing Risk in Defense Programs

This guide has described a recommended RIO management approach for DoD programs to apply early in program development and continuously throughout the acquisition life cycle. DoD programs also use other methods for specific risk management purposes at points in the life cycle.

This appendix discusses risk management as it relates to spectrum supportability and compatibility, information technology, software engineering, and digital engineering. The Risk Management Framework (RMF) and Mission-Based Cyber Risk Assessment processes may be used in addition to general risk management processes to inform spectrum supportability, electromagnetic protection (EP), cybersecurity and information systems programmatic risks. Programs should develop a method to map specialized spectrum supportability, EP, and cybersecurity risks and issues into their management processes and should evaluate cost, schedule, and performance risks associated with the implementation of spectrum supportability, EP, and cybersecurity requirements and testing.

A.1 Risk Management Framework for DoD Systems

DoDI 8510.01, "Risk Management Framework (RMF) for DoD Systems," brings a risk-based approach to the implementation of cybersecurity, supports cybersecurity integration early and throughout the system life cycle, promotes reciprocity to the maximum extent possible, and stresses continuous monitoring. DoDI 8500.01, "Cybersecurity," establishes a DoD cybersecurity program to protect and defend DoD systems. In accordance with DoDI 8510.01, the RMF replaces the DoD Information Assurance Certification and Accreditation Process and adopts the term "cybersecurity" in place of "information assurance."

The RMF process is applicable to all DoD systems, as well as to DoD partnered systems for which it has been agreed that DoD standards will be followed. All DoD systems must receive and maintain a valid authorization before beginning operations. Technologies below the system level do not require an Authority to Operate; however, these technologies must still complete specific RMF assessment procedures under the "Assess Only" process. The RMF integrates methodologies that support test and evaluation as a continuum.

The RMF process consists of seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. This process parallels the system life cycle, as the program initiates RMF activities at program or system inception (e.g., documented during capabilities identification or at the implementation of a major system modification).

The DoD governance structure implements the three-level approach to the cybersecurity risk management described in NIST SP 800-39. Level 1 is the Organization level. The organization

described in Level 1 is the OSD or strategic level. It addresses risk management at the DoD enterprise level. The key governance elements and resources in Level 1 are the DoD CISO, the Risk Executive Function, DoD Cybersecurity Architecture, RMF TAG, and RMF KS. Level 2 is the Mission or Business Processes. The key governance elements and resources in Level 2 are JCA CPM, PAO, DoD Component CIO, and DoD Component CISO. Level 3 is the Systems level. The key governance elements and resources in Level 3 are AOs and the System Cybersecurity Program.

A.2 Mission-Based Cyber Risk Assessments

DoDI 5000.89, "Test and Evaluation," requires acquisition programs to conduct Mission-Based Cyber Risk Assessments (MBCRAs). Cyber Table Top is a type of MBCRA – a methodology to analyze a system and its operations and identify and prioritize potential cyber risks as described in the DoD Cyber Table Top Guide (2021). The method is an intellectually intensive exercise that explores the effects of cyber-offensive operations on the capability of U.S. systems to carry out their missions. It is a wargame-like exercise that involves two teams with opposing missions: the military forces charged with executing an operational mission and the cyber mission forces attempting to oppose those military forces.

The CTT provides systems engineers, PMs, information system security managers, information system security engineers, testers, users/operators, and other analysts with information on cyber threats to the mission. Useful information includes potential system vulnerabilities, demonstrated means of exploitation of those vulnerabilities, and an assessment of the resulting mission impacts. This information enables leaders to allocate their limited resources more effectively toward delivering a system that will operate successfully in contested cyberspace.

The CTT, in conjunction with other tools and processes, provides the developers and the PM's engineering and test teams with opportunities to reduce risk throughout the life cycle of the acquisition program and reduces the likelihood of discovering cyber vulnerabilities during operational testing.

A.3 Software Engineering in RIO Management

A.3.1 Modern Software Development and Integration with RIO Management

Recent rapid advances in software engineering skills, technology, and modern software development practices (including but not limited to Agile/DevSecOps approaches, automation, pipelines, tools, metrics, continuous integration, continuous delivery, and continuous deployment) have proven successful in a competitive commercial marketplace. Modern software approaches using Agile are iterative and strive for continuous build, integration, and test (test and evaluation as a continuum). DevSecOps extends beyond Agile including a pipeline for deploying

to operations and addresses security throughout the methodology. To leverage useful commercial best practices, the Department is working to update policies and processes, modernize culture and workforce competencies, and provide enterprise-wide solutions to keep pace with modern advances in software development. The DoD Enterprise DevSecOps Fundamentals (2021) provides information on DevSecOps, including normalized definitions of DevSecOps concepts.

With the drive to more frequent releases and rapidly obtaining feedback from users, the modern approaches can allow programs to assess RIO more frequently and possibly retire risks while identifying new risks, issues, and opportunities. Most organizations have existing tools for RIO management and are transitioning to a more robust digital engineering environment that aligns with Agile and DevSecOps methodologies. RIO management is one area that would benefit from automation that ties into adopted commercial modern software practices and the Department's infrastructure. The challenge will be integrating Agile and DevSecOps approaches with the enterprise risk management process. Programs should consider establishing automated links from software development to feed the overall RIO management of a program and achieve a balance between modern software approaches and traditional risk management.

A.3.2. RIO in Agile and DevSecOps Practices

Agile development methodology generally has a product vision, a product road map, product backlog, a dashboard, or some way of managing work in a sprint and its relation to an iteration. During a sprint, the development team meets in a daily standup to discuss where they are on assigned work and any impediments. They may also discuss risks, issues, and opportunities. Some of the assigned work may be linked to a specific risk, and as work progresses, live updates can be made to risk or issue burn-down plans discussed earlier in the RIO Guide. The program may integrate the processes and tools into an automated approach to continually update risks, issues, and opportunities. This continuous update aligns with the DoD initiative test and evaluation as a continuum.

Figure A-1 illustrates a DevSecOps diagram and a relationship with a generic Agile process and some Agile artifacts. The following vignette illustrates the interaction of Agile and the RIO process.

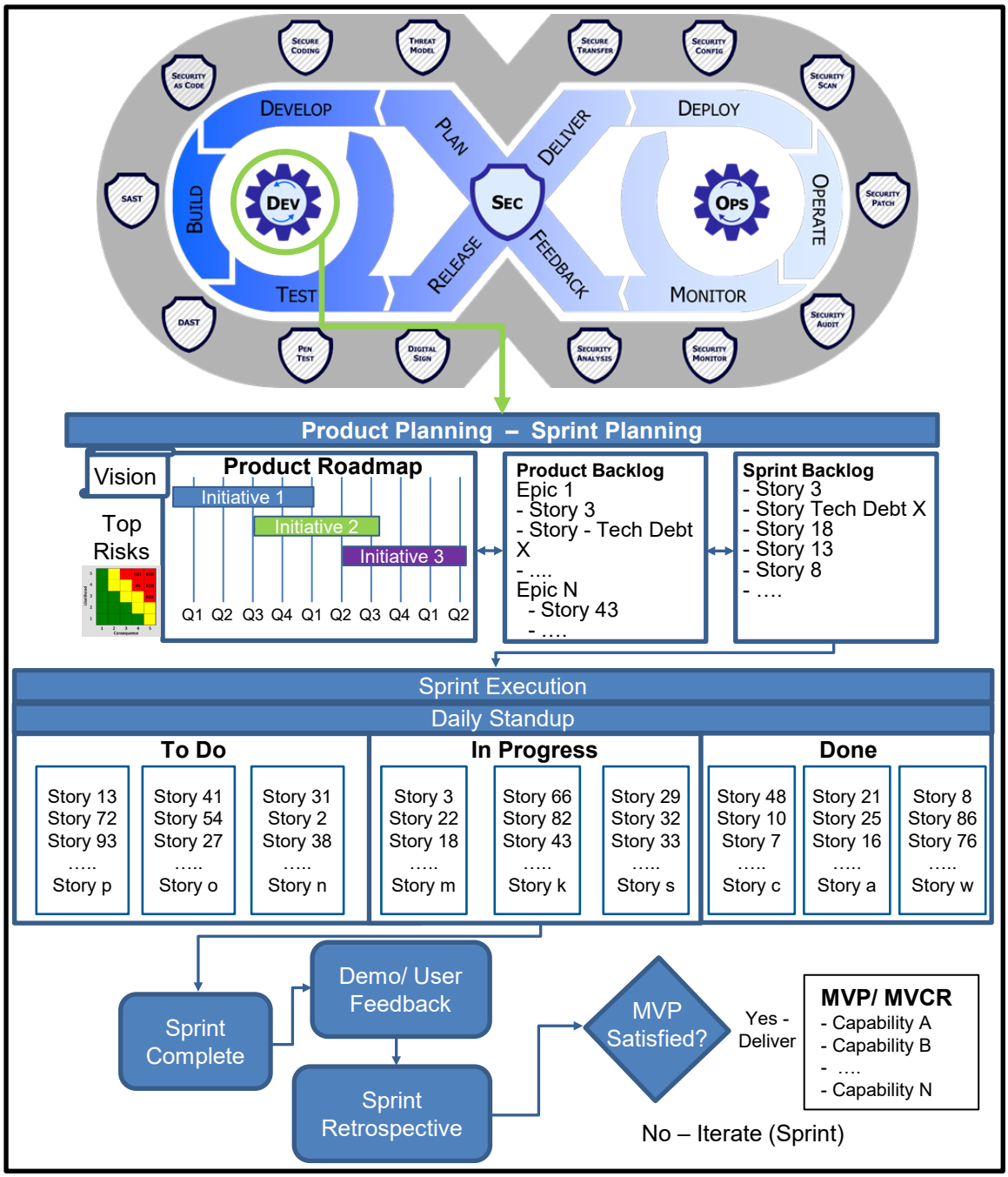


Figure A-1. DevSecOps Life Cycle and Generic Agile Process

Vignette: Agile and RIO Management of a Safety Concern

Background

The cross-functional product team has executed several sprints of development, obtained feedback from users, and has updated its product backlog after each sprint retrospective. While users have been pleased with the current capabilities, the product team has accumulated technical debt from taking a few shortcuts in development to meet schedule. The software developed so far works, but as more features are added, the current

architecture will not be the best way forward for performance, maintainability, and safety concerns.

The safety expert for the cross-functional team identified a safety concern in the prior sprint, but the team proceeded with the existing architecture that may not support obtaining a safety release for the Minimum Viable Product (MVP). The team linked this architectural technical debt to an original program risk on safety release approval and added it to the product backlog.

During the last sprint retrospective, some of the developers raised concerns about future maintenance of the code base. The concerns centered on an inherited monolithic module from fielded software that should be more modular and less tightly coupled. Without changes, e.g., refactoring, the code base could be problematic to modify as changes in one area may cause problems in other areas, thus requiring more changes to add features or fix defects. The team agreed the concerns were valid and added them to the technical debt of the product backlog. A future sprint or sprints would start addressing this maintainability and the safety architectural concerns.

Situation

During planning for this sprint, the team agreed that the safety and modularity technical debts should be addressed sooner rather than later. Both would need refactoring and modifying the architecture to resolve.

The safety concern arose because multiple components in the same computer process had different levels of rigor in safety requirements. This grouping violated architectural partitioning approaches to ensure a component, one developed and tested to a lower level of rigor, does not take down or corrupt a safety-critical function, possibly causing unsafe behavior for the product. Partitioning would require more development as it would require a different interprocess communication approach and partitioning modules based on the assigned levels of rigor in each component. The coupling and modularity would require refactoring and separating a large module into smaller parts.

Considering the effort, the team agreed they could accomplish the goal in two sprints. To keep the first sprint as a working product, the team decided to use a strangler architecture pattern to isolate parts not yet refactored or redesigned from parts that have moved to the new architecture. The team agreed to address part of the safety concern and part of the coupling concerns in this iteration and address the remaining architecture concerns in the next iteration. The team added the technical debt for this sprint to the sprint backlog.

Looking at the ongoing effort, the team has multiple risks. There is the previously identified program-level risk in obtaining a safety release in time for operational testing. There is a software maintainability risk that the code is fragile and changes in one area could break functionality in other areas. Finally, there is a risk that changes in the architecture may affect performance to an unacceptable level.

These risks may be managed in a traditional approach versus an agile approach (Figure A-2), as discussed in the following paragraphs.

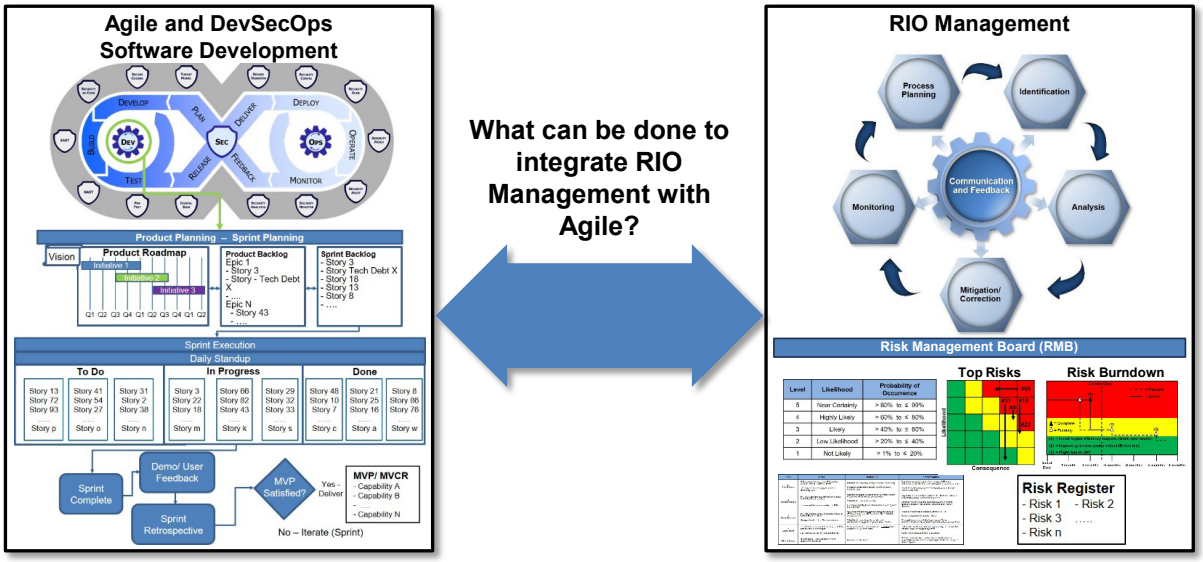


Figure A-2. Integrating RIO Management with Agile and DevSecOps

Traditional Approach to RIO Management

The safety release risk would be identified during the program planning, analyzed, and added to the risk register. The program would then determine its response to the risk, which would be to mitigate the risk. The safety engineer would be assigned to develop a mitigation plan for the risk, which most likely would use the items from safety processes to build steps to mitigate the risk and track those steps in a risk burn-down chart. Steps in the burn-down might be: review the architecture for safety concerns; develop fault tree analysis for safety-critical failures; develop safety tests; pass software testing for safety concerns; complete documentation for safety release; and finally obtain a safety release. This mitigation plan would be executed until the program obtains the safety certification.

The software maintainability risk, identified once the software team started working with the inherited code, would be taken to the Risk Management Board. Once the board agreed it was a risk, the program would perform additional analysis to determine its likelihood and consequence. Since the consequence criteria do not address future changes to the software and emphasizes a concern about meeting major milestones, product key performance measures, and cost overrun before fielding, the risk is rated highly likely, but low consequence. This information would be presented to the Risk Management Board, and the board could decide to accept the risk. If it becomes an issue, then the program will address it during sustainment of the software.

The performance risks resulting from architectural changes would go to the Risk Management Board, which would agree it is a risk, then assign the software team to analyze further and brief the board. Once briefed on the likelihood and consequences, the board would decide to mitigate the risk. The board would assign the software team to develop a mitigation plan. The software team's mitigation plan would involve prototyping two alternatives or more, picking a path forward in the architecture, and implementing the path. The prototyping efforts would be put into a risk burn-down chart and executed over the time necessary to complete the prototyping and analyze the alternatives. The software team would brief the results to the board and get agreement on a decision for a path forward.

Agile Approach to RIO Management

During program planning the safety risk would be identified, agreed on, and added to the risk register. The software development team would be organized in a cross-functional manner with team members who have expertise in safety engineering. Rather than developing a mitigation plan upfront, the safety engineer and the product owner would discuss what safety concerns need to be addressed and work together over multiple sprints to iterate the product to address the safety concerns.

Each sprint would offer continuous review of the architecture and its conformance to addressing any safety concerns. Each sprint would allow evolving the fault tree analysis based on current user stories in development, evolving failure mode tests in each sprint, and injecting failures in unit and integration tests to make the software more resilient for safety. A risk burn-down chart for the risk may be the following steps: fault tree analysis incorporated into the sprint cadence; passing of safety tests for sprint included in definition of done; artifacts for safety automatically generated from the sprint build, integration, and test; and obtaining the safety release.

The first two burn-down items could initially occur in one sprint. The automatic generation of artifacts may be implemented in one or more sprints depending upon the infrastructure and ecosystem of the software development team. These three steps, after one to two sprints, would enter continuous execution on each sprint as the team has collaboratively taken ownership of the safety implementation. The burn-down of the first three steps would move the risk to low, assuming the team continually addressed the needs of the safety engineer.

The only step remaining would be to obtain the safety release when needed, using the artifacts for that release. Since the artifacts are generated each sprint, those can be provided in early forms to the safety release authority to gain early feedback on adequacy. The Risk Management Board would monitor the continued execution of safety concerns or possibly retire the risk after a few sprints.

The software maintainability risk identified once the software team started working with the inherited code would be analyzed in a quick manner, and since the team is concerned about the ability to rapidly deploy changes, possibly due to cyber threats or new operational needs, it internally takes on the mitigation of the risk and moves forward making plans to mitigate. The team would report the risk and mitigation plans to the Risk Management Board. The plan consists of several steps: develop the decoupling approach; implement phase 1 of the decoupling approach; implement phase 2 of the decoupling approach; and monitor future changes for robustness of the revised architecture. Data on the impact of future changes breaking the delivery or requiring other changes will be collected using automated capabilities within the ecosystem to continuously evaluate the architecture and code fragility. This will allow rapid feedback so each sprint and the team can pivot quickly to address any identified concerns.

The performance risks due to architectural changes would be examined by the product team. Given the concern, the scrum master and product owner could decide to prototype two different approaches to determine which works best in their target environment.

Since the ecosystem has an established pipeline from development to test to deployment, minor configuration and script changes will allow two branches of the code base to be moved through the pipeline and assessed.

The current sprint would address the first three steps, or it would determine performance will not be met and something else needs to be done. If performance is met, then the next sprint will incorporate the architectural change. If performance is not met, then the program may need to make some significant decisions, which could be a major redesign of the product architecture, looking at other alternatives, getting relief on performance, or scrapping the product as it is not feasible to meet the performance requirements. The team, as well as the customer, would have evidence early in development to make an informed decision on the path forward.

Comparison of RIO Management Approaches

Table A-1 compares the two approaches described on the three risks, highlighting key areas to consider.

Table A-1. Comparison of Traditional and Agile Approaches on Vignette Risks

Risk	Traditional RIO	Agile RIO
Safety Release	• Reviewed Periodically at Board (Monthly or every other week) • Mitigation burn-down over long period of time • Artifacts finalized at end and Safety release approved • Risk may become issue late in development	• Reviewed at beginning of each sprint and daily at standup • Mitigation burn-down occurs in a couple of sprints • Continuous monitoring of safety as a quality attribute with cross-functional team • Additional safety tests added as more is learned
Code Maintainability	• Possibly ignored until product fielded, deferring technical debt • Perhaps no measurement of maintainability tracked during development leaving unknown risk after fielding	• Ownership by team ensures maintainability quality attribute is examined along the effort and improved as each sprint iterates • Addressed as part of the iterative approach • Evidential data collected to inform future risk for maintainability
Performance	• Assessed early with prototyping • Heavier process may slow down the start of prototyping as team awaits approval of risk mitigation plan • Other development may be slowed while prototyping different approaches	• Assessed early with prototyping • Team approach owns the risk and collectively decides to address risk mitigation without delay • Team reports activities up to higher management but is empowered to make decisions at their level

Whether a program integrates its RIO Management Process into daily Agile and DevSecOps is something the program needs to decide. Integrating RIO management into the daily activities offers the opportunity to continually examine risks as the product is developed and can allow frequent feedback to the program and the customer. The challenge will be linking the day-to-day activities and RIO assessments into an enterprise risk management process.

Initially, integrating this activity may consist of people in the loop aggregating the day-to-day risks, or micro-risks, into top-level program risks. Alternatively, it could be addressing the macro-risks identified at program initiation and breaking the risk mitigation into smaller tasks to work off during one or more sprints. Both approaches should be applied, but at the micro level in Agile and DevSecOps activities, RIO most likely will be measured on a different consequence scale with low fidelity, just expressed as a low, moderate, or high risk. To aggregate or integrate these into a top-level program risk register requires some further thought by a program on how they would integrate with the program's tailored consequence definitions.

A.3.3 Using Metrics to Enhance Software RIO Management

In Agile software development and DevSecOps practices, metrics provide feedback to the product team on team performance, pipeline flow, and product value delivery, where the value is a working product in the customer's hands meeting the customer's needs. The guide Software Engineering for Continuous Delivery of Warfighting Capability (2023) includes a chapter dedicated to these metrics and includes case studies on their use.

A good metric can allow the PM and other team leadership to make good decisions, whether at the program level or during the sprint day-to-day activity level. Good decisions potentially facilitate risk mitigation and preclude issues. Poor metrics can lead to bad decisions, which will not improve the program's risk and issue levels. If the metrics are not working to inform the necessary decisions, the program should change the metrics to make them more useful and informative. In the Agile methodology, that means to pivot.

Each sprint retrospective allows an opportunity for the team to review what went well and what not so well. The metrics collected on stories completed versus planned may highlight areas of further discussion when the team falls short. Is there hidden technical debt causing challenges in completing stories, or was the estimate of the effort just wrong? Early in a project, the estimates may be a little off, but if the staff has been stable and operating for a while, there may be more going on than a bad estimate.

The lead time for a change to move from the backlog to delivered product provides insight into future delivery of changes. Measuring this process reveals important information about how long it will take to roll out a change to the warfighter when a vulnerability or a critical new

functionality is discovered. If the time is too long, the team needs to examine the DevSecOps pipeline and how to further improve the flow so that delivery at the speed of relevance is viable.

Four core measures of a software team output are Size, Time, Effort, and Defects.

Size: Common measures of size in use by modern software teams include story points, user stories, features, epics, and initiatives. Other measures of size such as source lines of code (SLOC), function points, requirements, and feature points also have been used successfully. Whatever measure(s) of size is (are) chosen, the most important aspect is to be consistent. Reducing the story point count as the team matures, or increasing the count when defects are discovered, could introduce risk that manifests in uncertainty of the program team performance, as size is a fundamental measure of a team's output.

Time (duration): Agile teams tend to favor pivoting when customer feedback suggests a change in the product's functionality; however, the project overall still typically needs to deliver on a planned or contracted schedule. Generally, there is no explicit measure of schedule, as it just happens with the passage of time; however, using the passage of time as a denominator for metrics such as velocity, story point development, defect burn-down, etc., can be quite insightful. Not measuring duration can pose a risk. For example, a team that produces 1,000 story points cannot claim this measure is either good or bad without knowing over what length of time these story points were developed. Even then, story points are a measure calibrated differently per team and are difficult to compare across teams. The team objectively assesses how many story points a given user story is worth.

Effort: The application of team resources on the project is a major contributor to project cost. But effort can also help determine how well a software team is progressing in flight. Usually measured in units of hours, effort is an input to the development process. Metrics such as hours per story point or hours per feature can be used to assess the ability of a team to meet story point or feature plans, as well as budget constraints. Not measuring effort presents a risk of overspending one's budget or spending too much on low-value features or stories.

Defects: If software fails to meet expectations, defects are logged and described. Defects are generally described in terms of severity and can be analyzed in order to determine how and when they should be resolved. Metrics such as defects per story point, defects per sprint, or simple counts of blockers help to guide the development team as sprint plans are put in place, and whether or not a feature will meet quality expectations by the customer. Measuring defects and analyzing them in the context of customer expectations is critical.

Metrics that cover flow, team performance, and value delivered provide feedback to the team for continued improvement to reach a state of high performance, which ultimately lowers the risk of program failures.

A.4 Digital Engineering in RIO Management

A.4.1 Digital Engineering Overview

In accordance with the DoD Systems Engineering Guidebook (2022), digital engineering (DE) is the DoD's initiative to transform the way it conceives, designs, develops, delivers, operates, and sustains complex systems in a formidable and changing threat environment. DE is an integrated digital approach using authoritative sources of system data and models as a continuum throughout the development and life of a system. DE updates traditional systems engineering practices to take advantage of computational technology, modeling, analytics, and data sciences.

As evidenced across the Services and industry, DE is a necessary practice to support acquisition in an environment of increasing global challenges and dynamic threat environments. DoD's approach to implementing DE is to "securely and safely connect people, processes, data, and capabilities across an end-to-end digital enterprise. This will enable the use of models throughout the life cycle to digitally represent the system of interest (i.e., SoS, processes, equipment, products, parts) in the virtual world" (DoD Digital Engineering Strategy 2018, p. 3).

A.4.2 Suggested Activities in Digital Engineering Implementation to Reduce Risk

DoD is working to increase the use of DE in the AAF pathways. The three important views in implementing DE or model-based acquisition with respect to risk are: (1) risks introduced by modeling deficiencies, (2) risks reduced by enhanced use of modeling, and (3) modeling to predict or assess risks (i.e., modeling for uncertainty quantification in acquisition and in the use of models).

The failure modes, effects, and criticality analysis (FMECA) is a risk process. It identifies what could go wrong, likelihood of occurrence, and the severity (consequence) if the failure occurs. DoDI 5000.88 requires the FMECA for all defense acquisition programs to be based on the digital representation of the system and the use of digital artifacts. When implemented in a digital engineering ecosystem, it enables the flow of identified risks from design to manufacturing to product support.

DoD focuses considers the following DE challenges as part of risk reduction efforts:

- What DE investments the program made during prior stages of the life cycle
- The respective organization's experience and lessons learned in implementing DE within similar or adjacent projects or programs (e.g., organizationally adjacent; functionally adjacent)
- The remaining activities to be performed (e.g., design, testing, sustainment, retirement, reuse, etc.)

- Enterprise data management to ensure authoritative data and models are widely available or accessible
- Technical solutions to provide collaborative, agile, secure, interoperable, and responsive digital ecosystems
- Cybersecurity protection to data, networks, and hosting environments while managing access controls, data at rest, spillage control, and exfiltration mitigation
- Useful and shared examples of incremental DE or model-based systems engineering implementation and execution
- Growing the DE Body of Knowledge (DEBoK) (de-bok.org), a shared knowledge base containing authoritative sources and lessons learned
- Establishing a DE capability to support automated approaches for testing, evaluation, and deployment throughout the defense acquisition process
- Whether the Government has sufficient insight (WBS level) within the Digital Engineering Ecosystem to assess program progress, technical risk, etc.?
- Contractual intellectual property rights: Are they sufficient to support the program's development and sustainment strategies?
- Trained workforce, both contractor and Government, in digital engineering practices and methodologies
- Status and maturity of verified, validated, and accredited models for their planned usage (design, requirements development, sustainment, testing, etc.)
- Whether the Government will receive required models as Contract Data Requirements List (CDRL) items needed to support the program in sustainment

Data on failure modes, hazards, and defects are assessed as risks or issues differently across various communities. Their modeling is likely to reflect their current approach to analysis and attribution of severity and likelihood, but not necessarily likely to match the guidance currently in this document or to be reusable between models in a DE ecosystem.

A.5 Independent Technical Risk Assessment in RIO Management

A.5.1 ITRA Overview

In 2017, Congress began requiring the Department to conduct Independent Technical Risk Assessments (ITRAs) on Major Defense Acquisition Programs (MDAPs) in advance of milestone and production decisions. In accordance with DoDI 5000.88 and DoD ITRA Execution Guidance, ITRAs provide senior leaders with an independent view of program

technical risk, including the maturity of critical technologies and manufacturing processes. The Under Secretary of Defense for Research and Engineering (USD(R&E)) engineering team conducts ITRAs on Acquisition Category (ACAT) ID programs for USD(R&E) approval and maintains the policy and guidance for ITRAs. The Services or Agencies conduct ITRAs on ACAT IB/IC programs with the approval authority determined by the USD(R&E). When the USD(R&E) determines that the ACAT IB/IC program's ITRA should be approved by the USD(R&E), the OUSD(R&E) team works with the Service or Agency to process that assessment for USD(R&E) approval. ITRAs are conducted in accordance with DoDI 5000.88 policy and DoD ITRA Execution Guidance (2020).

A.5.2 ITRA Technical Risk Areas and Factors

The Defense Technical Risk Assessment Methodology (DTRAM) refers to eight technical risk areas and the seven factors.

Technical Risk Areas:

- Mission Capability
- Technology
- System Development and Integration
- MOSA (Modular Open System Approach)
- Software
- Security/Cybersecurity
- Manufacturing
- RAM (Reliability, Availability, Maintainability) and Sustainment

Assessment Factors:

- Scope and Requirements
- Design and Architecture
- Decision and Control
- Schedule
- Resources
- Evaluation
- Performance and Quality

A.5.3 ITRA Risk Categorization and Execution

The ITRA will document and characterize each risk in terms of consequence to the program and to any interdependent programs should the risk be fully realized, and the likelihood the risk will occur. If known, the cause of the event or condition also should be described. Risks will be analyzed using the likelihood and consequence criteria as established in section 2 of this guide. Using these predefined likelihood and consequence criteria will provide a structured means for consistent evaluation of risks. Any deviations from these criteria should be noted in the assessment along with associated rationale.

Assessors will underpin the assessment with engineering analysis and data. Risk consequence will be described as a potential deviation against cost, schedule, and performance in program plans or established baselines. Assessments will attempt to capture all cost, schedule, and performance impacts of a given risk. The consequence rating should capture the greatest anticipated impact in cost, schedule, or performance as if the risk were fully realized, that is, without further risk reduction or mitigation efforts.

Wherever possible, fully burdened costs should be used in risk assessments. For independent risk assessments, when evaluating likelihood, the independent team should consider the strength of the planned mitigation and the history of similar programs in successfully burning down and mitigating risks.

A.6 Technology Transfer Consideration in RIO Management

This guide primarily describes risk in technical or programmatic terms; however, research security issues, such as unwanted technological transfers to strategic competitors, may also pose an acute risk to the DoD's acquisition programs and technological advantage. Most technologies are not classified at their inception, including those with clear military applications. This leaves them at risk of exploitation by adversaries. Too often, adversaries and strategic competitors use publicly available funding and program information in the United States to locate relevant U.S. entities to target, including companies and universities funded by DoD to conduct R&D. Adversaries and strategic competitors may find ways to transfer technologies from such U.S. (and allied) entities; coerce companies to disclose intellectual property; and undercut free and fair markets.

Figure A-3 depicts an example of Unwanted Technology Transfer Mechanisms.

Source: OUSD(R&E) Science and Technology.

Figure A-3. Unwanted Technology Transfer Mechanisms

In accordance with DoDD 5000.01, DoDI 5000.02, and DoDI 5000.83, S&T managers and lead systems engineers are charged with tailoring technology area and protection planning as an S&T project transitions to a program of record through the AAF. OUSD(R&E) has established a number of documents to support S&T managers and lead systems engineers as they seek to mitigate threats to U.S. technology advantage. Documents such as the S&T Protection Guide and Program Protection outline and guidance discuss how to build an iterative record of risk management. As an example, at the start of an S&T project, S&T managers should conduct an initial risk assessment, and later they should draft and approve an S&T Protection Plan adapted to the particular acquisition pathway (i.e., grants, contracts, or in-house research). They should also implement S&T protection measures in later steps, such as the Broad Agency Announcement (BAA) and RFP, Source Selection, and Award.

While inherently part of an integrated approach to protection across the DoD acquisition life cycle, S&T protection management principles are distinct from program protection. Like program protection, S&T protection activities focus on protecting Essential Technology

Elements (ETEs) and enabling technologies to reduce compromise or loss of the DoD's technological edge and to guard against unwanted technology transfers.

Unlike program protection, S&T protection plans may not be required in every instance. S&T protection plans, if required, are based on an upfront risk review and technology element identification that accounts for the Critical Programs and Technologies List (CP&T) and Technology Area Protection Plans. The protection approach should be refreshed periodically throughout the program life cycle.

.

Appendix B. Program Risk Management 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.

B.1 Program Risk Management 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 PRMP document, but the same principles apply for issues and opportunities, which programs should likewise develop and document, combining into the PRMP document, if desired.

The PRMP 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 PRMP at the program's initial formulation and update it at intervals during the acquisition life cycle (e.g., when a program is re-baselined, 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 PRMP outline:

- **Introduction** – Overview of the purpose and objective of the PRMP, the strategy to implement continuous risk management, including 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 management process planning before contract award and add to or modify the risk management plan after contract award. Events that may drive updates include acquisition milestones, contract award, system-level technical reviews, a change to the Acquisition Strategy, program re-baselining, 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.).

B.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 engage their component spectrum management office (SMO) for assistance with conducting SSRAs and E3 assessments. 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 (Figure B-1). On fixed-price contracts, the contractor usually has the decision authority.

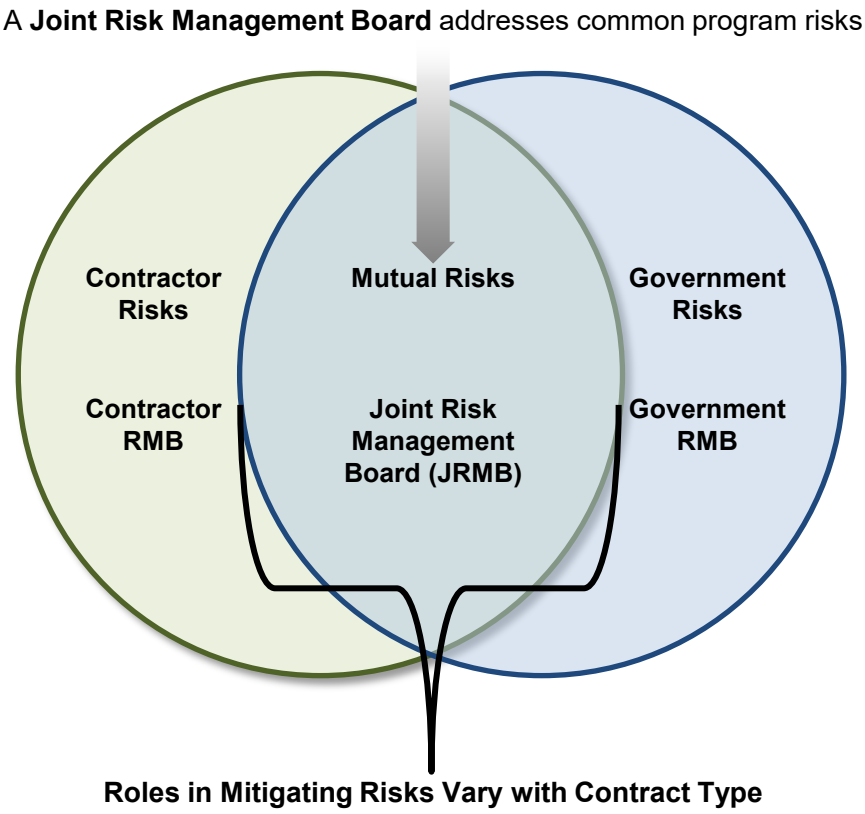


Figure B-1. Government and Contractor Joint Risk Management Boards

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 (ROMBs) 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.

B.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.

B.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 PRMP document.

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 B-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 B-2 may be eliminated for specific programs or risks.

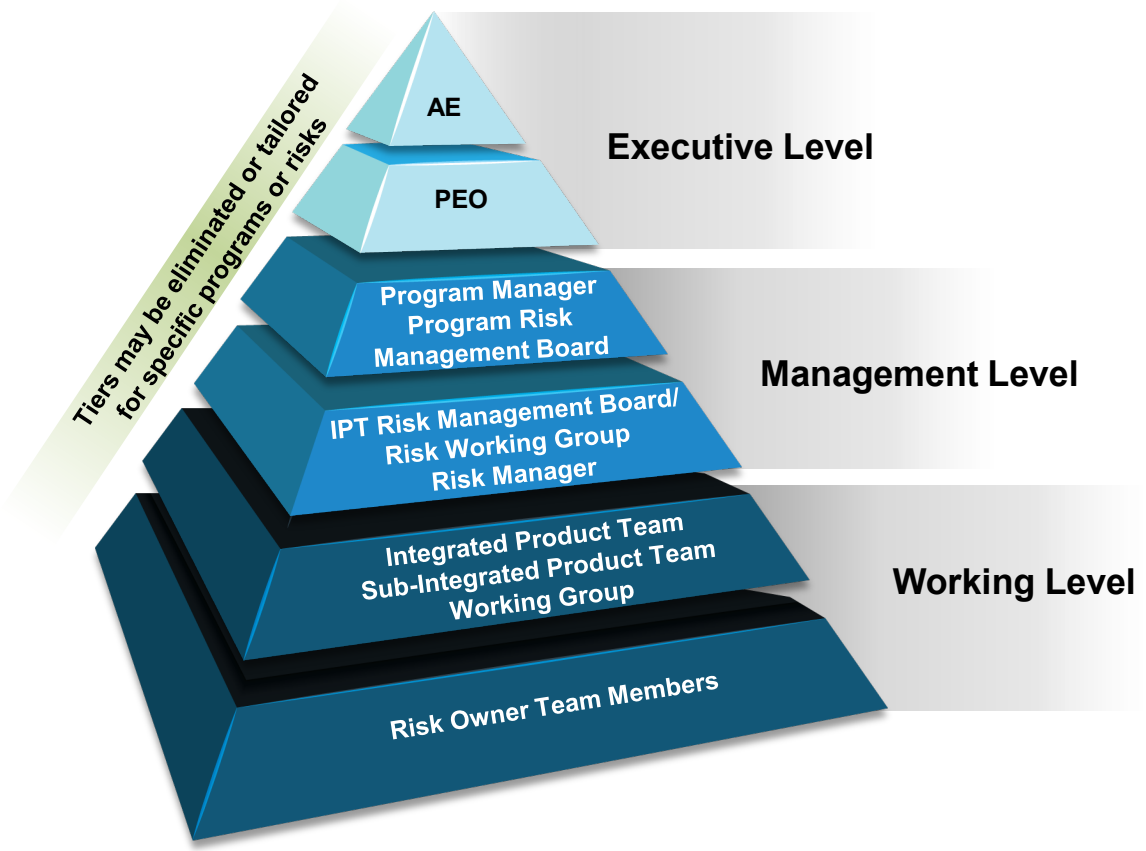


Figure B-2. Roles and Responsibilities Tiering

B.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.

B.4.2 Typical Contractor Responsibilities

- Strive to align internal risk processes as much as possible with the program's overall risk management process; 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.

B.4.3 Suggested Tiered Roles and Responsibilities

B.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.

B.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 PRMP.
- Establishes and executes an integrated risk management process with the contractor and key subcontractors; ensures the development of and approves the program's PRMP.
- Ensures the appropriate disciplines and IPTs are involved in the risk process (program management, engineering, contracting, information assurance, legal, financial management, EVM (cost control managers and cost schedule analyst), logistics, manufacturing, test and evaluation, quality assurance, and system safety) and spectrum management.
- 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 including 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 PRMP.
- 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/DA) 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 PRMP 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.

B.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 PRMP, and support the PM and RMB as required.
- Identify internal and external risks in accordance with the procedures documented in the program's approved PRMP. 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 PRMP.
- Assist the PM, as required, in reporting risk status to senior management personnel (PM/PEO/DA) 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 including 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 C. 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 while reviewing control accounts and work package to ensure comprehensive coverage of all tasks that must be examined for risk during risk identification sessions (see Section 2.2) 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 should 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.

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

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

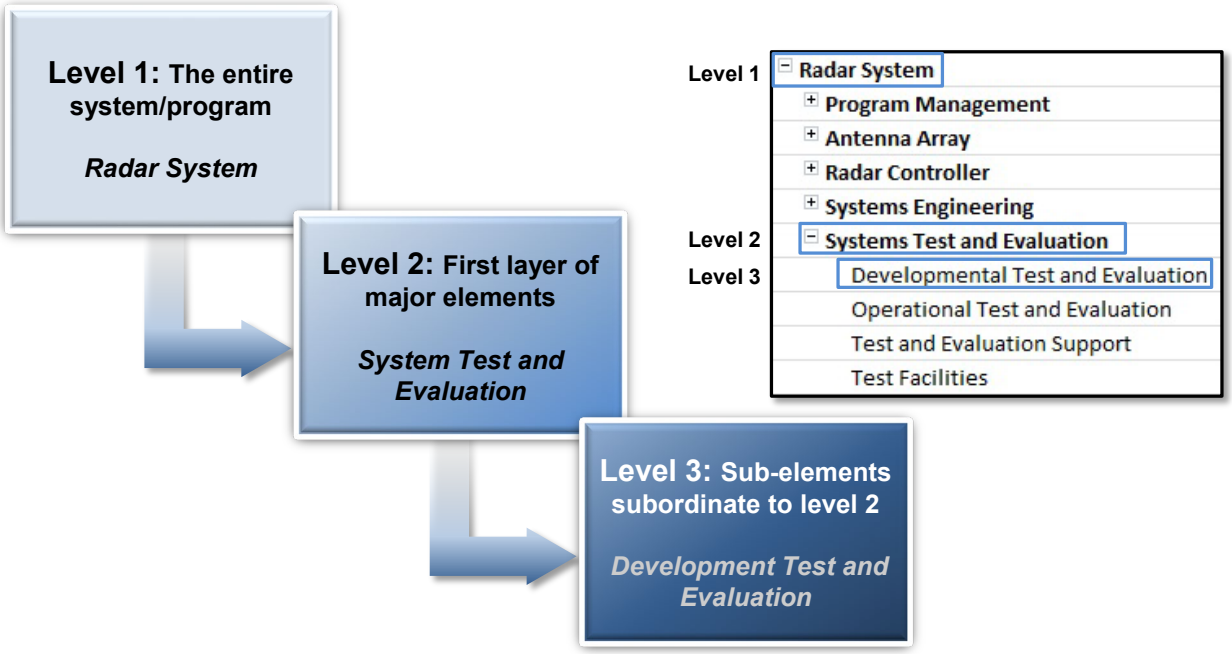


Figure C-1. Example of WBS Levels

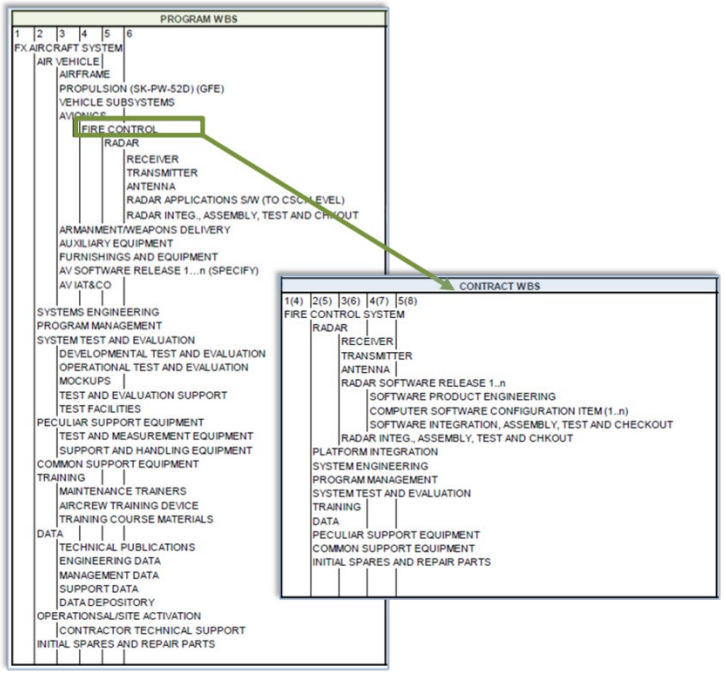


Figure C-2. Government and Contractor WBS Relationship

C.2 Integrated Master Plan and Integrated Master Schedule

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 event-based plan consisting of a hierarchy of program events, with each event supported by specific accomplishments, and each accomplishment associated with specific criteria to completed.

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 C-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.

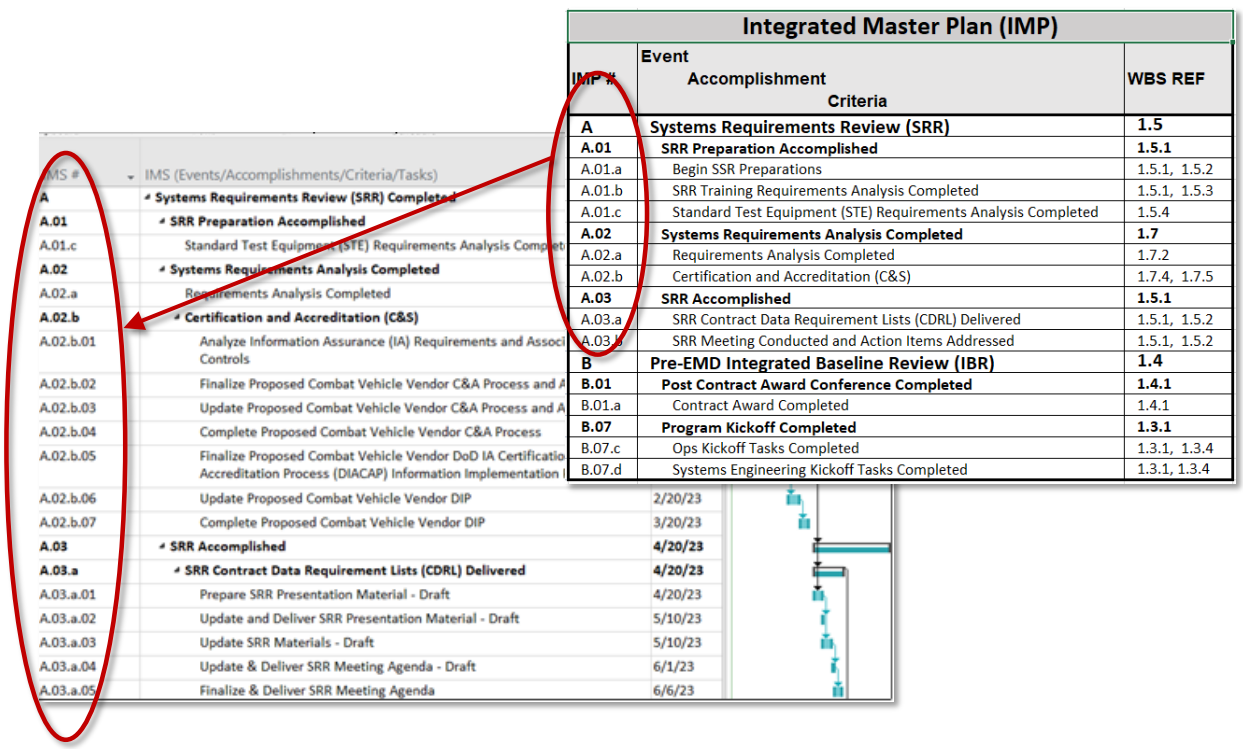


Figure C-3. IMP/IMS Creation and Implementation

Programs should regularly assess the health of the IMS through a schedule health assessment (SHA). The DCMA 14-point schedule metrics are an excellent tool to assess schedule quality, structural integrity, and overall health. Table C-1 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 needing improvement.

Table C-1. Sample 14-Point Schedule Health Assessment Metrics and Status

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, forecast 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%	

Source: DCMA.

C.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 measurement baseline is used for tracking and analyzing contract performance; however, in the case of firm fixed price contracts, EVM reporting may not be required. Other means and mechanisms to analyze and evaluate risk must be implemented.

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 control 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 using quantitative metrics to evaluate project performance to date in order to perform trend analysis and forecast future task execution concerns. If variances in cost and schedule appear in an Integrated Program Management Data and Analysis Report, 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 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 EIA-748 to ensure the validity of the information whenever EVM is required.

C.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.

C.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 should 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 C.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 2.2.2). 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 or 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.

C.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 should 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. Historical and forecasted cost and schedule performance data, such as earned value metrics, can inform risk levels. EVM estimates at completion (EAC) should be reviewed against risk analysis results as a crosscheck to confirm the outcome or identify areas needing additional analysis. 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.

C.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 typically will 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 C.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 D. Risk Management Process Implementation Example

The following example illustrates the application of a risk management process to the development of a hypothetical Unmanned Aerial Vehicle (UAV) Jammer using the MCA pathway. The example follows the steps outlined in Section 2.

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 D-1.

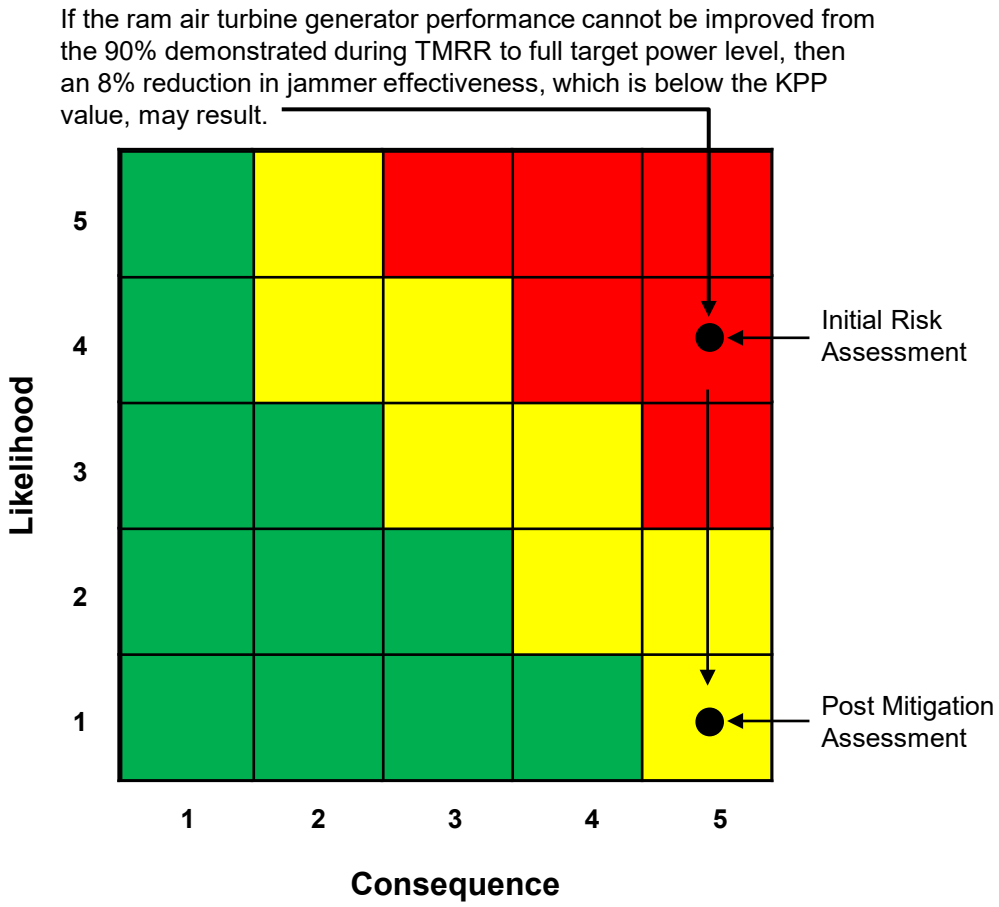


Figure D-1. Risk Matrix for Ram Air Turbine Generator

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.

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 D-2) for the improved generator. The vertical axis of the burn-down diagram spanned high, moderate, and low risks.

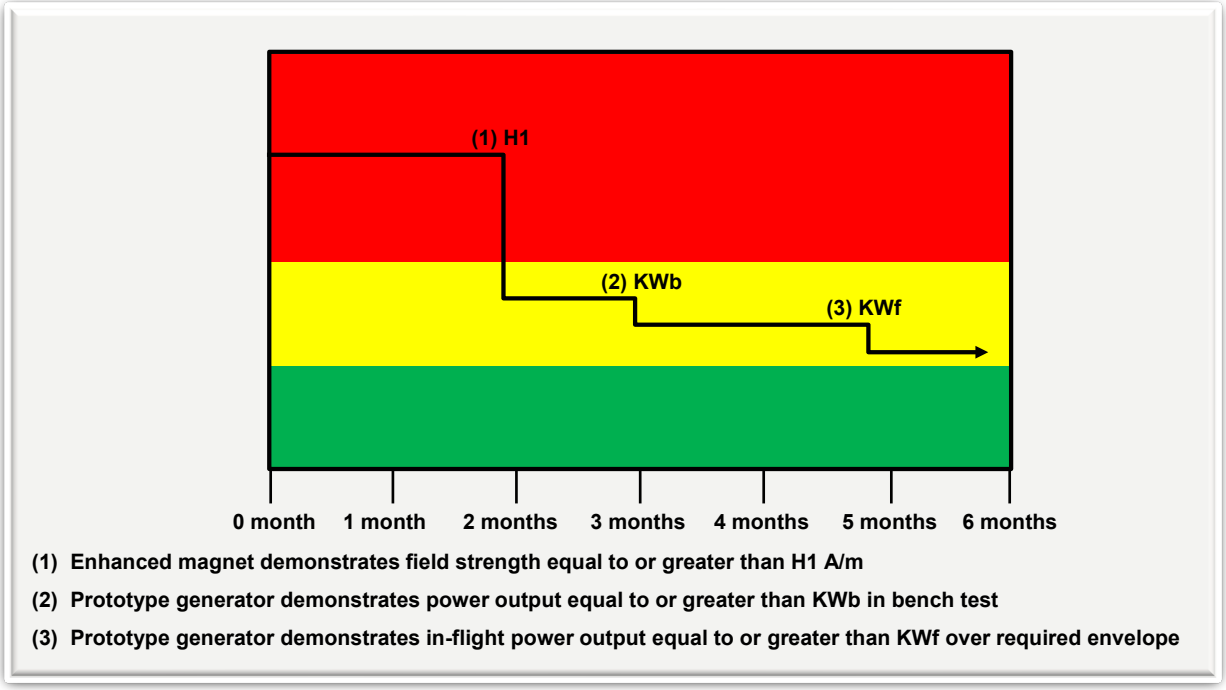


Figure D-2. Risk Burn-Down Diagram for Option A

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 D-3. The generator risk is displayed at the top right of the figure.

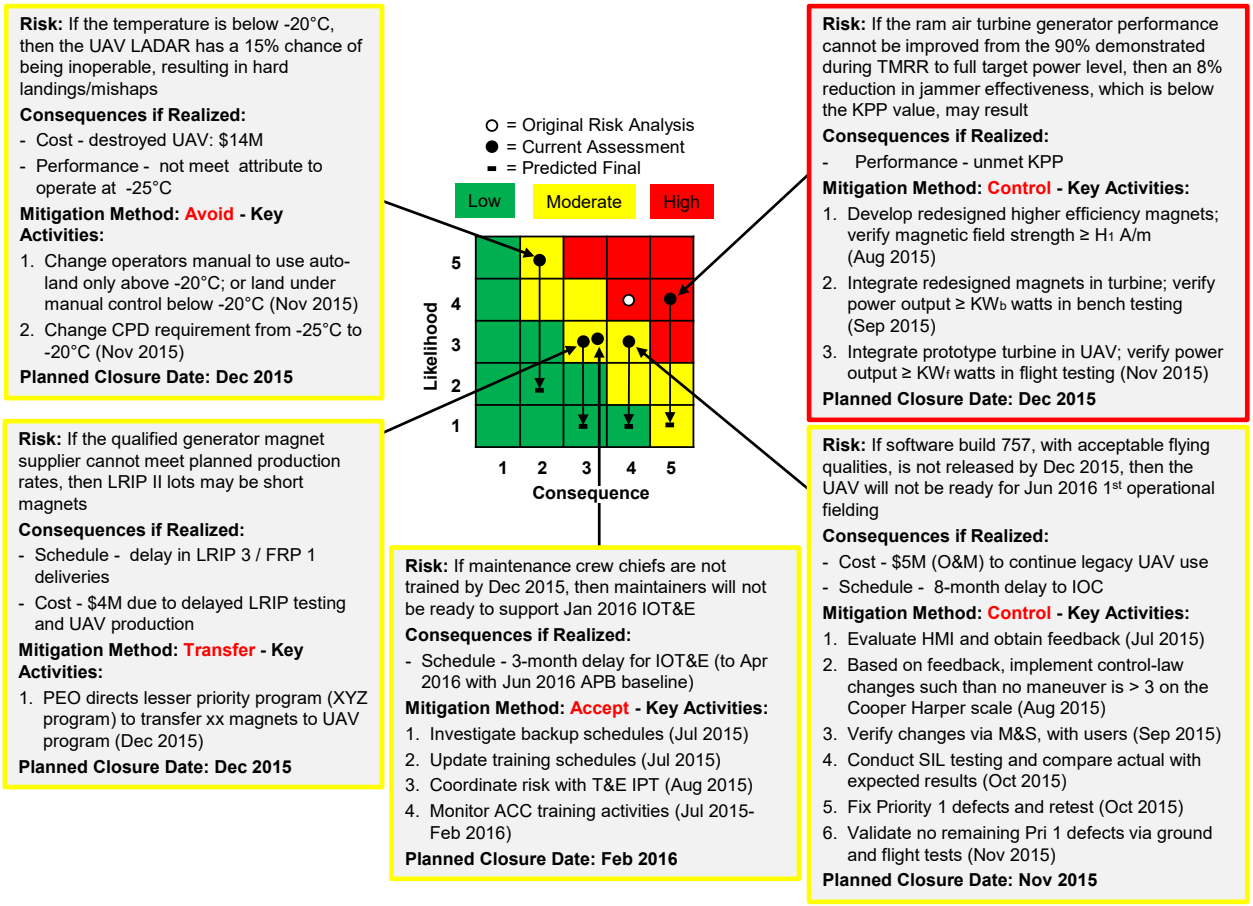


Figure D-3. Risk Reporting Chart

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

Glossary

Unless otherwise noted, the following definitions are for the purpose of this document.

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.

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.

Capability Needs Statement (CNS): A high-level capture of mission deficiencies, or enhancements to existing operational capabilities, features, interoperability needs, legacy interfaces, and other attributes that provides enough information to define various software solutions as they relate to the overall threat environment.

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: A sequence of discrete work packages and planning packages (or lower-level tasks or activities) in the network that has the longest total duration through an end point that is calculated by the schedule software application. Discrete work packages and planning packages (or lower-level tasks or activities) along the critical path have the least amount of float or slack (scheduling flexibility) and cannot be delayed without delaying the finish time of the end point effort. Essentially “critical path” has the same definition as “project critical path” with the exception that the end point can be a milestone or other point of interest in the schedule.

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

Electronic Attack (EA): Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability; considered a form of fires.

Electromagnetic Compatibility (EMC): The ability of systems, equipment, and device that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response.

Electromagnetic Environmental Effects (E3): The impact of the electromagnetic environment (EME) on the operational capability of military forces, equipment, systems, and platforms. E3 encompasses the electromagnetic effects addressed by the disciplines of EMC, EMI, EM vulnerability, EM pulse, electromagnetic protection, electrostatic discharge, and EMR hazards to personnel, ordnance, and fuels or volatile materials. E3 includes the effects generated by all EME contributors including RF systems, ultra-wideband devices, high-power microwave systems, lightning, and precipitation static.

Electromagnetic Environment (EME): The result of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment.

Electromagnetic Interference (EMI): Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance electronics and electrical equipment.

Electromagnetic Spectrum (EMS)-dependent system: All electronic systems, subsystems, devices, and/or equipment that depend on the use of the spectrum to properly accomplish their function(s) without regard to how they were acquired (full acquisition, rapid acquisition, Joint Concept Technology Demonstration, etc.) or procured (commercial off-the-shelf, government off-the-shelf, non-developmental items, etc.)

Electromagnetic Protection (EP): Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.

Electromagnetic Operating Environment (EMOE): The background electromagnetic environment and the friendly, natural, and adversarial electromagnetic order of battle within the electromagnetic area of influence associated with a given operational area.

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, 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 (likelihood = 5).

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 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, 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 typically will 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 Management Process (PRMP): 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 PRMP 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, 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 likelihood level (greater than 0, less than 5) 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 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: A process for identifying, implementing, assessing, and managing cybersecurity capabilities and services, expressed as security controls, and authorizing the operation of Information Systems (IS) and Platform Information Technology (PIT) systems (source: https://www.dau.edu/acquipedia/pages/articledetails.aspx#!245).

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 PRMP, 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 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).

Security Management Office (SMO): an office that supports ongoing spectral need and developmental work to enable all-domain operations to maintain continuous engagement across the Federal Government, commercial industry, and the international community.

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 MDA, 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 .

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.

Spectrum Supportability Risk Assessment (SSRA): Risk assessment performed by DoD Components for all EMS-dependent systems to identify risks as early as possible and affect design and procurement decisions. These risks are reviewed at acquisition milestones and are managed throughout the system's life cycle.

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.

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 controlling.

Acronyms

AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
AoA	Analysis of Alternatives
APB	Acquisition Program Baseline
APUC	Average Procurement Unit Cost
ARRT	Acquisition Requirements Roadmap Tool
AS	Acquisition Strategy
ASR	Alternative System Review
ATP	Authorization to Proceed
CAE	Component Acquisition Executive
CDD	Capability Development Document
CDR	Critical Design Review
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMO	Chief Management Office
CNS	Capability Needs Statement
COA	Course of Action
COR	Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CPD	Capability Production Document
CRA	Cost Risk Analysis
CSB	Configuration Steering Board
CTP	Critical Technical Parameter
CTT	Cyber Table Top
CVE	Common Vulnerabilities and Exposures
DA	Decision Authority
DAB	Defense Acquisition Board
DAES	Defense Acquisition Executive Summary
DAG	Defense Acquisition Guidebook
DAS	Defense Acquisition System

DAU	Defense Acquisition University
DBS	Defense Business Systems
DCMA	Defense Contract Management Agency
DE	Digital Engineering
DEBoK	Digital Engineering Body of Knowledge
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOT&E	Director Operational Test and Evaluation
DP	Developmental Planning
DTRAM	Defense Technical Risk Assessment Methodology
EAC	Estimate at Completion
EMD	Engineering and Manufacturing Development (phase)
EMV	Expected Monetary Value
ESOH	Environment, Safety, and Occupational Health
ETS	Engineering Technical Services
EVM	Earned Value Management
FCA	Functional Configuration Audit
FOC	Full Operational Capability
FRP	Full-Rate Production
FSM	Functional Services Manager
GOTS	Government off-the-shelf
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
IT	Information Technology
ITRA	Independent Technical Risk Assessment
JCIDS	Joint Capabilities Integration and Development System
JEON	Joint Emergent Operational Need

JRAC	Joint Rapid Acquisition Cell
JUON	Joint Urgent Operational Need
KPP	Key Performance Parameter
KSA	Key System Attribute
LCC	Life Cycle Cost
LRIP	Low-Rate Initial Production
MCA	Major Capability Acquisition
MBCRA	Mission-Based Cyber Risk Assessment
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
MDD	Materiel Development Decision
MFT	Multi-Function Team
MIPR	Military Interdepartmental Purchase Request
MOA	Memorandum of Agreement
MOSA	Modular Open Systems Approach
MOU	Memorandum of Understanding
MP	Mission Profile
MSA	Materiel Solution Analysis (phase)
MTA	Middle Tier of Acquisition
O&M	Operations and Maintenance
O&S	Operations and Support (phase)
OIPT	Overarching Integrated Product Team
OMS	Operational Mode Summary
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
OTRR	Operational Test Readiness Review
PAUC	Program Acquisition Unit Cost
P&D	Production and Deployment (phase)
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PEO	Program Executive Office or Program Executive Officer
PIT	Platform Information Technology
PM	Program Manager

PMR	Program Management Review
POA&M	Plan of Action and Milestones
PRA	Performance Risk Analysis
PRMP	Program Risk Management Process
PRR	Production Readiness Review
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RAA	Rapid Acquisition Authority
RAM	Reliability, Availability, and Maintainability
R&D	Research and Development
RDT&E	Research, Development, Test, and Evaluation
R&E	Research and Engineering
R&M	Reliability and Maintainability
RFI	Request for Information
RFP	Request for Proposal
RI3	Risk Identification: Integration and Ilities
RIO	Risk, Issue, and Opportunity
RMB	Risk Management Board
RMF	Risk Management Framework
ROI	Return on Investment
ROMB	Risk and Opportunity Management Board
RWG	Risk Working Group
SAG	Senior Advisory Group
SAT	Simplified Acquisition Threshold
S&T	Science and Technology
SCA	Security Control Assessor
SDS	Service Delivery Summary
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SEP	Systems Engineering Plan
SETR	Systems Engineering Technical Review
SFR	System Functional Review
SHA	Schedule Health Assessment

SIG	Senior Integration Group
SMART	Specific/Objective, Measurable, Achievable/Observable, Relevant, and Timely
SME	Subject Matter Expert
SOO	Statement of Objectives
SOW	Statement of Work
SR	Sustainment Review
SRA	Schedule Risk Analysis
SRR	System Requirements Review
SWAP-C	Size, Weight, Power, and Cooling
SVR	System Verification Review
SWE	Software Engineering
TEMP	Test and Evaluation Master Plan
TMRR	Technology Maturation and Risk Reduction (phase)
TPM	Technical Performance Measure
TRA	Technology Readiness Assessment
TRR	Test Readiness Review
UCA	Urgent Capability Acquisition
USD	Under Secretary of Defense
UAV	Unmanned Aerial Vehicle
UON	Urgent Operational Need
WBS	Work Breakdown Structure

References

DoD Issuances

DoD Instruction 3222.03, DoD Electromagnetic Environmental Effects (E3) Program, Change 2, October 10, 2017.
https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Instruction 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum, Change 1, October 17, 2017.
https://www.esd.whs.mil/Directives/issuances/dodi/

DoD Directive 5000.01, "The Defense Acquisition System," Change 1, July 28, 2022.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf?ver=IxP_j399Em4zTd4PqFjuTQ%3d%3d

DoD Directive 5000.71, "Rapid Fulfillment of Combatant Commander Urgent Operational Needs and Other Quick Action Requirements," October 18, 2022.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500071p.pdf

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," Change 1, June 8, 2022.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=0vzZVR1UG7nRmZKeGnSkHg%3d%3d

DoD Instruction 5000.74, Defense Acquisition of Services, Change 1, June 24, 2021.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500074p.pdf

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," Change 2, January 24, 2020.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500075p.PDF?ver=2020-01-24-132012-177

DoD Instruction 5000.80, "Operation of The Middle Tier of Acquisition (MTA)," December 30, 2019.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500080p.PDF?ver=2019-12-30-095246-043

DoD Instruction 5000.81, "Urgent Capability Acquisition," December 31, 2019.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500081p.PDF?ver=2019-12-31-133941-660

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," Change 1, May 21, 2021.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf?ver=fmz4Sx5tYVXnJZNKIoPoUQ%3d%3d

DoD Instruction 5000.85, "Major Capability Acquisition," Change 1, November 4, 2021.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500085p.pdf?ver=RYqeB690-qd-txjFEAZ72A%3d%3d

DoD Instruction 5000.87, "Operation of The Software Acquisition Pathway," October 2, 2020.
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?ver=virAfQj4v_LgN1JxpB_dpA%3d%3d

DoD Instruction 5000.88, "Engineering of Defense Systems," November 18, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500088p.PDF?ver=O8LFc8NzlyJX-SgM2Haalw%3d%3d

DoD Instruction 5000.89, "Test and Evaluation," November 19, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500089p.PDF?ver=Plc85E0-NVNide91K3XQLA%3d%3d

DoD Instruction 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF?ver=MIG3uLnzXl31QcvXJTZ5uA%3d%3d

DoD Instruction 5000.91, "Product Support Management for the Adaptive Acquisition Framework," November 4, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500091p.PDF?ver=qk1slCU3Y0c1acIDocWyJA%3d%3d

DoD Instruction 5000.95, "Human Systems Integration in Defense Acquisition," April 1, 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500095p.PDF

DoD Instruction 7041.03, "Economic Analysis for Decision-Making," September 9, 2015, Incorporating Change 1, October 2, 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/704103p.pdf

DoD Instruction 8500.01, "Cybersecurity", March 14, 2014, Incorporating Change 1, October 7, 2019 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

Other Sources

Agile Metrics Guide: Strategy Considerations and Sample Metrics for Agile Development Solutions, Version 1.2. Office of the Under Secretary of Defense for Acquisition and Sustainment, November 11, 2020. https://aaf.dau.edu/wp-content/uploads/2022/08/Agile-Metrics-Guide.pdf

CJCSM 3105.01A, "Chairman of The Joint Chiefs of Staff Manual-Joint Risk Analysis Methodology," October 12, 2021. https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203105.01A.pdf?ver=y3cH4s5UNyqJAXwxAYCL5Q%3d%3d

Collins, Christopher. "Test and Evaluation as a Continuum." PowerPoint presentation. Office of the Under Secretary of Defense for Research and Engineering, April 13, 2023. https://www.dau.edu/event/Test-and-Evaluation-as-a-Continuum-4-13-2023

Defense Acquisition University (DAU) Service Acquisition Mall (SAM). https://www.dau.edu/tools/Documents/SAM/home.html

Defense Contract Management Agency (DCMA) 14-Point Schedule Metrics. https://content1.dau.edu/EVM263-schedule-health-analysis-raw_93/content/#/

Defense Technical Risk Assessment Methodology (DTRAM). Version 6.4. Office of the Under Secretary of Defense for Research and Engineering, 2023.
https://www.cto.mil/sea/pg/

Digital Engineering Body of Knowledge (DEBoK). Office of the Under Secretary of Defense for Research and Engineering.
https://www.de-bok.org/

DoD Cyber Table Top Guide, Version 2. Office of the Under Secretary of Defense for Research and Engineering, September 2021.
https://www.cto.mil/sea/pg/

DoD Enterprise DevSecOps Fundamentals Version 2.1, September 2021.
https://dodcio.defense.gov/library/

DoD Digital Engineering Strategy. Office of the Under Secretary of Defense for Research and Engineering, 2018.
https://www.cto.mil/sea/pg/

DoD Independent Technical Risk Assessment (ITRA) Execution Guidance. Office of the Under Secretary of Defense for Research and Engineering, 2020.
https://ac.cto.mil/itra/

Government Accountability Office (GAO). Agile Assessment Guide: Best Practices for Agile Adoption and Implementation (GAO-20-590G), September 28, 2020.
https://www.gao.gov/products/gao-20-590g

Guidebook for Acquiring Engineering Technical Services (ETS), Version 2.0, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 2017.
https://www.cto.mil/sea/pg/

Human Systems Integration (HSI) Guidebook. Office of the Under Secretary of Defense for Research and Engineering, 2022.
https://www.cto.mil/sea/pg/

Human Systems Integration (HSI) RIO Management Tools.
https://www.dau.edu/cop/hsi/Lists/Tools/AllItems.aspx

Military Standard 882E, "Standard Practice for System Safety," May 11, 2012.

Mission Engineering Guide. Office of the Under Secretary of Defense for Research and Engineering, November 2020.
https://ac.cto.mil/wp-content/uploads/2020/12/MEG-v40_20201130_shm.pdf

NIST 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," Revision 2. National Institute of Standards and Technology, December 2018.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST SP 800-39, "Managing Information Security Risk." National Institute of Standards and Technology, 2011.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

Packard, David, et al. "A Quest for Excellence: Final Report to the President." President's Blue Ribbon Commission on Defense Management, June 1986.

Risk Identification: Integration and Ilities (RI3) Guidebook, Version 1.2, December 15, 2008.

Software Engineering for Continuous Delivery of Warfighting Capability. Office of the Under Secretary of Defense for Research and Engineering, April 2023. https://www.cto.mil/wp-content/uploads/2023/04/SWE-Guide-April2023.pdf

Systems Engineering Guidebook. Office of the Under Secretary of Defense for Research and Engineering, February 2022. https://www.cto.mil/sea/pg/

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

Office of the Executive Director for Systems Engineering and Architecture
Office of the Under Secretary of Defense for Research and Engineering
3030 Defense Pentagon
Washington, DC 20301-3030
osd-sea@mail.mil
https://www.cto.mil/sea/

Distribution Statement A. Approved for public release. Distribution is unlimited.
DOPSR Case # 23-S-3231