Downloaded from http://www.everyspec.com

Risk Management Guide for DoD Acquisition

Second Edition

May 1999

DEPARTMENT OF DEFENSE
DEFENSE ACQUISITION UNIVERSITY
DEFENSE SYSTEMS MANAGEMENT COLLEGE

PUBLISHED BY THE
DEFENSE SYSTEMS MANAGEMENT COLLEGE PRESS
FORT BELVOIR, VIRGINIA 22060-5565

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328

Downloaded from http://www.everyspec.com

Please E-Mail comments or recommended changes to:

Mcmahon_Paul@dsmc.dsm.mil

Bahnmaier_Bill@dsmc.dsm.mil

Downloaded from http://www.everyspec.com

ACQUISITION AND
TECHNOLOGY

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

RISK MANAGEMENT GUIDE

Acquisition reform has changed the way the Department of Defense (DoD) designs, develops, manufactures, and supports systems. Our technical, business, and management approach for acquiring and operating systems has, and continues to, evolve. For example, we no longer can rely on military specifications and standards to define and control how our developers design, build, and support our new systems. Today we use commercial hardware and software, promote open systems architecture, and encourage streamlining processes, just to name a few of the initiatives that affect the way we do business. At the same time, the Office of the Secretary of Defense (OSD) has reduced the level of oversight and review of programs and manufacturers' plants.

While the new acquisition model gives government Program Managers and their contractors broader control and more options than they have enjoyed in the past, it also exposes them to new risks. OSD recognizes that risk is inherent in any acquisition program and considers it essential that Program Managers take appropriate steps to manage and control risks.

In late 1996, the Under Secretary of Defense, Acquisition and Technology [USD(A&T)] tasked the Director, Test, Systems Engineering, and Evaluation (DTSE&E) to review DoD risk management practices and techniques. In response, DTSE&E / Systems Engineering established a Risk Management Working Group that examined the Services, individual acquisition programs, and commercial industry's treatment of risk. The results of the study served as the basis for the risk management section (2.5.2) in the *Defense Acquisition Deskbook*. The study also identified the need to update existing risk training material to reflect the new way DoD conducts business.

Downloaded from http://www.everyspec.com

This document is a product of a joint effort among the DTSE&E, the Defense Acquisition University, and the Defense Systems Management College. It is based on the material developed by the DoD Risk Management Working Group, included in the *Defense Acquisition Deskbook*.

Mark D. Schaeffer
Deputy Director, Test, Systems
Engineering and Evaluation /
Systems Engineering

Thomas M. Crean
President
Defense Acquisition University

Lenn Vincent
RADM, SC, USN
Commandant
Defense Systems Management College

Downloaded from http://www.everyspec.com

PREFACE

In December 1995, the Under Secretary of Defense, Acquisition and Technology [USD(A&T)], issued a memorandum entitled *Reducing Life Cycle Costs for New and Fielded Systems*, in which he established the policy and strategy to develop and field affordable weapon systems that are responsive to user's needs. One of the foundations of the strategy is the concept of "Cost as An Independent Variable" (CAIV), the Department of Defense (DoD) equivalent of commercial best practices. The CAIV concept recognizes that "there are risks to be taken and risks to be avoided. When risks are taken, we will put in place appropriate risk management and contingency plans."

Other initiatives, such as acquisition streamlining and revision of the DoD 5000 series documents, were ongoing when the USD(A&T) memorandum was published; each affected program risk**.** Also at this time, the DoD Inspector General was writing a critical report of the Department's management of risk; the report recommended measures to control risk of acquisition programs. Figure P-1 shows some of the initiatives that impact risk management.

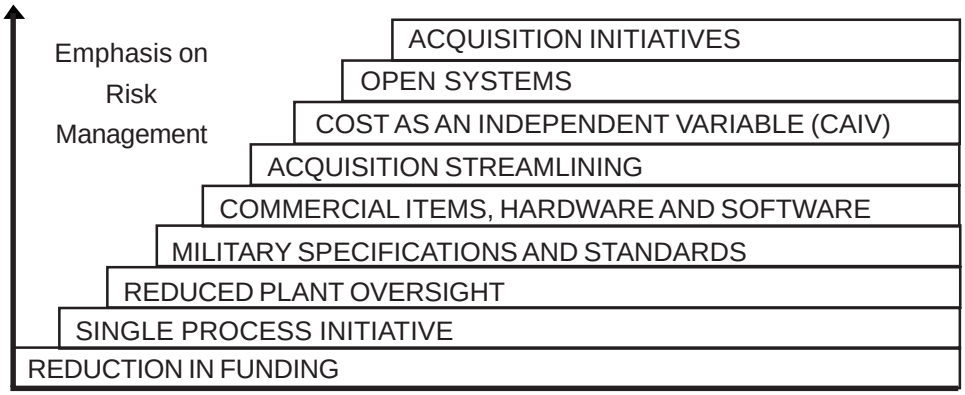


Figure P-1. DoD Renewed Emphasis on Risk Management

With these initiatives as the basis, the USD(A&T) tasked the Director, Test, Systems Engineering, and Evaluation (DTSE&E) to: (1) review DoD risk management practices and techniques, (2) determine whether new approaches were needed to improve risk management, and (3) report the results to USD(A&T).

In response, DTSE&E established a Risk Management Working Group composed of members of the Office of the Secretary of Defense (OSD) staff, representatives of the Services, and members of other DoD agencies involved in systems acquisition. This group reviewed pertinent DoD directives (DoDD) and regulations, examined how the Services managed risk, studied various examples of risk management by companies in commercial industry, and looked at DoD training and education activity in risk management. The Working Group coordinated with other related efforts in DoD. For example, the *Joint Aeronautical Commanders Group Risk Guide* was a valuable source of information. The workshops for the CAIV Flagship programs provided current, real-world examples of Program Managers implementing the CAIV initiative and risk management. Membership of the Working

Downloaded from http://www.everyspec.com

Group included a representative from USD(A&T) Acquisition Program Integration / Program Management (API / PM) who kept members informed on the status of the Integrated Program Management Initiative. Other sources of information were the Software Engineering Institute Risk Initiative, the Open Systems Initiative, and Safety and Cost Estimating communities. DTSE&E summarized the findings of the investigation and presented the results to the USD(A&T) in July 1996.

The findings and recommendations of the Working Group are summarized below.

Commercial Industries
• Focus of efforts is on getting a product to market at a competitive cost. • Companies have either a structured or informal Risk Management process. • Evolutionary approaches help avoid or minimize risk. • Most approaches employ risk avoidance, early planning, continuous assessment, and problem-solving techniques. • Structured approaches, when they exist, are similar to DoD's approach to Risk Management. The Working Group concluded that industry has no magic formula for Risk Management.
The Services
• The Services differ in their approaches to Risk Management. • Each approach has its strengths but no one approach is comprehensive. • Consolidation of the strengths of each approach could foster better Risk Management in DoD. The Working Group recommended that the *Defense Acquisition Deskbook* contain a set of guidelines for sound risk management practices, and further, that it contain a set of risk management definitions that are comprehensive and useful by all the Components.
DoD Policy
• The risk management policy contained in DoDD 5000.1 is not comprehensive. The Working Group recommended that DoDD 5000.1 be amended to include a more comprehensive set of risk management policies that focuses on: • The relationship between the CAIV concept and Risk Management. • Requirement that risk management be prospective (forward looking). • Establishment of risk management as a primary management technique to be used by Program Managers (PMs).

Downloaded from http://www.everyspec.com

DoD Procedures
• Risk Management procedures in DoD 5000.2-R are inadequate to fully implement the risk management policy contained in DoDD 5000.1. Procedures are lacking regarding the: – Scope of Risk Management – Purpose of Risk Management – Role of Milestone Decision Authorities – Risk Management's support of CAIV – Risk assessment during Phase 0. • Some key procedures may have been lost in transition from DoD 5000.2M to DoD 5000.2-R. The Working Group recommended that procedures in DoD 5000.2-R be expanded, using the *Defense Acquisition Deskbook* as the expansion means, in order to provide comprehensive guidance for the implementation of risk management policy.
DoD Risk Management Training
• Risk management training for the DoD acquisition corps needs to be updated and expanded, and Integrated Product Team (IPT) and Overarching IPT (OIPT) personnel need to be educated on the new and expanding role of risk management in DoD systems acquisition. • Risk Management knowledge level needs improvement. • Education is a key to getting the support of OIPTs and PMs. The Working Group recommended that the Defense Acquisition University (DAU) include training for Risk Management in all functional courses and develop a dedicated risk management course for acquisition corps personnel.

DTSE&E briefed the results to the Defense Manufacturing Council, an advisory body to the USD(A&T), which directed that the recommendations be incorporated in the *Defense Acquisition Deskbook*. Following that guidance, DTSE&E wrote the risk management portions of the *Deskbook*.

The *Risk Deskbook* write-up forms the basis for this *Guide*. The goal of the *Risk Management Guide* is to provide acquisition professionals and program management offices with a reference for dealing with system acquisition risks. It has been designed as an aid in classroom instruction and as a reference for practical applications.

This *Guide* reflects the efforts of many people. Mr. Mark Schaeffer, Deputy Director, Systems Engineering, DTSE&E, who chaired the Risk Management Working Group and Mr. Mike Zsak and Mr. Tom Parry from the DTSE&E, Systems Engineering Support Office, were the driving force behind the risk management initiative. Mr. Paul McMahon and Mr. Bill Bahnmaier from the DSMC faculty and Mr. Greg Caruth, Ms. Debbie Gonzalez, SFC Frances Battle, USA, SSgt Gerald Gilchrist, Sr., USAF, from the DSMC Press guided the composition of the *Guide*. Special recognition goes to the Institute for Defense Analyses team composed of Mr. Louis Simpleman, Mr. Ken Evans, Mr. Jim Lloyd, and Mr. Gerald Pike, who compiled the data and wrote major portions of the text.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

CONTENTS

Chapter 1 INTRODUCTION 1
1.1 Purpose and Scope 1
1.2 Organization of the Guide 1
1.3 Approach to Risk Management 2
1.4 DoD Risk Management Policies and Procedures 2

Chapter 2 RISK AND RISK MANAGEMENT 3
2.1 Introduction 3
2.2 Overview 3
2.3 Risk Management Structure and Definitions 4
2.4 Risk Discussion 6
2.4.1 Characteristics of Acquisition Risk 6
2.4.2 Program Products, Processes, Risk Areas, and Risk Events 6
2.5 Risk Planning 9
2.5.1 Purpose of Risk Plans 9
2.5.2 Risk Planning Process 9
2.6 Risk Assessment 10
2.6.1 Purpose of Risk Assessments 10
2.6.2 Risk Assessment Process 10
2.6.3 Timing of Risk Assessments 11
2.6.4 Conducting Risk Assessments 12
2.7 Risk Handling 17
2.7.1 Purpose of Risk Handling 17
2.7.2 Risk Handling Process 17
2.8 Risk Monitoring 20
2.9 Risk Documentation 21

Chapter 3 RISK MANAGEMENT AND DOD ACQUISITION PROCESS 23
3.1 Introduction 23
3.2 Overview 23
3.3 DoD Acquisition Process 23
3.4 Characteristics of the Acquisition Process 24
3.4.1 Integrated Product and Process Development (IPPD) 24
3.4.2 Continuous Risk Management 24
3.4.3 Program Stability 25
3.4.4 Reduction of Life-Cycle Costs 25
3.4.5 Event-Oriented Management 25
3.4.6 Modeling and Simulation 25
3.5 Risk Management Activities during Acquisition Phases 26
3.5.1 Phase 0 26
3.5.2 Subsequent Phases 27
3.6 Risk Management and Milestone Decisions 27

Downloaded from http://www.everyspec.com

3.7 Risk Management and the Acquisition Strategy 27
3.8 Risk Management and CAIV 28

Chapter 4 RISK MANAGEMENT AND PROGRAM MANAGEMENT 31
4.1 Introduction 31
4.2 Overview 31
4.3 Program Manager and Risk Management 31
4.3.1 Risk Management is a Program Management Tool 31
4.3.2 Risk Management is a Formal Process 32
4.3.3 Risk Management is Forward-Looking 32
4.3.4 Risk Management is Integral to Integrated Product and Process Development (IPPD) 33
4.4 Risk Management Organization in the PMO 33
4.4.1 Risk Management Organizational Structure 33
4.4.2 Risk Management Responsibilities 35
4.5 Contractor Risk Management 36
4.5.1 Contractor View of Risk 36
4.5.2 Government/Contractor Relationship 36
4.6 Risk Management and the Contractual Process 38
4.6.1 Risk Management: Pre-Contract Award 38
4.6.2 Early Industry Involvement: Industrial Capabilities Review 38
4.6.3 Developing the Request for Proposal 30
4.6.4 The Offeror's Proposal 42
4.6.5 Basis for Selection 42
4.6.6 Source Selection 43
4.7 Risk Management: Post-Contract Award 44
4.8 Risk Management Reporting and Information System 45
4.9 Risk Management Training 45

Chapter 5 RISK MANAGEMENT TECHNIQUES 49
5.1 Introduction 49
5.2 Overview 49
5.3 Risk Planning Techniques 49
5.3.1 Description 49
5.3.2 Procedures 50
5.4 Risk Assessment Techniques 51
5.4.1 Product (WBS) Risk Assessment 51
5.4.2 Process (DoD 4245.7-M) Risk Assessment 54
5.4.3 Program Documentation Evaluation Risk Identification 56
5.4.4 Threat and Requirements Risk Assessment 57
5.4.5 Cost Risk Assessment 59
5.4.6 Quantified Schedule Risk Assessment 60
5.4.7 Expert Interviews 62
5.4.8 Analogy Comparison/Lessons-Learned Studies 63
5.5 Risk Prioritization 63

Downloaded from http://www.everyspec.com

5.5.1 Description 63
5.5.2 Procedures 64
5.6 Risk-Handling Techniques 66
5.6.1 General 66
5.6.2 Risk Control 68
5.6.3 Risk Avoidance 71
5.6.4 Risk Assumption 72
5.6.5 Risk Transfer 72
5.7 Risk Monitoring 73
5.7.1 General 73
5.7.2 Earned Value Management 75
5.7.3 Technical Performance Measurement 76
5.7.4 Integrated Planning and Scheduling 76
5.7.5 Watch List 77
5.7.6 Reports 78
5.7.7 Management Indicator System 79
5.8 Risk Management Information Systems and Documentation 82
5.8.1 Description 82
5.8.2 Risk Management Reports 82
5.9 Software Risk Management Methodologies 83
5.9.1 Software Risk Evaluation (SRE) 85
5.9.2 Boehm's Software Risk Management 85
5.9.3 Best Practices Initiative Risk Management Method 85

APPENDIX A
DOD RISK MANAGEMENT POLICIES AND PROCEDURES A-1
1. DoD 5000.1 Defense Acquisition, March 1996 ..... A-1
2. DoD Regulation 5000.2-R. Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, March 15, 1996 ..... A-2
3. DoD Directive (DoDD) 5000.4, OSD Cost Analysis Improvement Group (CAIG), November 24, 1992 ..... A-6
4. DoD 5000.4-M Cost Analysis Guidance and Procedures, December 1992 ..... A-7

APPENDIX B
GENERIC RISK MANAGEMENT PLAN B-1
Sample Risk Management Plan B-1
Preface B-1
Sample Format for Risk Management Plan B-2
Sample Risk Management Plan for the XYZ Program (ACAT I, II) B-4
1.0 Introduction B-4
1.1 Purpose B-4
1.2 Program Summary B-4
1.2.1 System Description B-5
1.2.2 Acquisition Strategy B-5

Downloaded from http://www.everyspec.com

1.2.3 Program Management Approach B-5
1.3 Definitions B-5
1.3.1 Risk B-5
1.3.2 Risk Event B-5
1.3.3 Technical Risk B-6
1.3.4 Cost Risk B-6
1.3.5 Schedule Risk B-6
1.3.6 Risk Ratings B-6
1.3.7 Independent Risk Assessor B-7
1.3.8 Templates and Best Practices B-7
1.3.9 Metrics B-7
1.3.10 Critical Program Attributes B-7
2.0 Risk Management B-7
2.1 General Approach and Status B-7
2.2 Risk Management Strategy B-8
2.3 Organization B-9
2.3.1 Risk Management Coordinator B-9
2.3.2 Program Integrating Integrated Product Team (PIIPT) B-10
2.3.3 PIPTs B-10
2.3.4 XYZ Independent Risk Assessors B-10
2.3.5 Other Risk Assessment Responsibilities B-10
2.3.6 User Participation B-11
2.3.7 Risk Training B-11
3.0 Risk Planning B-11
3.1 Overview B-11
3.2 Risk Planning B-12
3.2.1 Process B-12
3.2.2 Procedures B-12
3.3 Risk Assessment B-13
3.3.1 Process B-13
3.3.2 Procedures B-14
3.4 Risk Handling B-19
3.4.1 Process B-19
3.4.2 Procedures B-19
3.5 Risk Monitoring B-20
3.5.1 Process B-20
3.5.2 Procedures B-20
4.0 Risk Management Information System and Documentation B-21
4.1 Risk Management Information System (RMIS) B-21
4.2 Risk Documentation B-22
4.2.1 Risk Assessment Documentation B-22
4.2.2 Risk Handling Documentation B-22
4.2.3 Risk Monitoring Documentation B-22
4.3 Reports B-22

Downloaded from http://www.everyspec.com

4.3.1 Standard Reports B-22
4.3.2 Ad Hoc Reports B-22
Annex A to XYZ Risk Management Plan—Critical Program Attributes B-23
Annex B to XYZ Risk Management Plan—Program Risk Reduction Schedule B-24
Annex C to XYZ Risk Management Plan— Program Metric Examples B-25
Annex D to XYZ Risk Management Plan—Management Information System and Documentation B-27
1.0 Description B-27
2.0 Risk Management Reports—XYZ Program B-27
2.1 Risk Information Form B-28
2.2 Risk Assessment Report B-28
2.3 Risk Handling Documentation B-28
2.4 Risk Monitoring Documentation B-28
3.0 Database Management System (DBMS) B-28
Sample Risk Management Plan for the ABC Program (ACAT III, IV) B-33
1.0 Introduction B-33
1.1 Purpose B-33
2.0 Program Summary B-33
2.1 Description B-33
2.2 Acquisition Strategy B-34
2.3 Program Management Approach B-34
3.0 Risk-Related Definitions B-34
3.1 Technical Risk B-34
3.2 Cost Risk B-35
3.3 Risk Ratings B-35
4.0 Risk Management Status and Strategy B-35
4.1 Risk Management Status B-35
4.2 Risk Management Strategy B-35
5.0 Organization B-36
5.1 Program Office B-36
6.0 Risk Management Structures and Procedures B-37
6.1 Risk Planning B-38
6.2 Risk Assessment B-38
6.2.1 Risk Identification B-39
6.2.2 Risk Analysis B-40
6.2.3 Risk Rating B-42
6.2.4 Risk Prioritization B-43
6.3 Risk Handling B-44
6.4 Risk Monitoring B-44
6.5 Risk Management Information System (RMIS), Documentation, and Reports B-45
Annex A to ABC Risk Management Plan—Critical Program Attributes B-47
Annex B to ABC Risk Management Plan—Program Risk Reduction Schedule B-48
1.0 Description B-48
2.0 Risk Management Forms and Reports B-50

Downloaded from http://www.everyspec.com

2.1 Risk Information Form B-50
2.2 Risk Monitoring Documentation B-50
2.3 WIPT Risk Summary Report B-51

APPENDIX C GLOSSARY C-1

APPENDIX D BIBLIOGRAPHY D-1

FIGURES

2-1 Risk Management Structure 5
2-2 Transition from Development to Production Critical Process Areas and Templates 9
2-3 A Risk Management Plan Format 10
2-4 Risk Assessment 12
2-5 Example of a WBS Dependent Evaluation Structure 14
4-1 Decentralized Risk Management Organization 34
5-1 Risk Planning Technique Input and Output 50
5-2 Sample Format for Risk Management Plan 52
5-3 Product (WBS) Risk Assessment Techniques Input and Output 53
5-4 Process (DoD 4245.7-M) Risk Assessment Technique Input and Output 55
5-5 Plan Evaluation Technique Input and Output 56
5-6 Phase 0 Correlation of Selected Documents (Example) 57
5-7 Threat and Requirement Risk Assessment Technique Input and Output 58
5-8 Cost Risk Assessment Top-Level Diagram 59
5-9 Schedule Risk Assessment Technique Input and Output 61
5-10 Expert Interview Technique Input and Output 62
5-11 Analogy Comparison/Lessons-Learned Studies Top-Level Diagram 64
5-12 Risk Prioritization Technique Input and Output 65
5-13 Risk Aggregation Techniques Input and Output 65
5-14 Sample of a List of Prioritized Risks 66
5-15 Example Showing Detailed List of Top-Level Risk Information 78
5-16 Example of More Complex Combination of Risk Level and Scheduled Tasks 79
5-17 Conceptual Risk Management and Reporting System 82

Appendix B

2-1 Risk Management and the Acquisition Process B-8
2-2 XYZ Risk Management Organization B-9
3-1 Risk Management Structure B-11
3-2 Risk Management Process B-18
3-3 Conceptual Risk Management and Reporting System B-27
5-1 ABC Risk Management Organization B-36
6-1 Risk Assessment Process B-43
7-1 Example Risk Tracking Report B-49
7-2 Sample Watch List B-50

Downloaded from http://www.everyspec.com

7-3 Example PIPT Risk Summary Report B-51

TABLES

2-1 Risk Assessment Approaches 15
2-2 Likelihood Criteria (Example) 16
2-3 Consequences Criteria (Example) 16
2-4 Overall Risk Rating Criteria (Example) 16
2-5 Risk Ratings (Example) 17
2-6 Overall Risk Rating (Example) 17
4-1 Notional Description of Risk Management Responsibilities 37
4-2 Significant Risks by Critical Risk Areas 40
4-3 Risk Management Reference Documents 46
5-1 Critical Risk Areas and Example Elements 54
5-2 Examples of Demonstration Events 75
5-3 Watch List Example 77
5-4 Examples of Product-Related Metrics 80
5-5 Examples of Product Metrics 81
5-6 Examples of Cost and Schedule Metrics 81
5-7 Database Management Systems Elements 84
5-8 Software Risk Management Steps 86
5-9 Top 10 Software Risks 86
5-10 Best Practices Initiative Risk Management Method 87
5-11 Software Risk Grouping 88
6-1 Likelihood Levels B-41
6-2 Risk Consequence B-42

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

1

INTRODUCTION

Risk has always been a concern in the acquisition of Department of Defense (DoD) systems. The acquisition process itself is designed, to a large degree, to allow risks to be controlled from conception to delivery of a system. Unfortunately, in the past, some Program Managers (PMs) and decision makers have viewed risk as something to be avoided. Any program that had risk was subject to intense review and oversight. This attitude has changed. DoD managers recognize that risk is inherent in any program and that it is necessary to analyze future program events to identify potential risks and take measures to handle them.

Risk management is concerned with the outcome of future events, whose exact outcome is unknown, and with how to deal with these uncertainties, i.e., a range of possible outcomes. In general, outcomes are categorized as favorable or unfavorable, and risk management is the art and science of planning, assessing, and handling future events to ensure favorable outcomes. The alternative to risk management is crisis management, a resource-intensive process that is normally constrained by a restricted set of available options.

1.1 PURPOSE AND SCOPE

This *Risk Management Guide* is designed to provide acquisition professionals and program management offices (PMOs) with a reference book for dealing with system acquisition risks. It is intended to be useful as an aid in classroom instruction and as a reference book for practical applications. Most of the material in this *Guide* is derived from the *Defense Acquisition Deskbook*. Readers should refer to Paragraph 2.5.2 of the *Deskbook* for any new information.

1.2 ORGANIZATION OF THE GUIDE

The *Risk Management Guide* discusses risk and risk management, defines terms, and introduces basic risk management concepts (Chapter 2).

Chapter 3 examines risk management concepts relative to the DoD acquisition process. It illustrates how risk management is an integral part of program management, describes interaction with other acquisition processes, and identifies and discusses the various types of acquisition risks.

Chapter 4 discusses the implementation of a risk management program from the perspective of a PMO. This chapter focuses on practical application issues such as risk management program design options, PMO risk management organizations, and criteria for a risk management information system (MIS).

Chapter 5, the final chapter, describes a number of techniques that address the aspects (phases) of risk management, i.e., planning, assessment, handling, and monitoring.

Downloaded from http://www.everyspec.com

This *Guide* is a source of background information and provides a starting point for a risk management program. None of the material is mandatory, PMs should tailor the approaches and techniques to fit their programs.

The *Risk Management Guide* also contains appendices that are intended to serve as reference material and provide backup detail for some of the concepts presented in the main portion of the *Guide*.

1.3 APPROACH TO RISK MANAGEMENT

Based on the DoD model contained in the *Deskbook* (described in Chapter 2), this *Guide* emphasizes a risk management approach that is disciplined, forward looking, and continuous.

In 1986, the Government Accounting Office (GAO), as part of an evaluation of DoD policies and procedures for technical risk assessments, developed a set of criteria as an approach to good risk assessments. These criteria, with slight modification, apply to all aspects of risk management and are encompassed in the *Guide's* approach. They are:

(1) **Planned Procedures.** Risk management is planned and systematic.

(2) **Prospective Assessment.** Potential future problems are considered, not just current problems.

(3) **Attention to Technical Risk.** There is explicit attention to technical risk.

(4) **Documentation.** All aspects of the risk management program are recorded and data maintained.

(5) **Continual Process.** Risk assessments are made throughout the acquisition process; handling activities are continually evaluated and changed if necessary; and critical risk areas are always monitored.

While these criteria are not solely sufficient to determine the "health" of a program, they are important indicators of how well a risk management process is being implemented.

1.4 DOD RISK MANAGEMENT POLICIES AND PROCEDURES

DoD policies and procedures that address risk management for acquisition programs are contained in four key DoD documents. DoDD 5000.1 contains the policy on risk management and is amplified further by the information in DoD 5000.2-R. The latter document integrates risk management into the acquisition process, describes the relationship between risk and various acquisition functions, and establishes some reporting requirements. DoDD 5000.4 and DoD 5000.4-M address risk and cost analysis guidance as they apply to the Office of the Secretary of Defense. Appendix A is an extract of existing risk management policies and procedures from all of these documents.

The DoD 5000 series contains strong statements on risk management but requires elaboration to help the PM establish an effective risk management program. The information furnished in the Risk Management section of the *Deskbook* supports and expands the contents of the DoD 5000 series.

The DoD risk management policies and procedures provide the basis for this *Guide*, which complements the *Deskbook* by elaborating on risk management concepts and by providing greater detail for applying techniques.

Downloaded from http://www.everyspec.com

2

RISK AND RISK MANAGEMENT

2.1 INTRODUCTION

This Chapter introduces the concepts of risk and risk management by explaining the DoD risk-related definitions and by identifying the characteristics of acquisition risks. It also presents and discusses a structured concept for risk management and its five subordinate processes.

2.2 OVERVIEW

The DoD risk management concept is based on the principles that risk management must be forward-looking, structured, informative, and continuous. The key to successful risk management is early planning and aggressive execution. Good planning enables an organized, comprehensive, and iterative approach for identifying and assessing the risk and handling options necessary to refine a program acquisition strategy. To support these efforts, assessments should be performed as early as possible in the life cycle to ensure that critical technical, schedule, and cost risks are addressed with mitigation actions incorporated into program planning and budget projections.

PMs should update program risk assessments and tailor their management strategies accordingly. Early information gives them data that helps when writing a Request for Proposal and assists in Source Selection planning. As a program progresses, new information improves insight into risk areas, thereby allowing the development of effective handling strategies. The net result promotes executable programs.

Effective risk management requires involvement of the entire program team and also requires help from outside experts knowledgeable in critical risk areas (e.g., threat, technology, design, manufacturing, logistics, schedule, and cost). In addition, the risk management process should cover hardware, software, the human element, and integration issues. Outside experts may include representatives from the user, laboratories, contract management, test, logistics, and sustainment communities, and industry. Users, essential participants in program trade analyses, should be part of the assessment process so that an acceptable balance among cost, schedule, performance, and risk can be reached. A close relationship between the Government and industry, and later with the selected contractor(s), promotes an understanding of program risks and assists in developing and executing the management efforts.

Successful risk management programs generally have the following characteristics:

- Feasible, stable, and well-understood user requirements and threat;
- A close relationship with user, industry, and other appropriate participants;

Downloaded from http://www.everyspec.com

- A planned and structured risk management process, integral to the acquisition process;

- An acquisition strategy consistent with risk level and risk-handling strategies;

- Continual reassessment of program and associated risks;

- A defined set of success criteria for all cost, schedule, and performance elements, e.g., Acquisition Program Baseline (APB) thresholds;

- Metrics to monitor effectiveness of risk-handling strategies;

- Effective Test and Evaluation Program;

- Formal documentation.

PMs should follow the guidelines below to ensure that a management program possesses the above characteristics.

- Assess program risks, using a structured process, and develop strategies to manage these risks throughout each acquisition phase.

- Identify early and intensively manage those design parameters that critically affect cost, capability, or readiness.

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

- Use test and evaluation as a means of quantifying the results of the risk-handling process.

- Include industry and user participation in risk management.

- Use Developmental Test and Evaluation (DT&E) and early operational assessments when appropriate.

- Establish a series of "risk assessment reviews" to evaluate the effectiveness of risk handling against clearly defined success criteria.

- Establish the means and format to communicate risk information and to train participants in risk management.

- Prepare an assessment training package for members of the program office and others, as needed.

- Acquire approval of accepted risks at the appropriate decision level.

In general, management of software risk is the same as management of other types of risk and techniques that apply to hardware programs are equally applicable to software intensive programs. However, some characteristics of software make this type of risk management different, primarily because it is difficult to:

- Identify software risk.

- Estimate the time and resources required to develop new software, resulting in potential risks in cost and schedule.

- Test software completely because of the number of paths that can be followed in the logic of the software.

- Develop new programs because of the rapid changes in information technology and an ever-increasing demand for quality software personnel.

2.3 RISK MANAGEMENT STRUCTURE AND DEFINITIONS

Although each risk management strategy depends upon the nature of the system being developed, research reveals that good strategies contain the same basic processes and structure shown in Figure 2-1. This structure is sometimes also referred to as

Downloaded from http://www.everyspec.com

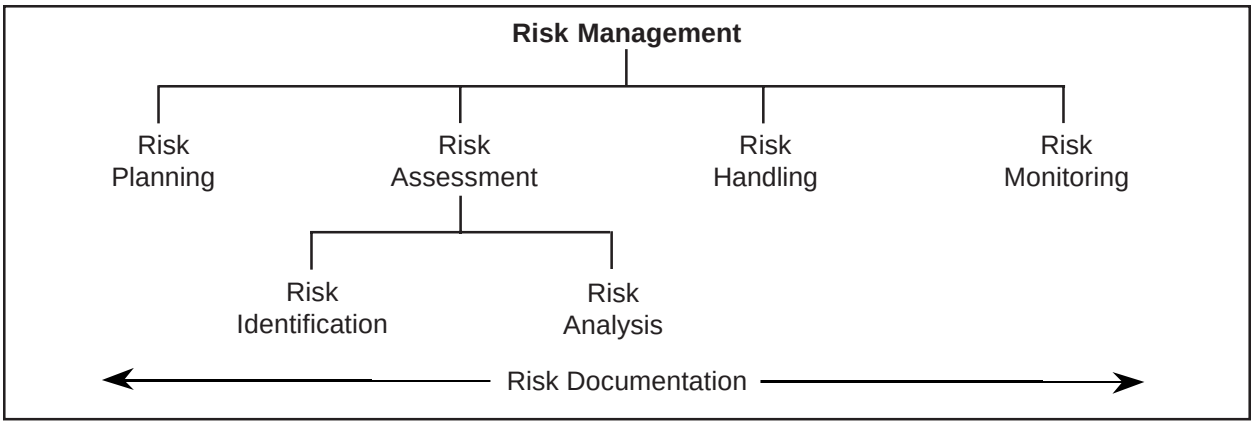


Figure 2-1. Risk Management Structure

the Risk Management Process Model. The application of these processes vary with acquisition phases and the degree of system definition; all should be integrated into the program management function.

The elements of the structure are discussed in the following paragraphs of this Chapter; however, in order to form a basis for discussion, the *Deskbook* definitions for the processes and elements of risk management include:

Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints and has two components: (1) the *probability* (or likelihood) of failing to achieve a particular outcome, and (2) the *consequences* (or impact) of failing to achieve that outcome.

Risk management is the act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program.

Risk planning is the process of developing and documenting an organized, comprehensive, and interactive strategy and methods for identifying and tracking risk areas, developing risk-handling plans, performing continuous risk assessments to determine how risks have changed, and assigning adequate resources.

Risk events, things that could go wrong for a program or system, are elements of an acquisition program that should be assessed to determine the level of risk. The events should be defined to a level that an individual can comprehend the potential impact and its causes. For example, a potential risk event for a turbine engine could be turbine blade vibration. There could be a series of potential risk events that should be selected, examined, and assessed by subject-matter experts.

The relationship between the two components of risk—probability and consequence—is complex. To avoid obscuring the results of an assessment, the risk associated with an event should be characterized in terms of its two components. There is still a need for backup documentation containing the supporting data and assessment rationale.

Risk assessment is the process of identifying and analyzing program areas and critical technical process risks to increase the likelihood of meeting cost, schedule, and performance objectives. *Risk identification* is the process of examining the

Downloaded from http://www.everyspec.com

program areas and each critical technical process to identify and document the associated risk. *Risk analysis* is the process of examining each identified risk area or process to refine the description of the risk, isolating the cause, and determining the effects. It includes risk rating and prioritization in which risk events are defined in terms of their probability of occurrence, severity of consequence (or impacts), and relationship to other risk areas or processes.

Risk handling is the process that identifies, evaluates, selects, and implements options in order to set risk at acceptable levels given program constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, and associated cost and schedule. The most appropriate strategy is selected from these handling options. For purposes of the *Guide*, risk handling is an all-encompassing term whereas risk mitigation is one subset of risk handling.

Risk monitoring is the process that systematically tracks and evaluates the performance of risk-handling actions against established metrics throughout the acquisition process and develops further risk-handling options, as appropriate.

Risk documentation is recording, maintaining, and reporting assessments, handling analysis and plans, and monitoring results. It includes all plans, reports for the PM and decision authorities, and reporting forms that may be internal to the PMO.

2.4 RISK DISCUSSION

Implicit in the definition of risk is the concept that risks are future events and that there is uncertainty associated with the program if these events occur. Therefore, there is a need to determine, as much as possible, the probability of a risk event occurring and to estimate the impact (consequences) if it occurs. The combination of these two factors determines severity. For example, an event with a low probability of occurring, yet with severe consequences, may be a candidate for handling. Conversely, an event with a high probability of happening, but the consequences of which do not affect a program, may be acceptable and require no handling.

To reduce uncertainty and apply the definition of risk to acquisition programs, PMs must be familiar with the types of acquisition risks, understand risk terminology, and know how to measure risk. These topics are addressed in the next several sections.

2.4.1 Characteristics of Acquisition Risk

Acquisition programs tend to have numerous, often interrelated, risks. They are not always obvious; relationships may be obscure; and they may exist at all program levels throughout the life of a program. Risks are in the PMO (program plans, etc.); in support provided by other Government agencies; in threat assessment; and in prime contractor processes, engineering and manufacturing processes, and technology. The interrelationship among risk events may cause an increase in one because of the occurrence of another. For example, a slip in schedule for an early test event may adversely impact subsequent tests, assuming a fixed period of test time is available.

Another important risk characteristic is the time period before a risk future event occurs; because time is critical in determining risk-handling options. If an event is imminent, the PMO must resort to crisis management. An event that is far enough in the future to allow management actions may be controllable. The goal is to avoid

Downloaded from http://www.everyspec.com

the need to revert to problem solving by managing risk.

An event's probability of occurrence and consequences may change as the development process proceeds and information becomes available. Therefore, throughout the development phase, PMOs should re-evaluate known risks on a periodic basis and examine the program for new risks.

2.4.2 Program Products, Processes, Risk Areas, and Risk Events

Program risk includes all risk events and their relationships to each other. It is a top-level assessment of impact to the program when all risk events at the lower levels of the program are considered. Program risk may be a roll-up of all low-level events; however, most likely, it is a subjective evaluation of the known risks by the PMO, based on the judgment and experience of experts. Any roll-up of program risks must be carefully done to prevent key risk issues from "slipping through the cracks." Identifying program risk is worthwhile because it forces the PMO to consider relationships among all risks and may identify potential areas of concern that would have otherwise been overlooked. One of the greatest strengths of a formal, continuous risk management process is the proactive quest to identify risk events for handling and the reduction of uncertainty that results from handling actions.

A program office has continuous demands on its time and resources. It is, at best, difficult, and probably impossible, to assess every potential area and process. To manage risk, the PMOs should focus on the critical areas that could affect the outcome of their programs. Work Breakdown Structure (WBS) product and process elements and industrial engineering and manufacturing processes contain most of the significant risk events. Risk events are determined by examining each WBS element and process in terms of sources or areas of risk. Broadly speaking, these sources generally can be grouped as cost, schedule, and performance, with the latter including technical risk. Following are some typical risk areas:

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

- **Requirements**. The sensitivity of the program to uncertainty in the system description and requirements except for those caused by threat uncertainty.

- **Design**. The ability of the system configuration to achieve the program's engineering objectives based on the available technology, design tools, design maturity, etc.

- **Test and Evaluation (T&E)**. The adequacy and capability of the T&E program to assess attainment of significant performance specifications and determine whether the systems are operationally effective and suitable.

- **Modeling and Simulation (M&S)**. The adequacy and capability of M&S to support all phases of a program using verified, valid, and accredited M&S.

- **Technology**. The degree to which the technology proposed for the program has been demonstrated as capable of meeting all of the program's objectives.

- **Logistics**. The ability of the system configuration to achieve the program's logistics objectives based on the system design, maintenance concept, support

Downloaded from http://www.everyspec.com

system design, and availability of support resources.

- **Production**. The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources such as facilities and personnel.

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

- **Capability of Developer**. The ability of the developer to design, develop, and manufacture the system. The contractor should have the experience, resources, and knowledge to produce the system.

- **Cost/Funding**. The ability of the system to achieve the program's life-cycle cost objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined).

- **Management**. The degree in which program plans and strategies exist and are realistic and consistent. The Government's acquisition team should be qualified and sufficiently staffed to manage the program.

- **Schedule**. The adequacy of the time allocated for performing the defined tasks, e.g., developmental, production, etc. This factor includes the effects of programmatic schedule decisions, the inherent errors in the schedule estimating technique used, and external physical constraints.

Critical risk processes are the developer's engineering and production processes which, historically, have caused the most difficulty during the development and/or production phases of acquisition programs. These processes include, but are not limited to, **design, test, production, facilities, logistics, and management**. These processes are included in the critical risk areas and are addressed separately to emphasize that they focus on processes. DoD 4245.7-M, *Transition from Development to Production*, describes them using templates. See Figure 2-2 for an example of the template for product development. The templates are the result of a Defense Science Board task force, composed of Government and industry experts, who identified engineering processes and control methods to minimize risk in both Government and industry. The task force defined these critical events in terms of the templates, which are briefly discussed later. The figure also shows **funding** as a process that, unlike others, is a Government process.

Additional areas, such as manpower, environmental impact, systems safety and health, and systems engineering, that are analyzed during program plan development provide indicators for additional risk. The PMO should consider these areas for early assessment since failure to do so could cause dire consequences in the program's latter phases.

In addition, PMs should address the uncertainty associated with security—an area sometimes overlooked by developers but addressed in the Acquisition System Protection (ASP) section of the *Deskbook* and Air Force Pamphlet ASPWG PH-1, *Acquisition System Protection Program Work Book*, September 1994. However, in addition to the guidance given there, PMs must recognize that, in the past, classified programs have experienced difficulty in access, facilities, clearances, and visitor control. Failure to manage these aspects of a classified program could adversely affect cost and schedule.

Downloaded from http://www.everyspec.com

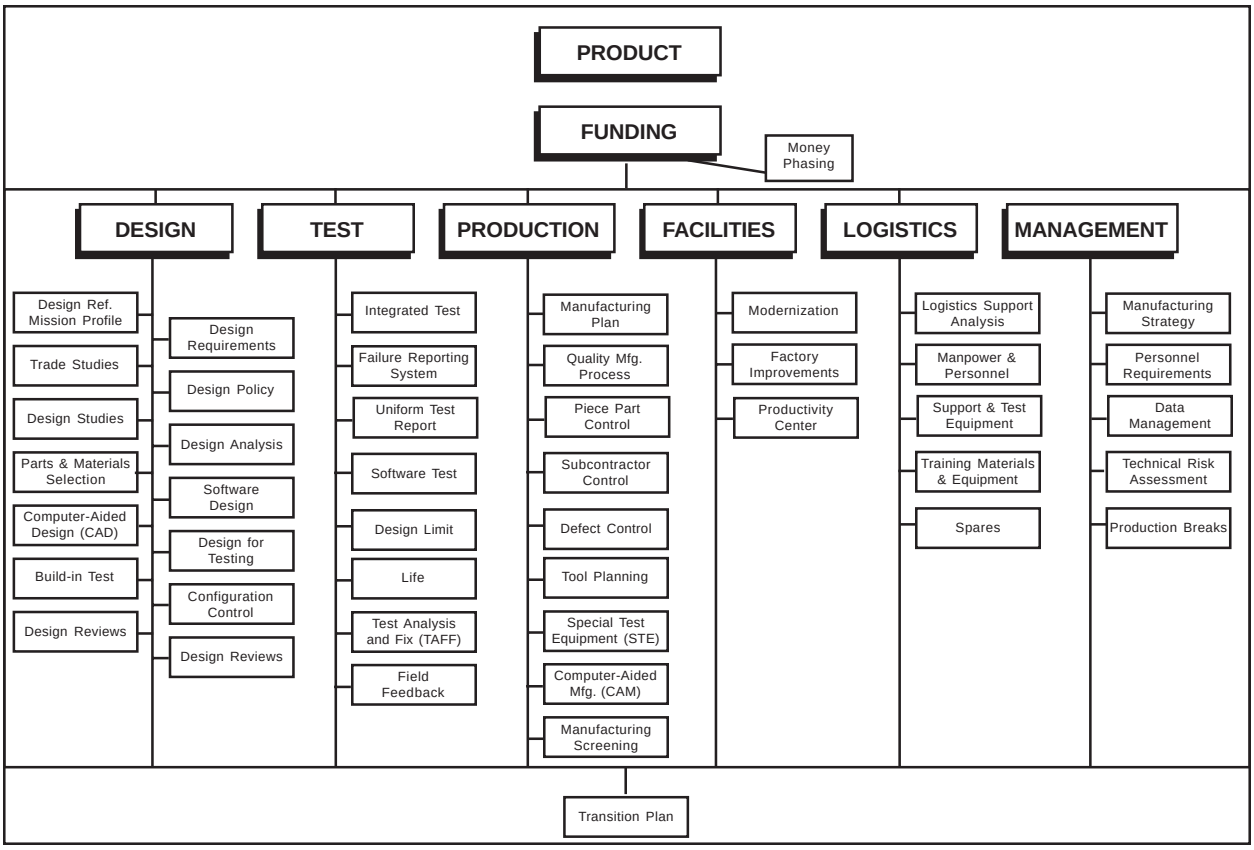


Figure 2-2. Critical Process Areas and Templates

2.5 RISK PLANNING

2.5.1 Purpose of Risk Plans

Risk planning is the detailed formulation of a program of action for the management of risk. It is the process to:

- Develop and document an organized, comprehensive, and interactive risk management strategy.
- Determine the methods to be used to execute a PM's risk management strategy.
- Plan for adequate resources.

Risk planning is iterative and includes describing and scheduling the activities and process to assess (identify and analyze), handle, monitor, and document the risk associated with a program. The result is the Risk Management Plan (RMP).

2.5.2 Risk Planning Process

The PMO should periodically review the plan and revise it, if necessary. Some events such as: (1) a change in acquisition strategy, (2) preparation for a major decision point, (3) technical audits and reviews, (4) an update of other program plans, and (5) preparation for a Program Objective Memorandum (POM) submission may drive the need to update an existing plan.

Planning begins by developing and documenting a risk management strategy. Early efforts establish the purpose and objective, assign responsibilities for specific areas, identify additional technical expertise needed, describe the assessment process and areas to consider, delineate procedures for consideration of handling options, define a risk rating scheme, dictate the reporting and documentation needs, and

Downloaded from http://www.everyspec.com

establish report requirements and monitoring metrics. This planning should also address evaluation of the capabilities of potential sources as well as early industry involvement and program.

The PM's strategy to manage risk provides the program team with direction and basis for planning. Initially formalized during a program's Concept Exploration Phase and updated for each subsequent program phase, the strategy should be reflected in the program's acquisition strategy, which with requirement and threat documents, known risks, and system and program characteristics are sources of information for PMO use to devise a strategy and begin developing a Risk Management Plan. Since the program's risks are affected by the Government and contractor team's ability to develop and manufacture the system, industry can provide valuable insight into this area of consideration.

The plan is the road map that tells the Government and contractor team how to get from where the program is today to where the PM wants it to be in the future. The key to writing a good plan is to provide the necessary information so the program team knows the objectives, goals, and the PMO's risk management process. Since it is a map, it may be specific in some areas, such as the assignment of responsibilities for Government and contractor participants and definitions, and general in other areas to allow users to choose the most efficient way to proceed. For example, a description of techniques that suggests several methods for evaluators to use to assess risk is appropriate, since every technique has advantages and disadvantages depending on the situation.

Appendix B contains two examples of a risk plan and a summary of the format is shown in Figure 2-3.

Introduction
Program Summary
Definitions
Risk Management Strategy and Approach
Organization
Risk Management Process and Procedures
Risk Planning
Risk Assessment
Risk Handling
Risk Monitoring
Risk Management Information System, Documentation and Reports

Figure 2-3. A Risk Management Plan Format

In a decentralized PMO risk management organization, the program's risk management coordinator may be responsible for risk management planning. See Sections 4.4, Risk Management Organizations, and 5.3, Risk Planning Techniques.

2.6 RISK ASSESSMENT

2.6.1 Purpose of Risk Assessments

The primary objective of assessments is to identify and analyze program risks so that the most critical among them may be controlled. Assessments are factors that managers should consider in setting cost, schedule, and performance objectives because they provide an indication of the likelihood of achieving the desired outcomes.

2.6.2 Risk Assessment Process

Risk assessment is the *problem definition* stage of management that identifies and analyzes (quantifies) program events in terms of probability and consequences. The results form the basis for most risk management actions. It is probably the most difficult and time-consuming part of the management process. There are no quick answers or shortcuts. Tools are available to assist evaluators in assessing risk, but

Downloaded from http://www.everyspec.com

none are totally suitable for any program and may be highly misleading if the user does not understand how to apply them or interpret the results. Despite its complexity, risk assessment is one of the most important phases of the risk process because the caliber and quality of assessments determine the effectiveness of a management program.

The components of assessment, identification and analysis, are performed sequentially with identification being the first step.

Risk identification begins by compiling the program's risk events. PMOs should examine and identify program events by reducing them to a level of detail that permits an evaluator to understand the significance of any risk and identify its causes, i.e., risk drivers. This is a practical way of addressing the large and diverse number of potential risks that often occur in acquisition programs. For example, a WBS level 4 or 5 element may generate several risk events associated with a specification or function, e.g., failure to meet turbine blade vibration requirements for an engine turbine design.

Risk events are best identified by examining each WBS product and process element in terms of the sources or areas of risk, as previously described in Paragraph 2.4.2.

Risks are those events that evaluators (after examining scenarios, WBS, or processes) determine would adversely affect the program. Evaluators may initially rank events by probability and consequence of occurrence before beginning analysis to focus on those most critical.

Risk analysis is a technical and systematic process to examine identified risks, isolate causes, determine the relationship to other risks, and express the impact in terms of probability and consequences.

In practice, the distinction between risk identification and risk analysis is often blurred because there is some risk analysis that occurs during the identification process. For example, if, in the process of interviewing an expert, a risk is identified, it is logical to pursue information on the probability of it occurring, the consequences, the time associated with the risk (i.e., when it might occur), and possible ways of dealing with it. The latter actions are part of risk analysis and risk handling, but often begin during risk identification.

Prioritization is the ranking of risk events to determine the order of importance. It serves as the basis for risk-handling actions. Prioritization is part of risk analysis.

Integrated Product Teams (IPTs) typically perform risk assessments in a decentralized risk management organization as described in Paragraph 4.4. If necessary, the team may be augmented by people from other program areas or outside experts. Paragraph 5.4, Risk Assessment Techniques, elaborates on this for each of the described assessment techniques.

2.6.3 Timing of Risk Assessments

The assessment process begins during the last half of Phase 0, Concept Exploration, and continues throughout the subsequent phases. The PMO should continually reassess the program at increasing levels of detail as the program progresses through the acquisition phases and more information becomes available. There are, however, times when events may require new assessments, i.e., a major change in the acquisition strategy. Paragraph 2.5.2 lists other events that could cause risk assessments to be performed.

Downloaded from http://www.everyspec.com

2.6.4 Conducting Risk Assessments

There is no standard approach to assessing risk because methods vary according to the technique employed, the phase of the program, and the nature of the program itself; however, some top-level actions are typically common to all methods. They are grouped in Figure 2-4 into pre-risk assessment activities, risk identification activities, and risk analysis activities. Each risk category or area, e.g., cost, schedule, and performance, includes a core set of assessment tasks and is related to the other two categories. This relationship requires supportive analysis among areas to ensure the integration of the assessment process. For example, a technical assessment probably should include a cost and schedule analysis in determining the technical risk impact. The results of the assessments, normally conducted by IPTs follow:

Performance/Technical Assessment (Includes technical areas of risk shown in Paragraph 2.4.2.)

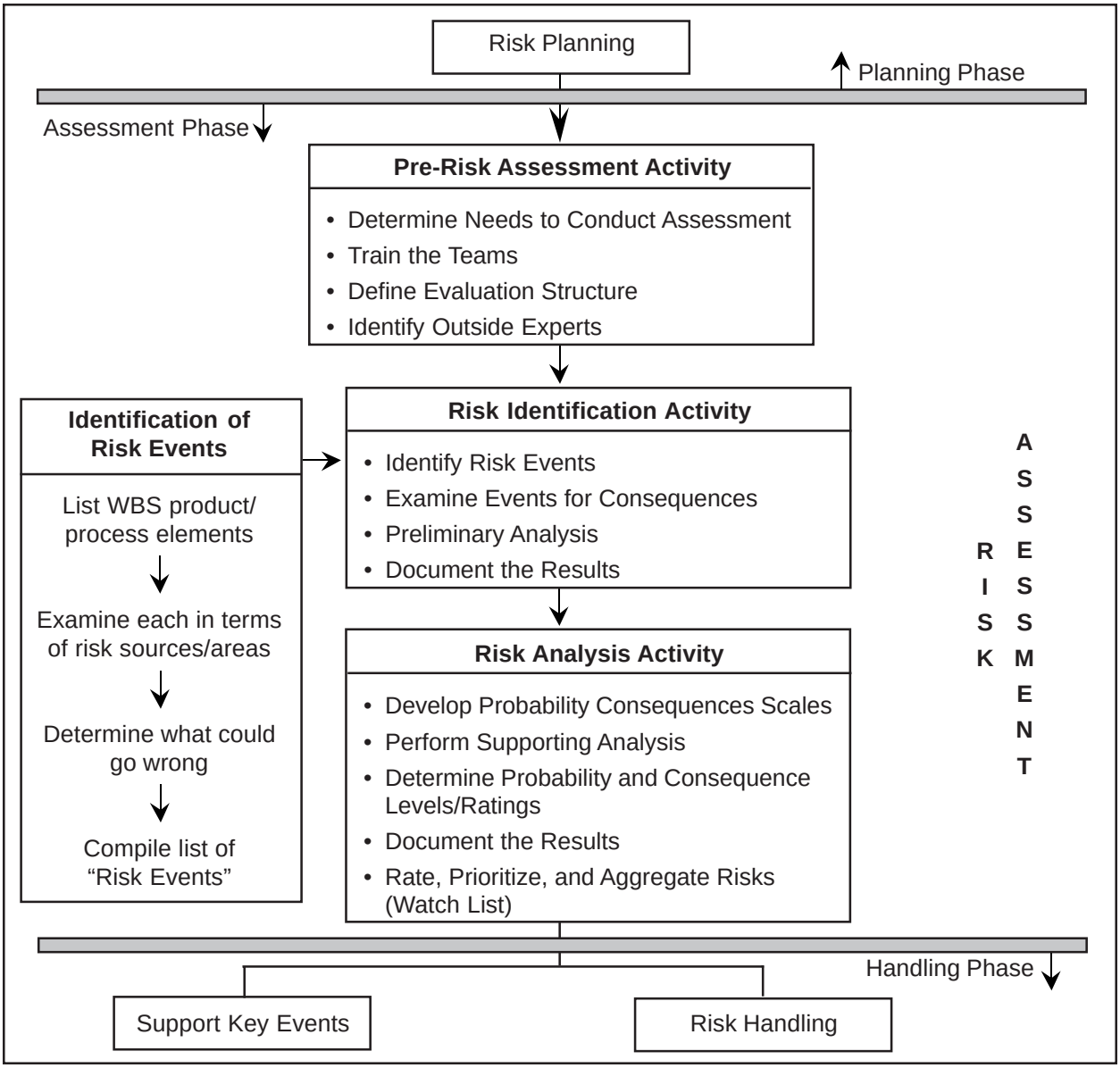


Figure 2-4. Risk Assessment

Downloaded from http://www.everyspec.com

- Provides technical foundation,
- Identifies and describes program risks, i.e., threat, technology, design, manufacturing, etc.,
- Prioritizes risks with relative or quantified weight for program impact,
- Analyzes risks and relates them to other internal and external risks,
- Quantifies associated program activities with both time duration and resources,
- Quantifies inputs for schedule assessment and cost estimate,
- Documents technical basis and risk definition for the risk assessment.

Schedule Assessment

- Evaluates baseline schedule inputs,
- Incorporates technical assessment and schedule uncertainty inputs to program schedule model,
- Evaluates impacts to program schedule based on technical team assessment,
- Performs schedule analysis on program integrated master schedule,
- Quantifies schedule excursions reflecting effects of cost risks, including resource constraints,
- Provides Government schedule assessment for cost analysis and fiscal year planning,
- Reflects technical foundation, activity definition, and inputs from technical and cost areas,
- Documents schedule basis and risk impacts for the risk assessment.

Cost Estimate and Assessment

- Builds on technical and schedule assessment results,
- Translates technical and schedule risks into cost,
- Derives cost estimate by integrating technical risk and schedule risk impacts with resources,
- Establishes budgetary requirements consistent with fiscal year planning,
- Determines if the phasing of funds supports technical and acquisition approach,
- Provides program cost excursions from:
  - — Near-term budget execution impacts,
  - — External budget changes and constraints.
- Documents cost basis and risk impacts.

2.6.4.1 Pre-Risk Assessment Activities. The Risk Management Plan may describe the actions that compose this activity. Typically, a program-level IPT may conduct a quick-look assessment of the program to identify the need for technical experts (who are not part of the team) and to examine areas that appear most likely to contain risk. The program's risk coordinator, or an outside expert, may train the IPTs, focusing on the program's risk strategy, definitions, suggested techniques, documentation, and reporting requirements. Paragraph 4.9, Risk Management Training, provides some suggestions for training.

2.6.4.2 Risk Identification Activity. To identify risk events, IPTs should break down program elements to a level where they, or subject-matter experts, can perform valid assessments. The information necessary to do this varies according to the phase of the program. During the early

Downloaded from http://www.everyspec.com

phases, requirement, threat documents, and acquisition plans may be the only program-specific data available. They should be analyzed to identify events that may have adverse consequences. A useful initial identification exercise is to perform a mission profile for the system as suggested in DoD 4245.7-M, *Transition from Development to Production*. Using this methodology, the developer creates a functional and environmental profile for the system and examines the low-level requirements that the system must meet to satisfy its mission requirements. The IPTs may then study these requirements to determine which are critical. For example, in an aircraft profile, it may be apparent that high speed is critical. If the speed requirement is close to that achieved by existing aircraft, this may not be a concern. However, if the speed is greater than that achieved by today's aircraft, it may be a critical risk area. Since aircraft speed depends, among other things, on weight and engine thrust, it would be desirable to enlist the help of a materials expert to address weight and an engine expert to assess engine-associated risk.

Another method of decomposition is to create a WBS as early as possible in a program. Figure 2-5 is a simple example of a decomposition based on the WBS for an aircraft. The figure shows an important requirement of the decomposition process, the establishment of goals (e.g., don't exceed the weight budget or objective). Risk events are determined by matching each WBS element and process to sources or areas of risk. Risk areas / sources are described in Paragraph 2.4.2 and Table 4-2.

During decomposition, risk events are identified from experience, brainstorming, lessons learned from similar programs, and guidance contained in the risk management plan. A structured approach previously discussed matches each WBS element and process in terms of sources or areas of risk. The examination of each event is an exploratory exercise to identify the critical risks. The investigation may show that risks are interrelated. For example, the weight of an aircraft affects its speed, but also impacts the payload, range, and fuel requirements. These have design and logistics consequences and may even affect the number of aircraft that must be procured to meet objectives.

Critical risks need to be documented as specified in the Risk Management Plan and

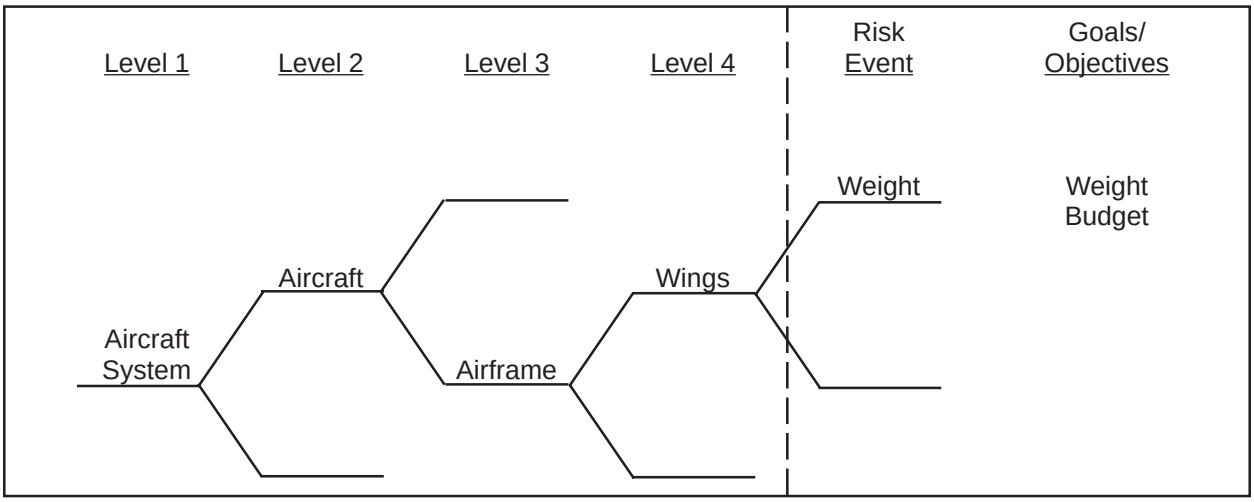


Figure 2-5. Example of a WBS Dependent Evaluation Structure

Downloaded from http://www.everyspec.com

may include the scenario that causes the risk, planned management controls and actions, etc. It may also contain an initial assessment of the consequences to focus the risk assessment effort. A risk watch list should be initiated as part of risk identification. It is refined during handling, and monitored/updated during the monitoring phase.

2.6.4.3 Risk Analysis Activity. Analysis begins with a detailed study of the critical risks that have been identified. The objective is to gather enough information about the risks to judge the probability of occurrence and the impact on cost, schedule, and performance if the risk occurs.

Impact assessments are normally subjective and based on detailed information that may come from:

- Comparisons with similar systems,
- Relevant lessons-learned studies,
- Experience,
- Results from tests and prototype development,
- Data from engineering or other models,
- Specialist and expert judgments,
- Analysis of plans and related documents,
- Modeling and simulation,
- Sensitivity analysis of alternatives.

Depending on the particular technique and the risk being analyzed, some supporting analysis may be necessary, i.e., analysis of contractor processes, such as design, engineering, fault tree analysis, engineering models, simulation, etc. Analyses provide the basis for subjective assessments.

A critical aspect of risk analysis is data collection. Two primary sources of data are interviews of subject-matter experts and analogy comparisons with similar systems. Paragraph 5.4 contains a technique for collecting both types of data for use in support of the techniques listed in Table 2-1. Periodically, sets of risks need to be prioritized in preparation for risk handling, and aggregated to support program management reviews. Paragraph 5.5, Risk Prioritization, describes methods for accomplishing this.

2.6.4.3.1 Risk Rating and Prioritization/Ranking

Ratings are an indication of the potential impact of risks on a program; they are a measure of the likelihood of an event occurring and the consequences of the event. They are often expressed as high, moderate, and low. Risk rating and prioritization/ranking are considered integral parts of risk analysis.

Risk Assessment Technique	Applicable Acquisition Phases	Applicable Risk Areas & Processes
Plan Evaluation/Risk Identification	All phases	Program Plans and critical communications with the developer
Product (WBS) Risk Assessment	All phases starting with the completion of the Contract WBS	All critical risk areas except threat, requirements, cost, and schedule
Process (DoD 4265.7-M) Risk Assessment	All phases but mainly EMD	All critical risk processes
Cost Risk Assessment	All phases	Cost critical risk areas
Schedule Risk Assessment	All phases	Schedule critical risk areas

Table 2-1. Risk Assessment Approaches

Downloaded from http://www.everyspec.com

A group of experts, who are familiar with each risk area (e.g., design, logistics, production, etc.) and product WBS element risk ratings, are best qualified to determine risk ratings. They should identify rating criteria for review by the PMO, who includes them in the Risk Management Plan. In most cases, the criteria will be based on the experience of the experts, as opposed to mathematically derived and should establish levels of likelihood and consequences that will provide a range of possibilities large enough to distinguish differences in risk ratings. At the program level, consequences should be expressed in terms of impact on cost, schedule and performance. Tables 2-2 and 2-3 are examples of likelihood and consequence criteria, and Table 2-4 contains an example of overall risk rating criteria, which considers both likelihood and consequences. Table 2-5 provides a sample format for presenting risk ratings.

Level	What is the Likelihood the Risk Event Will Happen?
a	Remote
b	Unlikely
c	Likely
d	Highly likely
e	Near certainty

Table 2-2. Likelihood Criteria (Example)

Rating	Description
High	Major disruption likely
Moderate	Some disruption
Low	Minimum impact

Table 2-4. Overall Risk Rating Criteria (Example)

Using these risk ratings, PMs can identify events requiring priority management (high or moderate risk likelihood or consequences). The document prioritizing the risk events is called a Watch List. Risk ratings also help to identify the areas that should be reported within and outside the PMO, e.g., milestone decision reviews. Thus, it is important that the ratings be portrayed as accurately as possible.

A simple method of representing the risk rating for risk events is shown in Figure 2-6. In this example, the PM has defined levels high, moderate, and low for the various combinations of likelihood and consequences.

There is a common tendency to attempt to develop a single number to portray the risk associated with a particular event. This approach may be suitable if both likelihood (probability) and consequences have been quantified using compatible cardinal scales or calibrated ordinal scales

Level	Given the Risk Is Realized, What Is the Magnitude of the Impact?		
	Performance	Schedule	Cost
1	Minimal or no impact	Minimal or no impact	Minimal or no impact
2	Acceptable with some reduction in margin	Additional resources required; able to meet need dates	<5%
3	Acceptable with significant reduction in margin	Minor slip in key milestones; not able to meet need date	5-7%
4	Acceptable; no remaining margin	Major slip in key milestone or critical path impacted	7-10%
5	Unacceptable	Can't achieve key team or major program milestone	>10%

Table 2-3. Consequences Criteria (Example)

Downloaded from http://www.everyspec.com

Priority	Area/ Process	Location	Title	Likeli-hood	Conse-quence	Time Constraints
1	Design	WBS 3.1	Design completeness	High	High	1-2 months
2						
3						

Table 2-5. Risk Ratings (Example)

Likelihood	1	2	3	4	5
e	L	M	H	H	H
d	L	M	M	H	H
c	L	M	M	M	H
b	L	L	L	M	M
a	L	L	L	L	M

Consequence

Figure 2-6. Overall Risk Rating (Example)

whose scale levels have been determined using accepted procedures (e.g., Analytical Hierarchy Process). In such a case, mathematical manipulation of the values may be meaningful and provide some quantitative basis for the ranking of risks.

In most cases, however, risk scales are actually just raw (uncalibrated) ordinal scales, reflecting only relative standing between scale levels and not actual numerical differences. Any mathematical operations performed on results from uncalibrated ordinal scales, or a combination of uncalibrated ordinal and cardinal scales, can provide information that will at best be misleading, if not completely meaningless, resulting in erroneous risk ratings. *Hence, mathematical operations should generally not be performed on scores derived from uncalibrated* ordinal *scales.* (Note: risk scales that are expressed as decimal values (e.g., a 5 level scale with values 0.2, 0.4, 0.6, 0.8 and 1.0) still retain the ordinal scale limitations discussed above.)

One way to avoid this situation is to simply show each risk event's likelihood and consequences separately, with no attempt to combine multiple risks. Other factors that may significantly contribute to the risk rating or prioritization of risk events, such as time sensitivity or resource availability, can also be shown. The prioritization or ranking should also be done based on a structural risk rating approach (e.g. Figure 2-6) coupled with expert opinion and experience. Prioritization or ranking is achieved through integration of risk events from lower to higher levels. This means that the effect of risk at lower WBS elements needs to be reflected cumulatively at the top or system level.

2.7 RISK HANDLING

2.7.1 Purpose of Risk Handling

Risk handling includes specific methods and techniques to deal with known risks and a schedule for accomplishing tasks, identifies who is responsible for the risk area, and provides an estimate of the cost and schedule associated with handling the risk, if any. It involves planning and execution with the objective of handling risks at an acceptable levels. The IPTs that assess risk should begin the process to identify and evaluate handling approaches to propose to the PM, who selects the appropriate ones for implementation.

2.7.2 Risk-Handling Process

The risk-handling phase must be compatible with the risk management plan and any additional guidance the PM provides. Paragraph 5.3 describes a technique that

Downloaded from http://www.everyspec.com

concentrates on planning. A critical part planning involves refining and selecting of the most appropriate handling options.

The IPTs that evaluate the handling options may use the following criteria as a starting point for assessment:

- Can the option be feasibly implemented and still meet the user's needs?

- What is the expected effectiveness of the handling option in reducing program risk to an acceptable level?

- Is the option affordable in terms of dollars and other resources (e.g., use of critical materials, test facilities, etc.)?

- Is time available to develop and implement the option, and what effect does that have on the overall program schedule?

- What effect does the option have on the system's technical performance?

Risk-handling options can include risk avoidance, risk control, risk transfer, risk assumption. Although the control risk-handling option is commonly used in defense programs, it should not automatically be chosen. All four options should be evaluated and the best one chosen for a given risk issue.

Risk control does not attempt to eliminate the source of the risk but seeks to reduce or mitigate the risks. It monitors and manages the risk in a manner that reduces the likelihood and/or consequence of its occurrence or minimizes the risk's effect on the program. This option may add to the cost of a program; however, the selected approach should provide an optional risk among the candidate approaches of risk reduction, cost effectiveness, and schedule impact. A sampling is listed below of the types of risk control actions available to the PMO. Paragraph 5.6.2 discusses them in more detail.

- **Multiple Development Efforts**. Create competing systems in parallel that meet the same performance requirements.

- **Alternative Design**. Create a backup design option that uses a lower risk approach.

- **Trade Studies.** Arrive at a balance of engineering requirements in the design of a system.

- **Early Prototyping**. Build and test prototypes early in the system development.

- **Incremental Development**. Design with the intent of upgrading system parts in the future.

- **Technology Maturation Efforts**. Normally, technology maturation is used when the desired technology will replace an existing technology which is available for use in the system.

- **Robust Design**. This approach, while it could be more costly, uses advanced design and manufacturing techniques that promote quality through design.

- **Reviews, Walk throughs, and Inspections.** These three actions can be used to reduce the likelihood and potential consequences of risks through timely assessment of actual or planned events.

- **Design of Experiments**. This engineering tool identifies critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.

- **Open Systems.** Carefully selected commercial specifications and standards whose use can result in lower risks.

Downloaded from http://www.everyspec.com

- **Use of Standard Items/Software Reuse.** Use of existing and proven hardware and software, where applicable, can substantially reduce risks.

- **Two-Phase Engineering and Manufacturing Development.** Incorporation of a formal risk reduction phase at the initial part of EMD. This technique is sometimes used instead of a formal PDRR phase if risk is moderate or low.

- **Use of Mock-ups**. The use of mock-ups, especially man-machine interface mock-ups, can be used to conduct early exploration of design options.

- **Modeling/Simulation**. Modeling and simulation can be used to investigate various design options and system requirement levels.

- **Key Parameter Control Boards**. The practice of establishing a control board for a parameter may be appropriate when a particular feature (such as system weight) is crucial to achieving the overall program requirements.

- **Manufacturing Screening**. For programs in Engineering and Manufacturing Development (EMD), various manufacturing screens (including environmental stress screening (ESS)) can be incorporated into test article production and low rate initial production (LRIP) to identify deficient manufacturing processes. ESS is a manufacturing process for stimulating parts and workmanship defects in electronic assemblies and units.

As you can see, there are numerous means that can be used to actively control risks.

Risk avoidance involves a change in the concept, requirements, specifications, and/or practices that reduce risk to an acceptable level. Simply stated, it eliminates the sources of high or possibly medium risk and replaces them with a lower risk solution and may be supported by a cost/benefit analysis. Generally, this method may be done in parallel with the up-front requirements analysis, supported by cost/requirement trade studies, which can include cost-as-an-independent-variable (CAIV) trades.

Risk Assumption. Risk assumption is an acknowledgment of the existence of a particular risk situation and a conscious decision to accept the associated level of risk, without engaging in any special efforts to control it. However, a general cost and schedule reserve may be set aside to deal with any problems that may occur as a result of various risk assumption decisions. This method recognizes that not all identified program risks warrant special handling; as such, it is most suited for those situations that have been classified as low risk. The key to successful risk assumption is twofold:

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it materializes. This includes identifying the specific management actions (such as retesting, additional time for further design activities) that may occur.

- Ensure that necessary administrative actions are taken to identify a management reserve to accomplish those management actions.

Risk-handling options have broad cost implications. The magnitude of these costs are circumstance-dependent. The approval and funding of handling options should be part of the process that establishes the program cost and performance goals. This should normally be done by the Program-

Downloaded from http://www.everyspec.com

Level Risk Management IPT or Risk Management Board. The selected handling option should be included in the program's acquisition strategy.

Once the acquisition strategy includes risk-handling approaches, the PMO can derive the schedule and identify cost, schedule, and performance, impacts to the basic program.

Risk Transfer. This action may reallocate risk during the concept development and design processes from one part of the system to another, thereby reducing the overall system risk, or re-distributing risks between the Government and the prime contractor or within Government agencies; or between members of the contractor team. It is an integral part of the functional analysis process. Risk transfer is a form of risk sharing and not risk abrogation on the part of the Government, and it may influence cost objectives. An example is the transfer of a function from hardware implementation to software implementation or vice versa. The effectiveness of risk transfer depends on the use of successful system design techniques. Modularity and functional partitioning are two design techniques that support risk transfer. In some cases, risk transfer may concentrate risk areas in one area of the design. This allows management to focus attention and resources on that area.

2.8 RISK MONITORING

The monitoring process systematically tracks and evaluates the effectiveness of risk-handling actions against established metrics. Monitoring results may also provide a basis for developing additional handling options and identifying new risks. The key to the monitoring process is to establish a cost, schedule, and performance management indicator system over the entire program that the PM uses to evaluate the status of the program. The indicator system should be designed to provide early warning of potential problems to allow management actions. Risk monitoring is not a problem-solving technique, but rather, a proactive technique to observe the results of risk handling and identify new risks. Some monitoring techniques can be adapted to become part of a risk indicator system:

- **Test and Evaluation (T&E)**. A well-defined (T&E) program is a key element in monitoring the performance of selected risk-handling options and developing new risk assessments.

- **Test-Analyze-and-Fix (TAAF)**. TAAF is the use of a period of dedicated testing to identify and correct deficiencies in a design.

- **Demonstration Events**. Demonstration events are points in the program (normally tests) that determine if risks are being successfully abated.

- **Earned Value (EV)**. This uses standard DoD cost/schedule data to evaluate a program's cost and schedule performance in an integrated fashion. As such, it provides a basis to determine if risk-handling actions are achieving their forecasted results.

- **Technical Performance Measurement (TPM)**. TPM is a product design assessment which estimates, through engineering analysis and tests, the values of essential performance parameters of the current design as effected by risk-handling actions.

- **Program Metrics**. These are used for formal, periodic performance assessments

Downloaded from http://www.everyspec.com

of the various development processes, evaluating how well the system development process is achieving its objective. This technique can be used to monitor corrective actions that emerged from an assessment of the critical risk processes.

- **Process Proofing**. Similar to Program Metrics, but aimed at manufacturing and support processes which are critical to achieving system requirements. Proofing simulates actual production environments and conditions to insure repeatedly conforming hardware and software.

- **Schedule Performance Monitoring**. This is the use of program schedule data to evaluate how well the program is progressing to completion.

Paragraph 5.7 describes several monitoring techniques, e.g., earned value.

The indicator system and periodic reassessments of program risk should provide the PMO with the means to incorporate risk management into the overall program management structure.

2.9 RISK DOCUMENTATION

A primary criteria for successful management is formally documenting the ongoing risk management process. This is important because:

- It provides the basis for program assessments and updates as the program progresses.

- Formal documentation tends to ensure more comprehensive risk assessments than if it is not documented.

- It provides a basis for monitoring risk-handling actions and verifying the results.

- It provides program background material for new personnel.

- It is a management tool for the execution of the program.

- It provides the rationale for program decisions.

The documentation should be done by those responsible for planning and collecting and analyzing data, i.e., IPT level in most cases.

Risk management reports vary depending on the size, nature, and phase of the program. Examples of some risk management documents and reports that may be useful to a PM are:

- Risk Management Plan,
- Risk information form,
- Risk assessment report,
- Risk handling priority list,
- Risk handling plan of action,
- Aggregated risk list,
- Risk monitoring documentation:
  - Program metrics,
  - Technical reports,
  - Earned value reports,
  - Watch list,
  - Schedule performance report,
  - Critical risk processes reports.

Most PMOs can devise a list of standard reports that will satisfy their needs most of the time; however, since there will always be a need for ad hoc reports and briefing and assessments, it is advisable to store

Downloaded from http://www.everyspec.com

risk information in a management information system (MIS). This allows you to derive standard reports and create of ad hoc reports, as needed. Paragraphs 4.8 and 5.8 discuss an MIS to support a risk management program.

Acquisition reform discourages Government oversight; therefore, formal contractor-produced risk documentation may not be available for most programs. However, program insight is encouraged, and PMOs can obtain information about program risk from contractor internal documentation such as:

- **Risk Management Policy and Procedures**. This is a description of the contractor's corporate policy for the management of risk. The procedures describe the methods for risk identification, analysis, handling, monitoring, and documentation. It should provide the baseline planning document for the contractor's approach to risk management.

- **Corporate Policy and Procedures Documents**. Corporations have policy and procedures documents that address the functional areas that are critical to the design, engineering, manufacture, test and evaluation, quality, configuration control, manufacture, etc., of a system. These documents are based on what the company perceives as best practices, and although they may not specifically address risk, deviation from these policies represents risk to a program. Internal company reports that address how well programs comply with policy may be required and will provide valuable information.

- **Risk Monitoring Report**. Contractors should have internal tracking metrics and reports for each moderate- or high-risk item. These metrics may be used to determine the status of risk reduction programs.

Downloaded from http://www.everyspec.com

3

RISK MANAGEMENT AND DOD ACQUISITION PROCESS

3.1 INTRODUCTION

This Chapter discusses the relationship between risk and the acquisition process, describes how risk is considered in design of the Acquisition Plan, and expresses the need to consider risk as early in the program as possible. Appendix A is a summary of the risk management requirements that are contained in DoDD 5000.1 and DoD 5000.2-R, DoD 5000.4, and DoD 5000.4-M.

3.2 OVERVIEW

The DoD acquisition process for the management of programs consists of a series of phases designed to reduce risk, ensure affordability, and provide adequate information for decision making. Acquisition officials are encouraged to tailor programs to eliminate phases or activities that result in little payoff in fielding time or cost savings. To effectively tailor a program, one needs to understand the risks present in the program and to develop a plan for managing these risks. DoD policy calls for the continual assessment of program risks, beginning with the initial phase of an acquisition program, and the development of management approaches before any decision is made to enter all subsequent phases.

The application of risk management processes (planning, assessment, identification, analysis, handling, and monitoring) is particularly important during Phase 0 of any program, when alternatives are evaluated, program objectives are established, and the acquisition strategy is developed. All of these activities require acceptance of some level of risk and development of plans to manage the risk.

As a program evolves into subsequent phases, the nature of the risk management effort will change. New assessments will be built on previous ones. Risk areas will become more specific as the system is defined.

Risk management should also be an integral part of any Source Selection process, from RFP preparation, through proposal evaluation, and after contract award. Throughout the program life, IPTs will play a key role in risk management activities.

3.3 DOD ACQUISITION PROCESS

The phases and milestones of the acquisition process provide a streamlined structure that emphasizes risk management and affordability. The phases are a logical means of progressively translating broadly-stated mission needs into well-defined system-specific requirements, and ultimately into operationally effective, suitable, and survivable systems. It is important to remember that the term “system” includes hardware, software, and the human element. Each phase is designed,

Downloaded from http://www.everyspec.com

among other things, to manage risks. Milestones are points in time that allow decision makers to evaluate the program status and determine if the program should proceed to the next phase. The Milestone Decision Authority (MDA) and PM tailor milestones and phases so that each milestone decision point allows assessment of program status and the opportunity to review plans for the next phase and beyond. The MDA should explicitly address program risks and the adequacy of risk management planning during the milestone reviews and establish exit criteria for progression to the next phase.

The contract schedule normally allows time for milestone decisions before spending begins in subsequent phases and should also permit demonstration of the exit criteria in time to support the milestone review. There are exceptions to this—driven by funding availability and option award dates. However, the objective is to provide proper fiscal control without delaying the acquisition decisions or contracts while adequately considering risk.

The acquisition strategy defines the business and technical management approach to meet objectives within program constraints with a primary goal to minimize the time and cost of satisfying a valid need, consistent with common sense and sound business practices. A PM prepares a preliminary acquisition strategy at Milestone 0 (that includes Phase 0 activities that focus on identifying risk and handling options). Later, the PM updates the strategy to support each milestone decision by describing activities and events planned for the upcoming phase and relating the accomplishments of that phase to the program's overall, long-term objectives. The risk associated with a program will significantly influence the acquisition strategy.

3.4 CHARACTERISTICS OF THE ACQUISITION PROCESS

The acquisition process that has evolved can be characterized in terms of the following concepts that are particularly relevant to the management of risk in programs.

3.4.1 Integrated Product and Process Development (IPPD)

IPPD integrates all acquisition activities in order to optimize system development, production, and deployment. Key to the success of the IPPD concept are the IPTs, which are composed of qualified and empowered representatives from all appropriate functional disciplines who work together to identify and resolve issues. As such, IPTs are the foundation for organizing for risk management.

3.4.2 Continuous Risk Management

PMs should focus on risk management throughout the life of the program, not just in preparation for program and milestone reviews. Program risks should be continuously assessed, and the risk-handling approaches developed, executed, and monitored throughout the acquisition process. Both the Government and contractors must understand risks as a program progresses through the various phases and milestone decision points, and must modify the management strategy and plan accordingly. While specific government and contractors risk management processes may likely be different, it is important that each party have a common and complete set of process steps (regardless of their names), and be able to exchange and clearly understand the other party's risk management documentation.

Downloaded from http://www.everyspec.com

3.4.3 Program Stability

Once a program is initiated, program stability is a top priority. Keys to creating program stability are realistic investment planning and affordability assessments. They must reflect an accurate and comprehensive understanding of existing or expected program risks. A risk management strategy must be developed early in the process, before actually initiating the program to ensure it is a stable one, recognizing that key issues affecting program stability may be external.

3.4.4 Reduction of Life-Cycle Costs

DoD considers the reduction of total cost to acquire and operate systems while maintaining a high level of performance for the user to be of highest priority. This is reflected, in part, through the introduction of the "Cost As an Independent Variable" (CAIV) concept. CAIV entails setting aggressive, realistic cost objectives early in an acquisition program and then managing all aspects of the program to achieve those objectives, while still meeting the user's performance and schedule needs. Inherent in the CAIV concept is the realization that risks must be understood, taken, and managed in order to achieve cost, schedule, and performance objectives. An understanding of risk is essential to setting realistic cost objectives. The PM and user representatives should identify risk and cost driving requirements during the generation of the Operational Requirement Document (ORD) in order to know where tradeoffs may be necessary.

3.4.5 Event-Oriented Management

Event-oriented management requires that decision makers base their decisions on significant events in the acquisition life cycle, rather than on arbitrary calendar dates. This management process emphasizes effective acquisition planning and embodies sound risk management. Decisions to proceed with a program should be based on demonstration of performance, through test and evaluation, and on verification that program risks are well-understood and are being managed effectively. Attainment of agreed-upon exit criteria is an indication that the PMO is managing risk effectively.

3.4.6 Modeling and Simulation

Properly used, models and simulations can reduce time, resources, and acquisition risk and may increase the quality of the systems being developed. Users of these models and simulations must have a good understanding of their capabilities and limitations and their applicability to the issues being addressed.

From a risk perspective, modeling and simulation may be used to develop alternative concepts during system design; predict performance in support of tradeoff studies; evaluate system design and support preliminary design reviews during design development; predict system performance and supplement live tests during testing; examine the military value of the system; determine the impact of design changes; hone requirements; and develop life cycle support requirements and assessments.

However, a key limitation through models and simulations is that the results are only as accurate and certain as the quality of the underlying relationships and input data. Blindly believing and using the output from models and simulations should never be done.

Downloaded from http://www.everyspec.com

3.5 RISK MANAGEMENT ACTIVITIES DURING ACQUISITION PHASES

Risk management activities should be applied continuously throughout all acquisition process phases. However, because of the difference in available information, the level of application and detail will vary for each phase. In Phase 0, management focuses on assessing the risks in the alternative concepts available to satisfy users needs and on planning a strategy to address those risks. For each of the subsequent phases, all four risk management activities may be applied with increasing focus on risk handling and monitoring.

The PM identifies objectives, alternatives, and constraints at the beginning of each phase of a program and then evaluates alternatives, identifies sources of project risk, and selects a strategy for resolving the risks. The PMO updates the acquisition strategy, risk assessments, and other aspects of program planning, based on analyses, for the phase of the acquisition.

Developers should become involved in the risk management process at the beginning, when users define performance requirements, and continue during the acquisition process until the system is delivered. The early identification and assessment of critical risks allow PMs to formulate handling approaches and to streamline the program definition and the RFP around critical product and process risks.

The following paragraphs address risk management in the different phases in more detail.

3.5.1 Phase 0

DoD 5000.2-R describes Phase 0 as normally consisting of studies that define and evaluate the feasibility of alternative concepts and provide the basis for the assessment of these alternatives in terms of their advantages, disadvantages, and risk levels at the Milestone (MS) I decision point. In addition to providing input to the Analysis of Alternatives, the PM develops a proposed acquisition program baseline (APB) and exit criteria for Phase I.

The APB documents the most important performance, cost, and schedule objectives and thresholds for the selected concepts. The parameters selected are such that a reevaluation of alternative concepts is appropriate if thresholds are not met. Exit criteria are events or accomplishments that allow managers to track progress in critical technical, cost, or schedule risk areas. They must be demonstrated to show that a program is on track.

In defining alternative concepts, PMs should pay particular attention to the threat and the user's requirements, which are normally stated in broad terms at this time. Risks can be introduced if the requirements are not stable, or if they are overly restrictive and contain specific technical solutions. Requirements can also be significant cost and schedule risk drivers if they require a level of performance that is difficult to achieve within the program budget and time constraints. Such drivers need to be identified as early in the program as possible.

The acquisition strategy should address the known risks for each alternative concept, and the plans to handle them, including specific events intended to control the risks. Similarly, the T&E strategy should reflect how T&E, with the use of M&S, will be used to assess risk levels and identify new or suspected risk areas.

A risk management strategy, derived in concert with the acquisition strategy, should be

Downloaded from http://www.everyspec.com

developed during this phase and revised and updated continually throughout the program. This strategy should include risk management planning that clearly defines roles, responsibilities, authority, and documentation for program reviews, risk assessments, and risk monitoring.

3.5.2 Subsequent Phases

During subsequent phases, concepts, technological approaches, and/or design approaches (selected at the previous milestone decisions) are pursued to define the program and program risks. Selected alternative concepts continue to be analyzed, and the acquisition strategy, and the various strategies and plans derived from it, continue to be refined.

Risk management efforts in these phases focus on: understanding critical technology, manufacturing, and support risks, along with cost, schedule, and performance risks; and demonstrating that they are being controlled before moving to the next milestone. Note that the accuracy of cost, schedule, performance risk assessments should improve with each succeeding program phase (e.g., more info, better design documentation, etc.). Thus, particular attention should be placed on handling and monitoring activities. Planning and assessment should continue as new information becomes available and new risk events are identified.

During these phases, the risk management program should be carried out in an integrated Government-contractor framework to the extent possible, that allows the Government to manage program risks, with the contractor responsible to the PM for product and process risks and for maintaining design accountability. Both the Government and contractors need to understand the risks clearly, and jointly plan management efforts. In any event, risk management needs to be tailored to each program and contract type.

3.6 RISK MANAGEMENT AND MILESTONE DECISIONS

Before a milestone review, the PM should update risk assessments, explicitly addressing the risks in the critical areas, such as threat, requirements, technology, etc., and identify areas of moderate or high risk.

Each critical technical assessment should be supported by subsystems' risk assessments, which should be supported by design reviews, test results, and specific analyses.

The PM should present planned risk mitigation actions for moderate- or high-risk areas at the milestone review to determine their adequacy and to ensure the efficient allocation of resources.

3.7 RISK MANAGEMENT AND THE ACQUISITION STRATEGY

In addition to providing the framework for program planning and execution, the acquisition strategy serves several purposes that are important to risk management:

- Provides a master schedule for research, development, test, production, deployment, and critical events in the acquisition cycle.

- Gives a master checklist of the important issues and alternatives that must be addressed.

- Assists in prioritizing and integrating functional requirements, evaluating alternatives, and providing a coordinated approach to integrate diverse functional

Downloaded from http://www.everyspec.com

issues, leading to the accomplishment of program objectives.

- Documents the assumptions and guidelines that led to the initiation and direction of the program.

- Provides the basis for the development and execution of the various subordinate functional strategies and plans.

The strategy structure should ensure a sound program through the management of cost, schedule, and performance risk. A good acquisition strategy acknowledges and identifies program risks and forms the basis for implementing a forward-looking, rather than reactive, effective risk management effort.

Acquisition strategy should describe how risk is to be handled and identify which risks are to be shared with the contractor and which are to be retained by Government. The key concept here is that the Government shares the risk with the contractor, but does not transfer risk to the contractor. The PMO always has a responsibility to the system user to develop a capable system and can never absolve itself of that responsibility. Therefore, all program risks, whether primarily managed by the PMO or by the contractor, must be assessed and managed by the PMO.

Once the program office has determined how much of each risk is to be shared with the contractor, it should assess the total risk assumed by the developing contractor (including subcontractors). The Government should not require contractors to accept financial risks that are inconsistent with their ability to handle them. Financial risks are driven, in large measure, by the underlying technical and programmatic risks inherent in a program. The Government contracting officer should, therefore, select the proper type of contract based on an appropriate risk assessment, to ensure a clear relationship between the selected contract type and program risk. An example would be the use of cost-reimbursable-type contracts for development projects.

3.8 RISK MANAGEMENT AND CAIV

The intention of CAIV is to establish balance between cost, schedule, performance, and risk early in the acquisition process and to manage to a cost objective. CAIV requires that PMs establish aggressive cost objectives, defined to some degree by the maximum level of acceptable risk. Risks in achieving both performance and aggressive cost goals must be clearly recognized and actively managed through:

(1) continuing iteration of cost / performance / schedule / risk tradeoffs,

(2) identifying key performance and manufacturing process uncertainties, and

(3) demonstrating solutions before production.

Whereas DoD has traditionally managed performance risk, equal emphasis must be placed on managing cost and schedule risks. An underlying premise of CAIV is that if costs are too great, and there are ways to reduce them, then the user and developer may reduce performance requirements to meet cost objections. Cost control and effective risk management involve planning and scheduling events and demonstrations to verify solutions to cost, schedule, performance risk issues.

User participation in the trade-off analysis is essential to attain a favorable balance between cost, schedule, performance, and

Downloaded from http://www.everyspec.com

risk. The PM and user representatives should identify risk and cost driving requirements during the generation of the ORD to know where tradeoffs may be possible. Risk assessments are critical to the CAIV process since they provide users and developers with essential data to assist in the cost, schedule, performance, risk trade decisions.

A cost for risk management is directly related to the level of risk and affects a program in two ways. First, costs are associated with specific handling activities, for example, a parallel development. Second, funds are needed to cover the known risks of the selected system approach (i.e., funds to cover cost uncertainty). PMs must include the anticipated expense of managing risk in their estimates of program costs. Decision makers must weigh these costs against the level of risk in reaching program funding decisions. CAIV requires that program funds support the level of accepted program risk and that risk management costs are included in setting cost objectives.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

4

RISK MANAGEMENT AND PROGRAM MANAGEMENT

4.1 INTRODUCTION

Risk management as a program management responsibility can be a comprehensive and responsive management tool if it is properly organized and monitored at the PM level. A formalized risk management program should be well-planned and forward-looking by identifying, analyzing, and resolving potential problem areas before they occur, and by incorporating monitoring techniques that accurately portray the status of risks and the efforts to mitigate them. Introduction of risk management early in a program emphasizes its importance and encourages contractors and members of the Government team to consider risk in the daily management functions.

This Chapter addresses the relationship between risk management and program management and suggests methods of introducing risk management in a program, organizing for risk, and training.

4.2 OVERVIEW

A PMO should organize for risk management, using existing IPTs. The PM may also want to use contractors to support management efforts or have experts not involved with the program perform independent assessments.

To use risk management as a program management tool, the information resulting from each of the risk processes should be documented in a usable form and available to members of the Government/industry program team. This information will provide the basis for reporting risk and overall program information, both internally and externally. Managing collection and dissemination of risk information can be enhanced through the use of a Management Information System (MIS).

4.3 PROGRAM MANAGER AND RISK MANAGEMENT

All PMs are responsible for establishing and executing a risk management program that satisfies the policies contained in DoDD 5000.1. A PM must balance program-unique requirements or circumstances (e.g., size of the PMO staff) against the demands of proven risk management principles and practices. This section addresses these principles and practices and provides a basis for establishing a PMO's risk management organization and related procedures. The following guidelines define an approach to risk management.

4.3.1 Risk Management is a Program Management Tool

Risk management should be integral to a program's overall management. PMs must take an active role in the process to ensure that their approach leads to a balanced use of program resources, reflects their overall management philosophy, and includes

Downloaded from http://www.everyspec.com

Government and contractors. Past DoD practices have generally treated risk management solely as a system engineering function, cost-estimating technique or possibly as an independent function distinct from other program functions. Today, risk management is recognized as a vital integrated program management tool that cuts across the entire acquisition program, addressing and interrelating cost, schedule, and performance risks. The goal is to make everyone involved in a program aware that risk should be a consideration in the design, development, and fielding of a system. It should not be treated as someone else's responsibility. Specific functional areas—such as system engineering—could be charged with implementing risk management, as long as they take the program management view towards it.

4.3.2 Risk Management is a Formal Process

Formal risk management refers to a structured process whereby risks are *systematically* identified, analyzed, handled, and monitored. (A recommended structure is described in Section 2 of this *Guide*.) A structured risk management process, which is applied early, continuously, and rigorously, provides a disciplined environment for decision making and for the efficient use of program resources. Through a disciplined process PMs can uncover obscure and lower-level risks that collectively could pose a major risk.

The need for a formal risk management process arises from the nature of risk and the complexity of acquisition programs. The numerous risks in an acquisition program are often interrelated and obscure and change in the course of the development process. A formal approach is the only effective method to sort through numerous risk events, to identify the risks and their interrelationships, to pinpoint the truly critical ones, and to identify cost-effective ways to reduce those risks, consistent with overall program objectives.

A structured process can reduce the complexity of an acquisition program by defining an approach to assess, handle, monitor, and communicate program risk. The systematic identification, analysis, and mitigation of risks also offers a reliable way to ensure objectivity, that is, minimize unwarranted optimism, prejudice, ignorance, or self-interest. Further, structure reduces the impact of personnel turnover and provides a basis for training and consistency among all the functional areas of a program. A structured risk program may also promote teamwork and understanding and improves the quality of the risk products.

4.3.3 Risk Management is Forward-Looking

Effective risk management is based on the premise that PMs must identify potential problems, referred to as risk events, long before they can occur and develop strategies that increase the likelihood of a favorable outcome to these problems. Application of this philosophy occurs primarily by using analytical techniques that give forward-looking assessments.

Typically, the early identification of potential problems is concerned with two types of events. The first are relevant to the current or imminent acquisition phase of a program (intermediate-term), such as satisfying a technical exit criteria in time for the next milestone review. The second are concerned with the future phase(s) of a program (long-term) such as potential risk events related to transitioning a system from development to production.

Downloaded from http://www.everyspec.com

By analyzing critical events, certain risks can be determined. To do this, one should consider the range of potential outcomes and the factors that determine those outcomes. Through risk handling, a PM then develops approaches that minimize risk factors. Paragraph 5.6 of this *Guide* describes some handling approaches.

Choosing the proper risk-handling options requires that a balance be struck between the resources required to implement those options and their payoffs (both intermediate and long-term) and the resources realistically available.

4.3.4 Risk Management is Integral to Integrated Product and Process Development (IPPD)

One of the tenets of IPPD is multidisciplinary teamwork through IPTs, which are an integral part of the defense acquisition oversight and review process. The Integrating IPT (IIPT) is a valuable resource to assist in developing a risk management plan and should be used accordingly. The PM should ensure that the requirements of the overarching IPT (OIPT) are reflected in the plan.

Working with the OIPT, the PM can establish the type and frequency of risk management information that an OIPT requires, and refine management organization and procedures. This should be done during the initial OIPT meetings. OIPTs will most likely require information concerning:

- Known risks and their characteristics, e.g., probability of occurrence and consequences,
- Planned risk-handling actions, funded and unfunded,
- Achievements in controlling risks at acceptable levels.

IIPTs and OIPTs may also require details on the PM's risk management program, access to the risk management plan, and the results of specific risk assessments. In addition, PMs may want to present selected information to IIPTs and OIPTs to help substantiate a position or recommendation, e.g., help support a budget request.

4.4 RISK MANAGEMENT ORGANIZATION IN THE PMO

The PM, after determining a preferred management approach, must organize the program office and establish outside relationships in order to manage risk. No particular organizational structure is superior; however, experience provides some insights into the development of effective risk management organizations. PMs should consider the following discussion in the context of their unique requirements and circumstances and apply those that are suitable to their specific needs.

4.4.1 Risk Management Organizational Structure

A major choice for each PM is whether to have a centralized or decentralized risk management organization. The PM may choose a centralized organizational structure until team members become familiar with both the program and the risk management process. In a centralized approach, the PM establishes a team that is responsible for all aspects of risk management. The team would write a plan, conduct assessments, evaluate risk-handling options, and monitor progress. Although this approach may be necessary early in a program, it tends to minimize the concept that risk management is a responsibility shared by all members of the acquisition team, whether Government or contractor.

Downloaded from http://www.everyspec.com

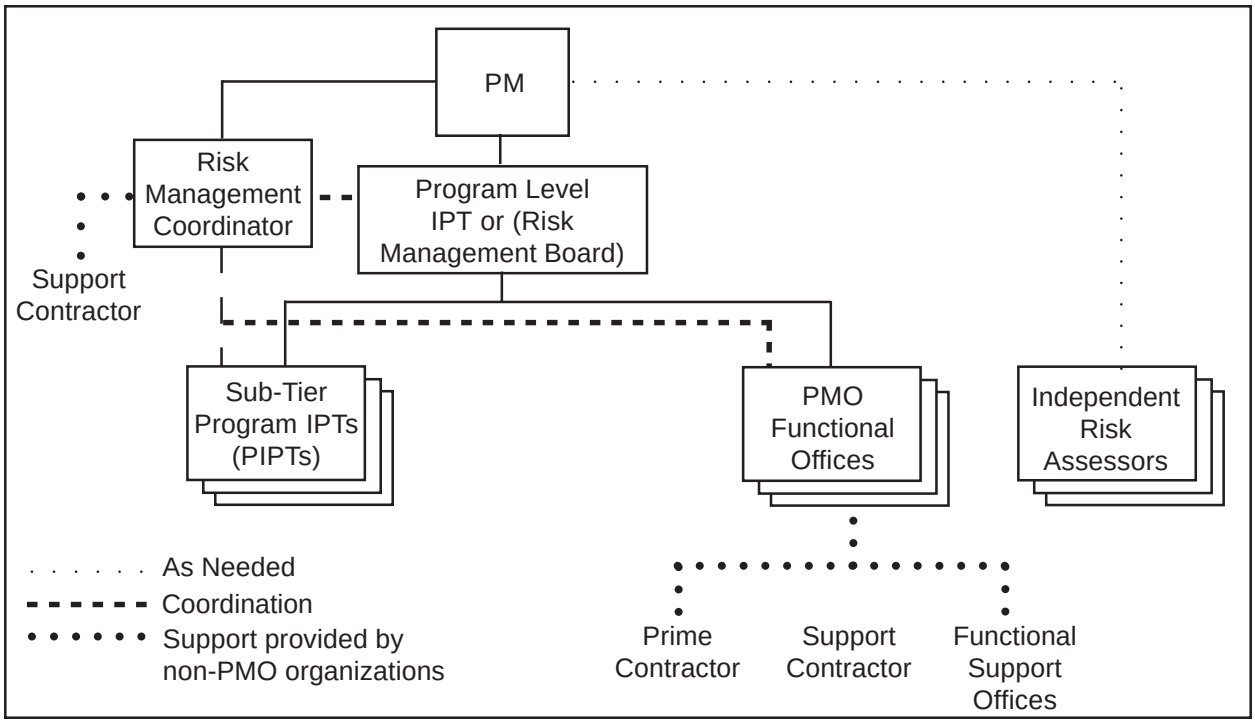


Figure 4-1. Decentralized Risk Management Organization

The PM may also choose to decentralize. The degree of decentralization depends on the assignment of responsibilities. Some level of centralization is almost always essential for prioritizing risk across the program. A program level integrating IPT (See Figure 4-1) or a Risk Management Board may be appropriate for this integrating function.

The decentralized risk management organization is the most widely used approach, which is compatible with the DoD's IPPD policy and generally results in an efficient use of personnel resources. In this approach, risk management is delegated to Program IPTs.

The following guidelines apply to all risk management organizations:

- The PM is ultimately responsible for planning, allocating resources, and executing risk management. This requires the PM to oversee and participate in the risk management process.

- The PM must make optimal use of available resources, i.e., personnel, organizations, and funds. Personnel and organizational resources include the PMO, functional support offices of the host command, the prime contractor, independent risk assessors, and support contractors.

- Risk management is a team function. This stems from the pervasive nature of risk and the impact that risk-handling plans may have on other program plans and actions. In the aggregate, risk planting, risk assessment, risk handling, and risk monitoring affect all program activities and organizations. Any attempt to implement an aggressive forward-looking risk management program without the involvement of all PMO subordinate organizations could result in confusion, misdirection, and wasted resources. The only way to avoid this is through teamwork among the PMO organizations and the prime contractor. The management organizational structure can promote teamwork by requiring strong

Downloaded from http://www.everyspec.com

connectivity between that structure, the various PMO organizations, and the prime contractor. The teams may use independent assessments to assist them, when required.

Figure 4-1 portrays a decentralized risk management organization. This example includes the entire PMO and selected non-PMO organizations, e.g., the prime contractor, who are members of the IPTs. The figure shows that risk management is an integral part of program management and not an additional or separate function to perform. Hence, separate personnel are not designated to manage risk, but rather all individuals are required to consider risk management as a routine part of their jobs. In the figure, the risk coordinator reports to the PM, but works in coordination with the Program IPT, functional offices, and the Program Level IPT. As shown, this organizational structure is suited to ACAT I programs, but PMs can tailor it to satisfy their specific requirements. The details are dependant upon the contract, type, statement of work, and other variable.

The organizational structure shows that the PM is ultimately responsible for risk management. There is a coordinator to assist with this responsibility and act as an "operations" officer. This may be a full-time position or an additional duty as the PM deems appropriate. The coordinator should have specific training and experience in risk management to increase the chance of successful implementation and to avoid common problems. A support contractor may assist the coordinator by performing administrative tasks associated with that office.

The Program Level IPT, composed of individuals from the PMO and prime contractor, ensures that the PM's risk management program is implemented and program results are synthesized into a form suitable for decision making by the PM and OIPT.

The inclusion of both Sub-Tier IPTs and PMO functional offices simply reflects that not all program management functions will be assigned to Sub-Tier IPTs for execution.

Independent risk assessors are typically hired when the PM has specific cost, schedule, performance concerns with a hardware or software product or engineering process and wants an independent assessment from an expert in a particular field. The duration of their services is normally short, and tailored to each program.

4.4.2 Risk Management Responsibilities

This section identifies the primary responsibilities that could be associated with a decentralized risk management organization. In assigning the responsibilities to the various organizational elements, the PM should strike a balance between a concentration of responsibilities at the higher levels and pushing them too far down the organizational structure.

The development of these responsibilities, in part, is based on the premise that risk management activities must be specific—and assigned to individuals, not groups. The responsibilities listed below are assigned to the leader of each organizational element, recognizing that the composition of each element will be program unique, i.e., number of assigned PMO personnel, prime contractor personnel, etc. The task of further assigning these responsibilities, along with tailoring them to satisfy the needs and requirements of each program, remains for PMs and their staffs to accomplish.

Downloaded from http://www.everyspec.com

Table 4-1 provides a description of the responsibilities associated with the decentralized risk management structure, sorted by notional organizational elements that may make up the risk management structure.

4.5 CONTRACTOR RISK MANAGEMENT

Experience has shown that managing a program's risks requires a close partnership between the PMO and the prime contractor(s). PMs must determine the type of support they need from their prime contractor, communicate these needs through the Request for Proposal (RFP) for each acquisition phase, and then provide for them in the contract. Preparation of the RFP and source selection are discussed in subsequent sections.

4.5.1 Contractor View of Risk

Contractors treat risk differently from the Government because each views risk from a different perspective. The PM, in executing his risk management program, needs to understand the contractor viewpoint.

Contractors typically divide risks into two basic types: business risks and program risks. Business risk, in the broadest sense, involves the inherent chance of making a profit or incurring a loss on any given contract. Program risk involves, among other things, technical, requirement, and design uncertainties. A contractor's efforts to minimize business risks may conflict with a Government PM's efforts to lower program risk.

While the government and contractors may have different views on specific cost, schedule, and performance risk levels / ratings, they generally have (or should have) similar views of the risk management process. One exception may be the requirements placed by corporate management—that could conflict with the Government view of program risk. The similarity, however, does not necessarily lead to the contractor having a competent internal risk management program. As a Project Management Institute (PMI) handbook points out, "On most (contractor) projects, responsibility for *Project Risk* is so pervasive that it is rarely given sufficient central attention." As a minimum, it is important that the PMO writes the RFP asking the contractor to describe its risk management process, including its approach to managing any specific areas.

4.5.2 Government/Contractor Relationship

The prime contractor's support and assistance is required even though the ultimate responsibility for risk management rests with the Government PM. Often, the contractor is better equipped to understand the program technical risks than the Government program office is. Both the Government and contractor need to share information, understand the risks, and develop and execute management efforts. The Government must involve the contractor early in program development, so that effective risk assessment and reduction can occur.

Therefore, risk management must be a key part of the contractor's management scheme. Although the Government does not dictate how the contractor should manage risk, some characteristics of a good Government / contractor relationship include:

- Clear definition of risks and their assignment.

- Flexibility for assignment of risks and risk management responsibilities among the teams.

Downloaded from http://www.everyspec.com

Personnel	Job Responsibility
Program Manager	Plan, organize, direct, and control risk management. Comply with DoDD 5000.1, DoD 5000.2-R, DoDD.4, and DoD 5000.4-M risk managements. Ensure that funds are available to support approved risk-handling plans. Inform and advise MDA, Cost Analysis Improvement Group (CAIG) and OIPT on program risk and its mitigation.
Risk Management Coordinator	Develop and maintain risk management plans. Provide risk management training. Define the risk reporting scales to be used by the program. Develop and maintain a risk management information system. Prepare risk management reports. Monitor compliance with DoDD risk management requirements. Ensure that risk management functions and tasks performed by the Sub-Tier IPTs and the PMO functional offices are fully integrated and in compliance with assigned tasks. Advise the PM and Program Level IPT on the use of risk management sources, i.e., host command functional support offices, etc. Evaluate risk assessments, risk-handling plans, and risk monitoring results as directed and recommend appropriate actions. Advise the PM on the use of independent risk assessors.
Program Level IPT (some PMOs use a Risk Management Board (RMB) for this responsibility)	Ensure that the risk management program is implemented, risk reduction is accomplished in conformance with the PM's strategy, and the risk management efforts of the Sub-Tier IPTs are integrated. Report risk events to the risk management coordinator. Evaluate whether Sub-Tier IPTs and PMO functional offices have identified critical risks and proposed risk-handling plans. Ensure that cost, schedule, and performance risks are compatible. Ensure that cost, schedule, and performance risks are combined in a manner consistent with the plan.
PMO Sub-Tier IPTs & Functional Offices (Process) and System Elements (Products)	Assess risks, recommending appropriate risk-handling strategies for each identified moderate and high risk, developing and implementing risk-handling plans, monitoring the results of risk-handling actions, and documenting all risk management analyses and findings within the team's product area. Coordinate all risk management findings and decisions with other Sub-Tier IPTs, PMO functional offices, the Program Level IPT, and the risk-management coordination office. Identify funding requirements to implement risk-handling plans. Identify the need for risk management training. Report risk events to the Program Level IPT and risk coordinator.
Independent Risk Assessors	Perform independent Risk assessment on critical risk areas or contractor engineering processes that the PM has specified. Report the results of those assessments to the PM. Work with the risk management coordinator.

Table 4-1. Notional Description of Risk Management Responsibilities

Downloaded from http://www.everyspec.com

- Strong emphasis on best management and technical practices which, if followed, avoid unnecessary risks.

Regarding RFP development, discussed later in this section, information is provided on how these characteristics should be addressed.

The Government/contractor partnership can be forged in at least two ways. First, the PMO should include the prime contractor(s) in the top-level risk planning and assessment activities. This includes understanding and factoring in such issues as user requirements, affordability constraints, and schedule limitations. Second, the PMO should include in advance specific risk assessment and handling tasks as key contractual efforts during the concept exploration and program definition and risk reduction phases.

Forming a joint Government/contractor evaluation team is a good way of fostering an effective partnership. This is especially true in a program's early stages when uncertainty is high and both parties must frequently assess risks. These assessments, properly handled, involve multidisciplinary efforts requiring subject-matter experts from both the prime contractor and Government. This joint team should evaluate the proposed program in detail and explore the inherent program risks, the proposed handling strategies, the detailed development schedule, and the contractor's developmental resources (people, facilities, processes, tools, etc.).

A management approach using multiple teams is the best approach to use, e.g., Sub-Tier IPTs. Joint team(s) should be established at the beginning of each development phase to assess the risks to be overcome in that phase and to determine the handling technique(s) to be used. Requirements for contractor participation on the team(s) should be identified in the RFP and subsequent contract.

4.6 RISK MANAGEMENT AND THE CONTRACTUAL PROCESS

4.6.1 Risk Management: Pre-Contract Award

The contractor's developmental and manufacturing processes and tools, the availability and skill of personnel, and the previous experience of the Government and contractor team all influence their ability to handle the proposed system development and production. Therefore, an effective risk management process includes an evaluation of the capabilities of the potential contractors.

4.6.2 Early Industry Involvement: Industrial Capabilities Review

An Industrial Capabilities Review is a powerful tool available to PMs for determining *general* industrial capabilities. To avoid potential problems in the subsequent competitive process and to ensure that a "level playing field" is maintained, an announcement in the *Commerce Business Daily* should be made to inform all potential offerors that the Government plans to conduct an Industrial Capabilities Review and to request responses from all interested parties. Below is a general approach that PMOs may find readily adaptable to any type of capability review. The basic steps in the process are to:

- Obtain the Source Selection Authority's approval to conduct the review.

- Establish the criteria for the capability.

- Identify the potential contractors who will participate in the review.

Downloaded from http://www.everyspec.com

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

- Select the review team, ensuring that it has the necessary mix of talent.

- Train the team on the purpose of the review and review criteria.

- Conduct the review and evaluate the results.

- Provide feedback to each contractor on the results of their review and assessment.

- Provide the results to the PM.

This review is an appraisal of general industrial capabilities and supports identifying potential program risks and best practices rather than evaluating specific contractors.

Regardless of the approach, the PMO should determine what specific information is needed. DoD 4245.7-M is a good guide to help tailor a set of questions for the contractors. The questions generally focus on two areas consistent with protection of contractor proprietary information.

- What is the state-of-the-art of the technology proposed for use in the system?

- What are the general developmental/manufacturing capabilities of the potential contractors (including experience, tools, processes, etc.) as compared to industry best practices?

Table 4-2 shows some of the specific areas or sources for risk identification. It includes a number of areas (threat, requirements, design, etc.) that have been shown through experience to contain risk events that tend to be more critical than others, and which ones should receive the most management attention. Risk events are determined by examining WBS element product and processes in terms of risk areas. Process areas are specifically addressed in DoD 4245.7M. They are general in that areas of risk could be present in any program from either source (WBS or process). They are intended as a list of "top-level" risk sources that will focus attention on a specific area. The PMO and contractor(s) will have to examine lower levels to understand the actual risks that are present in their program and to develop an effective management plan. The risks shown are not intended to serve as a simple checklist that one should apply directly, then consider the program risk-free if none of the listed risks are present.

An examination of the program in these areas can help to develop the final program acquisition strategy and the risk-sharing structure between the Government and industry. The PMO can also use the results to adjust the RFP for the next phase of the program.

4.6.3 Developing the Request for Proposal

The RFP should communicate to all offerors the concept that risk management is an essential part of the Government's acquisition strategy.

Before the draft RFP is developed using the results of the Industrial Capabilities Review, the PMO should conduct a risk assessment to ensure that the program described in the RFP is executable within the technical, schedule, and budget constraints. Based on this assessment, a program plan, an integrated master schedule, and life-cycle cost (LCC) estimate may be prepared. The technical, schedule, and cost issues should be discussed in the pre-proposal conference(s) before the draft

Downloaded from http://www.everyspec.com

Risk Area	Significant Risks
Threat	Uncertainty in threat accuracy. Sensitivity of design and technology to threat. Vulnerability of system to threat and threat countermeasures. Vulnerability of program to intelligence penetration.
Requirements	Operational requirements not properly established or vaguely stated. Requirements are not stable. Required operating environment not described. Requirements do not address logistics and suitability. Requirements are too constrictive—identify specific solutions that force high cost.
Design	Design implications not sufficiently considered in concept exploration. System will not satisfy user requirements. Mismatch of user manpower or skill profiles with system design solution or human-machine interface problems. Increased skills or more training requirements identified late in the acquisition process. Design not cost effective. Design relies on immature technologies or “exotic” materials to achieve performance objectives. Software design, coding, and testing.
Test and Evaluation	Test planning not initiated early in program (Phase 0). Testing does not address the ultimate operating environment. Test procedures do not address all major performance and suitability specifications. Test facilities not available to accomplish specific tests, especially system-level tests. Insufficient time to test thoroughly.
Simulation	Same risks as contained in the Significant Risks for Test and Evaluation. M&S are not verified, validated, or accredited for the intended purpose. Program lacks proper tools and modeling and simulation capability to assess alternatives.
Technology	Program depends on unproved technology for success—there are no alternatives. Program success depends on achieving advances in state-of-the-art technology. Potential advances in technology will result in less than optimal cost-effective system or make system components obsolete. Technology has not been demonstrated in required operating environment. Technology relies on complex hardware, software, or integration design.
Logistics	Inadequate supportability late in development or after fielding, resulting in need for engineering changes, increased costs, and/or schedule delays. Life-cycle costs not accurate because of poor logistics supportability analyses. Logistics analyses results not included in cost-performance tradeoffs. Design trade studies do not include supportability considerations.

Table 4-2. Significant Risks by Critical Risk Areas

Downloaded from http://www.everyspec.com

Risk Area	Significant Risks
Production/ Facilities	Production implications not considered during concept exploration. Production not sufficiently considered during design. Inadequate planning for long lead items and vendor support. Production processes not proven. Prime contractors do not have adequate plans for managing subcontractors. Sufficient facilities not readily available for cost-effective production. Contract offers no incentive to modernize facilities or reduce cost.
Concurrency	Immature or unproven technologies will not be adequately developed before production.
	Production funding will be available too early—before development effort has sufficiently matured. Concurrency established without clear understanding of risks.
Capability of Developer	Developer has limited experience in specific type of development. Contractor has poor track record relative to costs and schedule. Contractor experiences loss of key personnel. Prime contractor relies excessively on subcontractors for major development efforts. Contractor will require significant capitalization to meet program requirements.
Cost/Funding	Realistic cost objectives not established early. Marginal performance capabilities incorporated at excessive costs-satisfactory cost-performance tradeoffs not done. Excessive life-cycle costs due to inadequate treatment of support requirements. Significant reliance on software. Funding profile does not match acquisition strategy. Funding profile not stable from budget cycle to budget cycle.
Schedule	Schedule not considered in trade-off studies. Schedule does not reflect realistic acquisition planning. APB schedule objectives not realistic and attainable. Resources not available to meet schedule.
Management	Acquisition strategy does not give adequate consideration to various essential elements, e.g., mission need, test and evaluation, technology, etc. Subordinate strategies and plans are not developed in a timely manner or based on the acquisition strategy. Proper mix (experience, skills, stability) of people not assigned to PMO or to contractor team. Effective risk assessments not performed or results not understood and acted upon.

Table 4-2. Significant Risks by Critical Risk Areas (Continued)

Downloaded from http://www.everyspec.com

RFP is released. In this way, critical risks inherent in the program can be identified and addressed in the RFP. In addition, this helps to establish key risk-management contractual conditions. The RFP should encourage offerors to extend the contract WBS (CWBS) to reflect how they will identify all elements at any level that are expected to be high cost or high risk. The RFP should also encourage offerors to cite any elements of the CWBS provided in the draft RFP that are not consistent with their planned approach.

In the solicitation, PMs may ask offerors to include a risk analysis and a description of their management plans, and also to develop a supporting program plan and an integrated master schedule in their proposals. These proposals will support the Government's source selection evaluation and the formulation of a most probable cost estimate for each proposal. In addition, the RFP may identify the requirement for periodic risk assessment reports that would serve as inputs to the PM's assessment and monitoring processes thereby ensuring that risks are continuously assessed.

4.6.4 The Offeror's Proposal

The offerors should develop the proposed program plans and documentation at a level that is adequate to identify risks, develop associated management activities that they will use throughout the program, and integrate resources, technical performance measures, and schedule in the proposed program plans. Program plans should extend the CWBS to reflect the offeror's approach and include the supporting activities, critical tasks, and processes in the CWBS dictionary. The associated schedules for each should be incorporated into an integrated master schedule. Plans should also have an estimate of the funds required to execute the program and include a breakout of resource requirements for high-risk areas.

The information required and the level of detail will depend on the acquisition phase, the category, and criticality of the program, as well as on the contract type and value. However, the detail submitted with the proposal must be at a sufficiently low level to allow identification of possible conflicts in the planned acquisition approach and to support the Government's proposal evaluation. Generally, the CWBS should be defined below level 3, by the contractor, only to the extent necessary to capture those lower level elements that are high cost, high risk, or of high management interest.

4.6.5 Basis for Selection

DoD acquisition management must focus on balancing cost, schedule, performance, and risk by selecting the contractor team that provides the best value to the user within acceptable risk limits. Therefore, the RFP/Source Selection process must evaluate each offeror's capability for meeting product and process technical, cost and schedule requirements while addressing and controlling the risks inherent in a program.

The evaluation team should discriminate among offerors based upon the following:

- Risks determined by comparison with the best practices baseline.
- Ability to perform with a focus on the critical risk elements inherent in the program.
- Adherence to requirements associated with any mandatory legal items.
- Past performance on efforts similar to the proposed program being evaluated.

Downloaded from http://www.everyspec.com

The process of choosing among offerors may be enhanced if the evaluation team includes risk management as a "source selection discriminator." Risk management then becomes an important factor in the Source Selection Authority determination of who provides the most executable program.

4.6.6 Source Selection

The purpose of a source selection is to select the contractor whose cost, schedule and performance can best be expected to meet the Government's requirements at an affordable price. To perform this evaluation, the Government must assess both *proposal risk* and *performance risk* for each proposal. These risk assessments must be done entirely within the boundaries of the source selection process. Previous assessments of any of the offerors may not be applicable or allowable.

4.6.6.1 Proposal Risk. This refers to the risk associated with the *offeror's proposed approach* to meet the Government cost, schedule, and performance requirements. The evaluation of proposal risk includes an assessment of proposed time and resources and recommended adjustments. This assessment should be performed according to the definitions and evaluation standards developed for the source selection. Proposal risk is, in essence, a moderate expansion of past evaluation processes. Historically, evaluators selected contractors who demonstrated that they understood the requirements and offered the best value approach to meeting the Government's needs. The expansion on this concept is the specific consideration of risk.

Technical and schedule assessments are primary inputs to the most probable cost estimate for each proposal. It is important to estimate the additional resources needed to control any risks that have moderate or high risk ratings. Offerors may define them in terms of additional time, personnel loading, hardware, or special actions such as additional tests. However, whatever the type of the required resources, it is essential that cost estimates be integrated and consistent with the technical and schedule evaluations.

4.6.6.2 Performance Risk. A performance risk assessment is an evaluation of the contractor's past and present performance record to establish a level of confidence in the contractor's ability to perform the proposed effort.

A range of methods are available to the PM to evaluate performance risk. The Performance Risk Assessment Group (PRAG) is a group of experienced Government personnel that are appointed by the source selection advisory council Chairperson to permit performance risk to be used, if appropriate. Performance risk may be separately assessed for each evaluation factor or as a whole with the assessment provided directly to the source selection advisory council / authority for final decision or indirectly through the Source Selection Evaluation Board. The assessment relies heavily (although not exclusively) on the contractor performance evaluations and surveys submitted by the PMO and Defense Contract Management Command (DCMC).

4.7 RISK MANAGEMENT: POST-CONTRACT AWARD

Post-contract award risk management builds on the work done during the pre-contract award phase. With the award of the contract, the relationship between the Government and the contractor changes as teams are formed to address program risk. These teams should validate pre-contract award management plans by reviewing

Downloaded from http://www.everyspec.com

assessments, handling plans, and monitoring intentions. The extent of assessments increases as the contractor develops and refines his design, test and evaluation, and manufacturing plans. The Government PMO should work with the contractor to refine handling plans.

The process begins with an Integrated Baseline Review (IBR) after contract award to ensure that reliable plans and performance measurement baselines capture the entire scope of work, are consistent with contract schedule requirements, and have adequate resources assigned to complete program tasks. The IBR could be conducted to incorporate other steps identified below. These steps suggest an approach that the PMO might take to initiate the program's risk management plans and activities after contract award. They are intended to be a starting point, and the PMO should tailor the plan to reflect each program's unique needs.

- Conduct initial meeting with the contractor to describe the program's objectives and approach to managing risks. The PM may also present the risk management plan.

- Train members of PMO and contractor's organization on risk management basics, incorporating the program's management plan and procedures into the training.

- Review the pre-contract award risk plan with the PMO and contractor, revise it as necessary, and share results with the contractor.

- Conduct in-depth review of the pre-contract award risk assessments and expand the review to include any new information obtained since the award of the contract.

- Review and revise risk-handling plans to reflect the reassessment of risks.

- Review the program's documentation requirements with the contractor. Ensure that the PMO and contractor understand the purpose, format, and contents of various risk reports.

- Initially, it may be necessary to establish a formalized PMO-contractor risk management organization for the program, consistent with the terms of the contract.

- Working with the contractor, refine the risk-monitoring plans and procedures.

- Establish the program reporting requirements with the contractor. Describe the risk management information system that the program has established, including procedures for providing information for data entry, and identify reports for the PMO and contractor.

- In conjunction with the contractor, identify other risk-management activities that need to be performed.

- Manage the program risk in accordance with the risk management plan and contract.

- Working with the contractor, refine the risk-monitoring plans and procedures and develop appropriate measures and metrics to track moderate- and high-risk items.

4.8 RISK MANAGEMENT REPORTING AND INFORMATION SYSTEM

The PMO should have a practical method for risk-management reporting, and an information system that supports a risk management program. The reporting needs of the PM establish the type, format, and fre-

Downloaded from http://www.everyspec.com

quency of information sharing. The IPT concept suggests that the entire acquisition program team needs access to the risk management information, and the prime contractor(s) should have access to information, consistent with acquisition regulations. The reporting and information system chosen may be Government- or contractor-owned. See Chapter 5 for an example of an MIS.

4.9 RISK MANAGEMENT TRAINING

A successful management program depends, to a large extent, on the level of risk management training the PMO members and the functional area experts receive. The training will prepare them for critical tasks, such as risk assessments. DoD schools offer some risk-management training; however, PMs will need to organize and conduct principal training for the program office. A three-part framework for training covers program-specific risk management issues, general structure and process, and techniques.

(1) The program-specific training should ensure that everyone has a common vision. It should cover the acquisition strategy, the companion risk management plan, the PM's risk-management structure and associated responsibilities, and the MIS.

(2) The following topics provide a starting point for general training syllabus development. The final syllabus should be tailored to meet the program's specific needs. Table 4-3 provides a list of references that will be useful in developing the syllabus and lesson plans.

- Concept of Risk
- Risk Planning
- Risk Identification
- Risk Analysis (as applicable)
- Risk Handling
- Risk Monitoring.

(3) The third area of training concerns risk-management techniques, concentrating on the techniques the PMO plans to employ. The training should focus on how to use the techniques and should include examples of their use. Chapter 5, *Risk Management Techniques*, of this *Guide* provides a starting point. It contains a general discussion of a set of techniques that address all elements of the risk management process. The discussion of each technique contains a list of references that provide a more in-depth description of the technique. The set of techniques is not exhaustive and the program office should add to the list, if necessary.

Downloaded from http://www.everyspec.com

Document	Description
DoD 4245.7-M, *Transition from Development to Production*, September 1985.	Provides a structure for identifying technical risk areas in the transition from a program's development to production phases. The structure is geared toward development programs but, with modifications, could be used for any acquisition program. The structure identifies a series of templates for each of the development contractor's critical engineering processes. The template includes potential areas of risk and methods for reducing risk in each area.
Risk Management Concepts and Guidance, Defense Systems Management College, March 1989. (Superseded by this *Risk Management Guide*.)	Devoted to various aspects of risk management.
Systems Engineering Management Guide, Defense Systems Management College, January 1990, Section 15.	Devoted to risk analysis and management and provides a good overview of the risk management process.
Continuous Risk Management Guide, Software Engineering Institute, Carnegie Mellon University, 1996.	Provides a risk management methodology similar to the one described in the *Deskbook*. Its value is that is subdivides each process into a series of steps; this provides useful insights. Appendix A describes 40 risk-management techniques, the majority of which are standard management techniques adapted to risk management. This makes them a useful supplement to the *Deskbook* identified techniques.
A Systems Engineering Capability Maturity Model, Version 1.0 Software Engineering Institute (Carnegie Mellon University), Handbook SECMM-94-04, December 1994.	Describes one approach to conducting an Industry Capabilities Review. Section PA 10 (pp. 4-72–4-76) discusses software risk management. The material presented in this handbook also can be tailored to apply to system and hardware risk.
A Systems Engineering Capability Maturity Model, Version 1.01 Software Engineering Institute (Carnegie Mellon University), Technical Report, December 1996.	Describes an approach to assess the software acquisition processes of the acquiring organization and identifies areas for improvement.
Capability Maturity Model for Software (SM-CMM), Version 1.1,/CMU/SEI-93-TR-24, February 1993.	This is a tool that allows an acquiring organization to assess the software capability maturity of an organization.
Taxonomy-Based Risk Identification, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-93-TR-6 (ESC-TR-93-183, June 1993.	Describes a method for facilitating the systematic and repeatable identification of risks associated with the development of a software-intensive project. This method has been tested in active Government-funded defense and civilian software development projects. The report includes macro-level lessons learned from the field tests.
NAVSO P-6071.	Navy "best practices" document with recommended implementations and further discussion on the material in DoD 4245.7-M.
Risk Management, AFMC Pamphlet 63-101, July 1997.	An excellent pamphlet on risk management that is intended to provide PMs and the PMO with a basic understanding of the terms, definitions, and processes associated with effective risk management. It is very strong on how to perform pre-contract award risk management.

Table 4-3. Risk Management Reference Documents

Downloaded from http://www.everyspec.com

Document	Description
Defense Acquisition Deskbook	Primary reference tool for defense acquisition work force; contains over 1,000 mandatory and discretionary publications and documents which promulgate acquisition policy and guidance. (http://www.deskbook.osd.mil)
Acquisition Software Development Capability Evaluation, AFMC Pamphlet 63-103, 15 June 94.	Describes one approach to conducting an Industry Capabilities Review. This two-volume pamphlet was generated from material originated at Aeronautical Systems Center. The concepts support evaluations during source selection and when requested by IPTs. The material presented in this pamphlet also can be tailored to apply to system and hardware risk management.
Risk Management Critical Process Assessment Tool, Air Force SMC/AXD, Version 2, 9 June 1998.	Provides guidance and extensive examples for developing RFP Sections “L” and “M,” plus source selection standards or risk management. Also includes technical evaluation and review questions, which are helpful for assessing a risk management process; and risk trigger questions, which are helpful for risk identification.
NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*, October 1998.	Contains Navy approach to risk management with baseline information, explanations, and best practices that contribute to a well-founded technical risk management program.

Table 4-3. Risk Management Reference Documents (Continued)

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

5

RISK MANAGEMENT TECHNIQUES

5.1 INTRODUCTION

This Chapter provides top-level information on a number of techniques currently used in DoD, and a combination of techniques used by the Services, industry, and academia. Collectively, they focus on the components of the risk management process and address critical risk areas and processes. The write-ups describe the techniques and give information on their application and utility. The descriptions are at a level of detail that should permit potential users to evaluate the suitability of the techniques for addressing their needs; however, the material does not, in most cases, provide all the information that is required to use a technique. Readers will find that if a particular technique looks promising, they can obtain enough information from the references and tools that will enable program offices to apply them. The descriptions are in a format that aids comparison with other approaches.

5.2 OVERVIEW

Techniques are available to support risk management activities. None are required by DoD, but some have been successfully used in the past by DoD PMs. Many of the techniques support processes that are part of sound management and systems engineering and give Government and contractor PMs the tools for considering risk when making decisions on managing the program.

Several tools have been developed to support each of the components of the risk management process, i.e., planning, assessing, handling, and monitoring and documenting. Although tool developers may claim otherwise, none are integrated to totally satisfy all needs of a PM. Most likely, a PM will choose an overall risk strategy, write a plan to reflect his strategy, review the list of proven techniques to support the components of risk management, assess the techniques against the program's needs and available resources, tailor the techniques to suit the needs of the program, and train program office members to implement the plan.

5.3 RISK PLANNING TECHNIQUES

5.3.1 Description

This technique suggests an approach to risk planning; the process of developing and documenting an organized, comprehensive approach. It also suggests interactive strategy and methods for identifying and tracking risk drivers, developing risk-handling plans, performing continuous assessments to determine how risks have changed, and planning adequate resources. The risk planning technique is applicable to all functional areas in the program, especially critical areas and processes. Using the acquisition strategy as a starting point results in the development of a program risk management strategy, from which flows a management plan that provides the detailed information and direction

Downloaded from http://www.everyspec.com

necessary to conduct an effective management program. This risk management plan provides the PM with an effective method to define a program, one that fixes responsibility for the implementation of its various aspects, and supports the acquisition strategy.

The technique should first be used in Phase 0 following the development of the initial acquisition strategy. Subsequently, it may be used to update the management plan on the following occasions: (1) whenever the acquisition strategy changes, or there is a major change in program emphasis; (2) in preparation for major decision points; (3) in preparation for and immediately following technical audits and reviews; (4) concurrent with the review and update of other program plans; and (5) in preparation for a PMO submission.

The PMO risk management coordinator, if assigned, develops the risk management plan based on guidance provided by the PM, and coordinating with the Program Level IPT. To be effective, the PM must make risk management an important program management function and must be actively involved in the risk planning effort. Planning requires the active participation of essentially the entire PMO and contractor team.

5.3.2 Procedures

Figure 5-1 graphically depicts the process to be followed in applying this technique. The procedure consists of a number of iterative activities that result in the development of the risk management strategy and a Risk Management Plan.

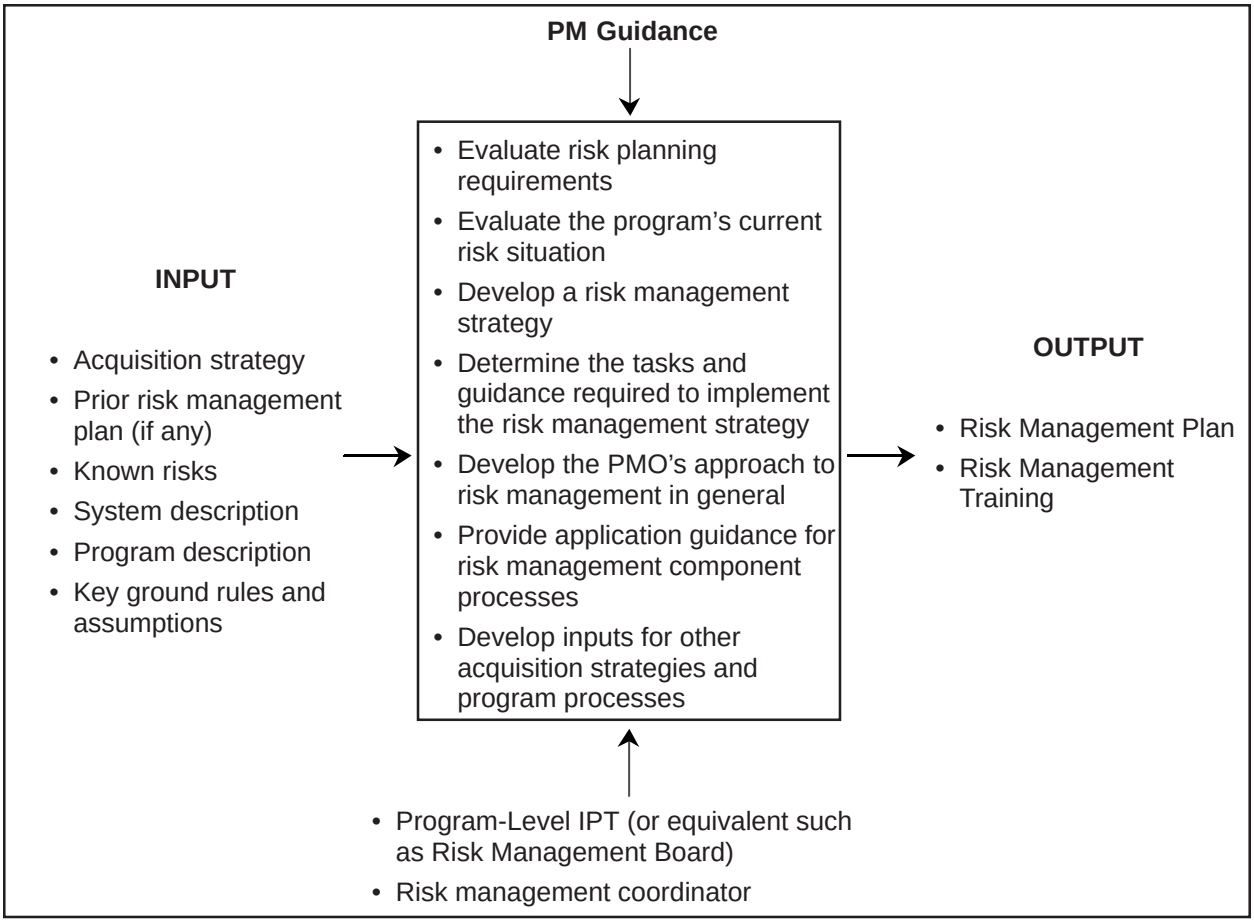


Figure 5-1. Risk Planning Technique Input and Output

Downloaded from http://www.everyspec.com

The acquisition strategy and related management planning efforts (program management, and systems engineering), program constraints, and any existing risk management planning are integrated and evaluated in the context of the PM's guidance, which provides the direction for the planning process. Typical types of PM guidance are concerns about certain categories of risk, guidance on funding of handling activities, emphasis to be placed on risk management training, and frequency and type of internal reports.

The integration and evaluation of the primary inputs establish the requirements and scope of the planning effort through an assessment of the program's current risk situation. The results of the assessment provide the basis for development of management strategy. The strategy should reflect the level of risk that the PM is prepared to accept, and should provide guidance on how and when known risks will be reduced to acceptable levels. It should also describe the risk management process the PMO will employ and the organization and structure of the management program, addressing things such as risk ratings, the use of an MIS, policy and procedures on sharing risk management information, and training.

The PMO should create an MIS early in the planning process. It will serve as a planning source and the data may be used for creating reports. It will also become the repository for all current and historical information related to risk. Eventually, this information may include risk assessment documents, contract deliverables, if appropriate, and other risk-related reports.

Based on the management strategy, the plan identifies specific tasks to be accomplished and assigns responsibility for their execution. The timing of these tasks should be incorporated into an integrated critical path master schedule or equivalent. Guidance for task execution and control should also be developed, covering such things as the suggested techniques to be used for each component, any assistance available to Sub-Tier IPTs, the use of funds, the policy on the use of independent risk assessors, etc. This information may be documented in a risk management plan. A sample format is shown in Figure 5-2. Appendix B contains two examples of a Risk Management Plan.

The contents of the risk management strategy and plan should be consistent with the acquisition strategy and other program plans derived from the acquisition strategy. Hence, it should be tailored to each program rather than attempting to use the same process and its implementation on all programs. This will help to ensure that risk is considered in all program activities and that it does not become a "stove pipe" function.

5.4 RISK ASSESSMENT TECHNIQUES

5.4.1 Product (WBS) Risk Assessment

5.4.1.1 Description. This technique identifies those risks associated with a given system concept and design. The difference between the process (DoD 4245.7-M) technique and this approach is that DoD 4245.7-M addresses the contractor's engineering and manufacturing *process* and this technique focuses on the resulting *product*. This technique is used to identify and analyze risks in the following critical risk areas: design and engineering, technology, logistics, production, concurrency, plus others as needed for both hardware and software.

The WBS is the starting point to describe contract work to be done and the resulting product and is the basis for determining risk events in each critical risk area. The risk events—events that *might* have a

Downloaded from http://www.everyspec.com

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

PROGRAM SUMMARY. This section contains a brief description of the program, including the acquisition strategy and the program management approach. The acquisition strategy should address its linkage to the risk management strategy.

DEFINITIONS. Definitions used by the program office should be consistent with DoD definitions for ease of understanding and consistency. However, the DoD definitions allow program managers flexibility in constructing their risk management programs. Therefore, each program's risk management plan may include definitions that expand the DoD definitions to fit its particular needs. For example, each plan should include, among other things, definitions for the ratings used for technical, schedule, and cost risk. (Discussion of risk rating is contained in *Acquisition Deskbook*, Section 2.5.2.1.)

RISK MANAGEMENT STRATEGY AND APPROACH. Provide an overview of the risk management approach, to include the status of the risk management effort to date, and a description of the program risk management strategy. See *Acquisition Deskbook*, Sections 2.5.2.1 and 2.5.2.3.

ORGANIZATION. Describe the risk management organization of the program office and list the responsibilities of each of the risk management participants. See *Acquisition Deskbook*, Section 2.5.2.3.

RISK MANAGEMENT PROCESS AND PROCEDURES. Describe the program risk management process to be employed, i.e., risk planning, assessment, handling, monitoring and documentation, and a basic explanation of these components. See *Acquisition Deskbook*, Section 2.5.2.1. Also provide application guidance for each of the risk management functions in the process. If possible, the guidance should be as general as possible to allow the program's risk management organization (e.g., IPTs) flexibility in managing the program risk, yet specific enough to ensure a common and coordinated approach to risk management. It should address how the information associated with each element of the risk management process will be documented and made available to all participants in the process, and how risks will be tracked, to include the identification of specific metrics if possible.

RISK PLANNING. This section describes the risk planning process and provides guidance on how it will be accomplished, and the relationship between continuous risk planning and this RMP. Guidance on updates of the RMP and the approval process to be followed should also be included. See Section 2.5.2.1 of the *Deskbook* for information on risk planning.

RISK ASSESSMENT. This section of the plan describes the assessment (identification and analysis) process. It includes procedures for examining the critical risk areas and processes to identify and document the associated risks. It also summarizes the analyses process for each of the risk areas leading to the determination of a risk rating. This rating is a reflection of the potential impact of the risk in terms of its variance from known Best Practices or probability of occurrence, its consequence, and its relationship to other risk areas or processes. This section may include:

- Overview and scope of the assessment process
- Sources of information
- Information to be reported and formats
- Description of how risk information is retained
- Assessment techniques and tools (see Section 2.5.2.4.2 of the *Deskbook*).

RISK HANDLING. This section describes the risk handling options, and identifies tools that can assist in implementing the risk handling process. It also provides guidance on the use of the various handling options for specific risks.

RISK MONITORING. This section describes the process and procedures that will be followed to monitor the status of the various risk events identified. It should provide criteria for the selection of risks to be reported on, and the frequency of reporting. Guidance on the selection of metrics should also be included.

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

Figure 5-2. Sample Format for Risk Management Plan

Downloaded from http://www.everyspec.com

detrimental impact on the system, subsystems, or components—are evaluated to identify and characterize specific risks ratings and prioritization.

This technique should be used shortly after the completion of the prime contractor's WBS. Thereafter, it should be used regularly up to the start of production. The technique can be used independently or in conjunction with other risk assessment techniques, such as the Process (DoD 4245.7-M) Risk Assessment technique. It may, if appropriate, also be used in conjunction with the Integrated Baseline Review (IBR), which is conducted within 6 months of contract award. See Section 1.4.2.4.3 of the *Deskbook* (http://www.deskbook.osd.mil) for a discussion of IBR. A World Wide Web Site is also available at www.acq.osd.mil./pm/ibrmats.htm, which discusses the IBR Process.

To apply this technique, joint Government and industry evaluation teams should examine the appropriate WBS levels in each Sub-Tier IPTs product area. If necessary, complementary industry-only teams may take an in-depth look at selected areas at lower WBS levels. At times, it may be desirable to include outside industry experts on the teams to aid in the examination of specific WBS elements or functional areas.

5.4.1.2 Procedures. Figure 5-3 depicts the process used in this technique. The first step is to review the WBS elements down to the level being considered, and identify risk events. This review should consider the critical areas (design and engineering, technology, logistics, etc.) that may help to describe risk events. Table 5-1 shows a partial listing of these elements.

Using information from a variety of sources, such as program plans, prior risk assessments, expert interviews, etc., the WBS elements are examined to identify specific risks in each critical area. The risk event, are then analyzed to determine probability of occurrence and consequences, along with any interdependencies and risk event priorities. Several techniques and tools are available to accomplish this, including, among others, technology assessments, modeling and simulation, hazard analysis, and fault tree analysis.

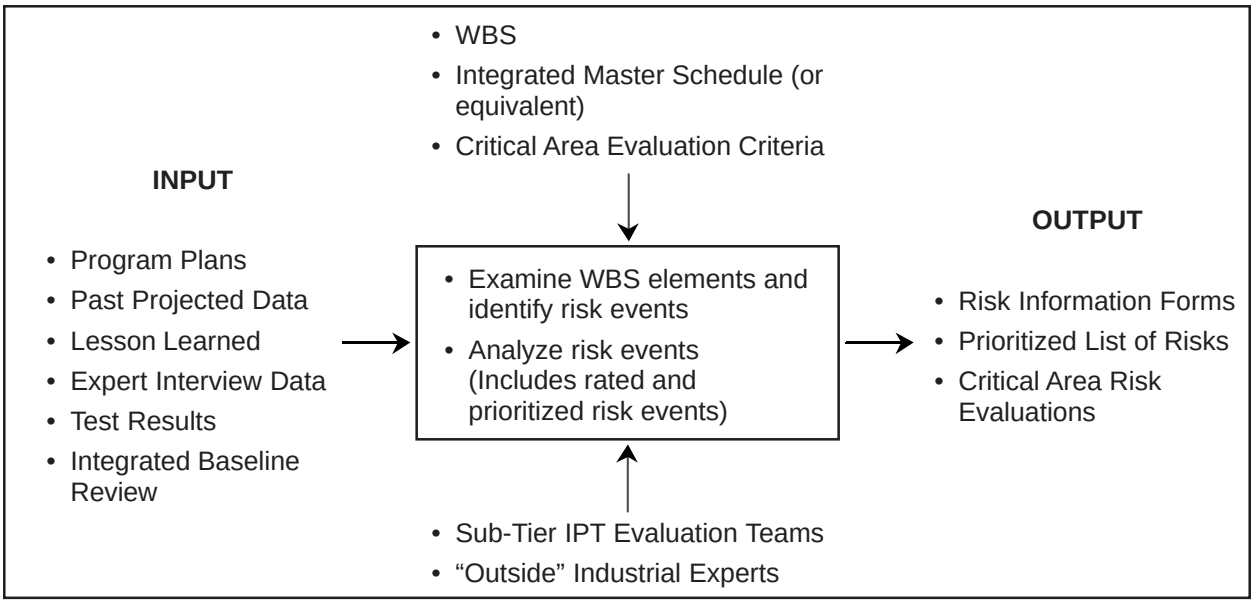


Figure 5-3. Product (WBS) Risk Assessment Technique Input and Output

Downloaded from http://www.everyspec.com

Critical Risk Areas	Example Elements	
Design and Engineering	Design/technology approach Operational environments External/internal interfaces Use of standard parts/program parts list System/subsystem critical design requirement	Integration requirements Human-machine interface Design growth capacity Design maturity Safety & health hazards Manpower, training and skill profiles
Logistics	Operations and Maintenance (O&M) concept System diagnostic requirement Repairability and Maintainability (R&M) requirements Supply support requirements Built-in Test (BIT) requirements	Support equipment requirements Maintenance interfaces Level of repair decisions Training equipment design
Testing	Integrated test Qualification testing Subsystem test limits	Test environmental acceleration Supportability test results
Manufacturing	Design producibility Manufacturing capability requirements Parts/assemblies availability	Special tooling/test equipment planning personnel availability Process/tooling proofing Production equipment availability
Concurrency	Program schedule adequacy	Development phases concurrency

Table 5-1. Critical Risk Areas and Example Elements

The results of this analysis should be documented in a program-specific standard format, such as a Risk Information Form (RIF). The risks, along with others identified using other techniques, can be prioritized and aggregated using the technique described later in this chapter.

5.4.2 Process (DoD 4245.7-M) Risk Assessment

5.4.2.1 Description. This technique is used to assess (identify and analyze) program technical risks resulting from the contractor's processes. It is based on the application of the technical risk area templates found in DoD 4245.7-M. These templates describe the risk areas contained in the various technical processes (e.g., design, test, production, etc.) and specify methods for reducing risks in each area. Success of any risk reduction efforts associated with this technique will depend on the contractor's ability and willingness to make a concerted effort to replace any deficient engineering practices and procedures with best industrial practices.

One of the primary benefits of this technique is that it addresses pervasive and important sources of risk in most DoD acquisition programs and uses fundamental engineering principles and proven procedures to reduce technical risks. The

Downloaded from http://www.everyspec.com

technique is accepted by many aerospace companies in normal business activities, and in fact, was developed by a group of Government and aerospace experts.

The technique is primarily applicable during Phases 0, and II of program development. In Phase 0 it provides a detailed checklist of processes that the contractor needs to address; in Phase II, the processes are being implemented in Low Rate Initial Production (LRIP). The description of each template in DoD 4245.7-M shows the phases in which the template should be applied. The specific timing of the application within the phases should be determined based on the type of program, the acquisition strategy and plans, and the judgment of program officials. It should also be used in preparation for milestone decisions and when preparing for source selection. This technique may be used independently or in conjunction with other risk assessment techniques. When feasible, a Government-industry evaluation team should be formed early in the program to apply this technique.

5.4.2.2 Procedures. Figure 5-4 shows the basic approach used in this technique. The DoD 4245.7-M templates are used in conjunction with the contract requirements and specifications to identify those technical processes critical to the program and to establish a program baseline of contractor processes. When possible, the program baseline should be determined by evaluating actual contractor performance, as opposed to stated policy. For example, design policy should be determined from interviewing designers and not simply from reviewing written corporate policies.

This program baseline should then be compared to a baseline of industry-wide

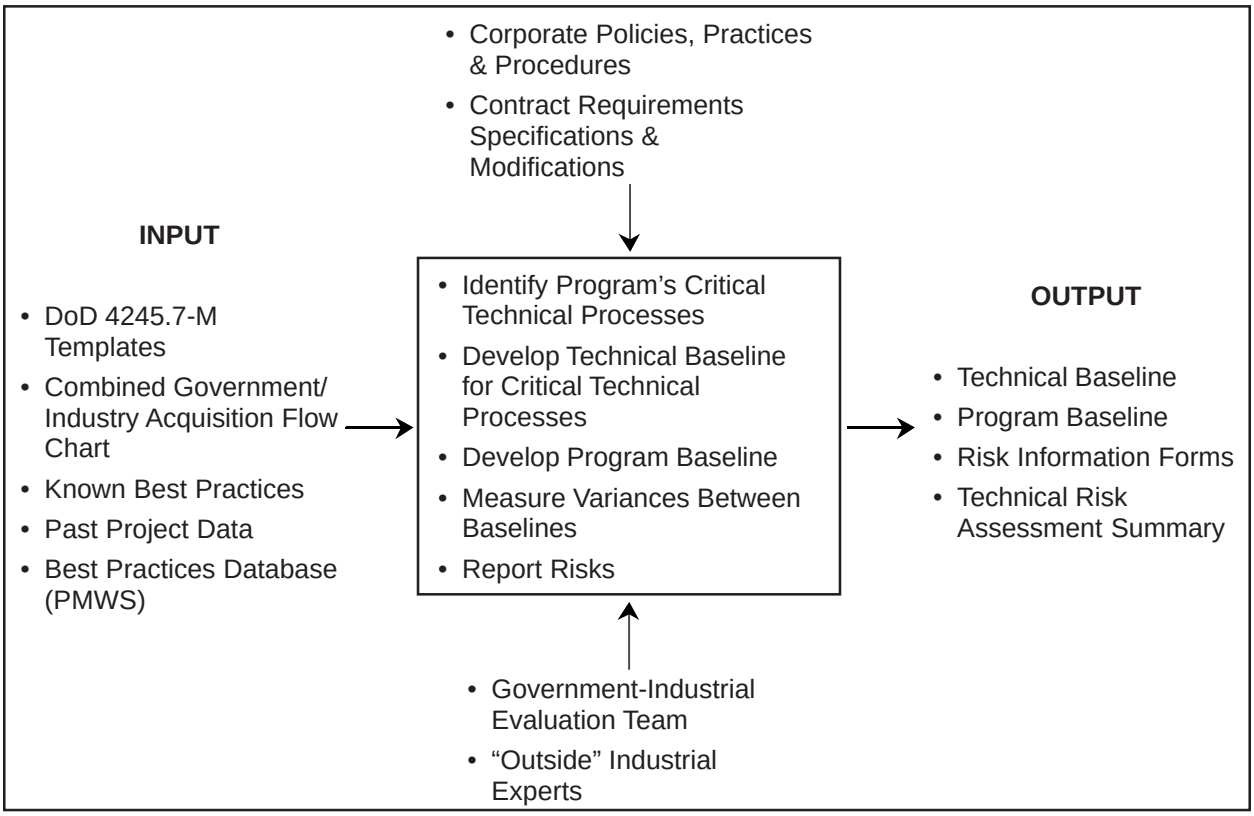


Figure 5-4. Process (DoD 4245.7-M) Risk Assessment Technique Input and Output

Downloaded from http://www.everyspec.com

processes and practices that are critical to the program. The baseline should be developed by reviewing and compiling known best practices in use by various companies in both defense and non-defense sectors. One source of best practices information is the Program Manager's Work Station (PMWS), a series of PC expert systems designed to aid in the implementation of DoD 4245.7-M. The point of contact for the PMWS is the Best Management Practices Center of Excellence (http://www.bmpcoe.org).

The differences between the two baselines are a reflection of the technical process risk present. These results should be documented in a standard format, such as a program-specific Risk Information Form (see MIS discussion this section) to facilitate the development of a risk handling and risk reporting plan.

5.4.3 Program Documentation Evaluation Risk Identification

5.4.3.1 Description. This technique provides a methodology for comparing key program documents and plans to ensure that they are consistent and traceable to one another. Program documents and plans are hierarchical in nature. If the contents (activities, events, schedules, requirements, specifications, etc.) of a document or plan do not flow from or support the contents of those above, below, or adjacent to it, there is a strong chance that risk will be introduced into the program or that known risks will not be adequately addressed. This technique reduces those risks and improves the quality of program documentation.

This technique can be used in any acquisition phase as documents or plans are being developed or updated. The comparison of program documentation and plans should be performed by a small team of experienced, knowledgeable personnel who are intimately familiar with the total program.

5.4.3.2 Procedures. Figure 5-5 shows the process used in this technique. The primary inputs to the process are the PMO documents that detail the steps involved in executing the program. These include, for example, the Mission Need Statement (MNS), ORD, acquisition plan, any master management plan, Test and Evaluation Master Plan (TEMP), manufacturing plan, etc. Another set of key input documents are those used to communicate with the prime contractor, e.g., WBS, specifications, Statement of Work (SOW) or equivalent

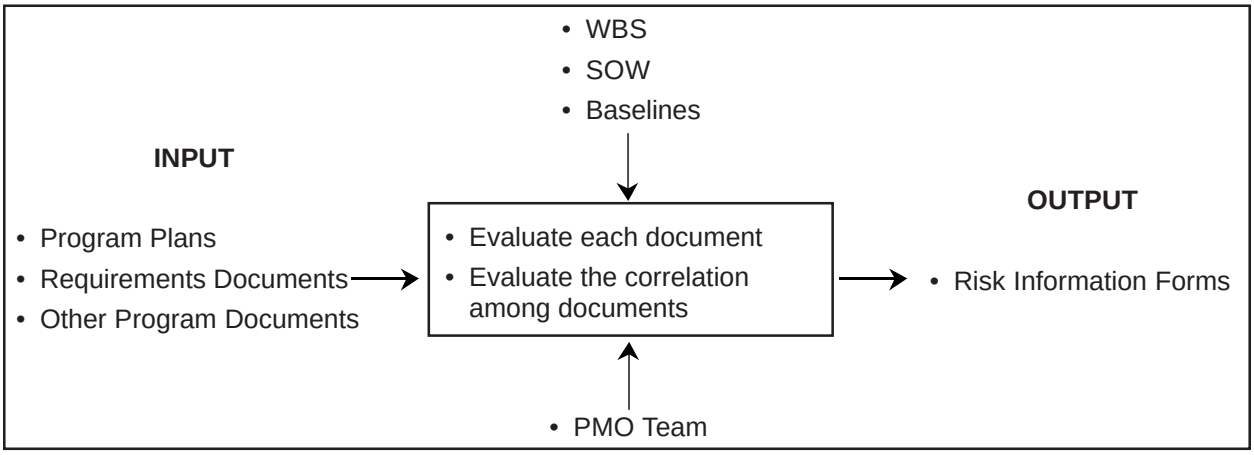


Figure 5-5. Plan Evaluation Technique Input and Output

Downloaded from http://www.everyspec.com

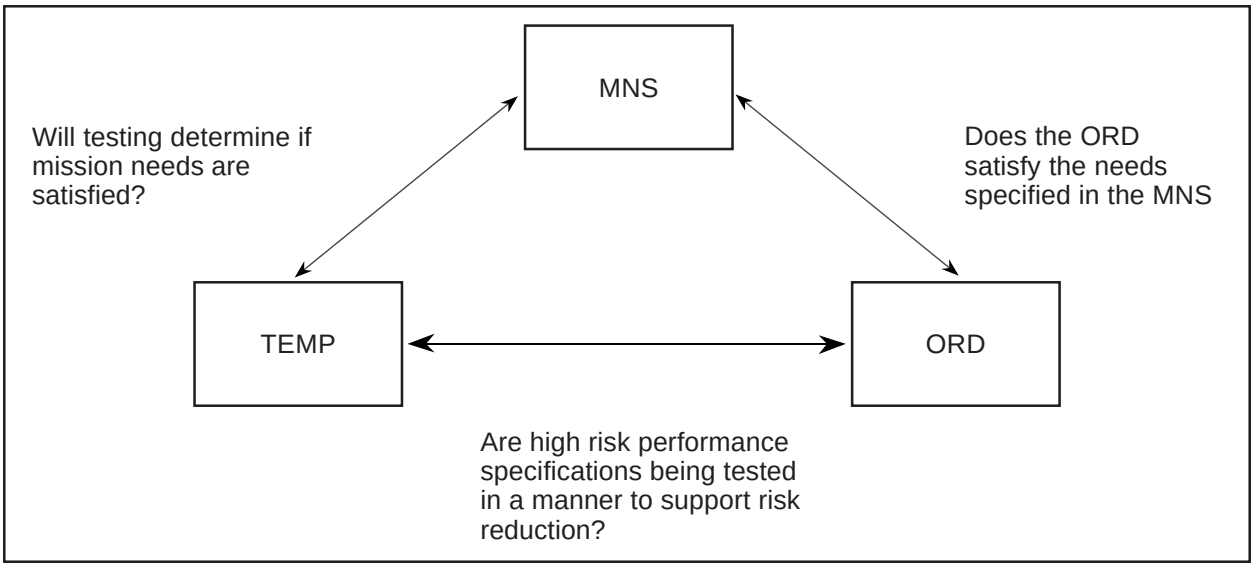


Figure 5-6. Phase 0 Correlation of Selected Documents (Example)

such as, Statement of Objectives, etc. Before any comparison, the PMO should review all documents for accuracy and completeness. Figure 5-6 shows an example of the type of correlation that should exist among the MNS, ORD, and TEMP during Phase 0.

If the comparison shows any gaps or inconsistencies, reviewers should identify them as possible risks on a Risk Identification Form (RIF), the output of this process.

5.4.4 Threat and Requirements Risk Assessment

5.4.4.1 Description. This technique describes an approach to assess risks associated with requirements and threat and to identify requirements and threat elements that are risk drivers. Because operational needs, environmental demands, and threat determine system performance requirements, to a large degree, they are a major factor in driving the design of the system and can introduce risk in a program. Further, with the introduction of CAIV, PMs and users are directed to examine performance requirements and identify areas that are not critical and are available for trade to meet cost objectives. Risk is a factor in CAIV considerations.

The requirements risk assessment process focuses on: determining if operational requirements are properly established and clearly stated for each program phase; ensuring that requirements are stable and the operating environment is adequately described; addressing logistics and suitability needs; and determining if requirements are too constrictive, thereby identifying a specific solution. The evaluation of the threat risk assessment process' maturity addresses: uncertainty in threat accuracy and stability, sensitivity of design and technology to threat, vulnerability of the system to threat countermeasures, and vulnerability of the program to intelligence penetration. PMs should view requirements in the context of the threat and accurately reflect operational, environmental, and suitability requirements in design documents.

PMs should use threat and requirements assessments during the early phases of program development and, as necessary,

Downloaded from http://www.everyspec.com

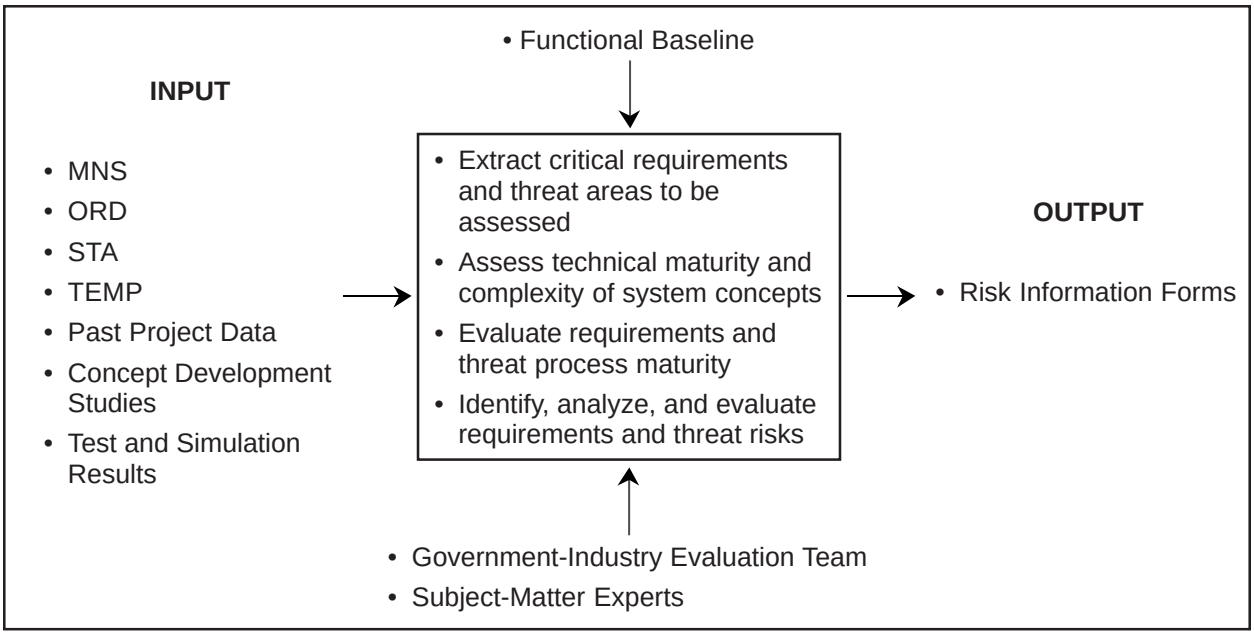


Figure 5-7. Threat and Requirement Risk Assessment Technique Input and Output

as the program advances through development. Early and complete understanding of the requirements and threat precludes misunderstandings between the requirements and development communities, helps to identify risk areas, and allows early planning to handle risk. Consequently, the user should be actively involved in this process from the beginning.

5.4.4.2 Procedures. Figure 5-7 depicts the process used in this technique. The basic approach is to conduct a thorough review of the documents containing performance requirements and threat information, e.g., ORD, TEMP, System Specification, Special Threat Assessment (STA), Design Reference Mission Profile, etc., to determine stability, accuracy, operating environment, logistics and suitability requirements, and consistency between these requirements and the threat considerations cited above. There should be an understanding between the users and the developers on Key Performance Parameters (KPPs) in order to identify the requirements that are most important and critical to program success. The Design Reference Mission Profile and Design Requirements templates in DoD 4245.7-M and the Program Documentation Evaluation Risk Identification technique may be useful in support of this technique.

Requirements should be thoroughly reviewed to identify those that drive performance. This will require the "flow down" of performance requirements to components and subassemblies and the identification of technologies / techniques to be used in these components / subassemblies that may significantly affect the system's ability to meet users' needs.

Designers should determine the sensitivity of system performance to the requirements and threat and identify risk drivers. Models and simulations are useful tools to determine this sensitivity. For example, the U.S. Army Materiel System Analysis Activity (AMSAA) has such an analytic model, the AMSAA Risk Assessment Methodology. The AMSAA point of contact can be reached at (410) 278-6626.

Downloaded from http://www.everyspec.com

The PMWS can also be useful. The risk identified in this technique should be documented in a program-specific format, such as a Risk Information Form (RIF) (see Annex B).

5.4.5 Cost Risk Assessment

5.4.5.1 Description. This technique provides a program-level cost estimate at completion (EAC) that is a function of performance (technical), and schedule risks. It uses the results of previous assessments of WBS elements and cost probability distributions developed for each of the elements. These individual WBS elements are aggregated using a Monte Carlo simulation to obtain a probability distribution of the program-level cost EAC probability distribution function. These results are then analyzed to determine the actual risk of cost overruns and to identify the cost drivers.

The use of these cost probability distributions as the basis for the program-level cost estimate results in a more realistic EAC than the commonly used single point estimates for WBS elements, since they address both the probability of occurrence and consequences of potential risk events. Their use also eliminates a major cause of underestimating (use of point estimates) and permits the evaluation of performance (technical) or schedule causes of cost risk. Thus, this technique provides a basis for the determination of an "acceptable" level of cost risk.

This technique can be used in any of the acquisition phases, preferably at least once per phase beginning in Phase 0 although suitable data may not exist until Phase I in some cases. It should be used in conjunction with performance (technical) and schedule risk assessments and may be performed by small Government-industry teams consisting of risk analysts, cost analysts, schedule analysts and technical experts who understand the significance of previous performance and schedule risk assessments. They should report to the Program IPT. This technique requires close and continuous cooperation among cost analysts and knowledgeable technical personnel and the support of the prime contractor's senior management to help get valid cost data.

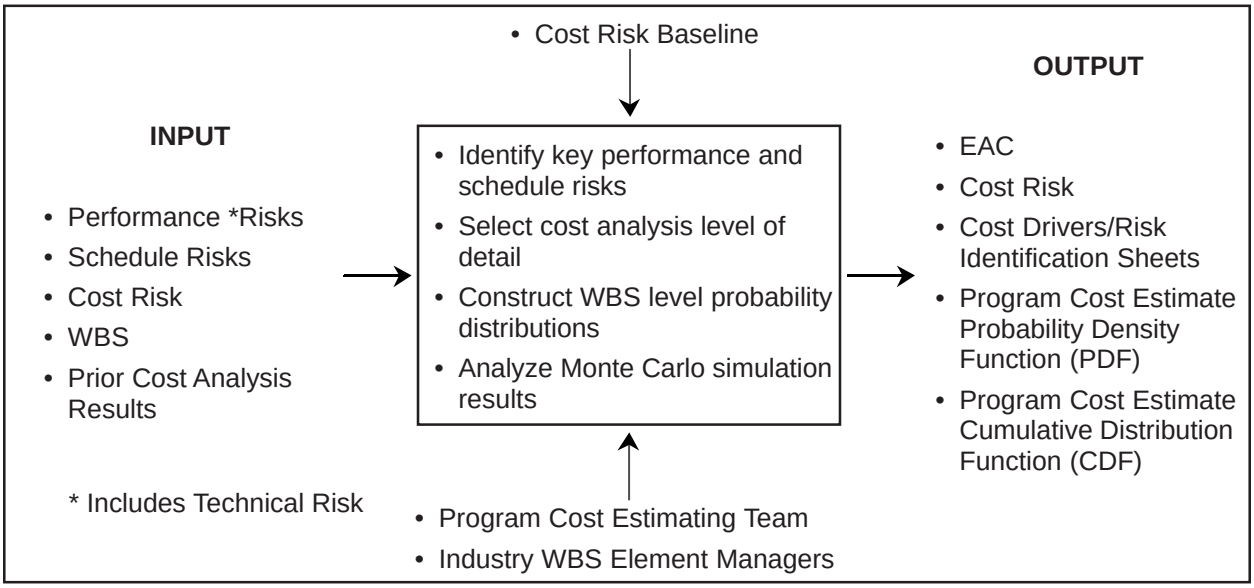


Figure 5-8. Cost Risk Assessment Top-Level Diagram

Downloaded from http://www.everyspec.com

5.4.5.2 Procedures. Figure 5-8 depicts the process used in applying this technique. The first step is to identify the lowest WBS level for which cost probability distribution will be constructed. The level selected will depend on the program phase; e.g., during Phase 0, it may not be possible to go beyond level 2 or 3, simply because the WBS has not yet been developed to lower levels. As the program advances into subsequent phases and the WBS is expanded, it will be possible and necessary to go to lower levels (4, 5, or lower). Specific performance (technical) and schedule risks are then identified for these WBS elements.

To develop the WBS elements cost probability distributions, the team, working with the prime contractor's WBS element managers, determines the cost range for each element being investigated. The cost range encompasses cost estimating uncertainty, schedule risk, and technical risk. The validity of the cost data used to construct the distribution is critical. In fact, collecting *good* data is the largest part of the cost risk job. Consequently, PMOs should place major emphasis on this effort.

The element cost probability distributions aggregated and evaluated are then using a Monte Carlo simulation program. All Monte Carlo processes contain limitations, but they are more informative than point estimates. Any number of these simulations are readily available to perform this aggregation, and one that meets the specific needs of the program should be selected. The results of this step will be a program-level cost EAC and a cost distribution that shows the cumulative probability associated with different cost values. These outputs are then analyzed to determine the level of cost risk and to identify the specific cost drivers. Cost risk is determined by comparing the EAC with the cost baseline developed as part of the acquisition program baseline. Since the EAC and program cost distribution are developed from WBS element risk assessments, it is possible to determine the cost risk drivers. The cost drivers can also be related back to the appropriate performance and schedule risks. The results of the analysis (cost risks and drivers) should be documented in RIFs.

5.4.6 Quantified Schedule Risk Assessment

5.4.6.1 Description. This technique provides a means to determine program-level schedule risk as a function of risk associated with various activities that compose the program. It estimates the program-level schedule by developing probability distributions for each activity duration and aggregating these distributions using a Monte Carlo simulation or other analytical tools. The resulting program-level schedule is then analyzed to determine the actual schedule risk and to identify the schedule drivers.

This technique expands the commonly used Critical Path Method (CPM) of developing a program schedule to obtain a realistic estimate of schedule risk. The basic CPM approach uses single point estimates for the duration of program activities to develop the program's expected duration and schedule. It invariably leads to underestimating the time required to complete the program and schedule overruns, primarily because the point estimates do not adequately address the uncertainty inherent in individual activities. The uncertainty can be caused by a number of factors and may be a reflection of the risk present in the activity.

Downloaded from http://www.everyspec.com

The quantified schedule technique accounts for uncertainty by using a range of time that it will take to complete each activity instead of single point estimates. These ranges are then combined to determine the program-level schedule estimate. This approach enables PMs to estimate early in a program if there is a significant likelihood of overrunning the program schedule and by how much. It also identifies program activities that are on the "highest risk path."

This technique can be used in any acquisition phase beginning with the completion of the first statement of work. The schedule probability distribution function for each key activity should be developed as soon as the activity is included in the master schedule. The distribution functions should be periodically reviewed and revised, if necessary, at least once per phase. The technique should be applied by a small Government-industry team consisting of schedule analysts and technical experts who understand the significance of prior risk performance assessments.

5.4.6.2 Procedures. Figure 5-9 shows the process used in this technique. The first step is to identify the lowest activity level for which duration/schedule probability distribution functions will be constructed. The WBS should be used as the starting point for identifying activities and constructing a network of activities. The WBS level selected will depend on the program phase.

Next, the contractor should construct a CPM schedule for these activities. To develop the activity duration probability distribution functions, the team, working with the prime contractor's WBS element managers, determines and analyzes duration range for each activity being investigated. This analysis should be done by schedule analysts working closely with knowledgeable technical people.

The activity duration probability distributions are aggregated using a Monte Carlo simulation program, such as ©Risk, Risk + for Microsoft Project, or Crystal Ball. The result of this step is a program-level schedule and distribution function that shows

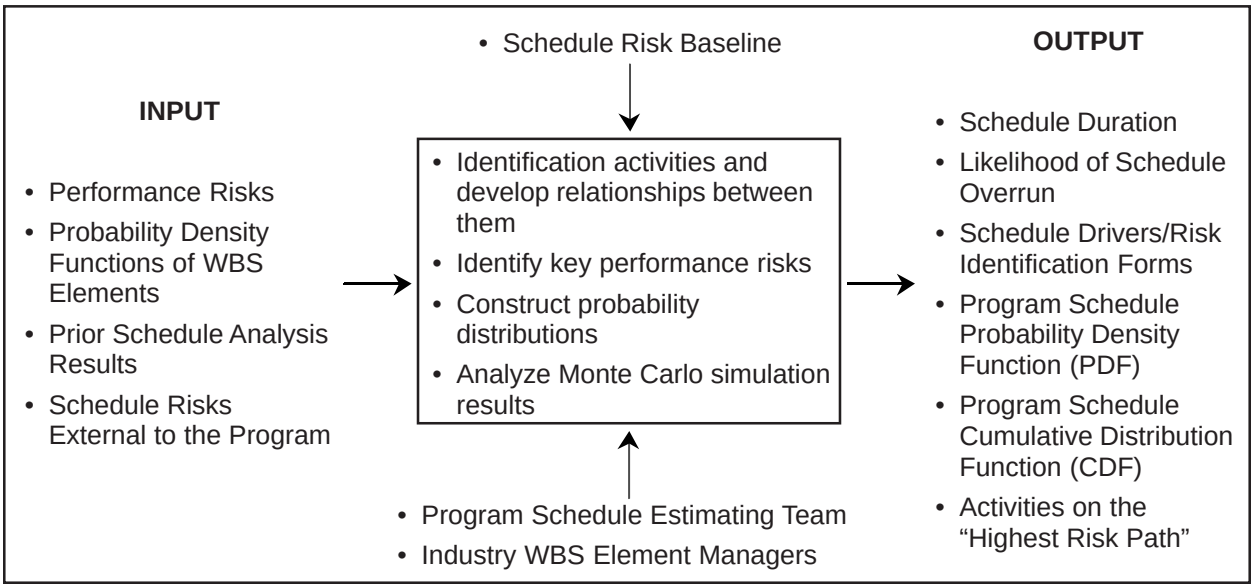


Figure 5-9. Schedule Risk Assessment Technique Input and Output

Downloaded from http://www.everyspec.com

the cumulative probability associated with different duration values. These outputs are then analyzed to determine the level of schedule risk and to identify the specific schedule drivers. Risk is determined by comparing the program-level schedule with the deterministic schedule baseline developed as part of the acquisition program baseline. The fact that the schedule and distribution are developed from WBS element risk assessments makes it possible to determine the schedule risk drivers. These drivers can also be related back to the appropriate performance risks. The results of the analysis (schedule risks and drivers) should be documented in RIFs. The analysis requires continued close cooperation between the schedule analysts and technical personnel familiar with the details of the program.

5.4.7 Expert Interviews

5.4.7.1 Description. A difficult part of the risk management process is data gathering. This technique provides a means for collecting risk-related data from subject-matter experts and from people who are intimately involved with the various aspects of the program. It relies on "expert" judgment to identify and analyze risk events, develop alternatives, and provide "analyzed" data. It is used almost exclusively in a support role to help develop technical data, such as probability and consequences information, required by a primary risk assessment technique. It can address all the functional areas that make up the critical risk areas and processes, and can be used in support of risk handling.

Expert judgment is a sound and practical way of obtaining necessary information that is not available elsewhere or practical to develop using engineering or scientific techniques. However, interviewers should be aware that expert opinions may be biased because of over-reliance on certain information and neglect of other information; unwarranted confidence; the tendency to recall most frequent and most recent events; a tendency to neglect rare events; and motivation. Results may have to be tempered because of these biases.

5.4.7.2 Procedures. Figure 5-10 depicts the process used in this technique. The first step in the process is to identify risk areas and processes that are to be evaluated using the expert interview technique. Other

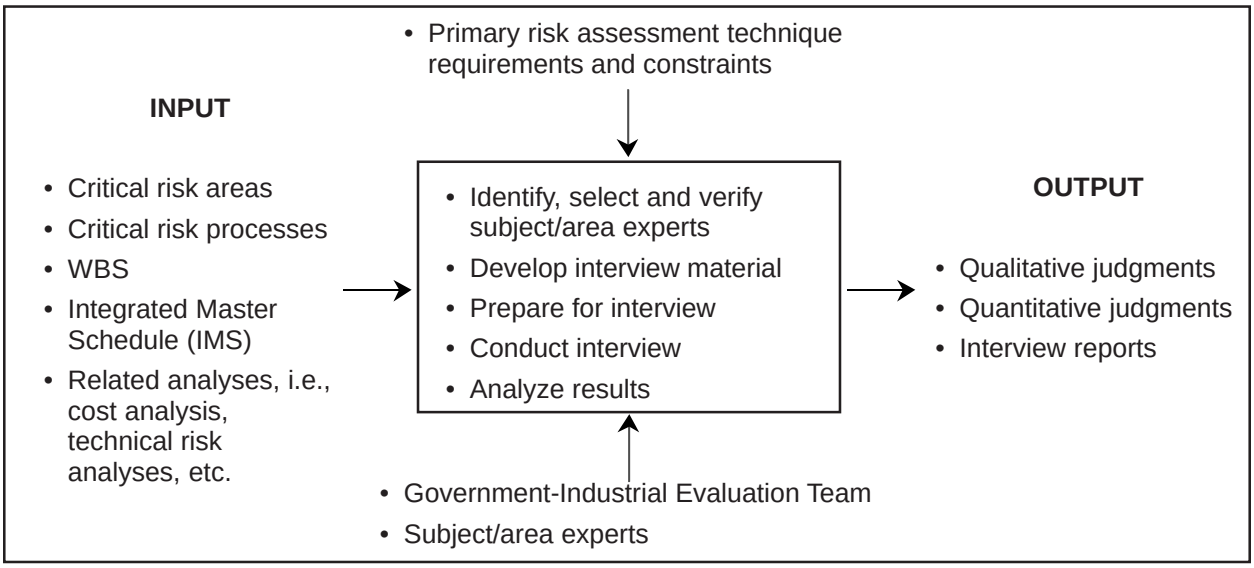


Figure 5-10. Expert Interview Technique Input and Output

Downloaded from http://www.everyspec.com

techniques described in this section (e.g., WBS Risk Assessment, Process Risk Assessment, etc.) can be used for this purpose.

Once the areas and processes are known, subject-matter experts and program/contractor personnel knowledgeable of the areas and processes should be identified to be interviewed. Similarly, qualified interviewers should be selected for each area and process.

Interviewers should prepare themselves by preparing a strategy and selecting a methodology for analysis and quantification of data. The references list sources for practical techniques for quantifying expert judgment.

After the interview, evaluators analyze the data for consistency, resolve any issues, and document the results. Commercial "Groupware" software is available to assist in compiling and documenting the results of interviews.

5.4.8 Analogy Comparison/ Lessons-Learned Studies

5.4.8.1 Description. This technique uses lessons learned and historical information about the risk associated with programs that are similar to the new system to identify the risk associated with a new program. It is normally used to support other primary risk assessment techniques, e.g., Product (WBS) Risk Assessment, Process Risk Assessment, etc. The technique is based upon the concept that "new" programs are originated or evolved from existing programs or simply represent a new combination of existing components or subsystems. This technique is most appropriate when systems engineering and systems integration issues, plus software development, are minimal. A logical extension of this premise is that key insights can be gained concerning aspects of a current program's risks by examining the successes, failures, problems, and solutions of similar existing or past programs. This technique addresses all the functional areas that make up the critical risk areas and processes.

5.4.8.2 Procedures. Figure 5-11 depicts the process used in this technique. The first step in this approach is to select or develop a baseline comparison system (BCS) that closely approximates the characteristics of the new system/equipment to as low a level as possible and uses the processes similar to those that are needed to develop the new system. For processes, industry-wide best practices should be used as a baseline. The PMWS is a useful tool for identifying these best practices.

Relevant BCS data are then collected, analyzed, and compared with the new system requirements. The BCS data may require adjustment to make a valid comparison; for example, apply appropriate inflation indices for cost comparisons, adjust design schedule for software evolution versus software development, etc. The comparisons can be a major source of risk assessment data and provide some indication of areas that should be investigated further.

5.5 RISK PRIORITIZATION

5.5.1 Description

This technique provides a means to prioritize the risks present in a program. It is a part of risk analysis. The prioritized list provides the basis for developing handling plans, preparing a handling task sequence list, and allocating handling resources.

When using this technique, PMs establish definitive criteria to evaluate the risks, such as, probability (likelihood) of failure, (P_F),

Downloaded from http://www.everyspec.com

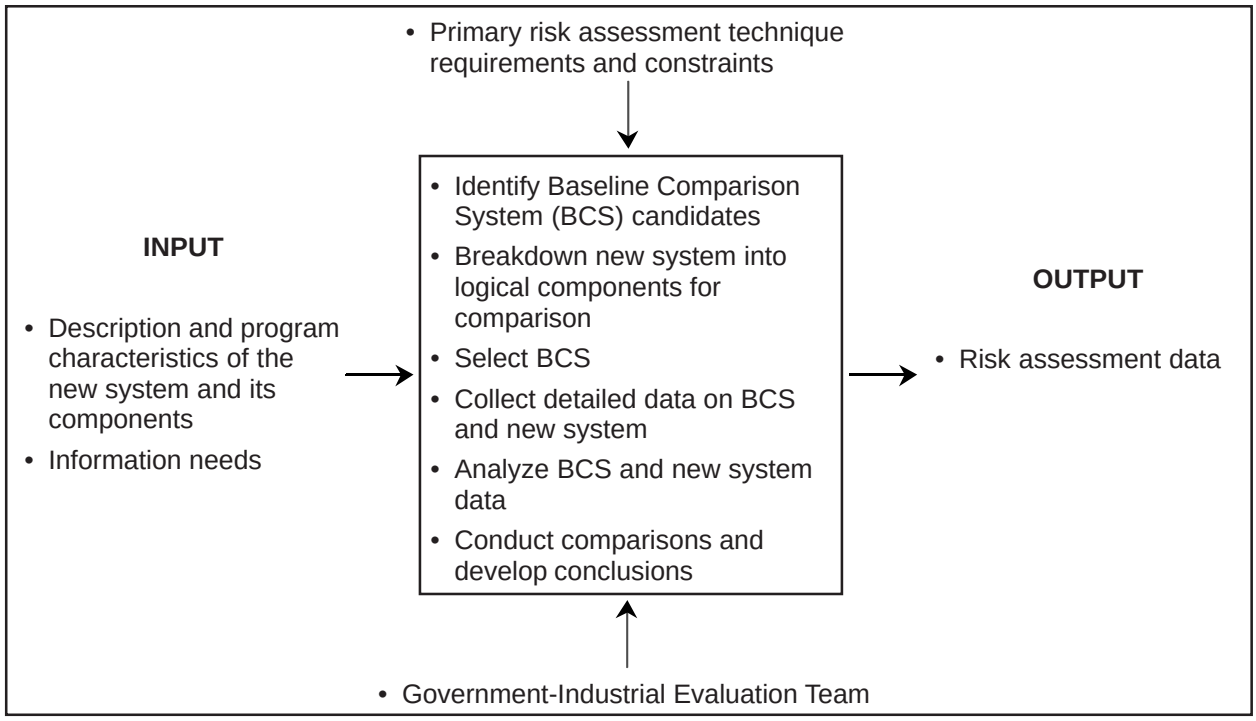


Figure 5-11. Analogy Comparison/Lessons Learned Studies Top-Level Diagram

and consequence of failure (C_F), along with any other factors considered appropriate. The risks are evaluated using qualitative expert judgment and multi-voting methods to prioritize and aggregate risks. (See References-SEI, *Continuous Risk Management*, 1996, for a discussion of multi-voting methods.) A qualitative approach using subject-matter experts is generally preferred in this technique because of the tendency to rely on ordinal values to describe P_F, C_F and the inherent inaccuracies resulting from any attempts to use quantifiable methods with derived from raw (uncalibrated) ordinal scales.

These techniques should be used appropriately during Phases 0, I, and II, at the conclusion of a major risk assessment undertaking, when there has been a significant change in the acquisition strategy, when risk monitoring indicates significant changes in the status of a number of risks, and prior to a milestone review.

The PMO risk management coordinator (if assigned) may function as a facilitator and support the program IPT in applying these techniques.

5.5.2 Procedures

Figure 5-12 depicts the process used to prioritize the risks present in a program. The inputs of this process are risks that have been identified.

The evaluation team, through consensus or as directed by the Risk Management Plan, selects the prioritization criteria. P_F and C_F should always be part of the criteria, along with any other appropriate factors. Urgency, an indication of the time available before the procedures for handling the specific risk must be initiated, is often considered in the evaluation. The PM may also choose to rank-order the prioritization criteria, e.g., consequence is more important than probability.

Downloaded from http://www.everyspec.com

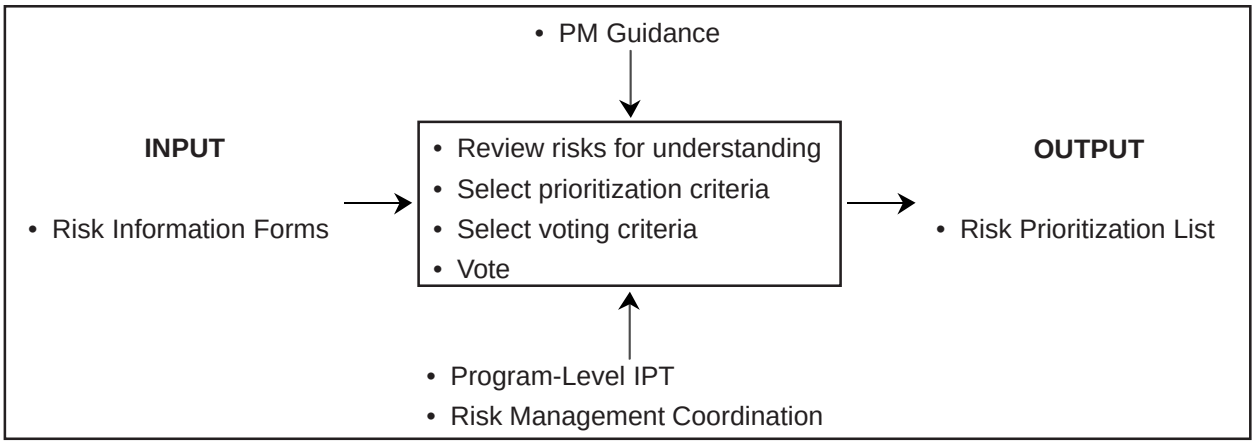


Figure 5-12. Risk Prioritization Technique Input and Output

A multi-voting method is useful to prioritize risks (see References-Scholtes, 1988; Linstone, 1975). The Delphi method is a simple and effective method of arriving at a consensus among a group of experts. The procedure is for team members to vote on the priority of each risk and tally the results, which are fed back to the team. Team members vote again and the process is repeated until no changes occur in the results. It is normal to reach the final outcome within a few voting sessions. If there are a large number of risks, they may be broken into smaller groups for ranking. As a general rule, no more than 10 items should be prioritized per vote. The results of the series of votes are documented in the risk prioritization list.

PM guidance, which operates as a technique control function, can be used, for example, to specify prioritization criteria and prescribe the format of the risk prioritization list.

5.5.2.1 Risk Aggregation. Figure 5-13 shows the process for this technique, which relies on qualitative judgment and multi-voting methods to summarize risks at the critical risk area and process level in terms of P_F and C_F. The risks identified in the RIFs and Risk Prioritization List are first

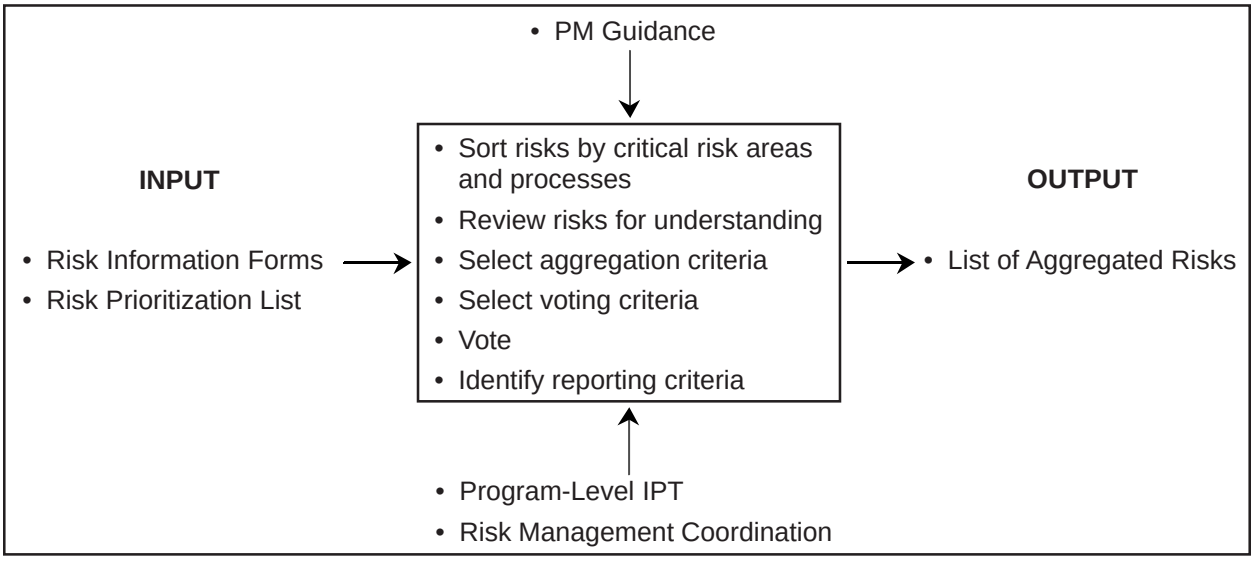


Figure 5-13. Risk Aggregation Technique Input and Output

Downloaded from http://www.everyspec.com

grouped according to critical risk areas and processes, and listed in priority sequence.

Within each area and process, the individual risks are evaluated against a set of established criteria to determine the overall aggregate risk rating for the area/process. Aggregation criteria needs to be established separately for P_F and C_F; P_F and C_F should not be combined into a single index, e.g., moderate risk. Examples of aggregation criteria include: (1) most undesirable P_F and C_F of all the risks within a risk area or process becomes the aggregated values for the area or process, or (2) the P_F and C_F for each area or process represents the mean value for that area or process.

The team then votes on each risk area and process to determine its rating for P_F and C_F, and the results are documented. In addition to the P_F and C_F ratings for each critical risk area and process, those risks that tend to "drive" the aggregate risk rating for the area/process should be included in a list of aggregated risks to give substance to the aggregated ratings, e.g., all risks in which either P_F or C_F are rated as high. Figure 5-14 provides a sample list of aggregated risks.

PROGRAM XY RISK STATUS

Risk Area Status: Design P_F: Hi C_F: Hi

Significant Design Risks:

1. Risk Title: Aircraft Weight P_F: Hi C_F: Hi

   Problem: Exceed aircraft weight budget by 10%. Decrease range-payload by 4%.

   Action: Developing risk-handling plan. User reviewing requirements.

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

Significant Logistics Risks: etc.

Figure 5-14. Sample of a List of Prioritized Risks

Risk Matrix is a software tool that is designed to aid in managing the identification, rating, and prioritization of key risks that might affect a project. It provides a structured method for prioritizing project risks and for tracking the status and effects of risk-handling efforts. The major feature that Risk Matrix offers the program office is a means to both rate and rank program risks. This is helpful in differentiating among risks that have the same rating. For example, if a program has eight risks that the program office has evaluated/rated as high, Risk Matrix provides the means to rank them in order of severity. The user can use this ranking as a guide to help focus risk-handling efforts. Risk Matrix was developed by the Air Force Electronic Systems Center (ESC) and The Mitre Corporation and is available to program offices free of charge. Another useful software tool to use in voting on risks is "Expert Choice"-based on the Analytical Hierarchy Process (AHP). Whatever software tool is used, the analyst should recognize that a number of inherent limitation exist with such software tools, (e.g. uninterested: on all of basing the voting process) that can lead to erroneous results.

5.6 RISK-HANDLING TECHNIQUES

5.6.1 General (e.g. Moderate and High Risk-Rated Items)

After the program's risks have been assessed, the PM must develop approaches to handle significant ones by analyzing various handling techniques and selecting those best fitted to the program's circumstances. The PM should reflect these approaches in the program's acquisition strategy and include the specifics on what is to be done to deal with the risk, when it should be accomplished, who is responsible, and the cost and schedule impact.

Downloaded from http://www.everyspec.com

As described in Chapter 2, there are essentially four risk-handling techniques, or options. *Risk avoidance* eliminates the sources of high risk and replaces them with a lower-risk solution. *Risk transfer* is the reallocation of risk from one part of the system to another, or the reallocation of risks between the Government and the prime contractor or within Government agencies. *Risk control* manages the risk in a manner that reduces the likelihood of its occurrence and / or minimizes the risk's effect on the program. *Risk assumption* is the acknowledgment of the existence of a particular risk situation and a conscious decision to accept the associated level of risk without engaging in any special efforts to control it. There is a tendency on many programs to select "control" as the risk-handling option without seriously evaluating assumption, avoidance, and transfer. There is a tendency on many programs to select "control" as the risk-handling option without seriously evaluating assumptions, avoidance, and transfer. This is unwise, since control may not be the best option, or even appropriate option in some cases. An unbiased assessment of risk-handling options should be performed to determine the most appropriate option.

In determining the "best" overall risk-handling strategy and specific techniques to be adopted, the following general procedures apply.

For each evaluated event risk, all potentially applicable techniques should be identified and evaluated, using the following criteria:

- **Feasibility**—Feasibility is the ability to implement the handling technique and includes an evaluation of the potential impact of the technique in the following areas:

  - Technical considerations, such as testing, manufacturing, and maintainability, caused by design changes resulting from risk-handling techniques.

  - Adequacy of budget and schedule flexibility to apply the technique.

  - Operational issues such as usability (man-machine interfaces), transportability, and mobility.

  - Organizational and resource considerations, e.g., manpower, training, and structure.

  - Environmental issues, such as the use of hazardous materials to reduce technical risk.

  - External considerations beyond the immediate scope of the program, such as the impact on other complementary systems or organizations.

- **Cost and schedule implications**—The risk-handling techniques have a broad range of cost implications in terms of dollars, as well as other limited resources, e.g., critical materials and national test facilities. The magnitude of the cost and schedule implications will depend on circumstances and can be assessed using such techniques as cost-benefit analyses and the cost and schedule assessment techniques previously described. The approval and funding of risk-handling techniques should be part of the trade-off process that establishes and refines the CAIV cost and performance goals.

- **Effect on the system's technical performance**—The risk-handling techniques may affect the system's capability to achieve the required technical performance objectives. This impact must be

Downloaded from http://www.everyspec.com

clearly understood before adopting a specific technique. As the risk-handling techniques are assessed, the PMO should attempt to identify any additional parameters that may become critical to technical performance as a result of implementing them. Trade studies and sensitivity analyses can be useful in determining the expected effectiveness of this approach.

Once the risk-handling technique is selected, a set of program management indicators should be developed to provide feedback on program progress, effectiveness of the risk-handling options selected, and information necessary to manage the program. These indicators should consist of cost and scheduling data, technical performance measures, and program metrics.

Subsequent paragraphs in this section describe the various risk-handling techniques cited above.

5.6.2 Risk Control

5.6.2.1 Description. In this risk-handling technique, the Government and contractor take active steps to reduce the likelihood of a risk event occurring and to reduce the potential impact on the program. Most risk-control steps share two features: they require a commitment of program resources, and they may require additional time to accomplish them. Thus, the selection of risk-control actions will undoubtedly require some tradeoff between resources and the expected benefit of the actions. Some of the many risk-control actions include the following:

Multiple Development Efforts—The use of two or more independent design teams (usually two separate contractors, although it could also be done internally) to create competing systems in parallel that meet the same performance requirements.

Alternative Design—Sometimes, a design option may include several risky approaches, of which one or more must come to fruition to meet system requirements. However, if the PMO studies the risky approaches, it may be possible to discover a lower-risk approach (with a lower performance capability). These lower-risk approaches could be used as backups for those cases where the primary approach(es) fail to mature in time. This option presumes there is some trading room among requirements. Close coordination between the developer and the user is necessary to implement lower capability options.

Trade Studies—Systems engineering decision analysis methods include trade studies to solve a complex design problem. The purpose of the trade studies is to integrate and balance all engineering requirements in the design of a system. A properly done trade study considers risks associated with alternatives.

Early Prototyping—The nature of a risk can be evaluated by a prototype of a system (or its critical elements) built and tested early in the system development. The results of the prototype can be factored into the design and manufacturing process requirements. In addition to full-up systems, prototyping is very useful in software development and in determining a system's man-machine interface needs. The key to making prototyping successful as a risk-control tool is to minimize the addition of new requirements to the system after the prototype has been tested (i.e., requirement changes not derived from experience with the prototype). Also, the temptation to use the prototype design and software without doing the necessary follow-on design and coding / manufacturing analyses should be avoided.

Downloaded from http://www.everyspec.com

Incremental Development—Incremental development is completion of the system design and deployment in steps, relying on pre-planned product improvements (P^3I) or software improvements after the system is deployed to achieve the final system capability. Usually, these added capabilities are not included originally because of the high risk that they will not be ready along with the remainder of the system. Hence, development is split, with the high-risk portion given more time to mature. The basic system, however, incorporates the provisions necessary to include the add-on capabilities. Incremenal development of the initial system requirements are achieved by the basic system.

Technology Maturation Efforts—Technology maturation is an off-line development effort to bring an element of technology to the necessary level so that it can be successfully incorporated into the system (usually done as part of the technology transition process). Normally, technology maturation is used when the desired technology will replace an existing technology, which is available for use in the system. In those cases, technology maturation efforts However, it can also be used when a critical, but immature, technology is needed. In addition to dedicated efforts conducted by the PMO, Service or DoD-wide technology improvement programs and advanced technology demonstrations by Government laboratories as well as industry should be considered.

Robust Design—This approach uses advanced design and manufacturing techniques that promote achieving quality through design. It normally results in products with little sensitivity to variations in the manufacturing process.

Reviews, Walk Throughs, and Inspections —These three risk control actions can be used to reduce the likelihood and potential consequences of risks through timely assessments of actual or planned events in the development of the product. They vary in the degree of formality, level of participants, and timing.

Reviews are formal sessions held to assess the status of the program, the adequacy and sufficiency of completed events, and the intentions and consistency of future events. Reviews are usually held at the completion of a program phase, when significant products are available. The team conducting the review should have a set of objectives and specific issues to be addressed. The results should be documented in the form of action items to be implemented by the PMO or contractor. The type of review will dictate the composition of the review team, which may include developers, users, managers, and outside experts.

A walk through is a technique that can be very useful in assessing the progress in the development of high or moderate risk components, especially software modules. It is less formal than a review, but no less rigorous. The person responsible for the development of the component "walks through" the product development (to include perceptions of what is to be done, how it will be accomplished, and the schedule) with a team of subject-matter experts. The team reviews and evaluates the progress and plans for developing the product and provides immediate and less formal feedback to the responsible person, thus enabling improvements or corrective actions to be made while the product is still under development. This technique is applied during the development phases, as opposed to reviews, which are normally held at the completion of a phase or product.

Downloaded from http://www.everyspec.com

Inspections are conducted to evaluate the correctness of the product under development in terms of its design, implementation, test plans, and test results. They are more formal and rigorous than either reviews or walk throughs and are conducted by a team of experts following a very focused set of questions concerning all aspects of the product.

Design of Experiments—This is an engineering tool that identifies critical design factors that are difficult to meet.

Open Systems—This approach involves the use of widely accepted commercial specifications and standards for selected system interfaces, products, practices, and tools. It provides the basis for reduced life-cycle costs, improved performance, and enhanced interoperability, especially for long life systems with short-life technologies. Properly selected and applied commercial specifications and standards can result in lower risk through increased design flexibility; reduced design time; more predictable performance; and easier product integration, support, and upgrade. However, a number of challenges and risks are associated with the use of the open systems approach and must be considered before implementation. These include such issues as: maturity and acceptability of the standard, and its adequacy for military use; the loss of control over the development of products used in the system; the amount of product testing done to ensure conformance to standards; and the higher configuration management workload required.

See *Deskbook* Section 1.2.2.2.5 for a more detailed discussion of the use of open systems. (Additional information is also available at the Open Systems Joint Task Force Website at www.acq.osd.mil/osjtf/.)

Use of Standard Items/Software Reuse—The use of standard items and software module reuse should be emphasized to the extent possible to minimize development risk. Standard items range from components and assemblies to full-up systems. A careful examination of the proposed system option will often find more opportunities for the use of standard items or existing software modules than first considered. Even when the system must achieve previously unprecedented requirements, standard items can find uses. A strong program policy emphasizing the use of standard items and software reuse is often the key to taking advantage of this source of risk control. Standard items and software modules have proven characteristics that can reduce risk. However, the PMO must be cautious when using standard items in environments and applications for which they were not designed. A misapplied standard item often leads to problems and failure. Similarly, if the cycle for a fielded product extends for many years, it is possible that key software tools and products will become obsolete or will no longer be supported. If this occurs, costly redesign may result if software redevelopment is necessary.

Two-Phase EMD—This risk control approach incorporates a formal risk-reduction effort in the initial part of the EMD phase. It may involve using two or more contractors with a down-select occurring at a predefined time (normally after the preliminary design review). A logical extension of this concept is the "spiral" development model, which emphasizes the evaluation of alternatives and risk assessments throughout the system's development and initial fielding.

Use of Mockups—The use of mockups, especially man-machine interface mock-ups, can be used to conduct early exploration

Downloaded from http://www.everyspec.com

of design options. They can assist in resolving design uncertainties and providing users with early views of the final system configuration.

Modeling/Simulation—The use of modeling and simulation can provide insights into a system's performance and effectiveness sensitivities. Decision makers can use performance predictions to assess a system's military worth not only before any physical prototypes are built, but also throughout the system life cycle.

Modeling and simulation can help manage risk by providing information on design capabilities and failure modes during the early stages of design. This allows initial design concepts to be iterated without having to build hardware for testing. The T&E community can use predictive simulations to focus the use of valuable test assets on critical test issues. They can also use extrapolated simulations to expand the scope of evaluation into areas not readily testable, thus reducing the risk of having the system fail in the outer edges of the "test envelope." Additionally, a model can serve as a framework to bridge the missing pieces of a complete system until those pieces become available.

Although modeling and simulation can be a very effective risk-handling tool, it requires resources, commitment to refine models as the system under development matures, and a concerted verification and validation effort to ensure that decisions are based on credible information.

Key Parameter Control Boards—When a particular parameter (such as system weight) is crucial to achieving the overall program requirements, a control board for that parameter may be appropriate. This board has representatives from all affected technical functions and may be chaired by the PM. It provides management focus on the parameter and signals the importance of achieving the parameter to the technical community. If staffed properly by all affected disciplines, it can also help avoid sacrificing other program requirements to achieve that requirement.

Manufacturing Screening—For programs in engineering, manufacture, and development (EMD), various manufacturing screens (including environmental stress screening (ESS)) can be incorporated into test article production and low-rate initial production to identify deficient manufacturing processes. ESS is a manufacturing process for stimulating parts and workmanship defects in electronic assemblies and units. These data can then be used to develop the appropriate corrective actions.

5.6.2.2 Procedures. Risk control involves developing a risk-reduction plan, with actions identified, resourced, and scheduled. Success criteria for each of the risk-reduction events should also be identified. The effectiveness of these actions must be monitored using the types of techniques described in Section 5.7.

5.6.3 Risk Avoidance

5.6.3.1 Description. This technique reduces risk through the modification or elimination of those operational requirements, processes or activities that cause the risks. Eliminating operational requirements requires close coordination with the users. Since this technique results in the reduction of risk, it should generally be initiated in the development of a risk-handling plan. It can be done in parallel with the initial operational requirements analysis and should be supported by a cost-benefit analysis.

Downloaded from http://www.everyspec.com

5.6.3.2 Procedures. Analyzing and reviewing the proposed system in detail with the user is essential to determine the drivers for each operational requirement. Operational requirements scrubbing involves eliminating those that have no strong basis. This also provides the PMO and the user with an understanding of what the real needs are and allows them to establish accurate system requirements for the critical performance. Operational requirements scrubbing essentially consists of developing answers to the following questions:

- Why is the requirement needed?
- What will the requirement provide?
- How will the capability be used?
- Are the requirements specified in terms of functions and capabilities, rather than a specific design?

Cost/requirement trade studies are used to support operational requirements scrubbing. These trades examine each requirement and determine the cost to achieve various levels of the requirement (e.g., different airspeeds, range, payloads). The results are then used to determine, with the user, whether a particular requirement level is worth the cost of achieving that level. Trade studies are an inherent part of the systems engineering process. (See *Deskbook* 2.6.1 for details on systems engineering process.)

5.6.4 Risk Assumption

5.6.4.1 Description. This technique is used in every program and acknowledges the fact that, in any program, risks exist that will have to be accepted without any special effort to control them. Such risks may be either inherent in the program or may result from other risk-controlling actions (residual risks). The fact that risks are assumed does not mean that they are ignored. In fact, every effort should be made to identify and understand them so that appropriate management action can be planned. Also, risks that are assumed should be monitored during development; this monitoring should be well-planned from the beginning.

5.6.4.2 Procedures. In addition to the identification of risks to be assumed, the following steps are key to successful risk assumption:

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it materializes. This includes identifying the specific management actions that will be used, for example, redesign, retesting, requirements review, etc.

- Whenever a risk is assumed, a schedule and cost risk reserve should be set aside to cover the specific actions to be taken if the risk occurs. If this is not possible, the program may proceed within the funds and schedule allotted to the effort. If the program cannot achieve its objectives, a decision must be made to allocate additional resources, accept a lower level of capability (lower the requirements), or cancel the effort.

- Ensure that the necessary administrative actions are taken to quickly report on the risk event and implement these management actions, such as contracts for industry expert consultants, arrangements for test facilities, etc., and report on occurrences of the risk event.

5.6.5 Risk Transfer

5.6.5.1 Description. This technique involves the reduction of risk exposure by the reallocation of risk from one part of the

Downloaded from http://www.everyspec.com

system to another or the reallocation of risks between the Government and the prime contractor, or between the prime contractor and its sub-contractor.

5.6.5.2 Procedures. In reallocating risk, design requirements that are risk drivers are transferred to other system elements, which may result in lower system risk but still meet system requirements. For example, a high risk caused by a system timing requirement may be lowered by transferring that requirement from a software module to a specially designed hardware module capable of meeting those needs. The effectiveness of requirements reallocation depends on good system engineering and design techniques. In fact, efficient allocation of those requirements that are risk drivers is an integral part of the systems engineering process. Modularity and functional partitioning are two design techniques that can be used to support this type of risk transfer. In some cases, this approach may be used to concentrate risk areas in one area of the system design. This allows management to focus attention and resources on that area.

For the Government / contractor risk-transfer approach to be effective, the risks transferred to the contractor must be those that the contractor has the capacity to control and manage. These are generally risks associated with technologies and processes used in the program—those for which the contractor can implement proactive solutions. The types of risks that are best managed by the Government include those related to the stability of and external influences on program requirements, funding, and schedule, for example. The contractor can support the management of these risks through the development of flexible program plans, and the incorporation of performance margins in the system and flexibility in the schedule. A number of options are available to implement risk transfer from the Government to the contractor: warranties, cost incentives, product performance incentives, and various types of fixed price contracts. A similar assessment of prime contractor versus sub-contractor allocation of risks can also be developed and used to guide risk transfer between these parties.

5.7 RISK MONITORING

5.7.1 General

Risk monitoring is a continuous process to systematically track and evaluate the performance of risk-handling actions against established metrics throughout the acquisition process. It should also include results of periodic reassessments of program risk to evaluate both known and new risks to the program. If necessary, the PMO should reexamine the risk-handling approaches for effectiveness while conducting assessments. As the program progresses, the monitoring process will identify the need for additional risk-handling options.

An effective monitoring effort provides information to show if handling actions are not working and which risks are on their way to becoming actual problems. The information should be available in sufficient time for the PMO to take corrective action. The functioning of IPTs is crucial to effective risk monitoring. They are the “front line” for obtaining indications that handling efforts are achieving their desired effects.

The establishment of a management indicator system that provides accurate, timely, and relevant risk information in a clear, easily understood manner is key to risk monitoring. Early in the planning phase of the process, PMOs should identify specific indicators to be monitored and information

Downloaded from http://www.everyspec.com

to be collected, compiled, and reported. Usually, documentation and reporting procedures are developed as part of risk management planning before contract award and should use the contractor's reporting system. Specific procedures and details for risk reporting should be included in the risk management plans prepared by the Government and the contractor.

To ensure that significant risks are effectively monitored, handling actions (which include specific events, schedules, and "success" criteria) developed during previous risk management phases should be reflected in integrated program planning and scheduling. Identifying these handling actions and events in the context of WBS elements establishes a linkage between them and specific work packages, making it easier to determine the impact of actions on cost, schedule, and performance. The detailed information on risk-handling actions and events should be contained in various risk management documentation (both formal and informal). Experience has shown that the use of an electronic on-line database that stores and permits retrieval of risk-related information is almost essential to effective risk monitoring. The database selected or developed will depend on the program. A discussion of risk management information systems and databases and suggested data elements to be included in the databases is contained later in this chapter.

Many techniques and tools are available for monitoring the effectiveness of risk-handling actions, and PMO personnel should select those that best suit their needs. Some monitoring techniques include:

Test-Analyze-And-Fix (TAAF)—TAAF is the use of a period of dedicated testing to identify and correct deficiencies in a design. It was originally conceived as an approach to improve reliability; it can also be used for any system parameter whose development could benefit from a dedicated period of testing and analysis. Although a valuable aid in the development process, TAAF should not be used in lieu of a sound design process.

Demonstration Events—Demonstration events are points in the program (usually tests) that are used to determine if risks are being successfully abated. Careful review of the planned development of each risk area will reveal a number of opportunities to verify the effectiveness of the development approach. By including a sequence of demonstration events throughout the development, PMO and contractor personnel can monitor the process and identify when additional efforts are needed. Demonstration events can also be used as information-gathering actions, as discussed before, and as part of the risk-monitoring process. Table 5-2 contains examples of demonstration events.

Process Proofing—When particular processes, especially those of manufacturing and support, are critical to achieving system requirements, an early process proof demonstration is useful to abate risk. If the initial proof is unsuccessful, time is still available to identify and correct deficiencies or to select an alternative approach.

No single technique or tool is capable of providing a complete answer—a combination must be used. In general, risk monitoring techniques are applied to follow through on the planned actions of the risk-handling program. They track and evaluate the effectiveness of handling activities by comparing planned actions with what is actually achieved. These comparisons may be as straightforward as actual versus planned

Downloaded from http://www.everyspec.com

ITEM	DEMONSTRATION EVENT	COMPLETION DATE
Rocket Motor	Three Case Burst Tests Propellant Characterization Thermal Barrier Bond Tests Ignition and Safe/Arm Tests Nozzle Assembly Tests	By completion of preliminary design
	10 Development Motor Firings — Temperature and Altitude Cycle — Vibration and Shock — Aging	By completion of final design
Central Computer	Test Breadboard Develop/Test Unique Microcircuits	By completion of preliminary design
	Build/Test Prototype	By completion of final design

Table 5-2. Examples of Demonstration Events

completion dates, or as complex as detailed analysis of observed data versus planned profiles. In any case, the differences between planned and actual data are examined to determine status and the need for any changes in the risk-handling approach.

PMO personnel should also ensure that the indicators / metrics selected to monitor program status adequately portray the true state of the risk events and handling actions. Otherwise, indicators of risks that are about to become problems will go undetected. Subsequent sections identify specific techniques and tools that will be useful to PMOs in monitoring risks and provide information on selecting metrics that are essential to the monitoring effort. The techniques focus primarily at the program level, addressing cost, schedule, and performance risks.

5.7.2 Earned Value Management

5.7.2.1 Description. Earned value (EV) is a management technique that relates resource planning to schedules and to technical performance requirements. It is useful in monitoring the effectiveness of risk-handling actions in that it provides periodic comparisons of the actual work accomplished in terms of cost and schedule with the work planned and budgeted. These comparisons are made using a performance baseline that is established by the contractor and the PM at the beginning of the contract period. This is accomplished through the Integrated Baseline Review (IBR) process. The baseline must capture the entire technical scope of the program in detailed work packages. The baseline also includes the schedule to meet the requirements as well as the resources to be applied to each work package. Specific risk-handling actions should be included in these packages. See *Deskbook* Section 2.B.2.1 for a more detailed discussion of Earned Value and IBR.

5.7.2.2 Procedures. The periodic EV data can provide indications of risk and the effectiveness of handling actions. When variances in cost or schedule begin to appear in work packages containing risk-handling

Downloaded from http://www.everyspec.com

actions, or in any work package, the appropriate IPTs can analyze the data to isolate causes of the variances and gain insights into the need to modify or create handling actions.

5.7.3 Technical Performance Measurement

5.7.3.1 Description. Technical performance measurement (TPM) is a technique that compares estimated values of key performance parameters with achieved values, and determines the impact of any differences on system effectiveness. This technique can be useful in risk monitoring by comparing planned and achieved values of parameters in areas of known risk. The periodic application of this technique can provide early and continuing predictions of the effectiveness of risk-handling actions or the detection of new risks before irrevocable impacts on the cost or schedule occur.

5.7.3.2 Procedures. The technical performance parameters selected should be those that are indicators of progress in the risk-handling action employed. They can be related to system hardware, software, human factors, and logistics—any product or functional area of the system. Parameter values to be achieved through the planned handling action are forecast in the form of planned performance profiles. Achieved values for these parameters are compared with the expected values from the profile, and any differences are analyzed to get an indication of the effectiveness of the handling action. For example, suppose a system requires the use of a specific technology that is not yet mature and the use of which has been assessed as high risk. The handling technique selected is risk control, and an off-line technology maturation effort will be used to get the technology to the level where the risk is acceptable. The technology is analyzed to identify those parameters that are key drivers, and performance profiles that will result from a sufficiently mature technology are established. As the maturation effort progresses, the achieved values of these parameters are compared with the planned profile. If the achieved values meet the planned profile, it is an indicator that the risk-handling approach is progressing satisfactorily; if the achieved values fall short of the expected values, it is an indicator that the approach is failing to meet expectations and corrective action may be warranted.

5.7.4 Integrated Planning and Scheduling

5.7.4.1 Description. Once a contract has been awarded, techniques such as integrated planning and scheduling (integrated master plans and integrated master schedules) can become invaluable program baseline and risk-monitoring tools. Integrated planning identifies key events, milestones, reviews, all integrated technical tasks, and risk-reduction actions for the program, along with accomplishment criteria to provide a definitive measure that the required maturity or progress has been achieved. Integrated scheduling describes the detailed tasks that support the significant activities identified in integrated planning and timing of tasks. Also, the integrated schedule can include the resources planned to complete the tasks. The events, tasks, and schedule resulting from integrated planning are linked with contract specification requirements, WBS, and other techniques such as TPM. When the events and tasks are related to risk-reduction actions, this linkage provides a significant monitoring tool, giving specific insights into the relationships among cost, schedule, and performance risks.

Downloaded from http://www.everyspec.com

5.7.4.2 Procedures. In integrated planning, the Government and contractor (or other performing activity) should identify key activities of the program, to include risk-handling actions and success criteria. The contractor should then prepare the integrated schedule reflecting the planned completion of tasks associated with these activities. As the program progresses, the PMO can monitor effectiveness of handling activities included in the integrated planning events and schedule by comparing observed activity results with their criteria and determining any deviations from the planned schedule. Any failures of handling actions to meet either the event criteria or schedule should be analyzed to determine the deviation's impact, causes, and need for any modifications to the risk-handling approach.

5.7.5 Watch List

5.7.5.1 Description. The watch list is a listing of critical areas which management should pay special attention to during program execution. It is a straightforward, easily prepared document that can range in complexity from a simple list of the identified risks to one that includes such things as the priority of the risk, how long it has been on the watch list, the handling actions, planned and actual completion dates for handling actions, and explanations for any differences. See Table 5-3 for an example watch list.

5.7.5.2 Procedures. Watch list development is based on the results of the risk assessment. It is common to keep the number of risks on the watch list relatively

Potential Risk Area	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
• Accurately predicting shock environment shipboard equipment will experience.	• Use multiple finite element codes & simplified numerical models for early assessments.	SEA 03P31	31 Aug 98		
	• Shock test simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SEA 03P31	31 Aug 99		
• Evaluating acoustic impact of the ship systems that are not similar to previous designs.	• Concentrate on acoustic modeling and scale testing of technologies not demonstrated successfully in large-scale tests or full-scale tests.	SEA 03TC	31 Aug 98		
	• Factor acoustic signature mitigation from isolated modular decks into system requirements. Continue model tests to validate predictions for isolated decks.	SEA 03TC	31 Aug 99		

Table 5-3. Watch List Example

Downloaded from http://www.everyspec.com

small, focusing on those that can have the greatest impact on the program. Items can be added as the program unfolds and periodic reassessments are conducted. If a considerable number of new risks are significant enough to be added to the watch list, it may be an indicator that the original assessment was not accurate and that program risk is greater than initially thought. It may also indicate that the program is on the verge of becoming out of control. If a risk has been on the watch list for a long time because of a lack of risk-handling progress, a reassessment of the risk or the handling approach may be necessary. Items on the watch list should be reviewed during the various program reviews/meetings, both formal and informal.

5.7.6 Reports

5.7.6.1 Description. Reports are used to convey information to decision makers and program team members on the status of risks and the effectiveness of risk-handling actions. Risk-related reports can be presented in a variety of ways, ranging from informal verbal reports when time is of the essence to formal summary-type reports presented at milestone reviews. The level of detail presented will depend on the audience.

5.7.6.2 Procedures. Successful risk management programs include timely reporting of results of the monitoring process. Reporting requirements and procedures, to include format and frequency, are normally developed as part of risk management planning and are documented in the risk management plan. Reports are normally prepared and presented as part of routine program management activities. They can be effectively incorporated into program management reviews and technical

Risk Management Status

Risk Plan #	Risk Issue	High	Moderate	Low	Status/Comment
94-12-9	Non-stock Listed Spares		●		Data still in review; need to assign part numbers.
94-12-10	Engineering Updates		→	Closed	Data reviewed; updates not required at this time.
94-12-11	Spares & Support		→	Closed	
94-12-12	Long Lead Requisitions		●		Spares listing approved in definitization conference. No current abatement plan.
94-12-13	T.O. Validation		→	Closed	Closed Issue.
94-12-14	**Lack of LSA Records for GFE**		●		**Contractor LSA plan submitted for approval; rescheduled for 5/95.**
94-12-15	Program Parts Obsolescence		→	●	Analysis in work, identifying last opportunity buys.
94-12-51	Design Maturity		→	Closed	Studying Commercial Mix Interface.
94-12-16	System Y Interface Definition		←		Questions about antenna location and cable raised risk.

Figure 5-15. Example Showing Detailed List of Top-Level Risk Information

Downloaded from http://www.everyspec.com

milestones to indicate any technical, schedule, and cost barriers to the program objectives and milestones being met. One example of a status presentation is shown in Figure 5-15. It shows some top-level risk information that can be useful to the PMO as well as others external to the program.

Although this level of reporting can provide quick review of overall risk status for identified problems, more detailed risk planning and status can be provided on individual risk items. For example, some program IPTs have combined risk level and scheduled activities to provide a graphical overview of risk status for either internal or external review. One method for graphically showing risk status for an individual item is shown in Figure 5-16.

5.7.7 Management Indicator System

5.7.7.1 Description. A management indicator system is a set of indicators or metrics that provide the PMO with timely information on the status of the program and risk-handling actions, and is essential to risk monitoring and program success. To be meaningful, these metrics should have some objective value against which observed data can be measured, reflecting trends in the program or lack thereof. Metrics should be developed jointly by the PMO and the contractor. The contractor's approach to metrics should be a consideration in the proposal evaluation process. If the contractor does not have an established set of metrics, this may be an area of risk that will need to be addressed.

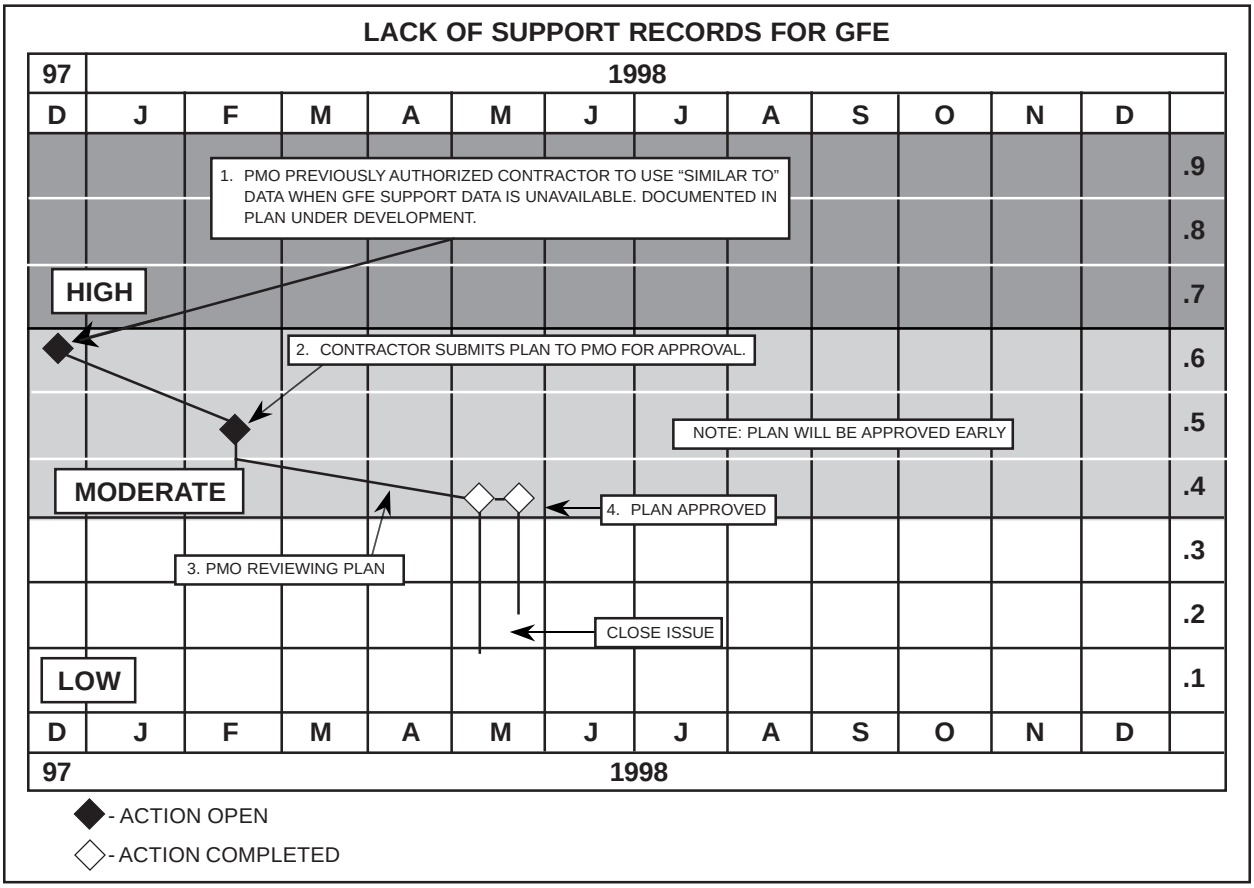


Figure 5-16. Example of More Complex Combination of Risk Level and Scheduled Tasks

Downloaded from http://www.everyspec.com

5.7.7.2 Procedures. Metrics can be categorized as relating to technical performance, cost, and schedule. Technical performance metrics can be further broken down into categories such as engineering, production, and support, and within these groups as either product- or process-related. Product-related metrics pertain to characteristics of the system being developed; they can include such things as planned and demonstrated values of the critical parameters monitored as part of the TPM process and system-unique data pertaining to the different steps in the development and acquisition processes. Table 5-4 provides examples of product-related metrics.

Process metrics pertain to the various processes used in the development and production of the system. For each program, certain processes are critical to the achievement of program objectives. Failure of these processes to achieve their requirements is symptomatic of significant problems. Metrics data can be used to diagnose and aid in problem resolution. They should be used in formal, periodic performance assessments of the various development processes and to evaluate how well the system development process is achieving its objectives. DoD 4245.7M, Transition from Development to Production, and other supporting documents such as NAVSO P-6071, Best Practices, identify seven process areas: funding, design, test, production, facilities, logistics, and management. Within each of these areas, a number of specific processes are identified as essential to assess, monitor, and establish program risk at an acceptable level; the documents also provide risk indicators that can be used as the basis for selecting specific process metrics. Another document, *Methods and Metrics for Product Success*, July 1994, published by the Office of the Assistant Secretary of the Navy (RD&A), Product Integrity Directorate, provides a set of metrics for use in assessing and monitoring the design, test, and production risk areas. Table 5-5 provides examples of process-related metrics.

Engineering	Requirements	Production	Support
Key Design Parameters Weight Size Endurance Range Design Maturity Open problems reports Number of engineering change proposals Number of drawings released Failure activities Computer Resource Utilization	Requirements Traceability Requirements Stability	Manufacturing Yields Incoming Material Yields Delinquent Requisitions Unit Production Cost Process Proofing	Special Tools and Test Equipment Support Infrastructure Footprint Manpower Estimates

Table 5-4. Examples of Product-Related Metrics

Downloaded from http://www.everyspec.com

Cost and schedule metrics can be used to depict how the program is progressing toward completion. The information provided by the contractor in the earned value management system can serve as these metrics, showing how the actual work accomplished compares with the work planned in terms of schedule and cost. Other sources of cost and schedule metrics include the contractor's cost accounting information and the integrated master schedule. Table 5-6 provides examples of cost and schedule metrics.

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

Table 5-6. Examples of Cost and Schedule Metrics

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

Table 5-5. Examples of Process Metrics

Downloaded from http://www.everyspec.com

5.8 RISK MANAGEMENT INFORMATION SYSTEMS AND DOCUMENTATION

5.8.1 Description

To manage risk, PMs should have a database management system that stores and allows retrieval of risk-related data. The risk-management information system provides data for creating reports and serves as the repository for all current and historical information related to risk. This information may include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The PM should consider a number of factors in establishing the management information system and developing rules and procedures for the reporting system:

- Assign management responsibility for the reporting system
- Publish any restrictions for entering data into the database
- Identify reports and establish a schedule, if appropriate
- Use standard report formats as much as possible
- Ensure that the standard report formats support all users, such as the PM, IPTs, and IIPTs
- Establish policy concerning access to the reporting system and protect the database from unauthorized access.

With a well-structured information system, a PMO may create reports for senior management and retrieve data for day-to-day program management. Most likely, the PM will choose a set of standard reports that suits specific needs on a periodic basis. This eases definition of the contents and structure of the database. In addition to standard reports, the PMO will need to create ad hoc reports in response to special queries, etc. Commercial database programs now available allow the PMO to create reports with relative ease. Figure 5-17 shows a concept for a management and reporting system.

5.8.2 Risk Management Reports

The following are examples of basic reports that a PMO may use to manage its risk program. Each office should tailor and amplify them, if necessary, to meet specific needs.

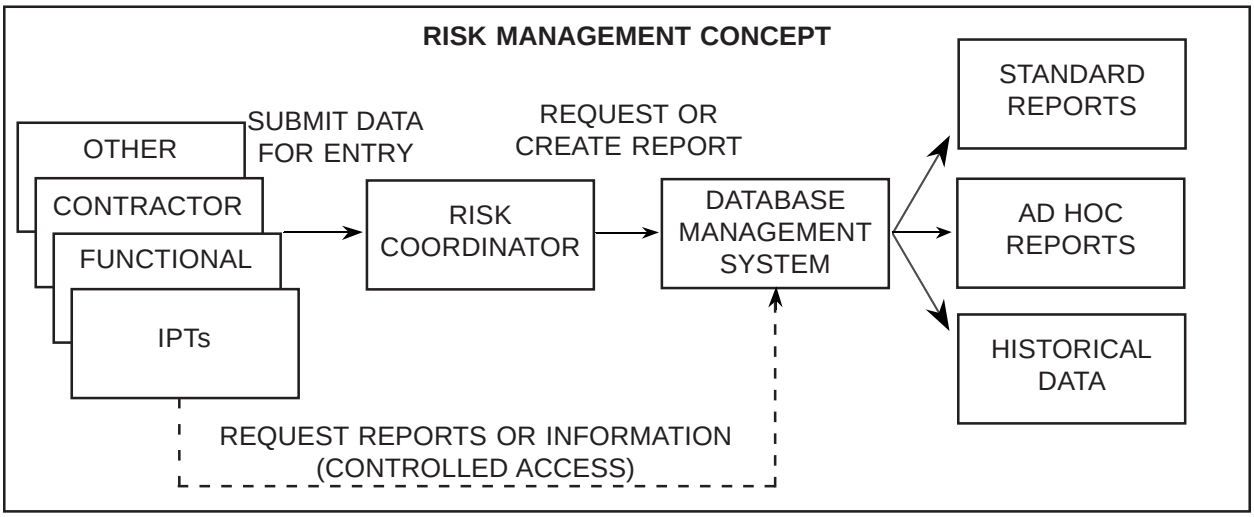


Figure 5-17. Conceptual Risk Management and Reporting System

Downloaded from http://www.everyspec.com

Risk Information Form. The PMO needs a document that serves the dual purpose of a *source* of data entry information and a *report* of basic information for the IPTs. The RIF serves this purpose. It gives members of the project team, both Government and contractors, a format for reporting risk-related information. The RIF should be used when a potential risk event is identified and updated over time as information becomes available and the status changes. As a source of data entry, the RIF allows the database administrator to control entries. To construct the database and ensure the integrity of data, the PMO should design a standard format for a RIF.

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

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

Risk Monitoring Documentation. The PM needs a summary document that tracks the status of high and moderate risks. He can produce a risk-tracking list, for example, that uses information that has been entered from the RIF. Each PMO should tailor the tracking list to suit its needs. If elements of needed information are not included in the RIF, they should be added to that document to ensure entry into the database.

Database Management System (DBMS). The DBMS that the PM chooses may be commercial, Government-owned, or contractor-developed. It should provide the means to enter and access data, control access, and create reports. Many options are available to users.

Key to the MIS are the data elements that reside in the database. The items listed in Table 5-7 are examples of risk information that might be included in a database that supports risk management. They are a compilation of several risk reporting forms used in current DoD programs and other risk document sources. “Element” is the title of the database field; “Description” is a summary of the field contents. PMs should tailor the list to suit their needs.

5.9 SOFTWARE RISK MANAGEMENT METHODOLOGIES

The management of risk in software intensive programs is essentially the same as for any other type of program. A number of methodologies specifically focus on the

Downloaded from http://www.everyspec.com

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PMO. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PMO compared to all other risks, e.g., a one (1) indicates the highest priority.
Data Submitted	Gives the date that the RIF was submitted.
Major System/ Component	Identifies the major system/component based on the WBS.
Subsystem/ Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) or the risk.
Description of Risk	Briefly describes the risk. Lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, includes how it is manifested (e.g., design and engineering, manufacturing, etc.)
Key Parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report, if appropriate.
Analyses	Briefly describes the analysis done to assess the risk. Includes rationale and basis for results.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's Risk Management Plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the program's Risk Management Plan.
Time Sensitivity	Estimates the relative urgency for implementing the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measures using metrics for tracking progress in implementing risk-handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk handling milestones.
Status Due Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

Table 5-7. Database Management System Elements

Downloaded from http://www.everyspec.com

software aspects of developmental programs and can be useful in identifying and analyzing risks associated with software. Several of these methodologies are described in the U.S. Air Force publication, *Guide to Software Acquisition and Management*. Three of these methodologies are described below.

5.9.1 Software Risk Evaluation (SRE)

This is a formal approach developed by the Software Engineering Institute (SEI) using a risk management paradigm that defines a continuous set of activities to identify, communicate, and resolve software risks. These activities are to identify, analyze, plan, track, and control. (The SEI activities are analogous to the activities of the risk management process defined in this section.)

This methodology is initiated by the PM, who tasks an independent SRE team to conduct a risk evaluation of the contractor's software development effort. The team executes the following SRE functions in performing this evaluation, and prepares findings that will provide the PM with the results of the evaluation:

- **Detection** of the software technical risks present in the program. An SEI Taxonomy-Based Questionnaire is used to ensure that all areas of potential risk are identified. This questionnaire is based on the SEI Software Development Risk Taxonomy, which provides a systematic way of organizing and eliciting risks within a logical framework.

- **Specification** of all aspects of identified technical software risks, including their conditions, consequences, and source.

- **Assessment** of the risks to determine the probability of risk occurrence and the severity of its consequences.

- **Consolidation** of the risk data into a concise format suitable for decision making.

A detailed discussion of the SRE methodology is found in Software Engineering Institute Technical Report CMU/SEI-94-TR-19, *Software Risk Evaluation Model, Version 1.0*, December 1994.

5.9.2 Boehm's Software Risk Management

This risk management methodology, developed by Barry W. Boehm and described in IEEE Software, *Software Risk Management: Principles and Practices*, January 1991, consists of two primary steps, each with three subordinate steps. This risk management structure is shown in Table 5-8.

Boehm provides a number of techniques that can be used to accomplish each of the steps in the methodology. For example, to assist in risk identification, he includes the top 10 top-level software risks, based on surveys of experienced software project managers. These risks are shown in Table 5-9, along with recommended techniques to manage them. Using this list as a starting point, managers and engineers can then develop lists of lower level risks to be assessed and resolved.

5.9.3 Best Practices Initiative Risk Management Method

The Software Acquisition Best Practices Initiative was instituted in 1994 to improve and restructure the software acquisition management process through the identification of effective practices used in successful software developments. One result of this effort was the publication of the *Program Manager's Guide to Software Acquisition Best Practices* by the Software Program Managers Network (SPMN). This document identified nine principal best

Downloaded from http://www.everyspec.com

Primary Steps	Secondary Steps	Description
Risk Assessment	Risk Identification	- Produces lists of project specific risk events
	Risk Analysis	- Assesses probability of risk event and consequences - Assesses compound risk resulting from risk event interaction
	Risk Prioritization	- Produces rank-ordered list of identified and analyzed risk events
Risk Control	Risk Management Planning	- Produces plan for addressing each risk event - Integrates individual risk event plans with each other and the overall plan
	Risk Resolution	- Establishes the environment and actions to resolve or eliminate risks - Tracks progress in resolving risks
	Risk Monitoring	- Provides feedback for refining prioritization and plans

Table 5-8. Software Risk Management Steps

Risk	Risk Management Techniques
Personnel Shortfalls	Staffing with top talent; job matching team building; key personnel agreements; cross training
Unrealistic schedules and budgets	Detailed multisource cost and schedule estimation; design-to-cost; incremental development; software reuse; requirements scrubbing
Developing the wrong software functions	Organizational analysis; mission analysis; operations concept formulation; user surveys; prototyping; early users' manuals
Developing wrong user interface	Task analysis; prototyping; scenarios; user characterization (functionality, style, workload)
Goldplating	Requirements scrubbing; prototyping; cost/benefit analysis; design-to-cost
Continuing stream of requirements changes	High change threshold; information hiding; incremental development (defer changes to later increments)
Shortfalls in externally furnished components	Benchmarking; inspections; reference checking; compatibility analysis
Shortfalls in internally performed tasks	Reference checking; pre-award audits; award-fee contracts; competitive design or prototyping; team building
Real-time performance shortfalls	Simulation; benchmarking; modeling; prototyping; instrumentation; tuning
Straining computer science capabilities	Technical analysis; cost-benefit analysis; prototyping; reference checking

Table 5-9. Top 10 Software Risks

Downloaded from http://www.everyspec.com

Best Practices Initiative Risk Management Method		
Address the Problem	**Practice Essentials**	**Check Status**
- Recognize that all software has risk - Attempt to resolve risk as early as possible when cost impact is less than it will be later in development	- Identify risks - Decriminalize risk - Plan for risk - Formally designate a Risk Officer - Include in budget and schedule a risk reserve buffer of time, money, and other resources - Compile database for all non-negligible risks - Prepare profile for each risk showing probability and consequences - Include all risks over full life cycle - Provide frequent risk status reports that include: -- Top 10 risk items -- Number of risk items resolved -- Number of new risk items -- Number of risk items unresolved -- Unresolved risk items on critical path - Probably costs for unresolved risks	- Risk Officer appointed? - Risk databases set up? - Risk assessments have clear impact on program plans and decisions? - Frequency and timeliness of risk assessment updates consistent with decision updates? - Objective criteria used to identify, assess, and manage risk? - Information flow patterns and reward criteria support identification of risk by all program personnel? - Risks identified throughout entire life cycle? - Risk management reserve exist? - Risk profile for every risk, and components updated regularly? - Risk management plan has explicit provisions for altering decision makers when risk becomes imminent?

Table 5-10. Best Practices Initiative Risk Management Method

practices that are essential to the success of any large-scale software development. The first of these nine is formal risk management. To assist in implementing this top practice, SPMN developed a three-part methodology consisting of the following steps: address the problem; practice essentials; and check status. Specific activities associated with these steps are shown in Table 5-10.

SPMN provides PMOs with specialized training programs covering the core disciplines and techniques for implementing this formal risk management practice, as well as the other best practices. SPMN also has available (or under development) a number of guidebooks designed to provide software developers and Program Managers with practical guidance for planning, implementing, and monitoring their programs.

SPMN can be contacted at (703) 521-5231, or on the Internet at http://spmn.com/.

In addition to the studies by Barry Boehm, and information on the SPMN, a survey was conducted by Conrow and Shishido (See Reference) which evaluated 10 prior studies and categorized the resulting risk issues across the studies into six categories and 17 total issues, as shown in Table 5-11. The very high degree of overlap between risk issues identified in the 10 underlying studies suggest that some risk issues are common to many software-intensive projects.

Downloaded from http://www.everyspec.com

Risk Grouping	Software Risk Issue
Project-Level	1. Excessive, immature, unrealistic or unstable requirements 2. Lack of involvement 3. Underestimation of project complexity or dynamic natures
Project Attributes	4. Performance shortfalls (includes errors and quality) 5. Unrealistic cost or schedule (estimates and/or allocated amounts)
Management	6. Ineffective project management (possible at multiple levels)
Engineering	7. Ineffective integration, assembly and test; quality control; specialty engineering; systems engineering or (possible at multiple levels) 8. Unanticipated difficulties associated with the user interface
Work Environment	9. Immature or untried design, processes or technologies selected 10. Inadequate work plans or configuration control 11. Inappropriate methods or tool selection or inaccurate metrics
Other	12. Poor planning 13. Inadequate or excessive documentation or review process 14. Legal or contractual issues (e.g., litigation, malpractice, ownership) 15. Obsolescence (includes excessive schedule length) 16. Unanticipated difficulties with subcontracted items 17. Unanticipated maintenance and/or support costs

Table 5-11. Software Risk Grouping

Downloaded from http://www.everyspec.com

APPENDIX A

DoD RISK MANAGEMENT POLICIES AND PROCEDURES

DoD policies and procedures that address risk management for acquisition programs are contained in four key documents:

- DoD Directive (DoDD) 5000.1, Defense Acquisition
- DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs
- DoDD 5000.4, OSD Cost Analysis Improvement Group
- DoD Manual 5000.4-M, Cost Analysis Guidance and Procedures

The relevant sections of each document are referenced in the *Defense Acquisition Deskbook* under Mandatory Direction and are displayed under DoD-Wide Practices. They present some strong statements on risk management but collectively are not sufficient to enable the establishment of an effective risk management program. The following are verbatim extracts of sections of the DoD 5000 series of documents that address risk management as part of acquisition policy and procedures. The reader should be aware that changes to the 5000 series could result in different paragraph numbers. The paragraph numbers are accurate through Change 3.

1. DoDD 5000.1 Defense Acquisition, March 1996

Para D.1.a **Integrated Management Framework**

"…The acquisition management system governed by this Directive provides for a streamlined management process that emphasizes risk management and affordability and that explicitly links milestone decisions to demonstrated accomplishments…."

Para D.1.d **Risk Assessment and Management**

"PMs and other acquisition managers shall continually assess program risks. Risks must be well understood, and risk management approaches developed, before decision authorities can authorize a program to proceed into the next phase of the acquisition process. To assess and manage risk, PMs and other acquisition managers shall use a variety of techniques, including technology demonstrations, prototyping, and test and evaluation. Risk management encompasses identification, mitigation, and continuous tracking and control procedures that feed back through the program assessment process to decision authorities. To ensure an equitable and sensible allocation of risk between government and industry, PMs and other acquisition managers shall select a contracting approach appropriate to the type of system being acquired."

Para D.2.a **Event-Oriented Management**

"The Department shall use a rigorous, event-oriented management process that emphasizes effective acquisition planning, improved and continuous communications with users, and prudent risk management by both the government and industry. Event-oriented means that the management process shall be based on significant events in the acquisition life-cycle and not arbitrary calendar dates."

Downloaded from http://www.everyspec.com

Para D.2.f **Modeling and Simulation**

"Models and simulations shall be used to reduce the time, resources, and risks of the acquisition process and to increase the quality of the systems being acquired. Representations of proposed systems (virtual prototypes) shall be embedded in realistic synthetic environments to support the various phases of the acquisition process, from requirements determination and initial concept exploration to the manufacturing and testing of new systems, and related training."

Para D.3.e **Tailoring**

"…MDAs shall promote flexible, tailored approaches to oversight and review based on mutual trust and a program's size, risk, and complexity."

2. DoD Regulation 5000.2-R. Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, March 15, 1996

Para 1.1 **Purpose**

"…Any singular MDAP or MAIS need not follow the entire process described below. However, cognizant of this model, the Program Manager (PM) and the Milestone Decision Authority (MDA) shall structure the MDAP or MAIS to ensure a logical progression through a series of phases designed to reduce risk, ensure affordability, and provide adequate information for decision making that will be provide the needed capability to the warfighter in the shortest practical time."

Para 1.2 **Overview of the Acquisition Management Process**

"…The acquisition process shall be structured in logical phases separated by major decision points called milestones. The process shall begin with the identification of broadly stated mission needs that cannot be satisfied by nonmateriel solutions. Acquisition program stakeholders shall consider the full range of alternatives prior to deciding to initiate a new MDAP or MAIS. Threat projections, system performance, unit production cost estimates, life-cycle costs, interoperability, cost-performance-schedule trade-offs, acquisition strategy, affordability constraints, and risk management shall be major considerations at each milestone decision point, including the decision to start a new program."

"…At program initiation, and after consideration of the views of the Working-Level Integrated Product Team (IPT) and Overarching IPT members, the PM shall propose, and the MDA shall consider for approval, the appropriate milestones, the level of decision for each milestone, and the documentation needed for each milestone. This proposal shall consider the size, complexity, and risk of the program. The determinations made at program initiation shall be reexamined at each milestone in light of then-current program conditions."

Para 1.4 **Acquisition Phases & Accomplishments**

"…Tailoring shall give full consideration to applicable statutes. The number of phases and decision points shall be tailored to meet the specific needs of individual PMs, based on objective assessments of a program's category status, risks, the adequacy of proposed risk management plans, and the urgency of the user's need. Tailored acquisition strategies may vary the way in which core activities are to be conducted, the formality of reviews and documentation, and the need for other supporting activities. ACAT II and III

Downloaded from http://www.everyspec.com

program managers shall work with their decision authorities to tailor any documentation and decision points to the needs of the individual program."

Para 1.4.2 **Phase 0: Concept Exploration**

"…Phase 0 typically consists of competitive, parallel short-term concept studies. The focus of these efforts is to define and evaluate the feasibility of alternative concepts and to provide a basis for assessing the relative merits (i.e., advantages and disadvantages, degree of risk) of these concepts at the next milestone decision point…."

Para 1.4.3 **Phase I: Program Definition and Risk Reduction**

"During this phase, the program shall become defined as one or more concepts, design approaches, and / or parallel technologies are pursued as warranted. Assessments of the advantages and disadvantages of alternative concepts shall be refined. Prototyping, demonstrations, and early operational assessments shall be considered and included as necessary to reduce risk so that technology, manufacturing, and support risks are well in hand before the next decision point. Cost drivers, life-cycle cost estimates, cost-performance trades, interoperability, and acquisition strategy alternatives shall be considered to include evolutionary and incremental software development."

Para 3.2.2.2.3 **Cost**

"…As the program progresses through later acquisition phases, procurement costs shall be refined based on contractor actual (or return) costs from program definition and risk reduction, engineering and manufacturing development, or from initial production lots. In all cases, the cost parameters shall reflect the total program and be realistic cost estimates, based on a careful assessment of risks and realistic appraisals of the level of costs most likely to be realized. The amount budgeted shall not exceed the total cost threshold estimated in the APB."

Para 3.2.3 **Exit Criteria**

"…Exit criteria are normally selected to track progress in important technical, schedule or management risk areas."

Para 3.3 **Acquisition Strategy**

"…Essential elements in this context include, but are not limited to, open systems, sources, risk management, cost as an independent variable, contract approach, management approach, environmental considerations, modeling and simulation approach, warranty considerations, and source of support. The PM shall also address other major initiatives that are critical to the success of the program.

…The acquisition strategy shall be tailored to meet the specific needs of individual programs, including consideration of incremental (block) development and fielding strategies. The benefits and risk associated with reducing lead time through concurrency shall be specifically addressed in tailoring the acquisition strategy."

Para 3.3.2.3 **Industrial Capability**

"The PM shall structure the acquisition strategy to promote sufficient program stability to encourage industry to invest, plan and bear risks. Program needs shall be met through reliance on a national technology and industrial base sustained primarily by commercial demands. Programs shall minimize the need for new defense-unique industrial capabilities. Foreign sources and international cooperative developments

Downloaded from http://www.everyspec.com

shall be used where advantageous and within limitations of the law (DFARS Part 225).

The program acquisition strategy shall analyze the industrial capability to design, develop, produce, support and, if appropriate, restart the program. (10 USC 2440). This analysis shall identify DoD investments needed to create new industrial capabilities, and the risks of industry being unable to provide program manufacturing capabilities at planned cost and schedule."

Para 3.3.3 **Cost, Schedule, and Performance Risk Management**

"The PM shall establish a risk management program for each acquisition program to identify and control performance, cost, and schedule risks. The risk management program shall identify and track risk drivers, define risk abatement plans, and provide for continuous risk assessment throughout each acquisition phase to determine how risks have changed. Risk reduction measures shall be included in cost-performance trade-offs, where applicable. The risk management program shall plan for backups in risk areas and identify design requirements where performance increase is small relative to cost, schedule, and performance risk. The acquisition strategy shall include identification of the risk areas of the program and a discussion of how the PM intends to manage those risks."

Para 3.3.4.2 **Cost Management Incentives**

"RFPs shall be structured to incentivize the contractor to meet or exceed cost objectives. Whenever applicable, risk reduction through use of mature processes shall be a significant factor in source selection. For industry, competition to win business, along with attendant business profit, is by far the most powerful incentive. Therefore, competition shall be maintained for as long as practicable in all acquisition programs."

Para 3.3.5 **Contract Approach**

"The acquisition strategy shall discuss the types of contracts contemplated for each succeeding phase, including considerations of risk assessment, reasonable risk-sharing by Government and contractor(s), and the incentive structure for contractors to decrease cost."

Para 3.3.5.1 **Competition**

"Component breakout shall be considered on every program and shall be done when there are significant cost savings (inclusive of Government administrative costs), when the technical or schedule risk of furnishing government items to the prime contractor is manageable, and when there are no other overriding Governmental interests (e.g., industrial capability considerations or dependence or contractor logistics support)."

Para 3.3.6.6 **Information Sharing and DoD Oversight**

"DoD oversight activities (i.e., contract administration offices, contracting offices, technical activities, and program management offices) shall consider all relevant and credible information that might mitigate risks and the need for DoD oversight before designing and applying direct DoD oversight of contractor operations."

Para 3.4 **Test and Evaluation**

"Test and evaluation programs shall be structured to integrate all developmental test and evaluation (DT&E), operational test and evaluation (OT&E), live-fire test

Downloaded from http://www.everyspec.com

and evaluation (LFT&E), and modeling and simulation activities conducted by different agencies as an efficient continuum. All such activities shall be part of a strategy to provide information regarding risk and risk mitigation, to provide empirical data to validate models and simulations, to permit an assessment, the attainment of technical performance specifications and system maturity, and to determine whether systems are operationally effective, suitable, and survivable for intended use."

Para 3.4.1 **Test and Evaluation Strategy**

6. "Early testing of prototypes in Phase I, Program Definition and Risk Reduction, and early operational assessments shall be emphasized to assist in identifying risks."

Para 3.4.2 **Developmental Test and Evaluation**

"Developmental test and evaluation programs shall:…

3. Support the identification and description of design technical risks;…

4. Assess progress toward meeting Critical Operational Issues, mitigation of acquisition technical risk, achievement of manufacturing process requirements and system maturity;… "

Para 3.4.3 **Certification of Readiness for Operational Test and Evaluation**

"…Risk management, measures and indicators, with associated thresholds, which address performance and technical adequacy of both hardware and software shall be defined and used on each program."

Para 3.5.1 **Life-Cycle Cost Estimates**

"The life-cycle cost estimates shall be:…

4. Neither optimistic nor pessimistic, but based on a careful assessment of risks and reflecting a realistic appraisal of the level of cost most likely to be realized."

Para 4.3 **Systems Engineering**

"…The system engineering process shall establish a proper balance between performance, risk, cost, and schedule, employing a top-down iterative process of requirements analysis, functional analysis and allocation, design synthesis and verification, and system analysis and control."

"System Analysis and Control. System analysis and control activities shall be established to serve as a basis for evaluating and selecting alternatives, measuring progress, and documenting design decisions. This shall include:

…The establishment of a risk management process to be applied throughout the design process. The risk management effort shall address the identification and evaluation of potential sources of technical risks based on the technology being used and its related design, manufacturing capabilities, potential industry sources, test and support processes, risk mitigation efforts, and risk assessment and analysis. Technology transition planning and criteria shall be established as part of the overall risk management effort."

Para 4.3.5 **Software Engineering**

"Software shall be managed and engineered using best processes and practices that are known to reduce cost, schedule, and performance risks."

Para 5.6 **Cost Analysis Improvement Group (CAIG) Procedures**

"The OSD CAIG is established in accordance with DoDD 5000.4. The DoD

Downloaded from http://www.everyspec.com

Component responsible for acquisition of a system shall work with the CAIG providing cost, programmatic, and technical information required to estimate costs and appraise cost risks, and shall facilitate visits of the CAIG staff to the program office, product centers, test centers, and system contractor(s)....”

Para 6.2.3 **Major Automated Information System Quarterly Report DD-C3I(Q) 1799**

“The quarterly Major Automated Information System (MAIS) status reporting system is designed to provide executive management at the Component and OSD levels with the program status, progress, issues, risks, and risk reducers. The quarterly report is essential to the early identification of problems and associated plans to initiate corrective actions. The PM shall provide the report to the MDA in a timely manner to permit prompt action to address reported issues and problems... .”

Para 6.4 **Contract Management Reports**

“The reports prescribed by this section shall be used for all applicable defense contracts and are required for effective management of defense acquisitions. Use of electronic media shall be required. The Work Breakdown Structure (WBS) used in preparing the reports covered by this section shall be in conformance with the program WBS (see 4.4.1). Except for high-cost or high-risk elements, the normal level of reporting detail required shall be limited to level three of the contract WBS.

Para 6.4.1 **Contractor Cost Data Reporting (CCDR)**

“...The following general policies guide the preparation and submission of CCDR data:

1. Level of Cost Reporting. Routine reporting shall be at the contract WBS level three for prime contractors and key subcontractors. In addition, detailed (i.e., sub level three) reporting shall be required only for those lower elements that address high risk, high value, or high technological interest areas of a program. Identifying these additional elements is a critical early assignment for program Cost Program-level IPT (which may include contractor membership, where appropriate and in accordance with applicable statutes (see 3.3.1)). Each element must be justified in terms of its contribution to efficient decision-making.”

3. DoD Directive (DoDD) 5000.4, OSD Cost Analysis Improvement Group (CAIG), November 24, 1992

Para D.1.h **Risk Assessment**

“The CAIG Chair report, in support of a milestone review, shall include quantitative assessments of the risk in the estimate of life-cycle costs. In developing an assessment of cost risk, the CAIG shall consider the validity of such programmatic assumptions of the CARDs as EMD schedules, rates of utilization of test assets, production ramp rates, and buy rates, consistent with historical information. The CAIG shall also consider uncertainties in inputs to any cost estimating relationships used in its estimates, as well as the uncertainties inherent in the calibration of the CERs, and shall consider uncertainties in the factors used in making any estimates by analogy. The CAIG shall consider cost and schedule risk implications of available assessments of the program’s technical risks, and may include the results in its cost-risk assessments. The CAIG may consider information on risk provided by any source, although primary reliance will be on the

Downloaded from http://www.everyspec.com

technical risk assessments that are the responsibility of the sponsoring DoD components, and of other OSD offices, in accordance with their functional responsibilities."

4. DoD 5000.4-M. Cost Analysis Guidance and Procedures, December 1992

Chapter 1: (Outline of CARD Basic Structure)

Para 1.2.1.x (..x..) **Subsystem Description**

"This series of paragraphs (repeated for each subsystem) describes the major equipment (hardware/software) WBS components of the system. The discussion should identify which items are off-the-shelf. The technical and risk issues associated with development and production of individual subsystems also must be addressed."

Chapter 2:

Para 2.0 **Risk**

"This section identifies the program manager's assessment of the program and the measures being taken or planned to reduce those risks. Relevant sources of risk include: design concept, technology development, test requirements, schedule, acquisition strategy, funding availability, contract stability, or any other aspect that might cause a significant deviation from the planned program. Any related external technology programs (planned or ongoing) should be identified, their potential contribution to the program described, and their funding prospects and potential for success assessed. This section should identify these risks for each acquisition phase (DEM/VAL, EMD, productions and deployment, and O&S)."

Para 2.B.9 **Sensitivity Analysis**

"The sensitivity of projected costs to critical program assumptions shall be examined. Aspects of the program to be subjected to sensitivity analysis shall be identified in the DoD CCA of program assumptions. The analysis shall include factors such as learning curve assumptions; technical risk, i.e., the risk of more development and/or production effort, changes in performance characteristics, schedule alterations, and variations in testing requirements; and acquisition strategy (multiyear procurement, dual sourcing, etc.)."

Para 2.C.3 **PM Presentation**

"The Program Manager's designated representative shall present the CAIG with the POE for each alternative under construction and explain how each is derived. This presentation shall cover the estimates and estimating procedures at the major subcomponent level (e.g., airframe, engine, major avionics subsystem, etc.). The presentation should focus on the items that are cost drivers and/or elements of high cost risk."

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

APPENDIX B

GENERIC RISK MANAGEMENT PLAN

SAMPLE RISK MANAGEMENT PLAN

Preface

DoDD 5000.1 requires that "PMs and other acquisition managers shall continually assess program risks" and that they "shall develop a contracting approach appropriate to the type of system being acquired." Further, DoD 5000.2-R states that for ACAT I Programs, "The PM shall establish a risk management program… to identify and control performance, cost, and schedule risks." Although the need for a risk management program and a risk management process are addressed throughout this regulation, there is no requirement for a formal Risk Management Plan (RMP). However, Program Managers (PMs) have found such a plan necessary to focus properly on the assessment and handling of program risk, a core acquisition management issue that Milestone Decision Authorities (MDAs) must rigorously address at appropriate milestones before making program decisions.

Attached is a sample format for a RMP that is a compilation of several good risk plans and the results of the DoD Risk Management Working Group Study. It represents the types of information and considerations that a plan, tailored to a specific program, might contain. There are also two example of Risk Management Plans—one for an ACAT I or II Program, the other for an ACAT III or IV Program. The *DoD Acquisition Deskbook*, Section 2.5.2, has general guidance and advice in all areas of risk management. Section 2.5.2.4 of the *Deskbook* contains information concerning the development of a risk management plan. The information in this *Guide* is consistent with, and in most cares identical to, the *Deskbook*.

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

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

The italicized text reflects the outline of a risk management plan found in the DoD Acquisition Deskbook section 2.5.2.4, Figure 2.5.2.4-2.

Downloaded from http://www.everyspec.com

SAMPLE FORMAT FOR RISK MANAGEMENT PLAN

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

PROGRAM SUMMARY. *This section contains a brief description of the program, including the acquisition strategy and the program management approach. The acquisition strategy should address its linkage to the risk management strategy.*

DEFINITIONS. *Definitions used by the program office should be consistent with DoD definitions for ease of understanding and consistency. However, the DoD definitions allow program managers flexibility in constructing their risk management programs. Therefore, each program's risk management plan may include definitions that expand the DoD definitions to fit its particular needs. For example, each plan should include, among other things, definitions for the ratings used for technical, schedule and cost risk. (Discussion of risk rating is contained in Acquisition Deskbook Section 2.5.2.1.)*

RISK MANAGEMENT STRATEGY AND APPROACH. *Provide an overview of the risk management approach, to include the status of the risk management effort to date, and a description of the program risk management strategy. See Acquisition Deskbook Sections 2.5.2.1 and 2.5.2.3.*

ORGANIZATION. *Describe the risk management organization of the program office and list the responsibilities of each of the risk management participants. See Acquisition Deskbook Section 2.5.2.3.*

RISK MANAGEMENT PROCESS AND PROCEDURES. *Describe the program risk management process to be employed; i.e., risk planning, assessment, handling, monitoring and documentation, and a basic explanation of these components. See Acquisition Deskbook Section 2521. Also provide application guidance for each of the risk management functions in the process. If possible, the guidance should be as general as possible to allow the program's risk management organization (e.g., IPTs) flexibility in managing the program risk, yet specific enough to ensure a common and coordinated approach to risk management. It should address how the information associated with each element of the risk management process will be documented and made available to all participants in the process, and how risks will be tracked, to include the identification of specific metrics if possible.*

RISK PLANNING. *This section describes the risk planning process and provides guidance on how it will be accomplished, and the relationship between continuous risk planning and this RMP. Guidance on updates of the RMP and the approval process to be followed should also be included. See Section 2.5.2.1 of the Deskbook for information on risk planning.*

RISK ASSESSMENT. *This section of the plan describes the assessment process and procedures for examining the critical risk areas and processes to identify and document the associated risks. It also summarizes the analyses process for each of the risk areas leading to the determination of a risk rating. This rating is a reflection of the potential impact of the risk in terms of its variance from known Best Practices or probability of occurrence, its consequence, and its relationship to other risk areas or processes. This section may include:*

Downloaded from http://www.everyspec.com

- *Overview and scope of the assessment process*
- *Sources of information*
- *Information to be reported and formats*
- *Description of how risk information is documented*
- *Assessment techniques and tools (see Section 2.5.2.4 of the Deskbook)*

RISK HANDLING. *This section describes the procedures that can be used to determine and evaluate various risk handling options, and identifies tools that can assist in implementing the risk handling process. It also provides guidance on the use of the various handling options for specific risks.*

RISK MONITORING. *This section describes the process and procedures that will be followed to monitor the status of the various risk events identified. It should provide criteria for the selection of risks to be reported on, and the frequency of reporting. Guidance on the selection of metrics should also be included.*

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

Downloaded from http://www.everyspec.com

SAMPLE RISK MANAGEMENT PLAN FOR THE XYZ PROGRAM (ACAT I, II)

1.0 INTRODUCTION

1.1 PURPOSE

This Risk Management Plan (RMP) presents the process for implementing proactive risk management as part of the overall management of the XYZ program. Risk management is a program management tool to assess and mitigate events that might adversely impact the program. Therefore, risk management increases the likelihood of program success. This RMP will:

- Serve as a basis for identifying alternatives to achieve cost, schedule, and performance goals,
- Assist in making decisions on budget and funding priorities,
- Provide risk information for Milestone decisions, and
- Allow monitoring the health of the program as it proceeds.

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

This is the second edition of the Risk Management Plan for the XYZ program. The initial plan concentrated on tasks leading to Milestone I (Phase 0); this plan concentrates on the tasks leading to Milestone II (Phase I). Subsequent updates to this RMP will shift focus to the later acquisition phases. There are changes in every area of the plan; they include refinement of the risk identification process. The PMO Risk Management Coordinator has been identified and training of IPT members has commenced.

1.2 PROGRAM SUMMARY

The XYZ program was initiated in response to Mission Need Statement (MNS) XXX, dated DD-MM-YYYY and Operational Requirements Document (ORD), dated DD-MM-YYYY. It is required to support the fundamental objective of U.S. defense policy as stated in Defense Planning Guidance (DPG) and the National Military Strategy. The XYZ system is based on the need for an integrated combat system to link battlefield decision makers. The XYZ mission areas are: (Delineate applicable areas).

The XYZ program will develop and procure 120 advanced platforms to replace the aging ABC platforms currently in the inventory. In order to meet force structure objectives, the XYZ system must reach Initial Operational Capability (IOC) (four platforms) by FY-07. The program is commencing an eight-year EMD phase that will be followed by a five-year procurement phase. The objectives of the EMD phase are to (discuss the specific objectives of this phase). The program has Congressional interest and is restricted to a Research and Development funding ceiling of $300 million.

Downloaded from http://www.everyspec.com

1.2.1 System Description

The XYZ will be an affordable, yet capable, platform taking advantage of technological simplification and advancements. The XYZ integrated Combat System includes all non-propulsion electronics and weapons. Subsystems provide capabilities in combat control, electronic warfare support measures (ESM), defensive warfare, navigation, radar, interior communications, monitoring, data transfer, tactical support device, exterior communications, and Identification Friend or Foe (IFF). Weapons systems are to be provided by the program offices that are responsible for their development. The Mechanical and Electrical (M&E) system comprises.... The Combat System, M&E systems, and subsystems provide the XYZ system with the capability and connectivity to accomplish the broad range of missions defined in the MNS and ORD.

1.2.2 Acquisition Strategy

The XYZ program initial strategy is to contract with one prime contractor in Program Definition/Risk Reduction (PDRR) for development of two prototype systems for test and design validation. Due to the technical complexity of achieving the performance levels of the power generation systems, the prime will use two sub-contractors for the engine development and down select to one producer prior to low rate initial production, which is scheduled for FY-04. Various organizations, such as the Government Research Laboratory will be funded to provide experts for assessment of specific areas of risk. The program has exit criteria, included in the list of Critical Program Attributes in Annex A, that must be met before progressing to the next phase.

1.2.3 Program Management Approach

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

1.3 DEFINITIONS

1.3.1 Risk

Risk is a measure of the inability to achieve overall program objectives within defined cost, schedule, and technical constraints and has two components: (1) the *probability* of failing to achieve a particular outcome and (2) the *consequences* of failing to achieve that outcome. For processes, risk is a measure of the difference between actual performance of a process and the known best practice for performing that process.

1.3.2 Risk Event

Risk events are those events within the XYZ program that, if they go wrong, could result in problems in the development, production, and fielding of the system. Risk events should be defined to a level such that the risk and causes are understandable and can be accurately

Downloaded from http://www.everyspec.com

assessed in terms of likelihood / probability and consequence to establish the level of risk. For processes, risk events are assessed in terms of process variance from known best practices and potential consequences of the variance.

1.3.3 Technical Risk

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

1.3.4 Cost Risk

This is the risk associated with the ability of the program to achieve its life-cycle cost objectives. Two risk areas bearing on cost are (1) the risk that the cost estimates and objectives are accurate and reasonable and (2) the risk that program execution will not meet the cost objectives as a result of a failure to handle cost, schedule, and performance risks.

1.3.5 Schedule Risk

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

1.3.6 Risk Ratings

This is the value that is given to a risk event (or the program overall) based on the analysis of the likelihood / probability and consequences of the event. For the XYZ program, risk ratings of Low, Moderate, or High will be assigned based on the following criteria. See Section 3.3.2 of this appendix for guidance on determining likelihood and consequences. When rating process variance from best practices, there is no rating of likelihood / probability, rather the level would be a measure of the variance from best practices (see Paragraph 3.3.2.3).

- **Low Risk:** Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Actions within the scope of the planned program and normal management attention should result in controlling acceptable risk.

- **Moderate Risk:** May cause some increase in cost, disruption of schedule, or degradation of performance. Special action and management attention may be required to handle risk.

- **High Risk:** Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Significant additional action and high priority management attention will be required to handle risk.

Downloaded from http://www.everyspec.com

1.3.7 Independent Risk Assessor

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

1.3.8 Templates and Best Practices

A "template" is a disciplined approach for the application of critical engineering and manufacturing processes that are essential to the success of most programs. DoD 4245.7-M, *Transition from Development to Production Solving the Risk Equation*, provides a number of such templates. For each template process described in DoD 4245.7-M, a Best Practice Information is described in NAVSO P-6071. These documents outline the ideal or low risk approach and thus serve as a baseline from which risk for some XYZ processes can be assessed.

1.3.9 Metrics

There are measures used to indicate progress or achievement.

1.3.10 Critical Program Attributes

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

2.0 RISK MANAGEMENT APPROACH

2.1 GENERAL APPROACH AND STATUS

DoD Directive 5000.1 states: "Risks must be well understood, and risk management approaches developed, before decision authorities can authorize a program to proceed into the next phase of the acquisition process." This policy is implemented in DoD Regulation 5000.2-R, with more detailed guidance provided in the individual Service regulation. The *Defense Acquisition Deskbook* (Section 2.5.2) provides additional guidance, advice, and wisdom on the management of risk. Figure 2-1 shows how the XYZ program risk management fits into the phases and milestones of the acquisition process.

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

The results of the Concept Exploration Phase of the program identified potential risk events and the Acquisition Strategy reflects the program's risk-handling approach. Overall, the

Downloaded from http://www.everyspec.com

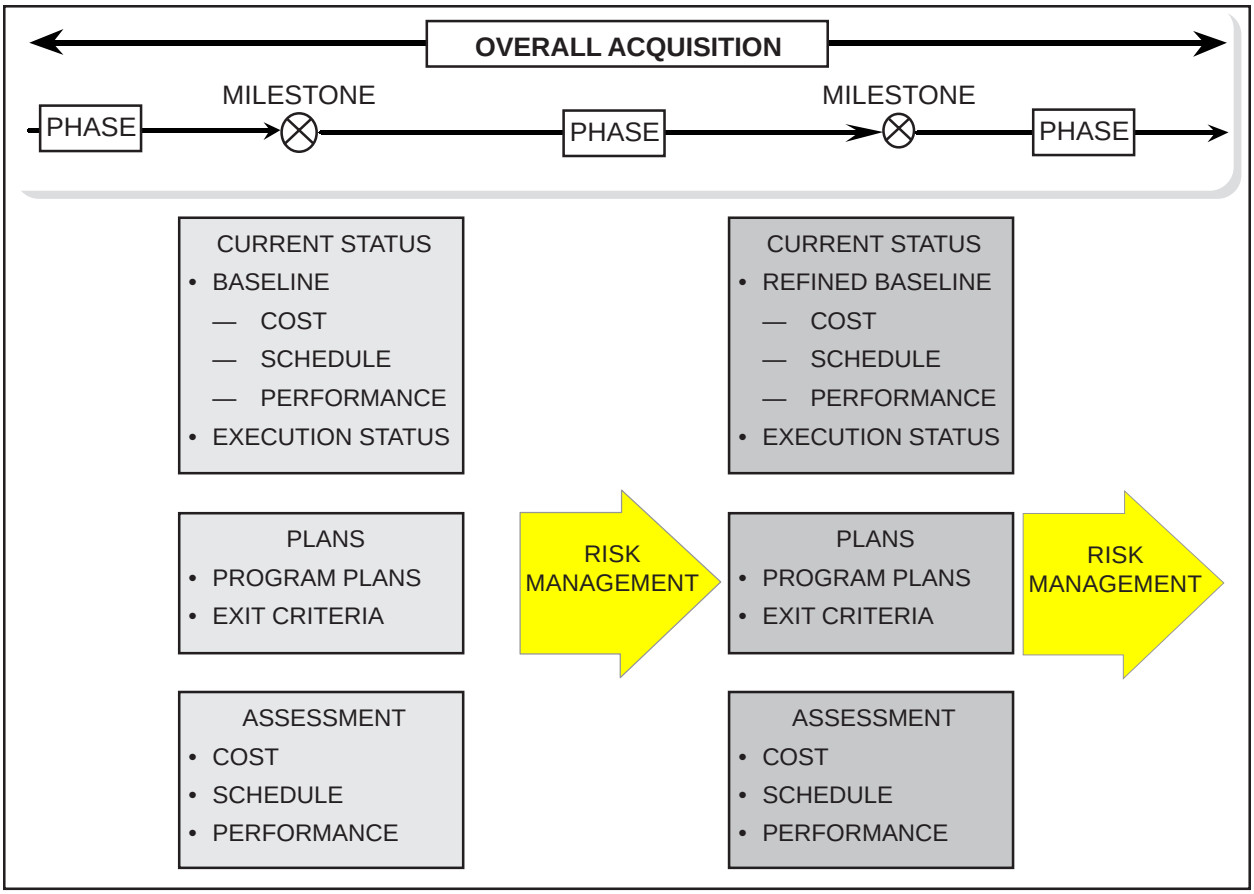


Figure 2-1. Risk Management and the Acquisition Process

risk of the XYZ program for Milestone I was assessed as moderate, but acceptable. Moderate risk functional areas were threat, manufacturing, cost, funding, and schedule. The remaining functional areas of technology, design and engineering (hardware and software), support, (schedule) concurrency, human systems integration, and environmental impact were assessed as low risk.

2.2 RISK MANAGEMENT STRATEGY

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

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

Downloaded from http://www.everyspec.com

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

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

2.3 ORGANIZATION

The risk organization for the XYZ program is shown in Figure 2-2. This is *not* a separate organization, but rather shows how risk is integrated into the program's existing organization and shows risk relationships among members of the program team.

2.3.1 Risk Management Coordinator

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

- Maintaining this Risk Management Plan
- Maintaining the Risk Management Database
- Briefing the PM on the status of XYZ program risk

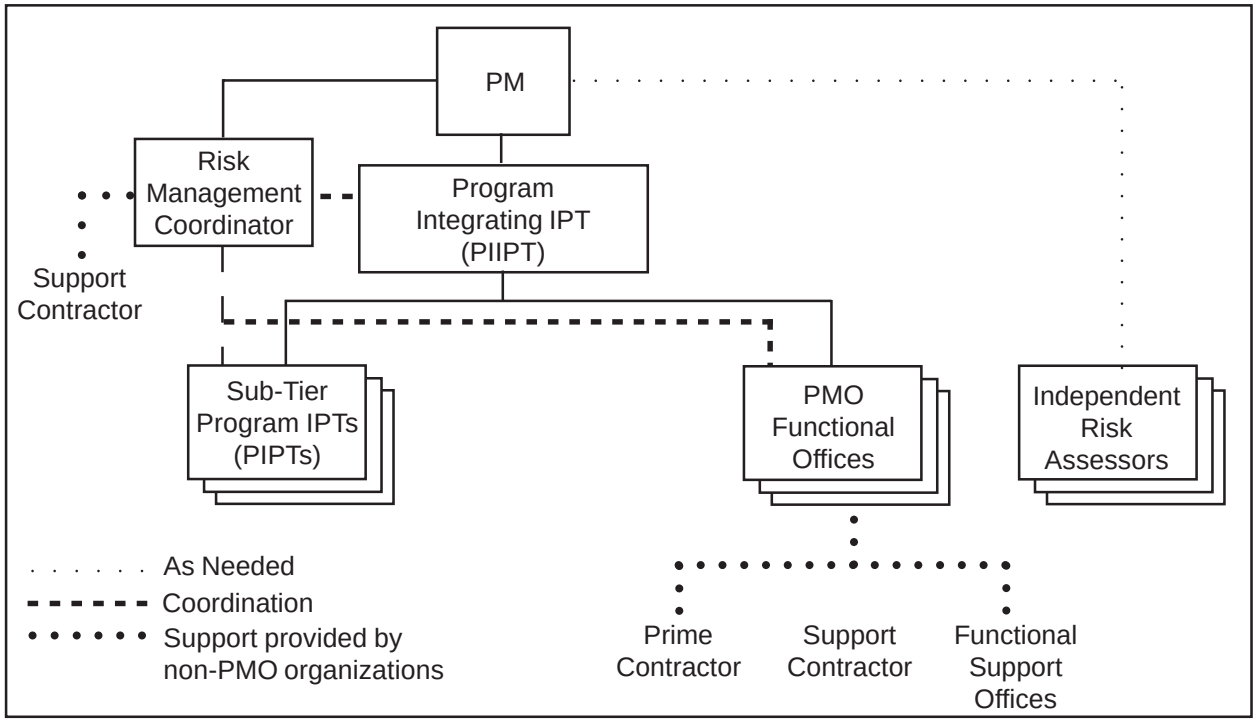


Figure 2-2. XYZ Risk Management Organization

Downloaded from http://www.everyspec.com

- Tracking efforts to reduce moderate and high risk to acceptable levels
- Providing risk management training
- Facilitating risk assessments and
- Preparing risk briefings, reports, and documents required for Program Reviews and the acquisition Milestone decision processes.

2.3.2 Program Integrating Integrated Product Team (PIIPT)

The PIIPT is responsible for complying with the DoD risk management policy and for structuring an efficient and useful XYZ risk management approach. The Program Manager is the Chair of the PIIPT. The PIIPT membership may be adjusted but is initially established as the chairs of the Program IPTs, designated sub-tier IPTs, and the Heads of PMO Functional Offices.

2.3.3 PIPTs

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

- Review and recommend to the Risk Management Coordinator changes on the overall risk management approach based on lessons learned.
- Quarterly, or as directed, update the program risk assessments made during Phase I.
- Review and be prepared to justify the risk assessments made and the risk mitigation plans proposed.
- Report risk to the Program Manager / Program Director, with information to the Risk Management Coordinator via Risk Information Forms (RIFs).
- Ensure that risk is a consideration at each Program and Design Review.
- Ensure Design / Build Team responsibilities incorporate appropriate risk management tasks.

2.3.4 XYZ Independent Risk Assessors

Independent Assessors made a significant contribution to the XYZ Milestone I risk assessments. The use of independent assessments as a means of ensuring that all risk areas are identified will continue, when necessary.

2.3.5 Other Risk Assessment Responsibilities

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

Downloaded from http://www.everyspec.com

2.3.6 User Participation

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

2.3.7 Risk Training

The key to the success of the risk efforts is the degree to which all members of the team, both Government and contractor are properly trained. The XYZ Program Office will provide risk training, or assign members to training classes, during acquisition Phases I and II. Key personnel with XYZ management or assessment responsibilities are required to attend. All members of the team will receive, at a minimum, basic risk management training. XYZ sponsored training is planned to be presented according to the schedule provided in Annex X (not provided).

3.0 RISK MANAGEMENT PROCESS AND PROCEDURES

3.1 OVERVIEW

This section describes XYZ program's risk management process and provides an overview of the XYZ risk management approach. The *Defense Acquisition Deskbook* defines risk management as "the act or practice of controlling risk. It includes risk planning, assessing risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program." Figure 3-1 shows, in general terms, the overall risk management process that will be followed in the XYZ program. This process follows DoD and Service policies and guidelines and incorporates ideas found in other sources. Each of the risk management functions shown in Figure 3-1 is discussed in the following paragraphs, along with specific procedures for executing them.

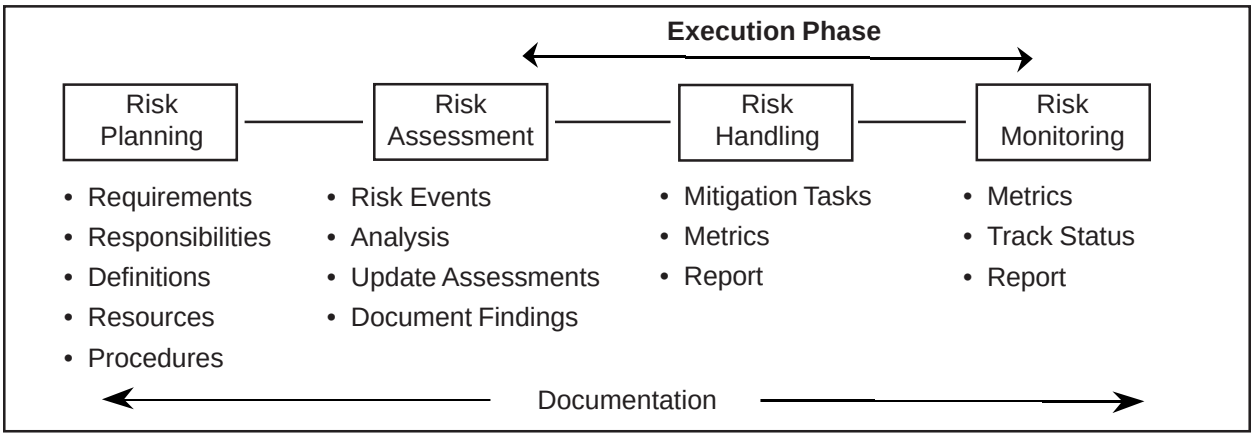


Figure 3-1. Risk Management Structure
(also referred to as The Risk Management Process Model)

Downloaded from http://www.everyspec.com

3.2 RISK PLANNING

3.2.1 Process

Risk planning consists of the up-front activities necessary to execute a successful risk management program. It is an integral part of normal program planning and management. The planning should address each of the other risk management functions, resulting in an organized and thorough approach to assess, handle, and monitor risks. It should also assign responsibilities for specific risk management actions and establish risk reporting and documentation requirements. This RMP serves as the basis for all detailed risk planning, which must be continuous.

3.2.2 Procedures

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

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

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

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

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

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

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

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

Downloaded from http://www.everyspec.com

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

- Commercial and Government developed risk management software.

The latter includes Government software, such as *Risk Matrix* developed by Mitre Corporation for the Air Force and the New Attack Submarine's *On-Line Risk Data Base (OLRDB)*.

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

3.3 RISK ASSESSMENT

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

3.3.1 Process

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

Risks will be identified by all IPTs and by any individual in the program. The lower-level IPTs can identify significant concerns earlier than otherwise might be the case and identify those events in critical areas that must be dealt with to avoid adverse consequences. Likewise, individuals involved in the detailed and day-to-day technical, cost, and scheduling aspects of the program are most aware of the potential problems (risks) that need to be managed.

3.3.1.2 Analysis. This process involves:

- Identification of WBS elements

- Evaluation of the WBS elements using the risk areas to determine risk events

- Assignment of likelihood / probability and consequence to each risk event to establish a risk rating

- Prioritization of each risk event relative to other risks.

Risk analysis should be supported by a study, test results, modeling and simulation, trade study, the opinion of a qualified expert (to include justification of his or her judgment), or

Downloaded from http://www.everyspec.com

any other accepted analysis technique. The *DoD Acquisition Deskbook*, Section 2524.2 describes a number of analysis techniques that may be useful. Evaluators should identify all assumptions made in assessing risk. When appropriate, a sensitivity analysis should be done on assumptions.

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

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

3.3.2 Procedures

3.3.2.1 Assessments—General. Risk assessment is an iterative process, with each assessment building on the results of previous assessments. The current baseline assessment is a combination of the risk assessment delivered by the contractors as part of Phase 0, the program office process risk assessment done before Milestone I, and the post-award Integrated Baseline Review (IBR).

For the program office, unless otherwise directed in individual tasking, program level risk assessments will be presented at each Program Review meeting with a final update not later than 6 months before the next scheduled Milestone decision. The primary source of information for the next assessment will be the current assessment baseline, and existing documentation such as, Phase 0 study results, the design mission profile that was done as part of Phase 0, the IBR, which will be conducted immediately after Phase I contract award, the contract WBS that is part of the IBR, industry best practices as described in the PMWS Knowledge base, the ORD, the Acquisition Program Baseline (APB), and any contractor design documents.

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

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

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

- **Step One**—Understand the requirements and the program performance goals, which are defined as thresholds and objectives (see 5000.2-R). Describe the operational (functional and environmental) conditions under which the values must be achieved by

Downloaded from http://www.everyspec.com

referring or relating to design documents. The ORD and APB contain Key Performance Parameters (KPPs).

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

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

- **Step Four**—Evaluate each WBS element against sources / areas of risk described in Table 4-2 of the DSMC *Risk Management Guide*, plus other sources / areas as appropriate.

- **Step Five**—Assign a probability and consequence to each risk event

- **Step Six**—Prioritize the risk events.

Following are indicators that IPTs may find helpful in identifying and assessing risk:

- **Lack of Stability, Clarity, or Understanding of Requirements:** Requirements drive the design of the system. Changing or poorly stated requirements guarantees the introduction of performance, cost, and schedule problems.

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

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

- **Any Process Lacking Rigor** should also be suspect; it is inherently risky. To have rigor, a process should be mature and documented, it should have been validated, and it should be strictly followed.

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

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

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

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

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

Downloaded from http://www.everyspec.com

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

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

- **DoD 4245.7-M, "Transition from Development to Production,"** is often called the "Templates" book because it identifies technical risk areas and provides, in "bullet" form, suggestions for avoiding those risks. It focuses on the technical details of product design, test, and production to help managers proactively manage risk. It also includes chapters on Facilities, Logistics, and Management, which make this a useful tool in identifying weak areas of XYZ planned processes early enough to implement actions needed to avoid adverse consequences.

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

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

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

- **PMWS** contains risk management software, "Technical Risk Identification and Mitigation System (TRIMS) and Knowledgebase." They provide a tailorable management system based on NAVSO P-6071 and DoD 4245.7-M. The PMWS provides a compact disk (CD) that contains the necessary programs for assessing a program's risk and software for program management. PMWS can be obtained by calling the Best Manufacturing Program (BMP) Office at (301) 403-8100.

- **New Nuclear Submarine (NSSN) On-Line Risk Database (ONLRB)** is a software tool may be used to support the XYZ Risk Management Process. The tool helps IPTs in the identification and assessment of risk and management of handling efforts.

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

Downloaded from http://www.everyspec.com

- **Requirements Documents** describe the output of our efforts. IPT efforts need to be monitored continuously to ensure requirements are met on time and within budget. When they aren't, there is risk.

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

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

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

3.3.2.3 Analysis. Risk analysis is an evaluation of the identified risk events to determine possible outcomes, critical process variance from known best practices, the likelihood of those events occurring, and the consequences of the outcomes. Once this information has been determined, the risk event may be rated against the program's criteria and an overall assessment of low, moderate, or high assigned. Figure 3-2 depicts the risk analysis process and procedures.

Critical Process Variance. For each process risk related event identified, the variance of the process from known standards or best practices must be determined. As shown in Figure 3-2, there are five levels (a-e) in the XYZ risk assessment process, with the corresponding criteria of *Minimal, Small, Acceptable, Large, and Significant*. If there is no variance then there is no risk.

Likelihood/Probability. For each risk area identified, the likelihood the risk will happen must be determined. As shown in Figure 3-2, there are five levels (a-e) in the XYZ risk assessment process, with the corresponding subjective criteria of *Remote, Unlikely, Likely, Highly Likely,* and *Near Certainty*. If there is zero likelihood of an event, there is no risk per our definition.

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

- **Technical Performance**: This category includes all requirements that are not included in the other three metrics of the Consequence table. The wording of each level is

Downloaded from http://www.everyspec.com

Risk Assessment Process

Level	What is the Likelihood the Risk Event Will Happen?
a	Remote
b	Unlikely
c	Likely
d	Highly likely
e	Near certainty

Process Variance refers to deviation from best practices. Likelihood/Probability refers to risk events.

ASSESSMENT GUIDE

Likelihood	1	2	3	4	5
e	L	M	H	H	H
d	L	M	M	H	H
c	L	M	M	M	H
b	L	L	L	M	M
a	L	L	L	L	M

Consequence

RISK ASSESSMENT

R **HIGH—**Unacceptable, Major disruption likely. Different approach required. Priority management attention required.

Y **MODERATE—**Some disruption. Different approach may be required. Additional management attention may be needed.

G **LOW—**Minimum impact. Minimum oversight needed to ensure risk remains low.

Level	Technical Performance	and/ or	Schedule	and/ or	Cost	and/ or	Impact on Other Teams
1	Minimal or no impact		Minimal or no impact		Minimal or no impact		None
2	Acceptable with some reduction in margin need dates		Additional resources required; able to meet		<5%		Some impact
3	Acceptable with significant reduction in margin		Minor slip in key milestones; not able to meet need date		5-7%		Moderate impact
4	Acceptable; no remaining margin		Major slip in key milestone or critical path impacted		7-10%		Major impact
5	Unacceptable major program milestone		Can't achieve key team or		>10%		Unacceptable

Figure 3-2. Risk Assessment Process

oriented toward design processes, production processes, life cycle support, and to retirement of the system. For example, the word "margin" could apply to weight margin during design, safety margin during testing, or machine performance margin during production.

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

- **Cost:** Since costs vary from component to component and process to process, the percentage criteria shown in the figure may not strictly apply at the lower levels of the WBS. These team leaders can set the percentage criteria that best reflects their situation. However, when costs are rolled up at higher levels (e.g., Program), the following definitions will be used: Level 1—no change, Level 2—<5%, Level 3—5-7%, Level 4—7-10%, and Level 5—>10%.

- **Impact on Other Teams:** Both the consequence of a risk and the mitigation actions associated with reducing the risk may impact another team. This may involve additional

Downloaded from http://www.everyspec.com

coordination or management attention (resources) and may therefore increase the level of risk. This is especially true of common technical processes.

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

Figure 3-2 is useful to convey information to decision makers and will be used primarily for that purpose. The PMO will use the Risk Tracking Report and Watch List. (See Annex D.)

3.4 RISK HANDLING

3.4.1 Process

After the program's risks have been identified and assessed, the approach to handling each significant risk must be developed. There are essentially four techniques or options for handling risks: avoidance, control, transfer, and assumption. For all identified risks, the various handling techniques should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, and the effect on the system's technical performance, and the most suitable technique selected. Section 2524.3 of the *DoD Acquisition Deskbook* contains information on the risk-handling techniques and various actions that can be used to implement them. The results of the evaluation and selection will be included and documented in the RMIS using the RIF. This documentation will include: what must be done, the level of effort and materials required, the estimated cost to implement the plan, a proposed schedule showing the proposed start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant Program activities / milestones (an example is provided in Annex B), recommended metrics for tracking the action, a list of all assumptions, and the person responsible for implementing and tracking the selected option.

3.4.2 Procedures

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

For each selected handling option, the responsible IPT will develop specific tasks that, when implemented, will handle the risk. The task descriptions should explain what has to be done,

Downloaded from http://www.everyspec.com

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

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

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

3.5 RISK MONITORING

3.5.1 Process

Risk monitoring systematically tracks and evaluates the performance of risk-handling actions. It is part of the PMO function and responsibility and will not become a separate discipline. Essentially, it compares predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk-handling actions. The effectiveness of the risk-monitoring process depends on the establishment of a management indicator system (metrics) that provides accurate, timely, and relevant risk information in a clear, easily understood manner. (See Annex D.) The metrics selected to monitor program status must adequately portray the true state of the risk events and handling actions. Otherwise, indicators of risks that are about to become problems will go undetected.

To ensure that significant risks are effectively monitored, risk-handling actions (which include specific events, schedules, and "success" criteria) will be reflected in integrated program planning and scheduling. Identifying these risk handling actions and events in the context of Work Breakdown Structure (WBS) elements establishes a linkage between them and specific work packages, making it easier to determine the impact of actions on cost, schedule, and performance. The detailed information on risk-handling actions and events will be included in the RIF for each identified risk, and thus be resident in the RMIS.

3.5.2 Procedures

The functioning of IPTs is crucial to effective risk monitoring. They are the "front line" for obtaining indications that risk-handling efforts are achieving their desired effects. Each IPT is responsible for monitoring and reporting the effectiveness of the handling actions for the risks assigned. Overall XYZ program risk assessment reports will be prepared by the XYZ Risk Management Coordinator working with the cognizant IPT.

Many techniques and tools are available for monitoring the effectiveness of risk-handling actions, and IPTs must ensure that they select those that best suit their needs. No

Downloaded from http://www.everyspec.com

single technique or tool is capable of providing a complete answer—a combination must be used. At a minimum, each IPT will maintain a watch list of identified high priority risks. See Section 2524.4 of the *DoD Acquisition Deskbook* for information on specific techniques.

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

The risk management process is continuous. Information obtained from the monitoring process is fed back for reassessment and evaluations of handling actions. When a risk area is changed to Low, it is put into a "Historical File" by the Risk Management Coordinator and it is no longer tracked by the XYZ PMO. The "owners" of all Low risk areas will continue monitoring Low risks to ensure they stay Low.

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

- Quarterly
- When the IPT determines that the status of the risk area has changed significantly (as a minimum when the risk changes from high to moderate to low, or vice versa)
- When requested by the Program Manager.

4.0 RISK MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION

The XYZ program will use the XXX database management system as its RMIS. The system will contain all of the information necessary to satisfy the program documentation and reporting requirements.

4.1 RISK MANAGEMENT INFORMATION SYSTEM (RMIS)

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

Downloaded from http://www.everyspec.com

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

4.2 RISK DOCUMENTATION

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

4.2.1 Risk Assessment Documentation

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

4.2.2 Risk Handling Documentation

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

4.2.3 Risk Monitoring Documentation

The PM needs a summary document that tracks the status of high and moderate risks. The Risk Management Coordinator will produce a risk tracking list, for example, that uses information that has been entered from the RMIS. This document will be produced on a monthly basis.

4.3 REPORTS

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

4.3.1 Standard Reports

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

4.3.2 Ad Hoc Reports

In addition to standard reports, the PMO will need to create ad hoc reports in response to special queries. The Risk Management Coordinator will be responsible for these reports.

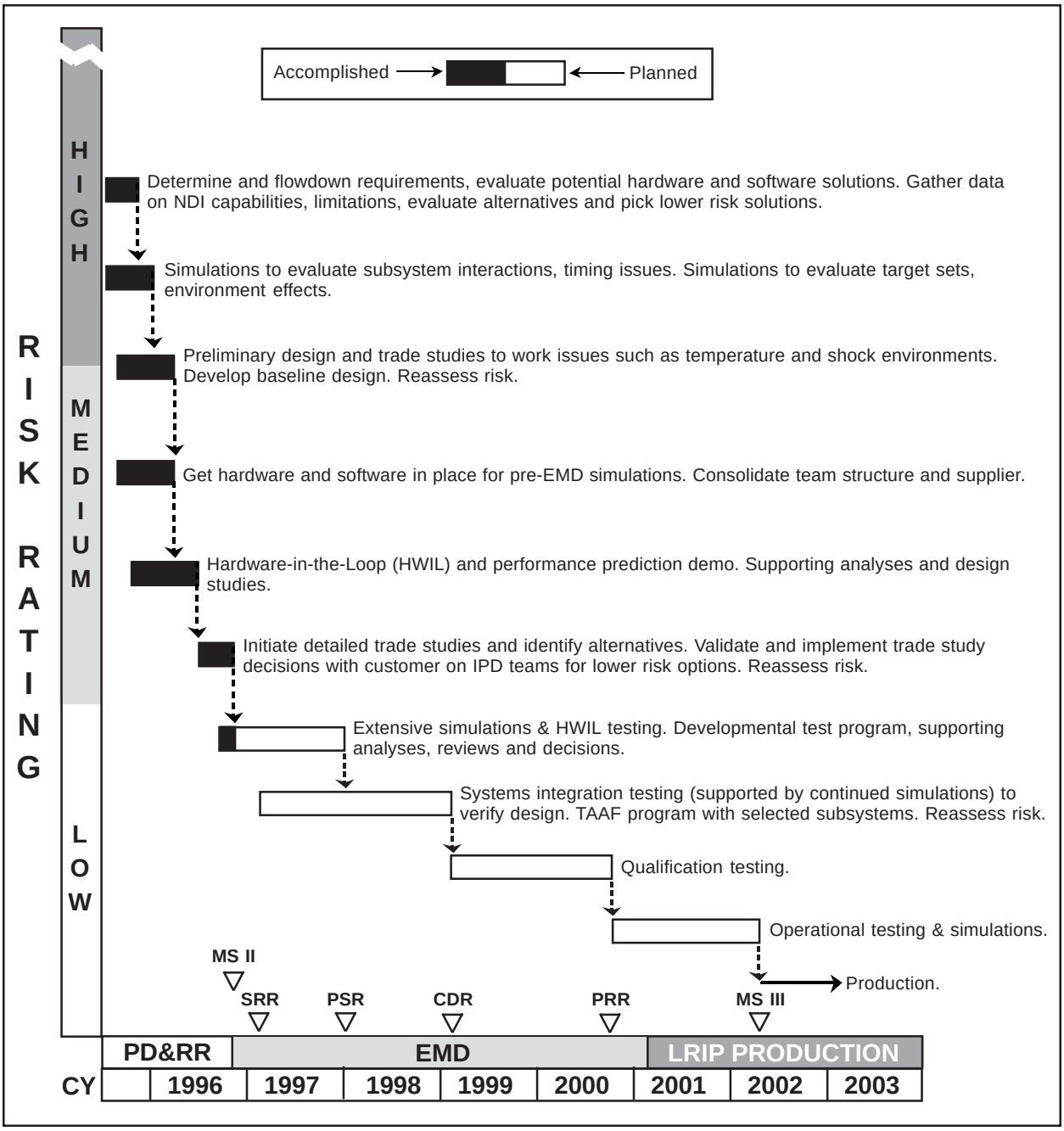
Downloaded from http://www.everyspec.com

ANNEX A
TO XYZ RISK MANAGEMENT PLAN
—CRITICAL PROGRAM ATTRIBUTES—

Category	Description	Responsible IPT	Remarks
Performance/Physical	Speed		
	Weight		
	Endurance		
	Crew Size		
	Survivability		
	Maneuverability		
	Size		
	Receiver Range		
	Transmitter Range		
	Data Link Operations		
	Recovery Time		
	Initial Setup		
	Identification Time		
	Accuracy Location		
	Probability of Accurate ID		
	Reliability		
	Maintainability		
	Availability		
	Etc.		
Cost	Operating and Support Costs		
	Etc.		
Processes	Requirements Stable		
	Test Plan Approved		
Exit Criteria	Engine Bench Test		
	Accuracy Verified by Test Data and Analysis		
	Toolproofing Completed		
	Logistics Support Reviewed by User		

Downloaded from http://www.everyspec.com

ANNEX B
TO XYZ RISK MANAGEMENT PLAN
—PROGRAM RISK REDUCTION SCHEDULE—



XYZ Program Risk Reduction Schedule (Example)

Downloaded from http://www.everyspec.com

ANNEX C
TO XYZ RISK MANAGEMENT PLAN
—PROGRAM METRIC EXAMPLES—

Examples of Product-Related Metrics

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

Examples of Process Metrics

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

Downloaded from http://www.everyspec.com

Examples of Cost and Schedule Metrics

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

Downloaded from http://www.everyspec.com

ANNEX D
TO XYZ RISK MANAGEMENT PLAN
—MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION—

1.0 DESCRIPTION

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

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

In addition to standard reports, the PMO will need to create ad hoc reports in response to special queries etc. The Risk Management Coordinator will be responsible for these reports. Figure 3-3 shows a concept for a management and reporting system.

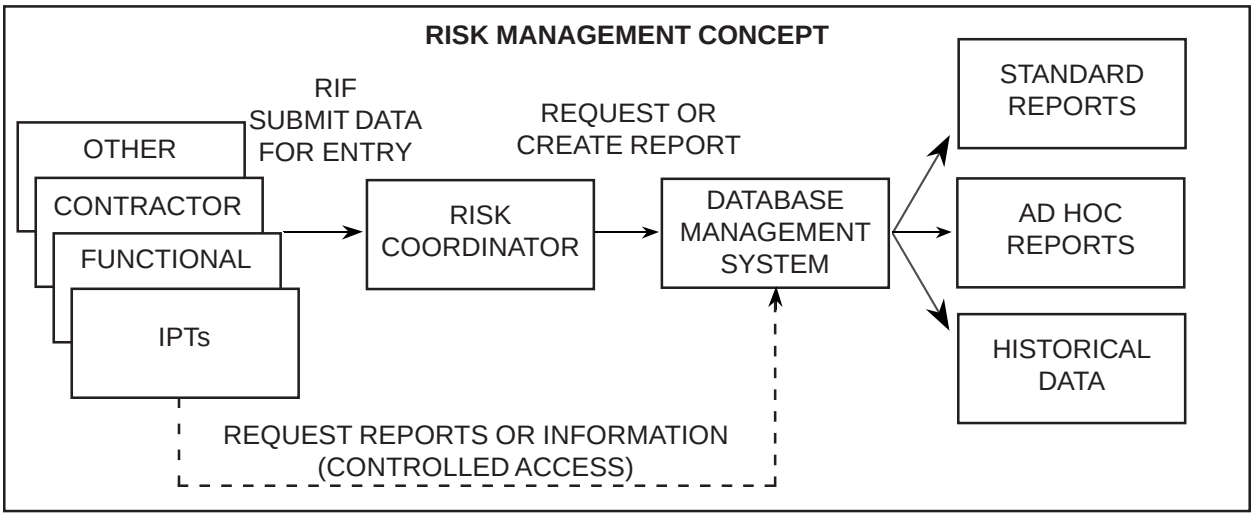


Figure 3-3. Conceptual Risk Management and Reporting System

2.0 RISK MANAGEMENT REPORTS—XYZ PROGRAM

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

Downloaded from http://www.everyspec.com

2.1 RISK INFORMATION FORM

The PMO needs a document that serves the dual purpose of a *source* of data entry information and a *report* of basic information for the IPTs, etc. The Risk Information Form (RIF) serves this purpose. It gives members of the project team, both Government and contractors, a format for reporting risk-related information. The RIF should be used when a potential risk event is identified and updated over time as information becomes available and the status changes. As a source of data entry, the RIF allows the database administrator to control entries. The format for a RIF is included on page B-30.

2.2 RISK ASSESSMENT REPORT

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

2.3 RISK-HANDLING DOCUMENTATION

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

2.4 RISK MONITORING DOCUMENTATION

The PM needs a summary document that tracks the status of high and moderate risks. The XYZ program will use a risk-tracking list that contains information that has been entered from the RIF. An example of the tracking report/list is shown on page B-31.

3.0 DATABASE MANAGEMENT SYSTEM (DBMS)

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

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

Downloaded from http://www.everyspec.com

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PMO. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PMO compared to all other risks, e.g., a one (1) indicates the highest priority.
Data Submitted	Gives the date that the RIF was submitted.
Major System/ Component	Identifies the major system/component based on the WBS.
Subsystem/ Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) or the risk.
Description of Risk	Briefly describes the risk. Lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, includes how it is manifested (e.g., design and engineering, manufacturing, etc.)
Key Parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report, if appropriate.
Analyses	Briefly describes the analysis done to assess the risk. Includes rationale and basis for results.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's Risk Management Plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the program's Risk Management Plan.
Time Sensitivity	Estimates the relative urgency for implementing the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measures using metrics for tracking progress in implementing risk handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk handling milestones.
Status Due Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

DBMS Elements

Downloaded from http://www.everyspec.com

Risk Information Form

Risk Identification Number Date
Risk Event:
Priority

Major System / Component / Functional Area:

Category:

Statement of Risk:
Description of Risk:

Key Parameters:
Assessment:

Analysis:

Process Variance
Probability of Occurrence:
Consequence:

Time Sensitivity:
Other Affected Areas:

Risk Handling Plans:

Risk Monitoring Activity:

Status
Status Date:

Assignment: Reported By:

Downloaded from http://www.everyspec.com

RISK TRACKING REPORT
(EXAMPLE REPORT)

I. Risk Area Status: Design P_F: Hi C_F: Hi

Significant Design Risks:

1. Title: System Weight P_F: Hi C_F: Hi
Problem: Exceed system weight by 10%; decreasing the range and increasing fuel consumption.
Action: Examining subsystems to determine areas where weight may be reduced. Reviewing the requirement. Closely watching the effect on reliability and survivability.

2. Title: Design Analysis P_v: Hi C_v: Hi
Problem: Failure Modes, Effects and Criticality Analysis (FMECA) is planned too late to identify and correct any critical single-point failure points prior to design freeze.
Action: Additional resources are being sought to expedite performance of FMECA.

II. Risk Area Status: Supportability P_F: Hi C_F: Mod / Hi
1. Title: Operational Support P_F: Hi C_F: Mod / Hi
Problem: Power supply subcontractor is in financial trouble and may go out of business. No other known sources exist.
Action: Doing trade study to see if alternative designs have a broader power supply vendor base. Prime contractor is negotiating with the subcontractor to buy drawings for development of second source.

Downloaded from http://www.everyspec.com

Potential Risk Area	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
• Accurately predicting shock environment shipboard equipment will experience.	• Use multiple finite element codes & simplified numerical models for early assessments.	SE03	31 Aug 98		
	• Shock test simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SE03	31 Aug 99		
• Evaluating acoustic impact of the ship systems that are not similar to previous designs.	• Concentrate on acoustic modeling and scale testing of technologies not demonstrated successfully in large-scale tests or full-scale trials.	SE031	31 Aug 98		
	• Factor acoustic signature mitigation from isolated modular decks into system requirements. Continue model tests to validate predictions for isolated decks.	SE032	31 Aug 99		

Watch List Example

Downloaded from http://www.everyspec.com

SAMPLE RISK MANAGEMENT PLAN FOR THE ABC PROGRAM (ACAT III, IV)

1.0 INTRODUCTION

1.1 PURPOSE

This Risk Management Plan (RMP) presents the process for implementing the comprehensive and proactive management of risk as part of the overall management of the *ABC* Program. Risk management is a program management tool to handle events that might adversely impact the program, thereby increasing the likelihood of success. This RMP describes a management tool that will:

- Serve as a basis for identifying alternatives to achieve cost, schedule, and performance goals,
- Assist in making decisions on budget and funding priorities,
- Provide risk information for Milestone decisions, and
- Allow monitoring the health of the program as it proceeds.

The RMP describes methods for assessing (identifying and analyzing), prioritizing, and monitoring risk drivers; developing risk-handling approaches, and applying adequate resources to handle risk. It assigns specific responsibilities for these functions, and prescribes the documenting, monitoring, and reporting processes to be followed.

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

2.0 PROGRAM SUMMARY

2.1 DESCRIPTION

The *ABC* Program is an ACAT III level program that was initiated in response to the NEW COM Operational Requirements Document (ORD) XXX, dated DD-MM-YYYY. The program will provide an *ABC* communications system that will be the common system (transmitter/receiver/controller) for all DoD components for UHF satellite communications. All DoD systems requiring UHF satellite communications procured subsequent to Initial Operational Capability (IOC) of the *ABC* system will incorporate it to meet their needs. The Bx Unmanned Air Vehicle is the lead system for integration. The program has completed the Program Definition and Risk Reduction phase and is preparing for a Milestone II decisions.

The system will be acquired using off-the-shelf UHF satellite communications systems. During Phase I of the program, two contractors delivered prototypes of their systems.

Downloaded from http://www.everyspec.com

One is a ruggedized commercial product and the other is built to military specifications. The Government tested both systems against functional and performance requirements and some environmental extremes. Although, each failed portions of the tests, both were evaluated as mature enough to represent an acceptable risk for proceeding to Phase II of the program, Engineering and Manufacturing Development.

2.2 ACQUISITION STRATEGY

The Government will invite the contractors that participated in Phase I of the program to submit proposals to refine their approached into a stable, interoperable, producible, supportable, and cost-effective design; validate the manufacturing or production process; and demonstrate system capabilities through testing. The Government will select one of the two proposals for Phase II of the program. The contractor, upon demonstration of exit criteria (See Annex A), will proceed with a Low Rate Initial Production (LRIP) of the system.

The IOC (20 systems) for the *ABC* system is required by FY-02 to support the fielding of the Bx UAV. Production capacity for the *ABC* system at IOC is expected to be 20 units per month to meet the demand of new systems.

2.3 PROGRAM MANAGEMENT APPROACH

The *ABC* Program Manager (PM) reports to the Program Director, Satellite Communications who has responsibility for all satellite communications systems. The *ABC* Program Office (PO) is composed of the PM and one assistant, with matrix support from the systems command organizations, and program management support from an external contractor. An integrated management approach will be used for this program. The government and selected contractor will have representation on Integrated Product Teams (IPTs) that will focus on cost, design, test, manufacturing, and support of the system. The PM chairs the government IPT that develops strategies for acquisition and contracts.

3.0 RISK-RELATED DEFINITIONS

The *Defense Acquisition Deskbook* (*DAD*) section 2521 contains the definitions for risk, risk management, risk events, and the terms associated with risk management that will be used by the *ABC* PO. Variation and clarification of definitions that appear in the DAD, as they are used in the ABC program are described below.

3.1 TECHNICAL RISK

This is the risk associated with the evolution of the design, production, and supportability of the *ABC* system affecting the level of performance necessary to meet the operational requirements. The contractor and subcontractors' design, test, and production processes (process risk) influence the technical risk and the nature of the product as depicted in the various levels of the Work Breakdown Structure (product risk). Process risks are assessed in terms of process variance fro known best practices and potential consequences of the

Downloaded from http://www.everyspec.com

variance. Product risks are assessed in terms of technical performance measures and observed variances from established profiles.

3.2 COST RISK

The risk associated with the ability of the program to achieve its life-cycle cost objectives. Two risk areas bearing on cost are (1) the risk that the cost estimates and objectives are accurate and reasonable and (2) the risk that program execution will not meet the cost objectives as a result of a failure to mitigate technical risks.

3.3 RISK RATINGS

This is the value that is given to a risk event (or the program overall) based on the analysis of the likelihood / probability and consequences of the event. For the *ABC* program, risk ratings of Low, Moderate, or High will be assigned based on the following criteria. See Section 6.2 give guidance on determining likelihood and consequences and defines the criteria.

4.0 RISK MANAGEMENT STATUS AND STRATEGY

4.1 RISK MANAGEMENT STATUS

As a result of the Program Definition and Risk Reduction Phase, the overall risk of the ABC Program for Milestone II is assessed as moderate, but acceptable. Moderate risk functional areas are environmental requirements; form, fit and function; integration; manufacturing; and cost.

4.2 RISK MANAGEMENT STRATEGY

The *ABC* Program risk management strategy is to handle program risks, both technical and non-technical, before they become problems, causing serious cost, schedule, or performance impacts. This strategy is an integral part of the Acquisition Strategy and the program management approach, and will be executed primarily through the Government-Contractor PIPT organization. The PIPTs will continuously and proactively assess critical areas (especially those listed in the previous paragraph) to identify and analyze specific risks and will develop options to mitigate all risks designated as moderate and high. The PIPTs will also identify the resources required to implement the developed risk-handling options. The PM, through the IIPT (Integrating Integrated Product Team), will review and approve the PIPT options. Once approved, the options will be incorporated into the program integrated master plan (IMP) and integrated master schedule (IMS). The PIPTs will monitor the effectiveness of the selected handling options, and adjust the risk handling approach as necessary.

IPTs will keep risk information current by using the risk management information system described in paragraph 6.5. Risk status will be reported at all program reviews. As new information becomes available, the PO and contractor will conduct additional reviews to ascertain if new risks exit. The goal is to be continuously looking to the future for areas that may severely impact the program.

Downloaded from http://www.everyspec.com

5.0 RISK MANAGEMENT ORGANIZATION

5.1 PROGRAM OFFICE

The *ABC* Program risk management organization is shown in Figure 5-1. This structure is integrated into the contractor and Government's existing organizations. Program Integrated Product Teams (PIPTs) will be formed for the functional areas that are critical to the success of the program. All functional areas not covered by a PIPT will be assessed and reviewed by the program Integrating Integrated Product Team (IIPT) co-chaired by the *ABC* PM and contractor PM, to ensure adequate vigilance against emerging risk areas. Independent risk assessors amy conduct reviews, when directed by the PM, to ensure the interface requirements of user systems are being met by the *ABC* system design.

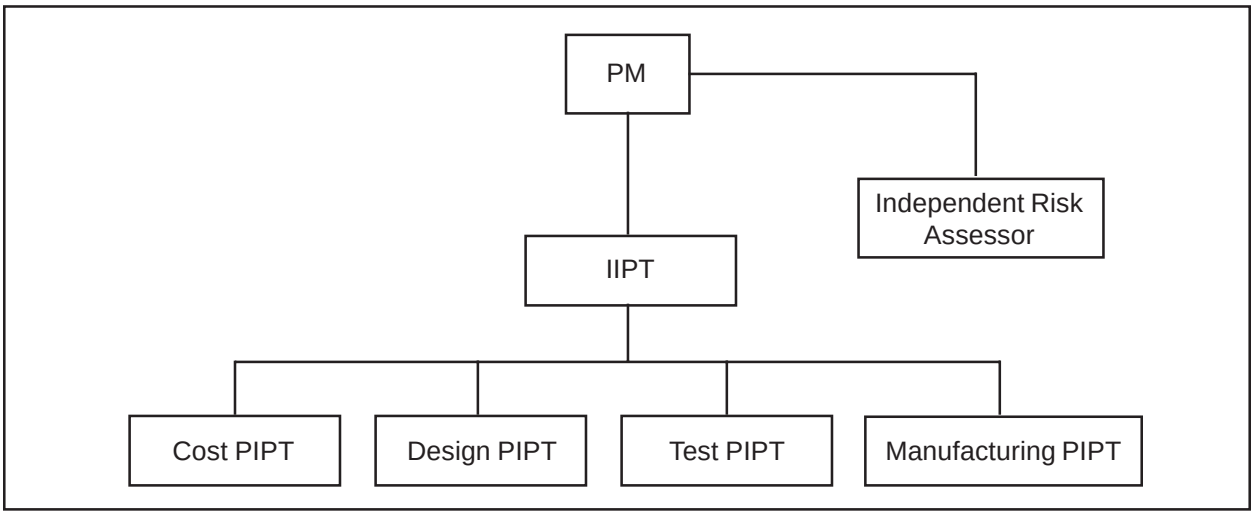


Figure 5-1. ABC Risk Management Organization

The PM the is overall coordinator of Risk Management Program and is responsible for:

- Maintaining this Risk Management Plan
- Maintaining the Risk Management Database
- Approving risk-handling options
- Incorporating risk-handling actions into the program master plan and schedule
- Briefing the decision makers on the status of *ABC* Program risk efforts
- Preparing risk briefings, reports, and documents required for Program Reviews and the acquisition Milestone decision processes.

IIPT

The IIPT is responsible for complying with the DoD risk management policy and for structuring an efficient and useful *ABC* risk management approach and supporting the Risk Management Coordinator / PM in carrying out his responsibilities. The PM and contractor

Downloaded from http://www.everyspec.com

PM Co-Chair the IIPT. The IIPT membership may be adjusted, but is initially established as the chairs of the PIPTs, a representative from the joint requirements and users' office, and a representative from the contractor.

PIPTs

The program PIPTs are the backbone of the program risk management efforts. They will execute the following responsibilities relative to their functional areas:

- Conduct risk assessments and develop risk-handling options, to include mitigation plans and resources required.
- Monitor effectiveness of risk-handling actions.
- Review and recommend to the PM changes in the overall risk management approach based on lessons learned.
- Update the risk assessments quarterly, or as directed.
- Ensure information in the Risk Management Database is current.
- Prepare risk status reports in their areas for all Program and Design Reviews.
- Ensure Design/Build Team responsibilities incorporate appropriate risk management tasks.
- Coordinate PIPT risk management activities with the IIPT.

6.0 RISK MANAGEMENT STRUCTURE AND PROCEDURES

The *ABC* program will use a structured risk management approach consisting of four elements: planning, assessment, handling, and monitoring. These elements and the general procedures to be used for each of them are described in subsequent paragraphs of this section. A number of guidance documents are useful in addressing these risk management elements, and should be used as appropriate by each PIPT. Some of these documents are listed below. (This list is not meant to be complete.)

- *Defense Acquisition Deskbook*-Section 2.5.2, Risk Management
- DSMC, *Risk Management Guide*, March 1998
- AFMC Pamphlet 63-101, Risk Management, 9 July 1997
- *The Navy's Best Practices Manual*, NAVSO P-6071, and *Top Eleven Ways to Manage Technical Risk*, NAVSO P-3686, provide insight into best practices.

Downloaded from http://www.everyspec.com

6.1 RISK PLANNING

Risk planning is essential for the execution of a successful risk management program. It will be done continuously by all PIPTs as an integral part of normal *ABC* program management. This RMP serves as the basis for all detailed risk planning, which must be continuous. The following paragraphs provide direction for the PIPTs on the conduct of risk planning for this program.

- PIPTs will develop an organized and thorough approach to assess, handle, and monitor risks. It will assign responsibilities for specific risk management actions and establish internal risk reporting and documentation requirements. The IIPT will monitor the planning activities of the PIPTs to ensure that they are consistent with this RMP and that appropriate revisions to this plan are made when required to reflect significant changes resulting from the PIPT planning efforts.

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

- Each PIPT will identify the resources required to implement the risk management actions. These resources include time, material, personnel, and cost. Training is a major consideration. All PIPT members should receive instruction on the fundamentals of risk management and special training in their areas of responsibility, if necessary. General risk management training will be arranged by the PO; PIPT leaders will identify any specialized training needs.

- This RMP establishes the basic documentation and reporting requirements for the program. PIPTs should identify any additional requirements, consistent with this RMP, that might be needed to effectively manage risk at their level.

6.2 RISK ASSESSMENT

The risk assessment process includes the identification of critical risk events / processes, the analyses of these events / processes to determine the likelihood of occurrence / process variance and consequences, and the priority of the risks. The output of this process provides the foundation for all the program risk-handling actions. Therefore, it is essential that all members of the *ABC* program team be as thorough as possible when identifying and analyzing risks. In addition to the normal areas of design , test, manufacturing, etc., PIPTs must identify and analyze the risks associated with such areas as manpower, environmental impact, system safety and health analysis, and security considerations. The *Defense Acquisition Deskbook*, Section 2524, provides information on various risk assessment techniques.

Risk assessments should be done by the PIPTs and the IIPT with active participation of both Government and contractor personnel. When necessary or appropriate, the PIPTs and the IIPT can direct a contractor-only assessment, or conduct a Government assessment. PIPTs and the IIPT should continually assess the risks in their areas, reviewing critical risk areas, risk ratings and prioritization, and the effectiveness of risk-mitigation actions whenever necessary to assess progress. The assessment process will be iterative,

Downloaded from http://www.everyspec.com

with each assessment building on the results of previous assessments. PIPTs and the IIPT will use the current assessment baseline as the starting point for their initial assessment during this phase. This baseline is a combination of the risk assessment delivered by the contractors as part of Phase 0, the PMO process risk assessment done before Milestone I, and the post award Integrated Baseline Review (IBR). Risk assessments will be updated and the results presented at all functional and program reviews, with a final update for this phase prepared not later than six months prior to the next scheduled Milestone decision.

6.2.1 Risk Identification

Each PIPT will review all aspects of their functional areas to determine the critical events that would prevent the program from achieving its objectives. They should apply the knowledge, best judgment and experience of the PIPT members, lessons learned from similar programs, and the opinion of subject-matter experts (SMEs) to identify these risk events. PIPTs should follow these general procedures to identify risk events:

- Understand the requirements and the program performance goals, which are defined as thresholds and objectives (see DoD 5000.2-R). Understand the operational (functional and environmental) conditions under which the values must be achieved as described in the Design Reference Mission Profile. The ORD and Acquisition Program Baseline (APB) contain Key Performance Parameters (KPPs).

- Determine technical / performance risks related to engineering and manufacturing processes. Identify those processes that are planned or needed to design, develop, produce, and support the system. Compare these processes with industry best practices and identify any variances or new, untried processes. These variances or untried practices are sources of risk. The contractor should review the processes to be used by its subcontractors to ensure they are consistent with best industry practices. Table 4-2 of the DSMC Risk Management Guide shows some of the specific of sources of process risk, and should be used by the PIPTs. NAVSO P-6071, Best Practices, which describes risks associated with design, test, production, facilities, logistics, management, and funding, should also be used by the PIPTs to identify risks.

- Determine technical / performance risks associated with the product (the ABC communications system) in the following critical risk areas: design and engineering, technology, logistics, concurrency, and manufacturing. The design and manufacturing PIPTs will identify the contract WBS elements down to level 3, and evaluate each of these elements to identify risk events. They will use a variety of methods to accomplish this: review of similar programs, existing program plans, expert opinion, etc.

- Identify schedule risk. Each PIPT will determine the schedule risk associated with its functional area. When identifying this schedule risk, they will consider the risk that the schedule estimate is accurate, and the risk that the established schedule can be met. The IIPT will monitor the development of the schedule risk in each PIPT, and consolidate these risks to identify overall program schedule risk.

Downloaded from http://www.everyspec.com

- Identify cost risk. Each PIPT will determine the cost risk associated with its functional area. They will identify risks associated with the accuracy of the cost estimates developed for their areas, and the risk that the established cost objectives will be met. The Cost PIPT will monitor the development of the other PIPT cost risk efforts, and consolidate their risks into a set of overall program cost risks.

- All identified risks will be documented in the RMIS, with a statement of the risk and a description of the conditions or situations causing concern and the context of the risk. See Paragraph 6.4 for guidance on documenting identified risks.

In identifying risks, PIPTs should be particularly alert for the following indicators. They are common sources of risk for all programs, and will be applicable to the *ABC* program.

- Requirements that are not clearly stated or stable,

- Failure to use Best Practices,

- Use of new processes materials, or applications of existing technologies,

- Use of processes lacking rigor in terms of maturity, documentation of established procedures, and validation,

- Insufficient resources—the people, funds, schedule, and tools, necessary for successful development, test, production and support of the *ABC* program,

- Lack of a formalized failure, reporting, analyze, and corrective action (FRACAS) system,

- Use of suppliers or subcontractors who are inexperienced in the processes for designing and producing required products,

- **Failure of prime contractor to effectively monitor processes and establish quality requirements for suppliers and subcontractors.**

6.2.2 Risk Analysis

Risk Analysis is an evaluation of the identified risk events to determine the likelihood of the events occurring and their consequences, to assign a risk rating based on the program criteria, and to prioritize the risks. Each PIPT and the IIPT are responsible for analyzing those risk events they identify. They may use subject matter experts for assistance, such as Field Activities, Service Laboratories, contractors, or outside consultants. The use of external assets will be coordinated through the PMO. The results of the analysis of all identified risks must be documented in the RMIS.

There are a number of techniques available to support risk analysis, to include studies, test results, modeling and simulation, and the opinions of qualified experts (to include justification of their judgment). The *DAD*, Section 2524.2 describes a number of analysis techniques that may be useful. Regardless of the technique used, PIPTs and the IIPT will identify all assumptions made in analyzing risk and, where appropriate, conduct a sensitivity analysis of assumptions.

Downloaded from http://www.everyspec.com

For each risk event, the following risk analysis guidelines will be used:

- **Likelihood/Probability**

For each risk identified, determine the likelihood that the event will occur. Five levels of likelihood will be used for the *ABC* program. Table 6-1 shows these levels and their definitions. PIPTs and the IIPT will assign one of these values to each identified risk event based on their analysis of the event. For example, if it is known that there will be a variance between the soldering process to be used for component *X* and the industry standard, this process variance risk event will be assigned a likelihood value of "e"—near. Similarly, if the Manufacturing PIPT determines that the schedule estimate for the fabrication of component *Y* is overly optimistic, and will probably not be attained, it would assign a likelihood level of *"c"* or *"d"* depending on its analysis of the schedule estimate.

Level	Likelihood of Occurrence
a	Remote
b	Unlikely
c	Likely
d	Highly likely
e	Near certainty

Table 6-1. Likelihood Levels

- **Consequence**

For each risk identified, the following question must be answered: *Given the event occurs, what is the magnitude of the consequence?* For the *ABC* program, consequence will be determined in each of four areas: technical performance, schedule, cost, and impact on other teams.

Technical Performance: This category relates to the risks associated with the processes to be used in the development, testing, and manufacturing of the ABC system, and the nature of the ABC communications system. It includes the form, fit, function, manufacturability, supportability, etc. Essentially, technical risk includes all requirements that are not part of cost and schedule. The wording of each consequence level is oriented toward design and production processes, life cycle support, and retirement of the system. For example, the word "margin" could apply to weight margin during design, safety margin during testing, or machine performance margin during production.

Schedule: The description in the Schedule is self-explanatory. The need dates, key milestones, critical path, and key team milestones are meant to apply to all program areas and PIPTs.

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

Downloaded from http://www.everyspec.com

Impact on Other Teams: Both the consequences of a risk and the mitigation actions associated with handling the risk may impact another team. This may involve additional coordination or management attention (resources), and may therefore increase the level of risk. This is especially true of mitigation actions that involve the use of common manufacturing processes and / or equipment.

PIPTs and the IIPT will evaluate each risk event in terms of these areas, and assign a level of consequence (1-5). Table 6-2 shows these 5 levels of consequence, and defines the levels for each area. This table will be used when assigning the consequence magnitude.

Level	Technical Performance	Schedule	Cost	Impact on Other Teams
1	Minimal or no impact	Minimal or no impact	Minimal or no impact	None
2	Acceptable with some reduction in margin	Additional resources required. Able to meet need dates	<5%	Some impact
3	Acceptable with significant reduction in margin	Minor slip in key milestone. Not able to meet need dates	5-7%	Moderate impact
4	Acceptable—no remaining margin	Major slip in key milestone or critical path impacted	7-10%	Major impact
5	Unacceptable	Can't achieve key team or major program milestone	>10%	Unacceptable

Table 6-2. Risk Consequence

6.2.3 Risk Rating

Each identified risk will be assigned a risk rating based on the joint consideration of event likelihood and consequence. This rating is a reflection of the severity of the risk and provides a starting point for the development of options to handle the risk. It is important to consider both the likelihood and consequences in establishing the rating, for there may be risk events that have a low likelihood, but whose consequences are so severe that the occurrence of the event would be disastrous to the program.

Figure 6-1 describes the risk rating process that will be used in this program. PIPTs and the IIPT will analyze each risk event to determine the likelihood and consequence values using the definitions in Tables 6-1 and 6-2; they will determine the consequence for each of the four areas (technical performance, schedule, cost, and team impact). The values will be used to determine the risk rating using the Assessment Guide in Figure 6-1. The Assessment Guide defines the risk rating associated with each combination of likelihood and consequence values, and will be used throughout the program. For example, consequence / likelihood level 1b corresponds to a risk rating of (L) LOW, level 4b corresponds to MODERATE risk, and level 5c corresponds to HIGH risk.

Those risk events that are assessed as MODERATE or HIGH will be submitted to the *ABC* PM on a Risk Identification Form (RIF). See Appendix B for the RIF format. PIPTs and the IIPT must actively manage these MODERATE and HIGH risks. They must also continu-

Downloaded from http://www.everyspec.com

ously assess the other identified risks in their areas to see if their ratings have become MODERATE or HIGH.

6.2.4 Risk Prioritization

PIPTs and the IIPT will prioritize the MODERATE and HIGH risks in their areas. This prioritization will provide the basis for the development of risk handling plans and the allocation of risk management resources. Prioritization will be accomplished using expert opinion within the PIPTs, and will be based on the following criteria:

- Risk Rating—Obviously HIGH-MODERATE.
- Consequence—Within each rating, the highest value of consequence, e.g., e.
- Urgency—How much time is available before risk-handling actions must be initiated.
- Likelihood—Within each rating, the highest value, e.g., "e."

Risk Assessment Process

Level	Likelihood of Occurrence
a	Remote
b	Unlikely
c	Likely
d	Highly likely
e	Near certainty

ASSESSMENT GUIDE

Likelihood	1	2	3	4	5
e	L	M	H	H	H
d	L	M	M	H	H
c	L	M	M	M	H
b	L	L	L	M	M
a	L	L	L	L	M

Consequence

RISK ASSESSMENT

HIGH—Unacceptable, Major disruption likely. Different approach required. Priority management attention required.

MODERATE—Some disruption. Different approach may be required. Additional management attention may be needed.

LOW—Minimum impact. Minimum oversight needed to ensure risk remains low.

Level	Technical Performance	Schedule	Cost	Impact on Other Teams
a	Minimal or no impact	Minimal or no impact	Minimal or no impact	None
b	Acceptable with some reduction in margin	Additional resources required. Able to meet need dates	<5%	Some impact
c	Acceptable with significant reduction in margin	Minor slip in key milestone. Not able to meet need dates	5-7%	Moderate impact
d	Acceptable—no remaining margin	Major slip in key milestone or critical path impacted	7-10%	Major impact
e	Unacceptable	Can't achieve key team or major program milestone	>10%	Unacceptable

Figure 6-1. Risk Assessment Process

Downloaded from http://www.everyspec.com

The IIPT will review the prioritized list of PIPT-developed risks, and integrate them into a single list of prioritized program risks, using the same criteria.

6.3 RISK HANDLING

After the program's risks have been identified, analyzed, and prioritized, PIPTs and the IIPT must develop an approach for handling each MODERATE and HIGH risk. For all such risks, the various handling techniques should be evaluated in terms of feasibility, expected effectiveness, cost and schedule implications, and the effect on the system's technical performance, and the most suitable technique selected. The *DAD* section 2524.3 contains information on the risk-handling techniques and various actions that can be used to implement them. Reducing requirements as a risk avoidance technique will be used only as a last resort, and then only with the participation and approval of the user's representative at the IIPT level.

The results of the evaluation and selection will be included and documented in the RMIS using the RIF. This documentation will include the following elements:

- What must be done,
- List of all assumptions,
- Level of effort and materials required,
- Resources needed that are outside the scope of the contract or official tasking,
- Estimated cost to implement the plan,
- Proposed schedule showing the proposed start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant Program activities / milestones,
- Recommended metrics for tracking risk-handling activity,
- Other PIPTs, risk areas, or other handling plans which may be impacted,
- Person responsible for implementing and tracking the selected option.

Risk handling actions will be integrated into program planning and scheduling, and incorporated into the IMP and IMS. PIPTs and the IIPT will develop these risk-handling actions and events in the context of Work Breakdown Structure (WBS) elements, establishing a linkage between them and specific work packages that makes it easier to determine the impact of actions on cost, schedule, and performance. The detailed information on risk-handling actions and events will be included in the RIF for each identified risk, and thus be resident in the RMIS.

6.4 RISK MONITORING

Risk monitoring is the systematic tracking and evaluation of the progress and effectiveness of risk-handling actions by the comparison of predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk-

Downloaded from http://www.everyspec.com

handling actions. The PIPTs and the IIPT will monitor all identified risks in their areas, with particular attention to those rated as HIGH or MODERATE. There are a number of techniques and tools available for monitoring the effectiveness of risk-handling actions. (See *DAD* section 2524.4 for information on specific techniques.) PIPTs and the IIPT must select those that best suit their needs. No single technique or tool is capable of providing a complete answer—a combination must be used. At a minimum, each PIPT and the IIPT will use the Risk Tracking Report (RTR) and Watch List for day-to-day management and monitoring of risks. See Annex B for examples of an RTR and Watch List. The status of risk-handling actions for all MODERATE and HIGH risks will be an agenda item at each program or functional area review.

For each identified risk, the PIPTs and IIPT will establish a management indicator system (metrics) that provides accurate, timely, and relevant risk monitoring information in a clear, easily understood manner. PIPTs and the IIPT should select metrics that portray the true state of the risk events and handling actions. See Annex C for an example of metrics that may be used.

MODERATE or HIGH risks will also be monitored by the *ABC* PM through the IIPT, using information provided by the appropriate PIPT, until the risk is considered LOW and recommended for "Close Out." PIPTs and the IIPT will continue to monitor LOW risk events in their areas to ensure that appropriate risk-handling action can be initiated if there are indications that the rating may change.

The status of the risks and the effectiveness of the risk-handling actions will be agenda items for all functional area and program reviews, and will be reported to the PM on the following occasions:

- Quarterly,
- When the IPT determines that the status of the risk area has changed significantly (as a minimum when the risk changes from high to moderate to low, or vice versa),
- When requested by the Program Manager.

6.5 RISK MANAGEMENT INFORMATION SYSTEM (RMIS), DOCUMENTATION, AND REPORTS

The *ABC* Program uses a modified version of Risk Matrix as its RMIS. The Risk Matrix database will contain all of the information necessary to satisfy the program documentation and reporting requirements. This information will include risk assessment documents, risk-handling plans, contract deliverables, if appropriate, and any other risk-related reports. The program office will use data from the RMIS to create reports for senior management and for day-to-day management of the program. The program produces a set of standard reports for periodic reporting and has the ability to create ad hoc reports in response to special queries.

Each PIPT and the IIPT are responsible for entering and maintaining accurate risk management data in the RMIS. A standard format Risk Information Form (RIF) Data will be

Downloaded from http://www.everyspec.com

used for data entry. A RIF will be completed and submitted when a potential risk event is identified, and will be updated as information becomes available as the assessment, handling, and monitoring functions are executed. See Annex B for a sample of the RIF. Annex B also contains examples of reports to be used in the *ABC* Program.

Downloaded from http://www.everyspec.com

ANNEX A
TO ABC RISK MANAGEMENT PLAN
—CRITICAL PROGRAM ATTRIBUTES—

Category	Description	Responsible IPT	Remarks
Performance/Physical	Transmitter Power		
	Weight		
	MTBF		
	Receiver Gain		
	EMP Survivability		
	Heat Dissipation		
	Size		
	Receiver Range		
	Transmitter Range		
	Data Link Operations		
	Interface Commonality		
	Initial Setup		
	Identification Time		
	Accuracy Location		
	Bandwidth		
	Reliability		
	Maintainability		
	Availability		
	Etc.		
Cost	Operating and Support Costs		
	Etc.		
Processes	Requirements Stable		
	Test Plan Approved		
Exit Criteria	Bench Test		
	Accuracy Verified by Test Data and Analysis		
	Toolproofing Completed		
	Logistics Support Reviewed by User		

Downloaded from http://www.everyspec.com

ANNEX B
TO ABC RISK MANAGEMENT PLAN
—MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION—

1.0 DESCRIPTION

In order to manage risk, we need a database management system that stores and allows retrieval of risk-related data. The Risk Management Information System provides data for creating reports and serves as the repository for all current and historical information related to risk. The PM is responsible for the overall maintenance of the RMIS, and he/she or his/her designee are the only persons who may enter data into the database.

The RMIS has a set of standard reports. If PIPTs or functional managers need additional reports, they should work with the PM to create them. Access to the reporting system will be controlled, however any member of the Government or contractor team may obtain a password to gain access to the information.

In addition to standard reports, the PO will need to create ad hoc reports in response to special queries, etc. The PM will be responsible for these reports.

Downloaded from http://www.everyspec.com

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PO. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PO compared to all other risks, e.g., a one (1) indicates the highest priority.
Data Submitted	Gives the date that the RIF was submitted.
Major System/Component or Process	Identifies the major system/component based on the WBS, or the process in which the risk event occurs.
Subsystem/ Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) or the risk.
Description of Risk	Briefly describes the risk; lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/ performance, include how it is manifested (e.g., design and engineering, manufacturing, etc.)
Key parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report (see next paragraph), if appropriate.
Analysis	Briefly describes the analysis done to assess the risk; includes rationale and basis for results.
Process Variance	States the variance of critical technical processes from known standards or best practices, based on definitions in the program's risk management plan.
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's Risk Management Plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the program's Risk Management Plan.
Risk Rating	Identifies the rating assigned to the risk based on the criteria established by the program.
Time Sensitivity	Estimates the relative urgency for implement the risk-handling option. If appropriate, identifies any other subsystem or process that this risk affects.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measurement and metrics for tracking progress in implementing risk-handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk handling milestones.
Status Due Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

DBMS Elements

Downloaded from http://www.everyspec.com

2.0 RISK MANAGEMENT FORMS AND REPORTS

The following are examples of basic reports and forms that are used in the *ABC* Program.

2.1 RISK INFORMATION FORM

The PO needs a document that serves the dual purpose of a source of data entry information and a report of basic information for the PIPTs, etc. The Risk Information Form (RIF) serves this purpose. It gives members of the project team, both Government and contractors, a format for reporting risk-related information. The RIF will be used when a potential risk event is identified and updated over time as information becomes available and the status changes. As a source of data entry, the RIF allows the database administrator to control entries. The format and information required in a RIF is detailed in the following table.

2.2 RISK MONITORING DOCUMENTATION

The PM needs a summary document that tracks the status of HIGH and MODERATE risks. The *ABC* program will use a Risk-Tracking Report (RTR) that contains information that has been entered from the RIF. An example of the RTR is shown in Figure 7-1. The PM and PIPTs must also be aware of upcoming deadlines and events to ensure they are not

RISK TRACKING REPORT
(EXAMPLE REPORT)

I. Risk Area Status: Design Likelihood: High Consequence: High

Significant Design Risks:

1. Title: System Weight Likelihood: High Consequence: High
Problem: Exceed system weight by 10%; decreasing the range and increasing fuel consumption.
Action: Examining subsystems to determine areas where weight may be reduced. Reviewing the requirement. Closely watching the effect on reliability and interoperability.

2. Title: Design Analysis Likelihood: High Consequence: High
Problem: Failure Modes, Effects and Criticality Analysis (FMECA) is planned too late to identify and correct any critical single-point failure points prior to design freeze.
Action: Additional resources are being sought to expedite performance of FMECA.

II. Risk Area Status: Supportability Likelihood: High Consequence: Moderate / High
1. Title: Operational Support Likelihood: High Consequence: Moderate / High
Problem: Power supply subcontractor is in financial trouble and may go out of business. No other known sources exist.
Action: Doing trade study to see if alternative designs have a broader power supply vendor base. Prime contractor is negotiating with the subcontractor to buy drawings for development of second source.

Figure 7-1. Example Risk Tracking Report

Downloaded from http://www.everyspec.com

caught unprepared for a result. A Watch List will be used to track upcoming events and activities. A sample Watch List is contained in Figure 7-2.

2.3 PIPT RISK SUMMARY REPORT

In addition to the RTRs for individual HIGH and MODERATE risks, PIPTs will prepare a periodic summary of the ratings for all the risks in their areas. Figure 7-3 provides an example of this report. The format for this summary is based on the Risk Assessment Guide shown in Figure 6-1. The entries in each cell of the matrix represent the number of identified risks with the corresponding likelihood and consequence values.

Potential Risk Event	Risk Reduction Actions	Action Code	Due Date	Date Completed	Explanation
• Accurately predicting shock environment shipboard equipment will experience.	• Use multiple finite element codes & simplified numerical models for early assessments.	SE03	31 Aug 99		
	• Shock test simple isolated structure, simple isolated deck, and proposed isolated structure to improve confidence in predictions.	SE03	31 Aug 99		
• Evaluating impact of circuit cards that are not similar to previous designs.	• Concentrate on modeling and scale testing of technologies not demonstrated successfully in large-scale tests or full-scale tests.	SE31	31 Apr 99		
	• Factor design and into system requirements. Continue model tests to validate predictions for isolated decks.	SE032	31 Aug 99		

Figure 7-2. Sample Watch List

Downloaded from http://www.everyspec.com

Likelihood					
e	0	1	0	1	0
d	0	0	1	1	2
c	3	2	1	0	0
b	4	3	5	2	1
a	5	3	1	1	2
	1	2	3	4	5
	Consequence				

Figure 7-3. Example PIPT Risk Summary Report

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

Examples of Process Metrics

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

Example of Cost and Schedule Metrics

Downloaded from http://www.everyspec.com

APPENDIX C

GLOSSARY

ACAT	Acquisition Category
AHP	Analytical Hierarchy Process
AMSAA	Army Materiel System Analysis Activity
APB	Acquisition Program Baseline
API / PM	Acquisition Program Integration / Program Management
ASP	Acquisition System Protection
BCS	Baseline Comparison System
BIT	Built-in Test
BMP	Best Manufacturing Program
CAIG	Cost Analysis Improvement Group
CAIV	Cost As an Independent Variable
CARDs	Cost Analysis Requirements Description
CCA	Component Cost Analysis
CCDR	Contractor Cost Data Reporting
CDF	Cumulative Distribution Function
CDR	Critical Design Review
CER	Cost Estimating Relationship
CPM	Critical Path Method
CWBS	Contract Work Breakdown Structure
DAD	Defense Acquisition Deskbook
DAU	Defense Acquisition University
DBMS	Database Management System
DCMC	Defense Contract Management Command
DEM / VAL	Demonstration / Validation
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DoDD	DoD Directives
DPG	Defense Planning Guidance

Downloaded from http://www.everyspec.com

DSMC	Defense Systems Management College
DT&E	Development, Test and Evaluation
DTSE&E	Director, Test, Systems Engineering, and Evaluation
EAC	Estimate At Completion
EMD	Engineering and Manufacturing Development
EMP	Electromagnetic Pulse
ESC	Electronic Systems Center
ESM	Electronic Warfare Support Measures
ESS	Environmental Stress Screening
EV	Earned Value
FMECA	Failure Mode, Effects and Criticality Analysis
FRACAS	Failure, Reporting, Analyze, and corrective Action
GAO	Government Accounting Office
GFE	Government Furnished Equipment
HWIL	Hardware-in-the-Loop
IBR	Integrated Baseline Review
IFF	Identification Friend or Foe
IIPT	Integrating Integrated Product Teams
IMS	Integrated Master Schedule
IMP	Integrated Master Plan
IOC	Initial Operational Capability
IPD	Integrated Product Development
IPPD	Integrated Product and Process Development
IPT	Integrated Product Teams
KPP	Key Performance Parameters
LCC	Life-Cycle Cost
LFT&E	Live-Fire Test and Evaluation
LRIP	Low Rate Initial Production

Downloaded from http://www.everyspec.com

M&E	Mechanical and Electrical
M&S	Modeling and Simulation
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDAPs	Major Defense Acquisition Programs
MIS	Management Information System
MNS	Mission Need Statement
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
MS	Milestone
MTBF	Mean Time Between Failure
NDI	Non-Developmental Item
NSSN	New Nuclear Submarine
O&M	Operations and Maintenance
OIPT	Overarching Integrated Product Team
OLRDB	On-Line Risk Data Base
ORD	Operational Requirement Document
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
PDF	Probability Density Function
PDRR	Program Definition/Risk Reduction
PIIPT	Program Integrating Integrated Product Team
PIPT	Program Integrated Product Team
PM	Program Manager
PMI	Project Management Institute
PMO	Program Management Office
PMWS	Program Manager's Work Station
POE	Program Office Estimate
POM	Program Objective Memorandum
PRAG	Performance Risk Assessment Group
PRR	Production Readiness Review
PSR	Program Status Report

Downloaded from http://www.everyspec.com

R&D	Research and Development
RD&A	Research, Development and Acquisition
R&M	Repairability and Maintainability
RAR	Risk Assessment Report
RFP	Request for Proposal
RIF	Risk Information Form
RMIS	Risk Management Information System
RMP	Risk Management Plan
RTR	Risk Tracking Report
SEI	Software Engineering Institute
SME	Subject-Matter Expert
SOW	Statement of Work
SPMN	Software Program Managers Network
SRE	Software Risk Evaluation
SRR	System Requirements Review
STA	Special Threat Assessment
STAR	Special Threat Assessment Report
T&E	Test and Evaluation
TAAF	Test-Analyze-and-Fix
TEMP	Test and Evaluation Master Plan
TPM	Technical Performance Measurement
TRIMS	Technical Risk Identification and Mitigation System
UAV	Unmanned Aerial Vehicle
UHF	Ultra-High Frequency
USC	United States Code
USD(A&T)	Under Secretary of Defense, Acquisition and Technology
WBS	Work Breakdown Structure

Downloaded from http://www.everyspec.com

APPENDIX D

BIBLIOGRAPHY

AFMC 63-101 Update, *Risk Management Handbook, Appendices to Augment AFMC Pamphlet 63-101*, 4 June 1996.

AFMC Pamphlet 63-101, *Risk Management*, 9 July 1997.

AFSMC, *Risk Management Critical Process Assessment Tool*, Version 2, 9 June 1998.

AMC-P 70-27, *Guidance for Integrated Product and Process Management, Volume 1, Concept Implementation*, 15 March 1996.

AMSAA Special Publication 71, *AMSAA Risk Assessment Primer*, 1995.

AT&T and Department of the Navy, *Practical Engineering Guides for Managing Risk: Moving a Design into Production*, McGraw-Hill, 1993.

AT&T and Department of the Navy, *Practical Engineering Guides for Managing Risk: Design To Reduce Technical Risk*, McGraw-Hill, 1993.

AT&T and Department of the Navy, *Practical Engineering Guides for Managing Risk: Design's Impact on Logistics*, McGraw-Hill, 1993.

AT&T and Department of the Navy, *Practical Engineering Guides for Managing Risk: Testing to Verify Design and Manufacturing Readiness*, McGraw-Hill, 1993.

Biery, F., D. Hudak and S. Gupta, "Improving Cost Risk Analysis", *The Journal of Cost Analysis*, Spring 1994, pp. 57-86.

Boehm, Barry W. "Software Risk Management: Principles and Practices," IEEE Software, January 1991.

Carnegie Mellon University, Software Engineering Institute, *Continuous Risk Management Guidebook*, 1996.

Charette, R. N., *Software Engineering Risk Analysis and Management*, McGraw-Hill, 1989.

Conrow, Edmond H., *The Use of Ordinal Risk Scales in Defense Systems Engineering*, 1995 Acquisition Research Symposium Proceedings, Defense Systems Management College, June 1995.

Conrow, Edmond H., "Some Limitations of Quantitative Risk Analysis Approaches Used in Project Management"—Developed for the Office of the Secretary of Defense, April 1998.

Conrow, Edmond H., and Patty S. Shishido, "Implementing Risk Management on Software-Intensive Projects," IEEE Software, May / June 1997.

CVN 77, *Risk Management Plan*, November 1998.

Downloaded from http://www.everyspec.com

DoD 4245.7M, *Transition from Development to Production*, September 1985.

DoD 5000.2-R, *Mandatory Procedures for Major Defense Acquisition Programs (MDBPs) and Major Automated Information System (MAIS) Acquisition Programs*, 1996.

DoD 5000.4-M, *Cost Analysis Guidance and Procedures*, 1992.

DoD Defense Acquisition Deskbook—Compendium of Acquisiton-Related mandatory and discretionary guidance, including risk management (http://www.deskbook.osd.mil).

DoD Inspector General Report 96-162, *Audit Report on the Audit of Risk Management Programs for Defense Acquisition Systems*, June 1996.

DoDD 5000.1, *Defense Acquisition*, 1996.

DoDD 5000.4, *OSD Cost Analysis Improvement Group*, 1992.

DSMC, *Earned Value Management Textbook*, December 1996.

DSMC, *Program Management Teaching Note, Acquisition Program Protection*, 12 January 1998.

DSMC, *Program Risk Management Teaching Note*, 15 December 1997

DSMC, *Scheduling Guide for Program Managers*, 1994.

DSMC, *System Engineering Management Guide*, 1990.

EIA Engineering Standard, IS-632, *Systems Engineering*, 1994.

Government Accounting Office, *Technical Risk Assessment: The Status of Current DoD Efforts*, PEMD-86-5, (Washington, DC), April 1986.

Hayes, R. W., et al., *Risk Management in Engineering Construction*, Special SERC Report by Project Management Group, UMIST, Thomas Telford LTD, London, December 1986.

Hulett, D.T., *Project Cost Risk Assessment*, Hulett & Associates, Los Angeles, CA, 1994.

Hulett, D.T., "Project Schedule Risk Assessment", *Project Management Journal*, March 1995

Hulett, D.T., "Schedule Risk Analysis Simplified", *Project Management Journal*, July 1996.

JLC Joint Group on Systems Engineering, *Practical Software Measurement*, March 27, 1996.

Keny, R. and D. Von Winterfield, "On the Use of Expert Judgment on Complex Technical Problems", *IEEE Transactions on Engineering Management*, Vol. 36, No. 2, May 1989, pp. 83-86.

Linstone, H. A., Turoff, M., *The Delphi Method Techniques and Application*, Addison-Welsey Publishing Company, Reading, MA, 1975.

MIL-STD-1388-1A, *Logistics Support Analysis*, Task 203—Comparative Analysis, 1988.

MIL-STD-961D, *Department of Defense Standard Practice: Defense Specifications*, March 1995.

NAVSO P-3686, *Top Eleven Ways to Manage Technical Risk*, October 1998.

Downloaded from http://www.everyspec.com

NAVSO P-6071, *Best Practices: How to Avoid Surprises in the World's Most Complicated Technical Process*, March 1986.

New Attack Submarine Risk Management Plan, Draft, 15 April 1994.

Office of the Assistant Secretary of the Navy (RD&A), *Methods and Metrics for Product Success*, July 1994.

Pariseau, Richard and Oswalt, Ivar, "Using Data Types and Scales for Analysis and Decision Making," *Acquisition Review Quarterly*, Spring 1994, pp. 145-159.

PMI, *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities*, preliminary edition, 1992.

PMI, *Project and Program Risk Management*, PMBOK Handbook Series - Volume 6, 1992.

Project Management Institute, *Project and Program Risk Management, A Guide to Managing Project Risks and Opportunities*, preliminary edition, PMBOK Handbook Series - Volume 6, 1992.

Risk Matrix, USAF Communications and Airspace Management System Program Office, (ESC / TG), ESC, Hanscom AFB, MA, (617) 377-4953

SBIRS Risk Management Implementation, Lockheed Martin presentation to Risk Management Symposium, Manhattan Beach, CA, June 2-4, 1997.

Scholtes, Peter R., *The Team Handbook: How to Use Teams to Improve Quality*, Madison, WI, Joiner Associates, Inc., 1988.

Smith, P. L. and S.A. Book, *Reducing Subjective Guesswork and Maintaining Traceability When Estimating the 'Risks' Associated With a Cost Estimate*, The Aerospace Corporation, 1992.

Software Engineering Institute (SEI), *Continuous Risk Management Guidebook*, 1996.

Space and Naval Warfare Systems Command, *Open Systems Acquisition & Supportability Guide*, NGCR Document No. AST 003, Ver 1.0, 31 December 1996.

TR-6304-3-1, *Air Force Warranty Cost/Benefit Analysis Handbook*, 30 September 1993.

Tri-Service Technical Brief, 002-93-08, *Environmental Stress Screening Guidelines*, July 1993.

Tri-Service Technical Brief, *The TAAF Process: A Technical Brief for TAAF Implementation*, January 1989.

Tversky, A. and D. Kahneman, "Judgment Under Uncertainty: Heuristics and Biases", *Science*, No. 185, September 1974, pp. 1124-31.

Tversky, A., D. Kahneman and P. Slovic, *Judgment Under Uncertainty: Heuristics and Biases*, Cambridge University Press, 1982.

Under Secretary of Defense (Acquisition & Technology) [USD(A&T)] Memorandum, *Reducing Life Cycle Costs for New and Fielded Systems.*

Downloaded from http://www.everyspec.com

U.S. Air Force, "Guidelines for Successful Acquisition and Management of Software Intensive Systems," Version 2, June 1996.

U.S Air Force Materiel Command, *Acquisition Risk Management Guide*, 1993.

U.S. Navy, *Methods and Metrics for Product Success: A Dual-Use Guide*, 1994.

Downloaded from http://www.everyspec.com

DSMC PRESS
WANTS TO HEAR FROM YOU

Please rate this publication in various ways using the following scores:
4—Excellent 3—Good 2—Fair 1—Poor O—Does not apply

Name of this publication Risk Management Guide

This publication:
A._____ is easy to read.
B._____ has a pleasing design and format.
C._____ successfully addresses acquisition management and reform issues.
D._____ contributes to my knowledge of the subject areas.
E._____ contributes to my job effectiveness.
F._____ contributes to my subordinate's job effectiveness.
G._____ is useful to me in my career.

H._____ I look forward to receiving this publication.
I._____ I read all or most of this publication.
J._____ I recommend this publication to others in acquisition workforce.

How can we improve this publication? Provide any constructive criticism for us to consider for the future.

What other DSMC publications do you read?

OPTIONAL
Name/Title_____
Company/Agency_____
Address_____
Work Phone ( )_____DSN_____FTS_____
Fax_____Email_____

_____Please mail me a brochure listing other DSMC publications.

_____Please send a free subscription to the following at the address above.
_____Acquisition Review Quarterly _____Acquisition Reform Today Newsletter

Copy this form and fax it to DSMC Press at (703) 805-2917.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com