NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVING THE U.S. NAVY'S EXECUTION OF TECHNICAL AUTHORITY THROUGH A COMMON RISK MANAGEMENT AND TECHNICAL ASSESSMENT PROCESS

by

Thomas Andrew Tomaiko

September 2008

Thesis Advisor:	David F. Matthews
Co-Advisor:	Benjamin J. Roberts

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2008	Master's Thesis

4. TITLE AND SUBTITLE Improving the U.S. Navy's Execution of Technical Authority Through a Common Risk Management and Technical Assessment Process	5. FUNDING NUMBERS
6. AUTHOR(S) Thomas Andrew Tomaiko	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

The focus of this paper is upon improving the U.S. Navy's execution of technical authority.

1. Technical authority targets compliance with technical criteria and standards.
2. This targeting must be done at the earliest stages of program development and addressed during development of the program acquisition strategy.
3. An executable acquisition strategy must take into consideration the Navy's technical authority responsibility.
4. A successful strategy needs to provide the industry sufficient time to fully develop plans and deliver products, especially in high-risk program areas, and incorporate a system engineering process where the technical authorities can perform their mission.
5. History has shown that costs will increase if technical risks are not adequately addressed.

The purpose of this focus — on improving execution of technical authority — is to reduce exposure to risks and costs. This thesis defines the relationship between program authority and technical authority, and improves the state of technical authority through common policy development and implementation.

14. SUBJECT TERMS technical authority, risk management, common risk management process, technical assessment, technical assessment process, risk analysis, systems engineering, systems engineering management, systems engineering process, program management	15. NUMBER OF PAGES 109
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPROVING THE U.S. NAVY'S EXECUTION OF TECHNICAL AUTHORITY THROUGH A COMMON RISK MANAGEMENT AND TECHNICAL ASSESSMENT PROCESS

Thomas Andrew Tomaiko
Commander, United States Navy Retired
B.S., United States Naval Academy, 1987
Master of Science in Naval/Mechanical Engineering- 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: Thomas Andrew Tomaiko

Approved by: COL. David F. Matthews, USA (Ret).
Thesis Advisor

Dr. Benjamin J. Roberts
Co-Advisor

Dr. David Olwell
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The focus of this paper is on improving the U.S. Navy's execution of technical authority.

1. Technical authority targets compliance with technical criteria and standards.
2. This targeting must be done at the earliest stages of program development and addressed during development of the program acquisition strategy.
3. An executable acquisition strategy must take into consideration the Navy's technical authority responsibility.
4. A successful strategy needs to provide the industry sufficient time to fully develop plans and deliver products, especially in high-risk program areas, and incorporate a system engineering process where the technical authorities can perform their mission.
5. History has shown that costs will increase if technical risks are not adequately addressed.

The purpose of this focus — on improving execution of technical authority — is to reduce exposure to risks and costs. This thesis defines the relationship between program authority and technical authority, and improves the state of technical authority through common policy development and implementation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

AUTHOR'S BACKGROUND NOTE

This thesis is a compilation of my work predominately adapted from my work as the DD 21 Program Risk Manager from September 1999 – September 2002. However, this thesis is also the product of my work from September 2002 to June 2007.

As the DD 21 Program Risk Manager, I was responsible for developing/implementing realistic program risk management plans, evaluating program-wide risk assessments, developing appropriate risk-handling plans, monitoring risk reduction efforts, and recommending appropriate actions to the DD2 Program Manager. I continued to refine and apply the risk management knowledge, skills, and abilities I developed initially during my follow-on work as the Assistant Program Manager for T-AKE/SSP/T-AOE(X)/RSLS Programs from September 2002 – July 2005; as the Deputy Director for Ship Survivability & Structural Integrity from July 2005 – April 2006; as the Director for Ship Survivability & Structural Integrity from April 2006 – January 2007; and finally as the Executive Assistant and Chief of Staff to the Deputy Commander for Ship Design, Integration, and Engineering Directorate of the Naval Sea Systems Command from January 2007 – June 2007.

From July 2005 to June 2007, I provided direct support to the Chief Engineer of the Navy in planning and executing the establishment of the NAVSEA Research & Systems Engineering (R&SE) Competency mandated by the Assistant Secretary of the Navy for Research, Development and Acquisition, ASN (RD&A). During this time, I also attended the Naval Postgraduate School Joint Executive Systems Engineering Management PD-21 (SEM-PD) program. The SEM-PD21 program is a joint engineering and management degree program that is offered through our Wayne E. Meyer Institute of Systems Engineering. According to the Office of the Secretary of Defense, this is a pioneering executive leadership program designed to prepare today's technical experts and systems engineers for successful careers as program leaders and technically grounded senior managers of their business enterprises without leaving the workplace.

In order to meet the thesis requirement of the PD-21 executive master's degree program, I adapted the work products I produced over the period from September 1999 to June 2007 to produce a thesis that not only met the requirements of the academic degree, but was also timely and useful to the Chief Engineer of the Navy.

This thesis draws upon my work experience and fits into my job requirements, so as to minimize the amount of time and effort that it took me to complete the PD-21 executive masters degree program thesis requirement, be able to perform my job, accomplish one of my goals, NAVSEA's goals, and the Chief Engineer of the Navy's goals to further and strengthen technical authority in the Navy.

ACKNOWLEDGMENTS

The author is grateful for the support of this work by the Naval Postgraduate School and the Naval Sea Systems Command, Washington, DC. The completion of this research project was due to the support and guidance of many. The author would like to thank Dr. Ben Roberts and Colonel Dave Matthews for their guidance and Ms. Janis Higginbotham for her help with editing and formatting this thesis. A special thanks to Rear Admiral Kevin McCoy and Mr. Mike Riley for their support. In addition, the author is especially grateful for the support and encouragement of his wife, Susan, and for the inspiration provided by their five children, Ivy, Isamu, Austin, Cameron, and Peyton, and by their close friends and family.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In 2006, the Assistant Secretary of the Navy for Research, Development and Acquisition, ASN (RD&A), mandated the transformation of Naval Sea Systems Command (NAVSEA) into a competency-aligned organization (CAO). A CAO fosters a competency-based approach to mission performance. A key objective of NAVSEA's new CAO is to improve program management authority and contract authority through more effective technical authority. A key challenge facing NAVSEA in establishing a new CAO, is aligning program management, contract, and technical competencies. This will require a common alignment of the engineering workforce across the Navy, as well as common policy development and implementation.

NAVSEA is establishing the Research & Systems Engineering (R&SE) Competency. The R&SE Competency is one of nine competencies in the NAVSEA CAO. The R&SE Competency will focus on leading the workforce, managing the workload, and delivering combat systems and hull, mechanical, and electrical (HM&E) products to U.S. Navy Fleet customers through integrated product teams (IPTs) using common processes, engineering support and certification, and five vector employee development models.

The Navy Systems Commands (SYSCOMs) are assessing and improving the state of technical authority through common policy development and implementation, competency alignment, and targeted funding. Common Systems Engineering and Technical Authority (SE/TA) policy development and implementation continue to show steady progress. Naval Facilities Command (NAVFAC) and Naval Supply Command (NAVSUP) have now adopted the TA policy instruction the Naval Aviation Systems Command (NAVAIR), NAVSEA, and the Space Warfare Systems Command (SPAWAR) established in January 2005. Common approaches and frameworks for implementing TA through system engineering (SE) processes are provided in the Naval Systems Engineering Guide, published in 2004. What the SYSCOMs need now is a common risk-management process, a common policy for developing Systems

Engineering Plans (SEAs), a common technical review process, a common total platform and interoperability certification process, and a common systems engineering training program.

A. PURPOSE

This thesis seeks to improve the U.S. Navy's execution of technical authority. It provides a common risk management and technical assessment process, defines data/information elements needed to assess and track risks, and gives an overview of risk management within the context of overall program execution. This thesis also illustrates a top-level view of the relationship risk management has with program management and systems engineering at a macro level, and thereby identifies and describes the interdependencies and information flow necessary to manage risks.

1. Risk Management in DoD Background

The Department of Defense (DoD) requires program managers and acquisition officials to continually evaluate program risks and assess those risks in a manner appropriate to the system being acquired. The risk management discipline has been mandated via the DoD 5000 series guidance that evolved through thorough study, review, and analysis of acquisition successes and failures [1]. Extensive studies of commercial and government best practices form the foundation for the DoD 5000 series [2]. In addition to the imperatives delineated in that top-level guidance, risk management is further emphasized in the DoD *Acquisition Guidebook* and is a key curriculum component for the Defense Acquisition University.

B. DEFINITIONS AND A COMMON RISK LEXICON

Arguably, the most important attribute of a common risk management and technical assessment process is a commonly used set of terms. The most common terms pertaining to risk management are presented in this chapter. Other terms that may be useful are defined in Appendix A.

1. Risk

Risk is a measure of the inability to achieve overall objectives within defined cost, schedule, and technical performance constraints [6]. It has two components: (1) the *likelihood* of failing to achieve a desired result and (2) the *consequences* of failing to achieve that result [6]. For processes, risk is a measure of the difference between the actual performance of a process and the known best practice for performing that process.

2. Risk Management

Risk management is the act or practice of dealing with uncertainty [6]. 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 [6]. Figure 1 provides an overview of risk management components.

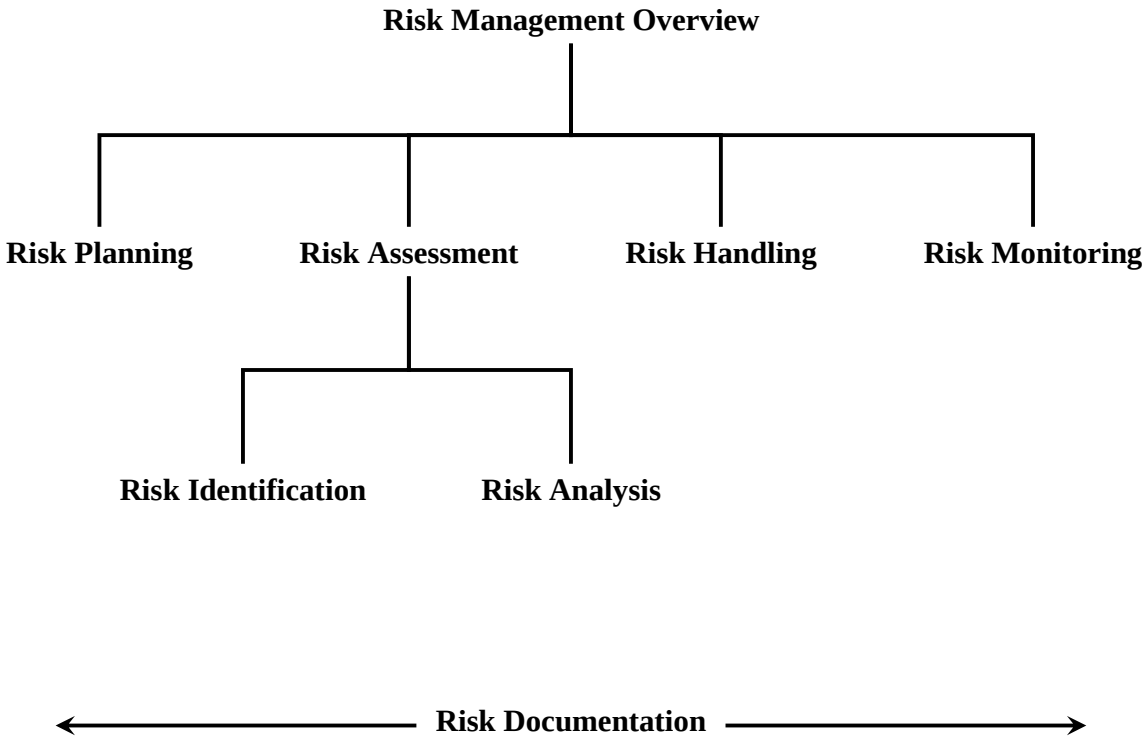


Figure 1. Overview of Risk Management Components, from [6].

Successful risk management depends upon appropriate tailoring of these risk management components to satisfy all relevant requirements beginning with the most critical ones. This requires focused management attention. In order to focus management attention on areas of uncertainty, which pose threats to program success, risk management must:

- Define, assess, and monitor metrics used to indicate program health
- Assess and characterize risks from the government's perspective
  - Set prioritizes based upon criticality of system and acquisition requirements
  - Establish (adjust) risk tolerance/risk acceptance levels to optimize return on investment
- Provide the organization with tools, training, and support so that risk management concepts and processes are routinely practiced and understood by all program participants.

Successful risk management is highly dependent upon the degree of interaction between the program management, risk management, and system engineering disciplines. Success is also dependent upon standardization and consistent application of risk assessment criteria that are traceable to overall program objectives.

DoD acquisition reform initiatives have empowered industry at the earliest possible stage of design development to achieve design capabilities and substantially lower total ownership cost. Therefore, DoD risk management must leverage industry risk management by:

- Establishing a program risk management process that includes (leverages) industry risk management
- Identifying Critical Program Attributes (CPAs)
- Defining risk assessment criteria that link to CPAs
- Provide tools, training, and risk planning

3. Technical Risk

Technical risks are those tied to design and production of the systems necessary to meet user requirements [6]. The contractors' and subcontractors' design, test, and production processes influence the technical risk [6]. The nature of the desired product or system is depicted in the various levels of the Work Breakdown Structure (WBS)

4. Cost Risk

Cost risks are uncertainties related to achieving total life cycle cost objectives [6]. Cost risk analysis, in general, examines: (1) the risk that cost estimates and objectives are not accurate and reasonable, and (2) the risk that program execution will not meet the cost objectives as a result of a failure to mitigate operational or development risks [6].

5. Schedule Risk

Schedule risks address the uncertainties linked to the adequacy of the time estimated and allocated for development, production, and fielding of the system [6]. Schedule risk is usually analyzed in terms of: (1) the risk that schedule estimates and objectives are not realistic and reasonable, and (2) the risk that program execution will fall short of schedule objectives as a result of failure to mitigate operational or development risks [6].

6. Risk Ratings

Risk ratings are calculated values based on the analysis of the likelihood and consequences of failure [6]. Qualitative risk ratings of low, moderate, or high can be assigned based on the following descriptive criteria.

- **Low Risk:** Has little potential to cause schedule disruption, increase cost, or degrade performance [6]. Normal contractor effort and normal government monitoring will probably be able to overcome uncertainties.

- **Moderate Risk:** Can potentially cause some disruption of schedule, increase in cost, or increase degradation of performance [6]. Special contractor

emphasis and close government monitoring will probably be able to overcome uncertainties. A moderate risk level indicates that the program manager's control may be needed to avoid significant impact to the program.

- **High Risk:** Likely to cause serious disruption of schedule, increase in cost, or increase degradation of performance even with special contractor emphasis and close government monitoring [6]. A high-risk level indicates the need for the program manager's control to avoid serious impact to the program.

7. Independent Risk Assessor

An independent risk assessor is an individual or committee that is not in the management chain or assigned to perform the tasks being assessed [6]. Use of independent risk assessors is a technique used to ensure that all risk areas are identified and that consequence and likelihood (or process variance) of not meeting operational performance requirements or development requirements are properly understood [6]. The technique can be used at different program levels (e.g., Program Office, Service Field Activities, and Contractors) [6]. The program manager will approve the use of independent assessors [6]. In general, risk managers, department heads, and functional area experts will recommend independent assessments as circumstances dictate.

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 [6]. DoD 4245.7-M, *Transition from Development to Production, Solving the Risk Equation*, provides several examples of these templates [6]. For each template process described in DoD 4245.7-M, a corresponding best practice is described in NAVSO P-6071 [6]. These documents outline the ideal or low risk approach and thus serve as a baseline to assess risk for some processes [6]. It should be noted that the best practices are continuously evolving. The DoD has instituted a variety of acquisition reform initiatives to keep pace with evolving business trends and to take advantage of successful methods. In that

regard, a common risk management and technical assessment process must maintain currency to the degree possible in order to provide program participants with an understanding of emerging best practices that can be used as benchmarks to assess program processes and procedures.

9. Metrics

Metrics are measures used to indicate progress or achievement. Risk metrics fall into two principal categories: (1) risk management metrics, which are used to indicate risk management progress; and (2) metrics used to indicate program health. Defining, monitoring, and assessing these metrics is critical to the overall risk assessment process. Executing these functions facilitates establishing linkages between designs and requirements.

Examples of both metrics categories are found in Appendix B. Further discussion of metrics and their use in risk analysis is contained in Chapter II, Section B.

10. Critical Program Attributes

Critical Program Attributes (CPA) are performance, cost, and schedule metrics that are vital to program success [6]. They are derived from various sources, such as the Acquisition Program Baseline (APB), exit criteria for the next program phase, Key Performance Parameters (KPPs), test plans, judgment of program experts, and other sources. These attributes are tracked to determine the progress in achieving the final required value.

11. Reference

Metrics may be qualitative or quantitative and are referenced to either operational performance or a development requirement. Ultimately, all operational performance and development requirements are related to program objectives or to a process best practice.

12. Technical Assessment Process (TAP)

Implementing a common risk management and technical assessment process requires a Technical Assessment Process (TAP) instruction to assess progress in achieving program objectives. (See Chapter II, Sections C and E for more details.) The TAP provides an assessment hierarchy, a structure akin to a WBS, tailored for the program. The TAP hierarchy establishes the organizational structure for documenting and reporting assessment results including risks. In analyzing risk, the TAP hierarchical structure is used to ensure risk assessment is directly linked to technical assessment. An Integrated Assessment Tool (IAT) is essential to assist in this process. An IAT serves to link technical assessment data with cost and schedule data, further supporting a consolidated assessment process and reporting procedures. Key features of an IAT are presented in the following paragraphs.

13. Integrated Assessment Tool (IAT)

An IAT is a risk management communication tool. It defines the risk program data/information needs required to support program management. An IAT captures the normalized assessment results of the technical, cost and schedule assessments, including the particular references/scenarios/metrics used to conduct each individual assessment. Included in an IAT are risk identification, analysis, mitigation, and tracking fields used to manage program risks. Data/information fields include:

- Scenario—Operational Situation (OPSIT) definition or Concept of Operations (CONOPS) definition. Different scenarios may dictate different risk indicators.
- Metric Utility—Indicates the significance of the metric. Metrics that indicate failure to achieve either desired or required performance would have moderate or high metric utility. Key Performance Parameters (KPPs) represent the program's vital metrics and, therefore, have high metric utility. Metric utility may be used to highlight the significance of a particular high or moderate risk and/or its mitigation plan.

- Normalized Estimate—The estimated assessment as to the design's ability to meet performance or operational thresholds. Functional area experts who assign technical assessment metrics will determine this value. Estimates are normalized to a scale from –1 to +2, where 0 indicates the threshold level and +1 indicates the objective.
- Estimate Uncertainty—Lower and upper confidence levels applied to the normalized estimate that indicate the degree of uncertainty in the normalized estimate. It is based upon best engineering judgment, testing, modeling and simulation, past experience, and other factors.
- Risk Description—A concise statement summarizing risk analysis results links failure probability to the consequence of failure to achieve desired or required performance.
- Analysis Source—Primary data source supporting the risk assessment (e.g., best engineering judgment, modeling and simulation, test results, engineering report, etc.)
- Cost Exposure—Cost adjustments required to mitigate risk.
- Schedule Exposure—Schedule adjustments required to mitigate risk.
- Resource Status—Degree to which resources have been planned and programmed to address identified risks.
- Fallback Options—Description of options included as mitigation measures. Options should include cost, schedule, and performance impacts.
- Post Mitigation Probability of Failure P_f—Estimate of probability of failure to meet or threshold requirements after mitigation.
- Post Mitigation Consequence of Failure C_f—Estimate of consequence of failure to meet program objectives after mitigation.

THIS PAGE INTENTIONALLY LEFT BLANK

II. COMMON RISK MANAGEMENT PROCESS

A. RISK MANAGEMENT STRATEGY

The risk management strategy is designed to correspond with the acquisition strategy. While risk management execution resides with industry, risk management responsibility resides with the government program manager. The government must assess industry risk management programs. The government must also perform independent risk assessments as a part of the TAP. The risk management strategy:

- Encourages integration with overall program management and fosters excellence in industry's execution of their own risk management programs
- Focuses on procuring the best possible system within the constraints levied upon the program by adjusting risk tolerance/risk acceptance levels in order to optimize return on investment
- Sets program priorities based upon the criticality of system and acquisition requirements
- Assesses and characterizes industry's risks from the government's perspective
- Assesses and evaluates the industry's risk management programs and their viability (See Appendix C for criteria).
- Provides the program organization with appropriate tools, training, and support so that risk management concepts and processes are routinely practiced and understood by program participants
- Supports the program manager and the System Technical Assessment and Review (STAR) Panel in characterizing, assessing, and reporting risks; during the overall program risk characterization (See Appendix D for a sample format to maintain and present program risks)

- Develop independent risk identification, assessment, mitigation, and tracking capabilities required to manage government-unique risks (not specifically industry risks).

B. RISK MANAGEMENT — AN OVERVIEW

The purpose of this chapter is to provide an overview of risk management within the context of program management. Figure 2 presents a top-level view of the relationship risk management has with program management and systems engineering. Although clear lines of demarcation between these three disciplines are presented, these are highly-interdependent and integrated. Successful risk management is highly-dependent upon the degree of integration between these three areas. Success is also dependent on standardization and consistent application of risk assessment criteria that are traceable to overall program objectives.

Figure 2 illustrates, at a macro level, the interdependencies and information flow necessary to manage risks. Program objectives, as illustrated, have been translated into requirements by program management using top-level mission definitions. These definitions, included in both the Initial Capabilities Document (ICD) and Capabilities Development Document (CDD), are translated into system requirements that industry designs must satisfy.

The program manager interprets and transforms the user's original requirements to program participants including industry and the government's systems engineering and risk management teams. The systems engineering teams perform comprehensive technical assessments of proposed industry designs. Part of this technical assessment, as illustrated, is a risk analysis.

The risk management team contributes to risk analysis by defining risk assessment criteria that link to program objectives. A standardized set of numerical values linked to qualitative descriptors comprise these criteria. Risk analysis considers and assigns consequence of failure (C_f) and probability of failure (P_f) criteria selected from the standardized numerical values. Program risks are the primary output of the risk

analysis process. The severity of risks or risk factor (R_f), is determined by the product of C_f and P_f. Moderate and high Risks are monitored, tracked, and reported as indicated by Figure 2.

In addition to providing standardized risk analysis criteria, the risk management team provides tools, training, and risk planning.

The most severe risks are communicated directly with program management because of their potential negative impact.

As indicated in Figure 2, the STAR Panel plays a major role in the risk management process. It receives the outputs of the risk analysis process and performs review, adjudication, prioritization, and strategy development. The STAR Panel reports its findings to the program manager.

Once high and moderate risks have been reported to the program manager, risk handling options are evaluated and implemented.

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 [6]. In general, options include:

- **Risk Control** – Seeks to reduce or mitigate risks instead of eliminating the source of the risk [6]
- **Risk Avoidance** – Eliminates sources of unacceptable risk and replaces them with a lower risk solution [6]
- **Risk Assumption** – Acknowledgement and acceptance of the level of risk for a particular risk situation [6]
- **Risk Transfer** – Reallocation of risk from one part of a system to another [6]

Numerous possible risk control or mitigation actions should be considered. Creativity in risk control is encouraged and fostered by the collaborative IPT process. General guidance concerning possible risk control alternatives is provided in Appendix E.

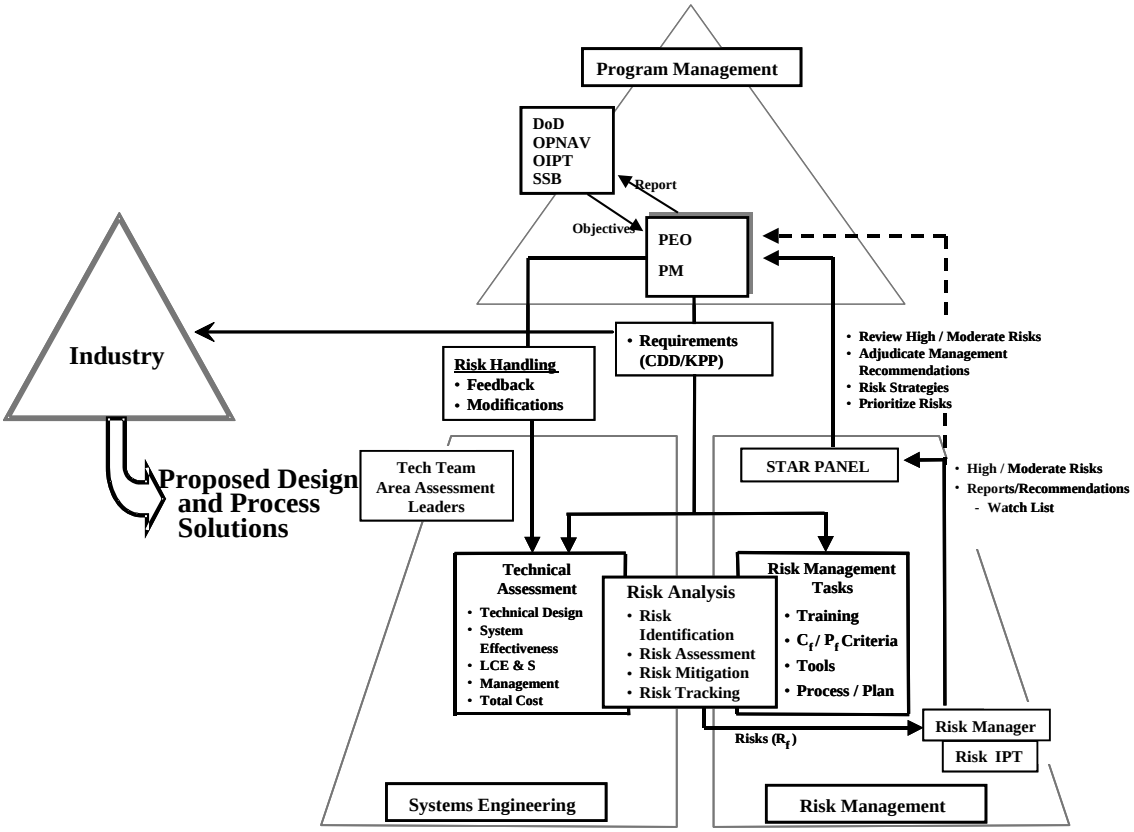


Figure 2. Top-level view of the relationship between risk management and program management and systems engineering.

1. The Risk Analysis Process

The risk analysis process steps shown in Figure 3 are explained in the sections that follow.

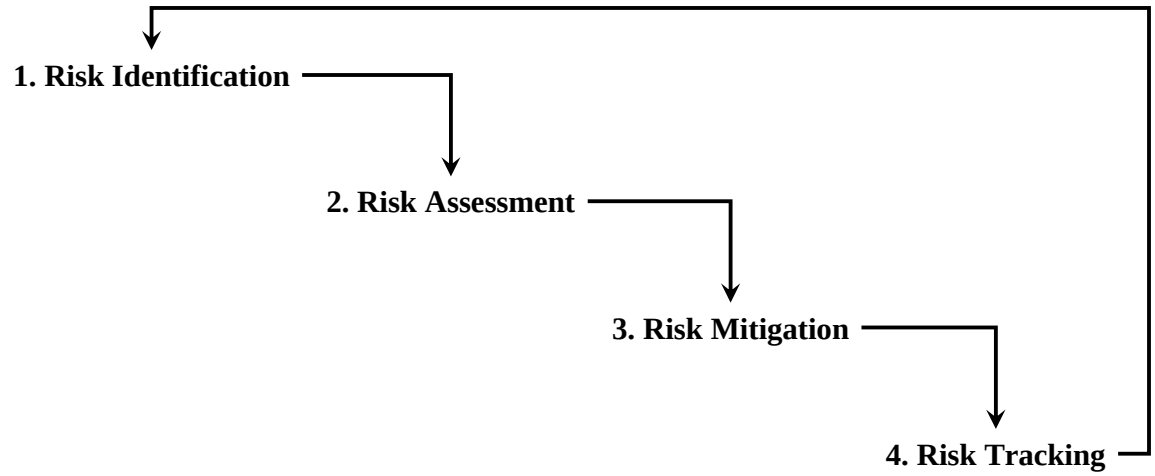


Figure 3. Risk Analysis Process.

2. Risk Identification

Risk identification is the process of examining system designs and critical technical processes to identify and document associated risk. Each person involved with the design, construction/manufacture, operation, support, and disposal of the system should be cognizant of associated risks. The earlier risks are identified, the easier they will be to manage and the less negative impact they will have upon program cost, schedule, and performance objectives. A selection of risk identification methods is presented in Appendix F**.**

The risk management IPT maintains a tool box containing tools that can be used in conjunction with risk identification and other risk management processes. These tools are listed and described in Appendix G. The tool box is not intended to be all-inclusive, for the array of specialized and emerging methodologies continues to grow as research and lessons learned are applied in both commercial and government program

management communities. This selected list is continuously expanding and program participants should use this resource, as required, to enhance individual assessments.

3. Risk Assessment

Risk assessment represents the next step in the overall risk management process and is intended to provide a priority ranking for all identified risks. In the risk management process, both operational and development functional areas are assessed.

In conducting risk assessments, evaluators should not routinely conclude that risks represent weaknesses or strengths. As illustrated in Table 1, either case is possible. It is important for evaluators to discriminate between the two. Risks are part of the overall program management process and should be used to gain insight into designs, CONOPs, and development plans. Credibility can be supported by properly recognizing and categorizing risk.

In general, a risk is a strength if its resolution represents a significant enhancement of existing capabilities and falls within the program's cost and schedule envelope. A risk can be characterized as a strength if it is identified and adequately defined so that its degree of uncertainty and its impact/consequence can be assessed. It must include a reasonable mitigation plan, including fallback options that can be executed within the constraints of the program.

Conversely, a risk that has not been addressed with a reasonable mitigation plan, or a mitigation plan that cannot be executed within program constraints, represents a weakness. A risk represents a weakness if it has been ignored or omitted by industry. Lesser weaknesses are indicated if the risks are inadequately defined, if the risk consequences are understated, or if no fallback options are available.

Table 1. Risks as Strengths and Weaknesses.

Risks as Strengths and Weaknesses		
	Strength	**Weakness**
Undefined Risk	**Not Applicable**	**Possible**
Unmitigated Risk	**Not Applicable**	**Possible**
Feasible Mitigation	**Possible**	**Not Applicable**
Viable Fallback	**Possible**	**Not Applicable**

4. Risk Mitigation

Once risk has been identified and assessed, Step 3, risk mitigation, is executed. As part of this step, the risk owner develops a mitigation plan consisting of specific tasks that, when implemented, will reduce the stated risk to an acceptable level. This does not necessarily mean reducing the risk to "low." In most cases, "no risk" is a symptom of lack of progress in engaging and applying innovative technologies. This position concerning risk tolerance levels allows for some degree of risk acceptance, particularly if it leads to future gains in terms of performance, schedule, and/or cost.

The risk mitigation process requires localizing the source of the identified risk and being careful not to confuse symptoms with cause. It is the source that will receive the necessary mitigation resources. Once the source has been localized, a mitigation plan must be developed that describes what has to be done, when, by whom, the level of effort, and the material or facilities required to mitigate risk to an acceptable level. Valid risk mitigation strategies should include contingency plans in the event that planned mitigation efforts fail. A proposed schedule for accomplishing these actions is required, as well as a cost estimate, if possible. The "DoD 4245.7-M Templates" and "NAVSO P-6071 Best Practices" manuals described in Appendix G are two excellent sources for assisting program participants in developing solid mitigation plans.

5. Risk Tracking

Risk tracking, Step 4, is based upon the principles of ownership and open communication. The originator is the owner of a reported risk and retains cognizance for reporting that risk's status. Ownership includes implementing plans for mitigating moderate and high-risk areas.

To ensure risk is adequately tracked, program managers should ensure that risk is an agenda item at every appropriate meeting or review. Openly discussing risk provides an opportunity to collaborate on risk reduction. Communicating risk improves awareness and allows early actions to minimize adverse consequences.

Risk items and mitigation plan status should be reported to the program manager and STAR Panel:

a. Quarterly;

b. When 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); or

c. When requested by the program management team.

When tracking and reporting risk areas, adhere to the following ground rules:

a. Always provide sufficient information to the level of detail required for others to understand all aspects of a particular risk, its mitigation plan, and status.

b. The cognizant engineer or analyst is responsible for each risk area. Ownership is critical to the risk management process and should not be delegated without higher level approval.

c. Changes to the risk description should be limited to corrections or clarifications to the original description. A significant difference in risk description should be considered a candidate for reporting a new risk area.

d. Rationale should be provided whenever the assessed risk changes between categories low, moderate, and high.

e. Both reordering the risk mitigation tasks or adding additional actions or mitigation tasks are considered acceptable without reporting it as a new risk area.

f. As a general rule, any risk that has been entered into an appropriate database, and reported to a higher authority, must be retained. The close out of each risk area will be based on the merit of the status of associated mitigation actions.

g. Metrics should be identified and maintained to measure progress in minimizing unacceptable risk or maintaining desired risk.

h. Close-out of risk areas is generally the responsibility of the cognizant engineer or analyst, but the latest status must include justification.

6. Continuous Risk Management

An arrow from Step 4 returning to Step 1 in Figure 3 indicates that risk analysis process is a continuous activity. Thus, the arrow could just as well return to Step 2, denoting the change in priority of a risk area, or to Step 3, denoting a need to modify the risk mitigation plans.

C. RISK MANAGEMENT ORGANIZATION AND RESPONSIBILITY

Risk management during program definition and engineering phases is comprised of the following:

- **Executive Level Risk Management** – Program risks are identified, analyzed, tracked, and reported at the most senior levels of the program. Risks considered and analyzed are of the most consequential nature, thus meriting executive level scrutiny. Analysis is conducted primarily using personnel with vast acquisition and technical experience. Lessons learned and historical perspectives form the basis of the assessment. Since risks often emerge unexpectedly (budget cuts, test failures, slippages), this level of risk management is usually conducted on an ad hoc basis and is often focused on mitigation.

- **Program-Wide Risk Management** – is comprised of risk analysis, assessment, and tracking during functional area meetings. Risk should be a regular agenda item in functional area meetings and reviews.
- **Risk Management and the Technical Assessment Process (TAP)** – The TAP specifies the process, criteria, and hierarchy to be used as well as the Integrated Assessment Tool (IAT) to perform program-wide risk management. (See Appendix H for a sample instruction to implement a common risk management and technical assessment process.)
- **Risk Management IPT** – This team is responsible for maintaining a current risk profile for the program. They are also responsible for providing program participants with appropriate tools, processes, and guidance to interactively and collaboratively manage risk.

1. Roles and Responsibilities

Risk management success is contingent upon it being an "all hands" evolution. The program sponsor regularly asks that the program report risk status. As a stakeholder, the sponsor helps determine the criticality of program requirements. All engineers, analysts, and support personnel with discrete responsibilities and assignments in the program should be cognizant of uncertainties associated with their cost, schedule, or technical area. The common risk management and technical assessment process is designed to integrate the risk analysis with program cost, schedule, and systems engineering analyses. It provides broad-based diagnostic scrutiny in order to support successful system acquisition.

Table 2 presents an overview of risk management roles and responsibilities. It should be emphasized that the program manager is ultimately responsible for the risk program as defined in the DoD 5000 series.

Table 2. Risk Management Program Roles and Responsibilities.

Title	Unique Role in Risk Management (If Applicable)	Risk Identification	Risk Analysis	Risk Mitigation Development	Risk Mitigation Assessment	Risk Tracking & Refinement	Risk Training
Program Manager	Overall Risk Management Program Responsibility	E	E	E	E	E	E
Deputy PM		E	E	E	E	E	E
Industry Program Manager(s)	Overall Risk Management Responsibility	E	E	E	E	E	E
Industry Risk Managers	Define and execute Industry Risk Management Programs	E/T	E/T	E/T	E/T	E/T	E/T
Technical Director	Responsible for TAP and Integration of Risk Assessment Into Technical Assessment Process	E/T	E/T	E/T	E/T	E/T	E/T
Risk Manager	*See Notes that follow	E/T	E/T	E/T	E/T	E/T	E/T
Department Heads		E/T	E/T	E/T	E/T	E/T	E/T
Functional Area Leaders	Risk Management in Specific Focus Area	T	T	T	T	T	T
Tech Team Leader	Independent technical assessment including risk	E/T	E/T	E/T	E/T	E/T	E/T
Tech Team		T	T	T	T	T	T
STAR Panel	Program-wide risk assessment and adjudication	T	T	T	T	T	T

Legend: E = Executive Lead (review, approve, reprioritize, approve, track)
T = Focus on Specific Technical Areas (identify, assess, prioritize, track)

Risk Manager

- Reports to the technical director with direct access to the program manager
- Maintains an interdisciplinary understanding of program-wide risk
- Is the central advocate for risk management including administrative responsibility for the program
- Interfaces directly with industry risk managers, and maintains currency concerning status of industry reported risks
- Coordinates with Functional Area Leaders (FALs) for assessment of industry risk issues and mitigation plans
- Establishes and maintains risk management metrics on industry and government risk management progress
- Facilitates risk assessments, provides appropriate risk assessment tools, and provides guidance to FALs for uniform display of risk issues
- Maintains the program risk database
- Produces and maintains a program risk watch list
- Interfaces with the STAR panel to develop and adjudicate system risks and the program-wide risk watch list
- Conducts training required in order for all program staff to execute the risk management program
- Briefs the program manager on the status of program risk
- Recommends independent risk assessments as required to support program objectives

The following organizations and individuals have roles and responsibilities that are integral to the risk management program. Their risk management responsibilities are described below.

Stakeholder Steering Board (SSB)

Central to the process executed by the SSB is identification and assessment of program risks. Through extensive interaction with Cognizant Technical Authorities

(CTAs), the SSB identifies risks. It also vets risk and critical integration areas as part of the TAP. An important SSB function noted is the confirmation of what government resources need to be applied to resolve technical risks.

System Technical Assessment and Review (STAR) Panel

The STAR panel is integral to program risk management. The panel is comprised of experienced executive-level acquisition professionals. Because of their extensive experience, they are assigned the responsibility of adjudicating, modifying, and characterizing the program risks. They will review the bottom-up risk assessments generated by functional areas, IPTs, and competing teams, and modify these assessments appropriately. They will also perform top-down risk assessments using appropriate weighting tools provided by the risk IPT as required.

Tech Team

Tech Team is a group comprised of primarily government specialists in the technical disciplines associated with system design and construction. Cognizant Technical Authorities (CTAs) (e.g., Naval Surface Warfare Center, SEA 03, SEA 05) provide personnel who populate the Tech Team and work exclusively for the government. The Memorandum of Understanding (MOU) between the program and Tech Team includes the requirement to assess risk associated with the industry designs. Tech Team uses the TAP risk assessment process as well as periodic independent risk assessments in technical specialty areas. As noted above, the Tech Team works closely with the SSB to assess and characterize industry risks.

Industry Risk Managers

These managers develop, operate, and manage industry risk management programs that satisfy program and DoD objectives. They coordinate efforts with the program risk manager to provide access to risk data in a readily usable format. Additionally, they coordinate and integrate as appropriate, cross-team risk management functions.

D. THE RELATIONSHIP BETWEEN GOVERNMENT AND INDUSTRY IN RISK MANAGEMENT PROGRAMS

The government risk management program includes and leverages industry risk management programs. Industry, in developing preliminary design options, must include risk management as an integral component of their overall program management and systems engineering processes. The government risk manager maintains visibility and dialogue with industry so that clear understanding of risk processes, risks identified by industry, and risk mitigation progress are clearly understood. This insight will be collected, analyzed, and used to assess industry designs and their potential for successful production and delivery of the system.

Figure 4 illustrates the relationship between the Navy's risk management program and industry's. The figure depicts identical risk processes being executed by the Navy and industry; however, industry has distinctive risk processes that are unique to their programs.

In addition to assessing industry risk management programs, the Navy's risk management assessment will examine industry team proposals, designs, and processes in the context of risk. This process captures high and moderate risks not captured or mischaracterized by industry risk programs. It provides for independent Navy assessments of the uncertainties associated with industry designs. The basic building blocks of risk management, however, are comprised of the continuous four-step process depicted. The Navy risk management program interfaces with industry risk management to maintain insight and visibility in risk identification, assessment, analysis/mitigation, and monitoring/tracking, as shown.

Individual risk items contain certain common elements that can be used to characterize the risk. The quality assurance checklist, in Appendix I, is provided to assist risk assessors in obtaining the required program risk information. Program metrics will be used to assess industry designs/plans. In this manner, risk is independently assessed, characterized, and reported as the program proceeds. Outputs of the risk management program derived through this interaction are listed in Figure 4.

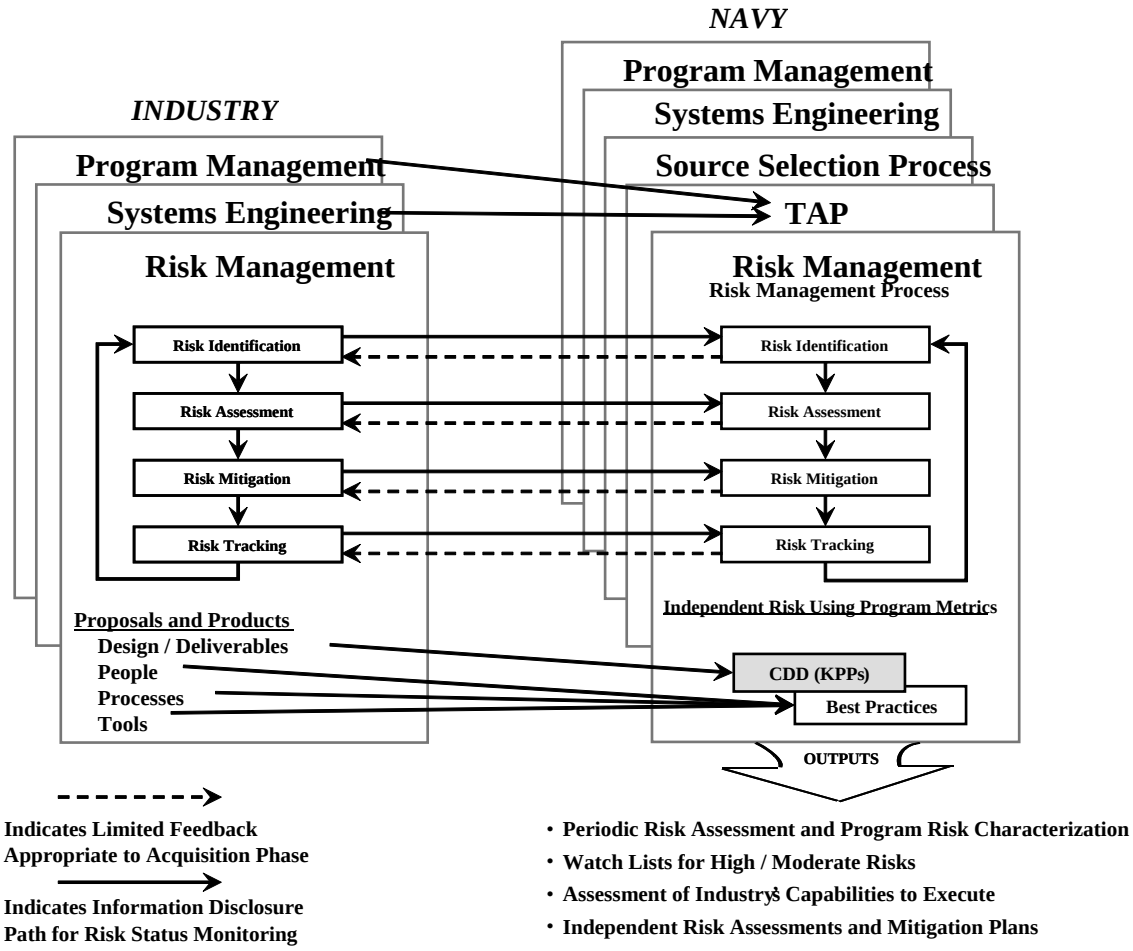


Figure 4. Relationship between the Navy's risk management program and industry's risk management programs.

E. TAP RISK MANAGEMENT PROCESS AND PROCEDURES

Continuous review of industry risks will be performed as illustrated in Figure 4. Dialogue with industry risk managers will be maintained by the risk IPT. Significant findings and changes to status (missed milestones, schedule slippage, technology breakthroughs, risk retirement, et cetera) will be documented and included in the program risk characterization. The risk manager will report these findings to the STAR panel on a regular basis.

Risk management will employ an Integrated Assessment Tool (IAT) described in Chapter A, Section B.13. The IAT uses the TAP instruction as a baseline for executing

risk analysis and management in an organized fashion. The TAP instruction requires Assessment Area Leaders (AALs) to identify, analyze, and report high and moderate risks based upon government risk assessments. The IAT is designed to assist government evaluators in executing this function.

The TAP instruction provides an assessment structure. A sample of that structure is depicted in Figure 5. This structure, which assessment teams have some latitude to modify, is used as a baseline checklist to ensure that all program focus areas are analyzed for merits and deficiencies in industry-proposed solutions. The IAT is populated with the identical hierarchy in order to assess risk across the evaluation spectrum. Key Performance Parameters (KPPs) and key operational requirements are identified as program imperatives. These are specifically noted in the TAP and IAT so that proposed solutions addressing KPPs and key operational requirements are given significantly more scrutiny because of their importance.

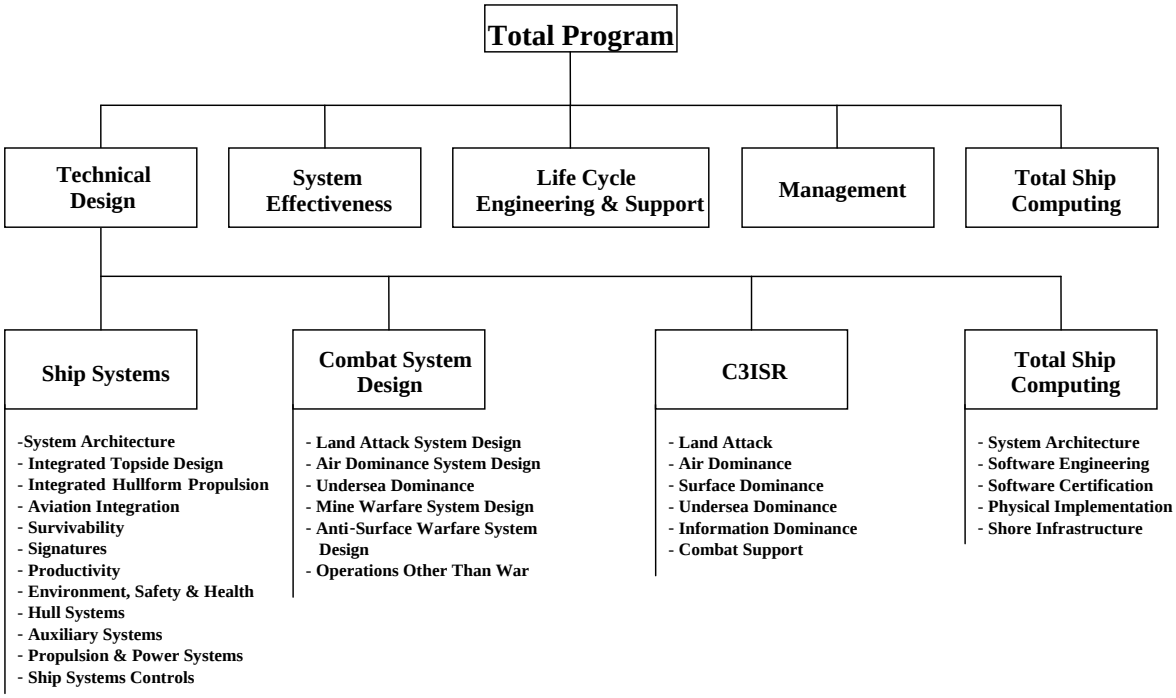


Figure 5. TAP Hierarchy – A Sample

Performing program risk assessment using the TAP structure as a reporting framework has significant advantages. It assures that technical assessment risk analysis results are integrated into a consolidated assessment process and are linked together tying systems engineering, operational analysis, economic analysis, and business case analysis. Figure 6 illustrates the assessment process relationship.

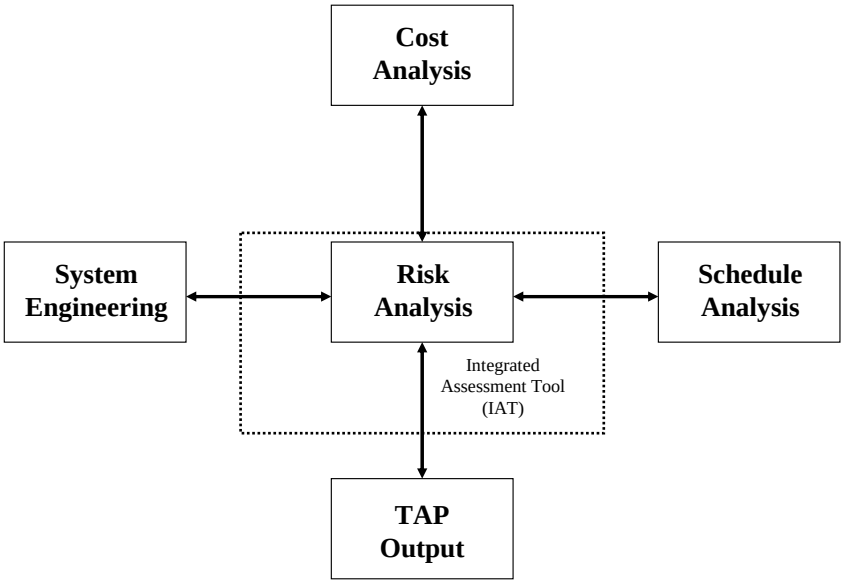


Figure 6. Consolidated Assessment Process

1. TAP Integrated Assessment Tool (IAT)

Purpose: The IAT is used as a tool to support program management and generate risk characterization reports for internal use and external reporting.

Description: The IAT is tailored to support program requirements. It is comprised of two principal parts. The first is an assessment input form that incorporates the TAP instruction hierarchy. The assessment input form allows further decomposition to facilitate in-depth analysis of more complex focus areas. The additional layers are primarily used to support operational performance categories where more analysis layers may be required.

The second part of the IAT is the standardized probability of failure (P_f) and consequence of failure (C_f) lookup tables to assist teams in assessing operational and development function risks using standardized program criteria. This standardized risk characterization is consistent with critical program attributes (top level program objectives).

The lookup tables are comprised of definitions linked to numerical scales that define the P_f and C_f. Operational functions can be characterized in terms of product and process risks. Development functions are characterized by process risks. Separate tables, criteria, and metrics for product and process risks are provided in the sample lookup tables in Appendix J.

a. Functional Assessments of Risks using the IAT

As illustrated in Figure 7, the TAP is divided into operational and developmental risk functions. The analytical processes for assessing an operational function as opposed to a development function can be quite different, requiring distinctive logic for each.

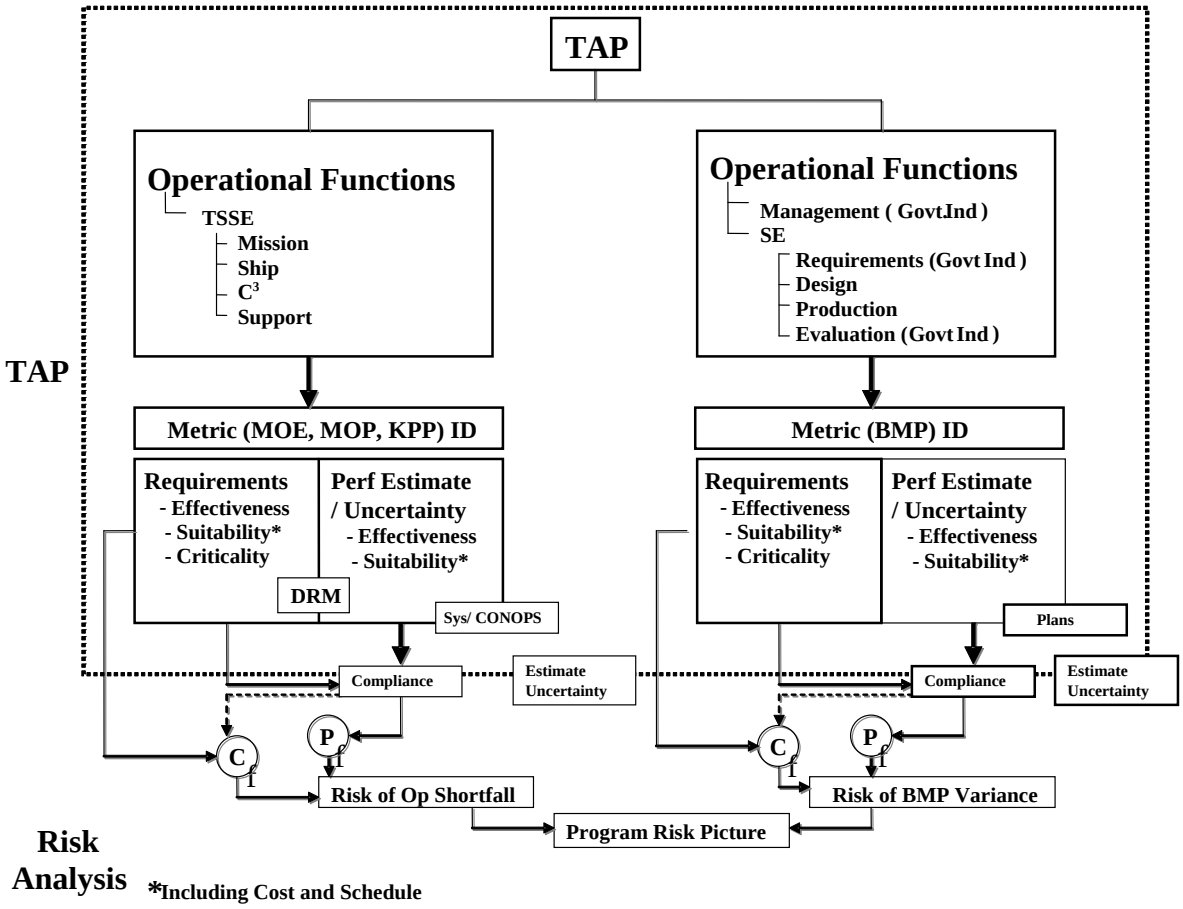


Figure 7. Relationship between risk analysis and the TAP

The TAP provides general guidance concerning the analytical processes for assessing probabilities and consequences of failure (P_f and C_f) for all operational and development functions. It should be noted that some functional areas will have to adapt this general guidance to their own assessment process.

b. Operational Functions

Operational function analysis is illustrated on the left side of Figure 7. Operational functions are those functions that characterize system performance capabilities. These are defined in terms of Required Operational Capabilities (ROC) and Planned Operational Environment (POE) using or employing a proposed Concept of Operations (CONOPs). P_f and C_f derivation for operational functions is discussed below:

P_f Derivation: For technical performance metrics associated with operational functions (i.e., MOEs, MOPs, KPPs), the compliance of the estimated performance with the required/expected P_f value is expressed as the fraction of the estimated range of performance falling below the required value. The estimated range of performance shall take into account uncertainties in the estimates. Figure 8 illustrates this concept.

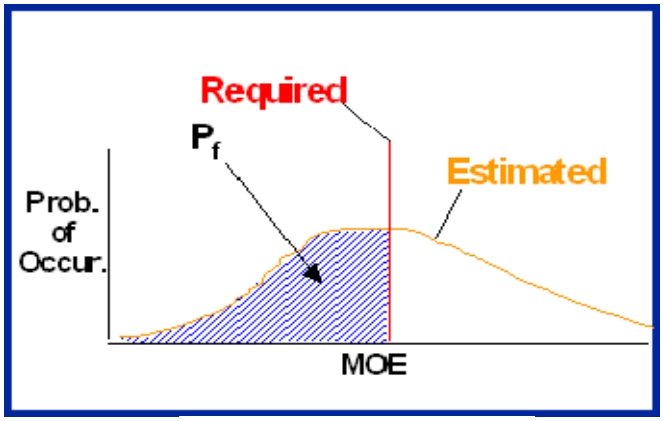


Figure 8. Relationship between estimated value and required value.

This same concept is applied to the comparison of operational suitability metric estimates with their required/expected values. For example: comparison of (1) operational cost estimates to the appropriate budget threshold, (2) schedule estimates to threshold milestones, (3) availability estimates to threshold availability. Use of this generic, engineering-based criterion helps normalize risk assessments across functional areas. Grouping or designating risks by operational scenario is part of the TAP assessment process. This grouping accommodates risk assessments for CONOPs variations. Referencing P_f to a specific metric helps to focus the risk definition and facilitates mitigation.

C_f Derivation: Criticality is associated with each threshold requirement/expectation by assessing the failure consequences to the operational mission. This rating supports the integrated risk assessment described above. Linkage of mission

level consequences to a lower-level metric failure should consider the effects of system/CONOPS design (e.g., from system redundancies).

c. Development Functions

Development function analysis is depicted on the right side of Figure 7. As illustrated in Figure 7, the metrics used to assess development functions are broadly categorized into two components—management and systems engineering. The distinctions of these two categories are discussed below.

(1) Management: The program management process controls the program participants' overall execution and control of the program. It includes integration and coordination of all other processes applied to the program as well as an optimal allocation of resources. It provides for communications with all of the program's stakeholders so that their functionality and roles are facilitated in an efficient, cost conscious manner. Principal management components are discussed below:

Planning: The planning process includes the capability to forecast, assess, anticipate, assign, and document resources in a proactive manner. It provides cost, schedule, and technical baselines from which the program can proceed.

Monitoring and Control: This process includes the capability to track and assess performance against established baselines, to reallocate resources to meet objectives, to ensure that contractual and other commitments are fully met, and to provide rigor and order across all disciplines in the program. It is an iterative process facilitated by robust communications with all participants.

Improvement: This spiral process leverages corporate and personnel experience. It includes technology insertion, personnel training, and capitalization on lessons learned from programs of similar complexity. Management sets improvement objectives with appropriate metrics and implementation schemas such as statistical process control. Quality certification is usually a credential that ensures appropriate improvement processes and philosophies are in place.

(2) Systems Engineering: The systems engineering process is the governing technical management process leading to product development. The product or collection of products addresses all aspects of system performance. Systems engineering provides the primary technical interface and integration with other key processes. Collectively, systems engineering ensures that all cost, technical, and schedule requirements are met. The primary components of systems engineering are presented below:

Requirements Definition: This process represents the ability to analyze and understand user requirements stipulated in top-level documents (e.g., Initial Capabilities Document, Capabilities Development Document, etc.) and translates them into a system that addresses the entire life cycle. Requirements are usually assessed via modeling and simulation, war-gaming, and other operations analysis tools that facilitate full understanding of requirements. Performance parameters, interoperability, testability, supportability, and other constraints are considered in the assessment process. Tools, such as prototypes and computer simulations, facilitate cost effective traceability and therefore are critical to requirements definition and synthesis.

Design: Design is a multifaceted process that begins with functional allocation and ultimately yields a product baseline. Synthesis, or preliminary or detail design, translates the functional and performance requirements into a description of the complete system that satisfies requirements. Solutions are incrementally defined as the design process is executed, and are comprised of specifications and drawings that serve as the baseline for transition to production.

Production: The production process is the ability to produce the system, subsystems, and components that comprise the design. The production process is characterized in terms of processes, facilities, personnel, planning, and other appropriate resources necessary to manufacture, fabricate, integrate, or assemble the system.

Evaluation: Evaluation is comprised of analysis, simulation, testing, and validation functions that incrementally determine progress in satisfying the technical requirements and program objectives. Technical management, configuration

management, deficiency reporting, risk management, performance-based product management, and other diagnostics are central to the process.

Development functions are assessed in relation to best practices. P_f is expressed as a function that indicates the degree of variance from these best practices. The estimated range of performance in the TAP tool takes into account uncertainties in the estimates. The C_f is derived by assessing the development function's impact on the program objectives and the operational mission. Appendix K provides a list of sample development functional assessment questions evaluators might consider in assessing competitor processes against best practices.

d. Risk Analysis Characterization Using IAT

In general, each element in the TAP hierarchy can be represented by a Measure of Effectiveness (MOE) as described with appropriate metrics. Operational metrics are usually defined by measures such as range, speed, or endurance. Developmental metrics are defined in terms of measures such as schedule maturity, number of qualified people, or past performance record. Using these metrics, a range of desired performance is established and recorded in the IAT. This data can be presented graphically in a histogram.

(1) Risk Definition within the IAT. The IAT captures risk definition information including title, description, and analysis source. These data are useful in providing additional details beyond those derived in calculating R_f. Functional assessment teams can characterize their areas in some detail by populating these fields.

e. Risk Mitigation within the IAT

Following the identification and assessment of a high or moderate risk, a plan to mitigate or reduce the risk needs to be developed. The IAT allows evaluators to capture and assess these mitigation plans.

Data concerning the entire mitigation plan picture can be captured by the IAT. Data/information includes a mitigation plan summary, cost and schedule

requirements, assessment of how the contractor has funded and scheduled execution of the mitigation plans, and other trend/assessment data. Analysis of this data/information in the IAT will facilitate the assessment of mitigation plan adequacy.

F. RISK MITIGATION GUIDANCE

High and moderate risks require mitigation plans. Many tasks in a mitigation plan will be peculiar to the type of risk being anticipated, however, some mitigation techniques apply to more than one risk type. These are included in the program acquisition strategy based upon lessons learned and analyses of other programs. Several of these proven techniques are listed below:

- Communications venues in the mitigation plan, such as government participation in IPTs, or collaborative work structures, are good mitigation process techniques.

- Modeling and simulation should be used to design, test, build, and operate ships in a computer environment before building hardware.

- The use of government and contractor testing, especially in the early stages of development, can help to evaluate design solutions related to risk mitigation. Land based engineering sites can be useful in the risk mitigation effort.

- The contractor should develop, and the Navy review, the system performance and physical specs. This allows a systematic approach to evaluating, understanding, and integrating the design.

- The use of trade studies should apply to a wide number of risk mitigation plans.

- Design reviews are an excellent forum for technical personnel to provide candid feedback on efforts to control and mitigate risk.

- Risk management should be proactive and include methods to identify, assess, track, and mitigate risk throughout the organization.

- The design requirements should stress features that are both upgradeable and flexible, thus facilitating the ability to accept risk when the pay-off is significant.

III. CONCLUSIONS AND RECOMMENDATIONS

Establishing a common risk management process and tool can improve the U.S. Navy's execution of technical authority by targeting compliance with technical criteria and standards from the earliest stages of program development during evolution of the program acquisition strategy throughout the program's life cycle. A successful strategy needs to provide the industry sufficient time to fully develop plans and deliver products, especially in program high-risk areas, and incorporate a systems engineering process where the technical authorities can perform their mission. If technical risks are not adequately addressed, history has shown that costs will increase.

A. ADVANTAGES OF A COMMON RISK MANAGEMENT PROCESS

A common risk management and technical assessment process helps focus program management attention on areas of uncertainty that pose threats to program success. It helps:

- Define, assess, and monitor metrics used to indicate program health
- Assess and characterize risks from government's perspective
  - Set prioritizes based upon criticality of system and acquisition requirements
  - Establish (adjust) risk tolerance/risk acceptance levels to optimize return on investment
- Provide program personnel the means to implement risk management routinely and ensures process is practiced and understood by all program participants

Successful risk management is highly dependent upon the degree of interaction between the program management, risk management, and systems engineering disciplines. Success is also dependent upon standardization and consistent application of risk assessment criteria that are traceable to overall program objectives.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

This thesis achieved its purpose of improving execution of technical authority by defining the relationship between program authority and technical authority and describing how to assess and improve the state of technical authority through common policy development and implementation. Still, more work needs to be done. Future research necessary to help the SYSCOMs implement a common risk management process includes development and deployment of an Integrated Assessment Tool (IAT). Future research also needs to include promulgating a common policy for developing Systems Engineering Plans, a common technical review process, a common total platform and interoperability certification process, and a common systems engineering training program.

Implementation of the recommendations provided by this thesis will improve communication and coordination of acquisition risks between the SYSCOMs newly-established program management and technical competencies, which will substantially reduce the U.S. Navy's risk and cost exposure on all current and future acquisition programs.

APPENDIX A — RISK TERMS AND DEFINITIONS

Term	Definition
CAIV	Cost as an Independent Variable is a performance trade off approach which establishes cost as a hard constraint on selection of capability and confidence investments.
Campaign	The highest level (strategic) objectives of a military solution to a broad threat situation. Composed of a number of mission objectives.
Certification	The act of attesting by report, letter, certificate, or message that performance of an equipment or system meets prescribed criteria. The word carries the connotation of a guarantee.
Compliance	The difference between measured or estimated performance and required performance.
Confidence	A metric for the uncertainty that the estimate of predicted performance will be realized. A component of technical risk assessment encompasses the confidence bounds of a distribution and the uncertainty in the distribution itself.
CONOPS	Concept of Operations — defines system use (functional allocation and execution). Includes strategic and tactical guidance and their governing doctrine and rules of engagement. Reflects both operational constraints and system/technology requirements.
Consequence (C_f)	See Section 1.2
Correlation, Metric	Interdependence of metric values.
Cost Model	Relates total ship design to life cycle cost. When capability and confidence are analytically linked cost, CAIV-based design trades can be made.
Criticality	A function attribute that indicates the importance of the function to system-level capability.
CTP	Critical Technical Parameters are metrics of special interest to test oversight at the program manager and test activity levels. This term includes KPPs and additional metrics specified by such oversight or in the ICD.
Demonstration	A test focused on a specific outcome (usually one having a high probability of success).
Direct Observations	Performance or compliance distribution or metric values derived from test measurements of the subject function output.
Distribution	The spectrum of performance or compliance metric value variations due to intrinsic variability or to scenario influences.
DRM	Design Reference Mission is a collection of scenarios to be used as design and evaluation benchmarks. The collection addresses

Term	Definition
	assignments of all durations from campaign to engagement and so serves as a reference for Total System Systems Engineering.
Effectiveness Model	A description of how MOEs or MOSs depend on MOPs. High fidelity models could include MOP dependencies on lower-level metrics and operating conditions.
Engagement	Fundamental warfare area tasks for prosecution of one or many specific threats within the associated threat category.
Exit Criteria	Conditions specified in the Acquisition Decision Memorandum (ADM) which must be met before the Milestone Decision Authority (MDA) will allow a program to proceed into the next phase of development. May include indicators that selected KPPs or CTPs thresholds can be met.
KPP	Key Performance Parameters are metrics of particular interest to oversight. Achieving their threshold values is essential for program continuation. The ICD defines them.
Measure	An "instrumentable" representation of a function outcome.
Metric	See Appendix B.
Mission	Intermediate objectives of a military action. Comprised of a number of operations separated by platform availability activities (transit, re-supply, crewing, recovery, et cetera)
Model	A descriptive, algorithmic, data-based, or physical representation of a system, procedure, or environment. See Simulation.
MOE	Measures of Effectiveness are metrics associated with high-level, design-independent, functions, which specify government's interest in what needs to be done. The term is derived from the per-function effectiveness metrics because high-level function outputs are usually binary (already stated in terms of a desired outcome) so that performance and compliance distributions are equivalent. Values generated by effectiveness models. May be decomposed into MOPs.
MOP	Measures of Performance are metrics associated with intermediate functions which may be design dependent, and reflect how industry plans to meet the need through integration of technology. The term is derived from the per-function performance metrics of high interest to designers at this functional level. May be decomposed into TPs.
MOS	Measures of Suitability – Same as MOE, but keyed to secondary (resource) outputs, or to any function supporting primary output availability.
Observability	The confidence with which a metric value can be estimated by reduction of test data. A function of data quality and the sensitivity of the metric to the directly observed function.
Operation	The tactical objectives of a military action. Comprised of a sequence of engagements, possibly executed concurrently across warfare areas to address simultaneous threats.

Term	Definition
OPSIT	Operational situation describes the scenario for an operation, the organic functions to be applied, and the external assets available for use.
OSA	Open Systems Architecture supports flexible system upgrades through modular design.
Outcome	A general term for the result of a specific test or evaluation. A direct observation.
Parameter	A general term referring to any of a set of elements used to describe the characteristics or behavior of something. Scenario parameters include environment, threat and CONOPS parameters.
Performance Metric	The basic representation of function output. Measurable values (continuous or discrete) whose distribution is determined by external operating conditions and intrinsic system capability. Computed performance metrics (e.g., an average) are often used to characterize the distribution.
Performance Model	Sub-system models which generate MOP values. They represent execution of intermediate, design-dependent functions and integrate technology models.
Probability (Pf)	See Section 1.2.
Process	The set of steps used to accomplish a function.
Product	The hardware or software delivery made in response to a requirement.
Risk	See Section 1.2.
Risk Assessment	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 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 Documentation	The recording, maintaining, and reporting assessments, handling analysis and plans, and monitoring results. It includes all plans, reports for the program manager and decision authorities, and reporting forms that may be internal to the PMO.
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

Term	Definition
	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 Handling	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. Risk handling is an all-encompassing term whereas risk mitigation is one subset of risk handling.
Risk Monitoring	The process that systematically tracks and evaluates the performance of risk-handling actions again established metrics throughout the acquisition process and develops further risk-handling options, as appropriate.
Risk Planning	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.
Scenario	The operational context for system employment. Includes specification of threat and physical environments, defended assets, available external resources, and constraints on operations (CONOPS).
Simulation	The execution of a model to show dynamic effects. May be conceptual, constructive, virtual, or live (rehearsal).
System	A physical view of the functional hierarchy. “System”, “sub-system”, and “component” refer to physical views of high-, intermediate-, and low-level function groupings respectively. “System of Systems” (SoS) is a collection of inter-operating systems. Development optimizes system capability within programmatic constraints and within the context of possible participation in a SoS.
Test	The collection of direct observations of real-world function outcomes.
Testability	The capability to determine a metric value with required confidence within cost and schedule constraints.
Threat	A probable danger or negative consequence.
Utility	Indicates significance or usefulness.
Validation	The process of determining the manner and degree to which a model is an accurate representation of the real world from the perspective of the intended uses of the model.
Verification	The process of determining that a model implementation accurately represents the developer’s conceptual description and specifications.

APPENDIX B — RISK METRICS

Risk management metrics comprise two basic categories. The first is risk management program metrics. These metrics indicate the quality and effectiveness of the risk management program. Using an Integrated Assessment Tool (IAT) and TAP process, significant data/information can be assembled that are used to characterize the effectiveness and efficiency of the overall risk management program.

The second metric category provides insight and understanding as to the overall health of the program relative to technical, cost, and schedule parameters. These metrics can be subdivided into various regimes depending upon the product or process being examined. Program metrics, including cost and schedule measures, are increasingly given added attention because budgetary constraints and the drive to leverage technology.

Examples of these two categories of risk metrics are presented below:

RISK MANAGEMENT PROGRAM METRICS

These metrics are statistical characterizations of the risk management program. Executive level metrics reporting performed by the risk manager and the STAR panel include:

- A prioritized number of high, moderate, and low risks segregated by industry and by risks unique to the Navy.
- An indication of the rate of change in the numbers of risks by category indicating how risk management is evolving.
- An indication of risk handling or mitigation progress over time.

The examples that follow are by no means all-inclusive, but are presented to illustrate the range of available data and various perspectives upon that data.

Number of Risks	KPP/ICD Related	Navy Unique Risks	Industry (Navy Assessment)	Industry (Self Assessment)
High				
Moderate				
Low				
Retired				

The TAP and IAT facilitate the collection of metric data related to metric utility and risk uncertainty levels. Collection of this data may enhance understanding of the risk management program.

PROGRAM HEALTH METRICS

By focusing performance measurements on the most critical engineering product development processes and results, the program will ensure that Fleet and DoD needs are met. The program KPPs and key operations requirements objectives must be met and metrics assessing the designs help the program determine both overall and incremental progress against those objectives. In general, these metrics provide system performance measures such as speed, rates of fire, endurance, power requirements, and others. Individual assessment areas will define metrics related to risks in the TAP. ASN (RD&A) guidance suggests that engineering metrics be divided into design, test, and production metric categories. These categories have been decomposed into numerous sub-components that should be considered by evaluators. The following tables are provided to assist program risk assessment personnel.

PROCESS METRICS EXAMPLES

(Source: "Methods and Metrics for Product Success" ASN RDA)

Category	Subcategory	Examples
Design	Design Reference Mission Profile	Contractor has developed functional profiles defined in terms of time, level of severity, frequency of cycles for both wartime and peacetime. Profiles include Life Cycle Support and associated costs.
	Design Requirements	Requirements are verified at the Systems Requirements Review (SRR).
	Trade Studies	Trade studies are prioritized against design requirements.
	Design Policy	Design policy is promulgated across industry team and integrated.
	Design Process	Design has been analyzed for cost, performance, manning, etc.
	Design Analysis	Appropriate standardized design analyses are ongoing, identified, or scheduled (e.g. Stress Analysis, Stability Analysis, Sneak Circuit Analysis, etc.)
	Parts and Materials Selection	What de-rating criteria are used? (There are hundreds of criteria in this area depending on item.)
	Software Design	Independently established software certification credentials.
	Computer Aided Design	Percent of design activity that is computer aided.
	Design for Testing	Are Human Factors considered in the test program.
	Built-in Test (BIT)	Criteria used for determining BIT; cost of BIT
	Configuration Control	Configuration Management Plan completeness and cross team adoption of the Plan.
	Design Reviews	Percent of design completion at Design Review milestones (e.g., 20% at PDR)
	Design Release	Projected versus actual engineering man-hours expended
Test	Integrated Test Plan	Integrated Test Plan covers all disciplines.
	Failure Reporting System	Is there a corporate failure reporting policy?
	Uniform Test Report	Standard test reporting formats established across the team.
	Software Test	Coverage of instruction blocks is clearly defined.

Category	Subcategory	Examples
	Design Limit	Percentage of hardware validated at extreme limits.
	Life	The contractor draws life test environments from operational mission profiles.
	Test, Analyze, and Fix	Test environments are based on worst case mission profile extremes.
	Field Feedback	Problem and failure data available in real time to appropriate personnel.
Production	Manufacturing Plan	Manufacturing is included in the design process.
	Quality of Manufacturing Process	Quality certification credentials have been obtained.
	Piece Part Control	Do suppliers certify quality levels?
	Subcontractor Control	Are technical issues included in subcontractor agreements (not just cost and contractual)?
	Defect Control	Is the defect reduction program demonstrated on previous programs effective?
	Tool Planning	Are trade studies used to assess cost effective tool selection and procurement?
	Special Test Equipment	Are market surveys conducted to justify special test equipment?
	Computer Aided Manufacturing (CAM)	What percentage of machine processing is performed by CAM?
	Manufacturing Screening	Are vibration and thermal analysis conducted appropriately?

EXAMPLES OF PRODUCT-RELATED METRICS
(Source: "Risk Management Guide for DoD Acquisition)

Category	Subcategory	Examples
Engineering	Key Design Parameters	Weight
		Size
		Range
		Endurance
	Design Maturity	Open Problem Reports
		Number of Change Proposals
		Number of Drawings Released
Production	Unit Production Cost	
	Material Availability	
Support	Manpower Availability	
	Special Tools	
	Test Equipment	
Lifecycle Cost	Cost per Steaming Hour	
	Crew Size	

EXAMPLES OF COST AND SCHEDULE RELATED METRICS
(Source: "Risk Management Guide for DoD Acquisition")

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

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C — ASSESSMENT OF RISK MANAGEMENT PROGRAMS

Industry risk management programs will be assessed and evaluated through the review of ongoing risk management programs, deliverables associated with the programs, and proposed solutions for future risk management execution. Industry will be encouraged to seek and propose creative, cost effective risk management solutions. Industry will be evaluated in terms of risk management products, risk management processes, teamwork/integration with the industry/government structure, and proposed risk management tools. They will also be assessed in terms of their risk evaluation processes and the quality of their mitigation planning process. Criteria considered in evaluating these areas are presented below.

1.0 Industry Risk Management Programs

1.1 Risk Management Products

Definition: The development and delivery of risk management team products, including a risk management plan, risk watch list, risk assessment criteria, periodic risk status reports, and risk training instruction; the integration of risk management into other product deliverables, including the TEMP and ITP.

Assessment Indicators:

- Has the risk management team (RMT) provided a risk management plan (RMP)?
  - Does the RMP provide an organized, comprehensive, interactive risk management strategy? Is the RMP in accordance with the program manager's risk management strategy?
  - Does the RMP define how to integrate risk management into the technical assessment process using systems engineering principles?

  - Does the plan provide guidelines for risk identification, assessment, mitigation plan development, monitoring, and reporting?
  - Does the plan provide the functional interface between IPT members, IPT risk representatives, and the RMT?
- Has the RMT provided training to IPTs to incorporate risk management into their technical assessment process, to properly assess risk, and to appropriately and effectively plan for and carry out risk mitigation activities?
- Do test plan deliverables adequately link testing to risk reduction?

1.2 Risk Management Processes

Definition: The implementation of the risk management plan, including the functional interface and process flow between the IPTs and risk management team. The IPTs identify and assess risk according to the risk management plan, develop mitigation plans, and report risk in the risk database tracking tool.

Assessment Indicators:

- Has the RMT updated the RMP to suit its current requirements, including response to changes in acquisition strategy, or preparation of major decision milestones?
- Does the risk management process promote benchmarking evaluation processes against best practices?
- Does the RMP address risk process flow to define the interface between program management, the IPTs, and the RMT?
- Does the risk management process flow direct decisions to the program management?

1.3 Teamwork/Integration

Definition: The organizational structure of the risk management team, including risk manager and support staff, and risk representatives from program management and the IPTs.

Assessment Indicators:

- Is the RMT adequately staffed and funded?
- Is the Program Management Team actively participating?
- Do the IPTs have designated risk representatives which interface with the RMT?
- Does the RMT meet regularly with the PM and IPTs to ensure that the RMP is properly and continuously being executed?
- Is the RMT staffed properly with experienced systems engineers trained in risk management?
- Does the RMT promote communication between IPT risk representatives to identify cross-functional risks?
- Does the RMT identify system-level risks?

1.4 Risk Management Tools

Definition: The functional element developed by the Risk Management Team and used by the IPTs to enter, monitor, and report identified risks and associated mitigation plans. Provides the capability to report risk metrics and risk status.

Assessment Indicators:

- Has the RMT provided a risk database tool for risk monitoring, tracking, and reporting?

- Does the tool include self-contained training for risk definition and assessment?
- Does the tool provide for the inclusion of effectiveness (technical performance) and suitability (cost and schedule exposure) metrics within risk records?
- Does the tool provide for the reporting of watch lists?
- Does the tool provide for the reporting of risk metrics?
- Does the tool provide for the reporting of program risk status?
- Does the tool provide for linking reported risks to the IMS, tests, demonstrations, and budget items?

2.0 Evaluating Risk

2.1 Assessing Risk

Definition: The establishment of criteria to assess risk, including criteria for probability/likelihood of shortfall relative to a requirement or expectation, consequence of shortfall event should it occur, and resulting risk level (criteria for High, Moderate, and Low risk).

Metrics:

- Number and Percentage of active risks based on failure to meet specified requirement/expectation
- Average Age of Active Risks (also average of High, Moderate, Low)

Assessment Indicators:

- Are risk assessments consistent with the definitions in the RMP?
- Are risk assessments consistent with (government) program RMP definitions? Are industry assessed high risks of high risk to (government) program?
- Do industry risks adequately span (government) program risks?

2.2 Establishing Mitigation Plans

Definition: The development of activities intended to reduce identified risk to manageable and acceptable levels. Ensure that developed plans are executable within critical time constraints.

Metrics:

- Number and Percentage of High and Moderate Risks without Mitigation Plans
- Percentage of mitigation tasks budgeted
- Percentage of mitigation tasks scheduled

Assessment Indicators:

- Are mitigation plans developed for High and Moderate risks? Are these plans captured in a Risk Mitigation Plan deliverable?
- Do mitigation tasks meet program schedule constraints?
- Are mitigation tasks linked to the IMS?
- Are mitigation tasks formally budgeted?
- Are mitigation tasks linked to demonstrations/tests?

3.0 Monitoring Risk

Definition: The continuous process of systematically tracking and evaluating the performance of risk-handling actions against established metrics. Conduct periodic reassessments of program risk to evaluate current and new risks. Identify additional risk-handling options.

3.1 Mitigation Activity Status

Definition: Monitor the status of risk mitigation activities to ensure that they remain on schedule.

Metrics:

- Number and Percentage of High/Moderate risks with overdue mitigation plans
- Number and Percentage of High/Moderate risks with incomplete mitigation plans

Assessment Indicators:

- Is industry on course to mitigate risk?

3.2 Reporting Risk

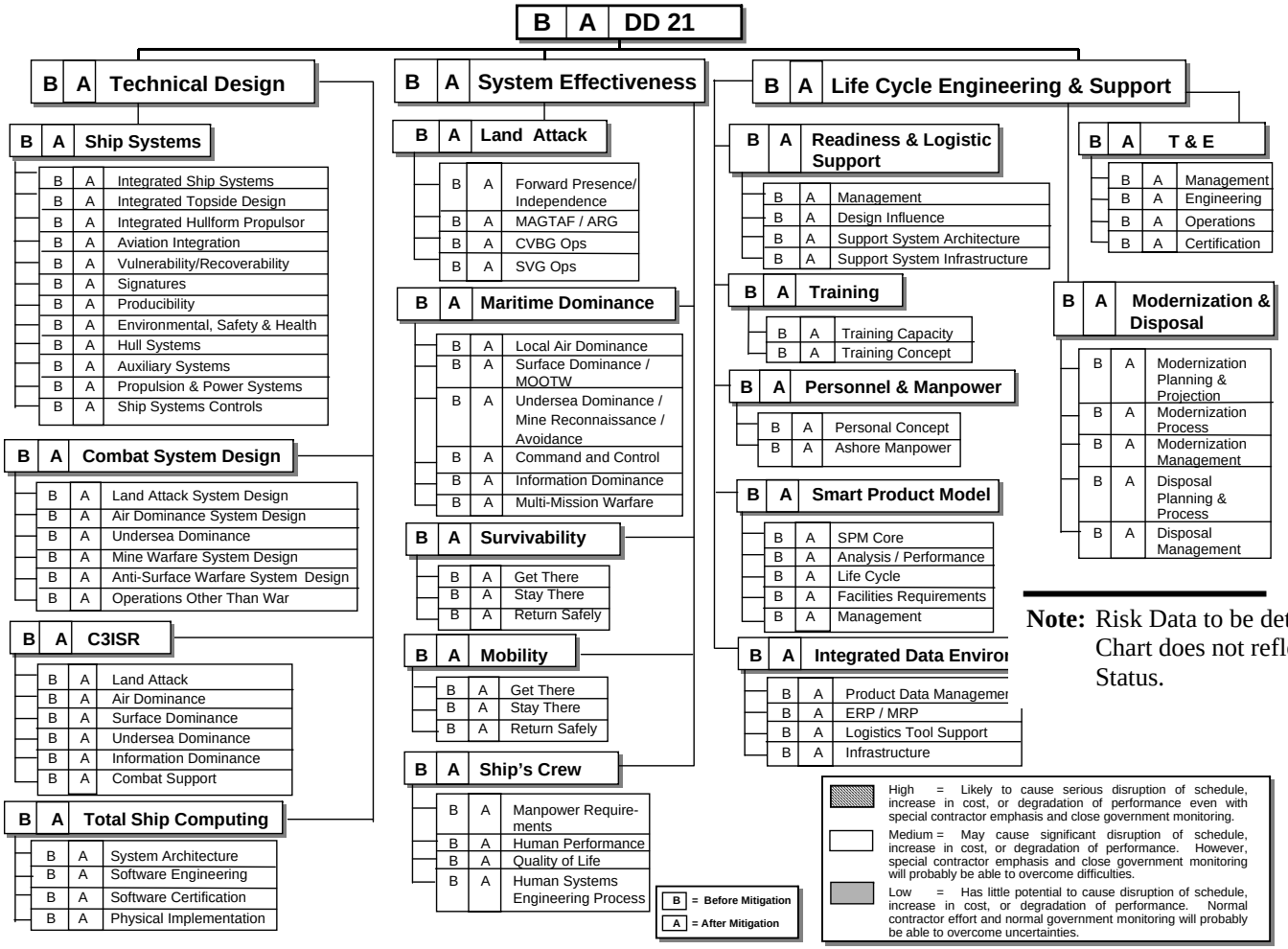
Definition: Recording, maintaining, and reporting assessments, handling analysis and plans, and monitoring results.

Assessment Indicators:

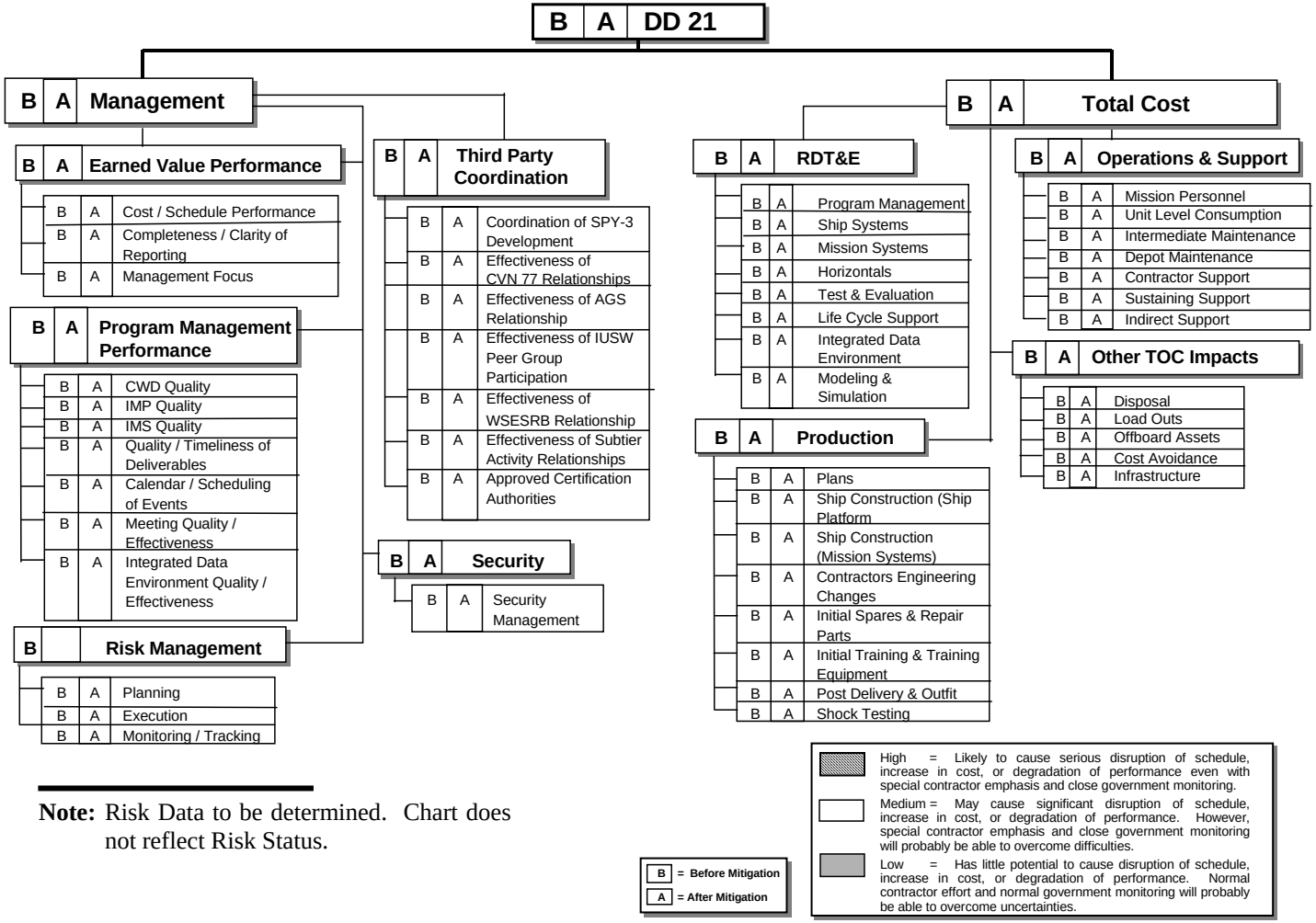
- Is industry reporting accurate, timely, and relevant risk information in a clear, easily understood manner?
- Are risk reports generated by industry at regular intervals?
- Are prioritized risk watch lists provided to program management for action and direction?

APPENDIX D — PROGRAM RISK CHARACTERIZATION CHARTS – A SAMPLE

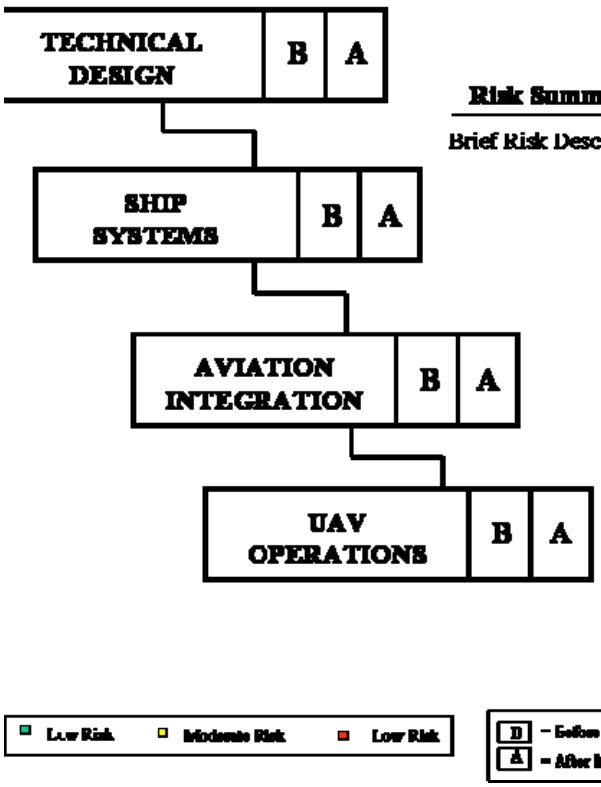
Figure 2.1-1



Note: Risk Data to be determined. Chart does not reflect Risk Status.



Note: Risk Data to be determined. Chart does not reflect Risk Status.



Risk Summary	Mitigation	Risk Retired by
Brief Risk Description	Key Mitigation Events	Date or Milestone

The most severe risks impacting DD21 Critical Program Attributes, Operational Requirements, or Key Performance Parameters (KPPs) will be reported in this format, In this manner discrete risks and mitigation plans are communicated to senior DoD and Navy Management for consideration and potential action

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E — RISK CONTROL ALTERNATIVES

Risk Category	Risk Control Alternatives
Technical	• Multiple development efforts • Alternative Designs • Trade Studies • Early prototyping • Incremental Development • Technology maturation efforts • Robust design • Reviews, walk-throughs, and inspections • Design of experiments • Open systems • Use of Standard items/software reuse • Two-phased engineering and manufacturing development • Use of mock-ups • Modeling and simulation • Key parameter control boards • Manufacturing screening
Schedule	• Multiple development efforts • Alternative Designs • Trade Studies • Modeling and simulation • Key parameter control boards
Cost	• Multiple development efforts • Alternative Designs • Trade Studies • Incremental Development • Technology maturation efforts • Open systems • Use of Standard items/software reuse • Use of mock-ups • Modeling and simulation • Key parameter control boards • Manufacturing screening

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F — METHODS FOR IDENTIFYING RISKS

The following include some (but not all) recommended ***methods*** for identifying risk:

a. ***Best Judgment*** is the knowledge and experience of the collective multi-disciplined IPT members and is the most common source of risk identification.

b. ***Understanding the Prime Contractor's critical processes*** is key to recognizing, and therefore identifying risk. The amount of deviation from considered best practices relates to the level of risk being encountered.

c. ***Understanding the Subcontractors' critical processes*** is just as important as understanding the Prime's. Visibility into Subcontractor processes has not been common practice but should be because of the potential impact to program cost, schedule and performance.

d. ***New Processes*** should always receive dedicated attention, 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 these processes, there is risk.

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

f. ***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.

g. ***Defining an Unknown,*** or defining all unknowns, is being proactive in risk management. A team (e.g., IPT) approach is essential because some unknowns may be "known" to certain members and "unknown" to others. Collectively, the team should be able to list all the unknowns. Unknowns include incomplete design efforts, testing not yet performed, and similar unfinished work. The challenge is to define the unknowns, identify the resources (people, funds, time, tools and materials) needed to complete the work (making them "knowns"), then monitoring these plans to completion. Unknowns are risk areas until they are defined, the necessary actions are planned, and the required effort is found to be within the scope of cost and schedule estimates.

h. ***Changing Requirements*** contain inherent risk in completing the job on schedule and within the budgeted funding. The impact of this risk must be assessed and controlled.

i. ***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 which needs to be addressed.

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

k. ***Qualified Supplier Availability*** is key to keeping risk LOW. A supplier who is not experienced with the processes for designing and producing a specific product is not a qualified supplier. To qualify, a supplier may require resources that have not been planned and therefore this risk issue must be addressed.

l. ***Lack of Resources: People, Funds, Time, Tools, and Materials*** are necessary ingredients for successfully implementing a process. If any is inadequate, there is risk.

m. ***Unqualified People: Knowledge and Experience*** (and possibly other attributes) may not fit the processes being implemented. When there isn't a fit, there is risk.

APPENDIX G — RISK MANAGEMENT TOOL BOX

These tools are briefly described below and can support all four steps of the risk management process. The tool box is not intended to be all inclusive, providing only a selection of proven tools used by similar programs. Other tools, such as those from the commercial sector, from other programs, or the software vendor community can also support the program risk management process.

a. ***Risk Management Plan***. As its name implies, this document defines the risk management and risk assessment processes. Changes to these processes will be reflected in this document as they occur.

b. ***DoD 4245.7-M***, "Transition from Development to Production," is often called the "Templates" manual because it identifies technical risk areas as experienced by leading industry experts and provides, in "bullet" form, suggestions for avoiding those risks. The manual lacks detail, addressing historic technical considerations of product design, test, and production to help managers be proactive in managing risk. It focuses on activity necessary for optimum readiness for production. The chapters describe an overall Design process that emphasizes understanding all the stresses that can cause the product to fail during its operating life and encourages the use of design margins to accommodate those stresses while striving for early design maturity. They describe a Test process that verifies that the product is designed to worst-case stress conditions and is mature before it is released to production. They describe a Production process that ensures that the manufacturing process/processes are qualified and that the design can be "built to print." Chapters on Funding, Facilities, Logistics, and Management may prove useful in identifying weak areas of program planned processes early enough to implement actions needed to avoid adverse consequences.

c. The ***NAVSO P-6071 Best Practices*** manual was developed by the Navy to add depth to the all the processes in DoD 4245.7-M. The format is exceptionally user-friendly and most of the fundamental guidelines, developed over a decade ago, are still applicable today.

d. ***Risk Indicators*** are developed at the program level to measure progress toward meeting program objectives, and should be developed by each IPT for the same reasons. Risk indicators may be specification requirements, contract requirements, or measurable parameters from any agreement or tasking. The goal is to establish an early benchmark, then monitor progress toward achieving program objectives.

e. ***NAVSO P-3686,*** "Top Eleven Ways to Manage Technical Risk" is a useful document focusing on Technical Risk Management. Technical risk, and the degree to which critical technical processes can be controlled, is a significant driver of all other program risks. The conscientious implementation of this guide, in conjunction with the aforementioned DoD 4245.7-M and NAVSO P-6071, will ensure an effective Risk Management Program. As a bonus, NAVSO P-3686 contains over 35 links to Internet sites containing a wealth of scientific and technical information.

f. ***PMWS (TRIMS), or Other Software Applications.*** PMWS contains risk management software, "*Technical Risk Identification and Mitigation System (TRIMS).*" TRIMS is a tailorable management system based on the Template processes. Diskettes, which contain the necessary programs for accessing BMP◊NET from IBM-compatible or Macintosh computers with a modem, and answers to other questions regarding PMWS, can be obtained by calling the Best Manufacturing Program (BMP) Office at (703) 696-8483 or the help desk at (703) 538-7253. Internet address: "http:/www.bmpcoe.org/pmws.html."

g. ***Requirements Documents*** describe the specific needs of program hardware and software. IPT efforts need to be monitored continuously to ensure requirements are met on time and within budget.

h. ***Contracting for Risk Management*** helps ensure that the organizations involved with the details of the technical processes of design, test, and production are involved with managing risk. The principle here is that these organizations are normally the first to identify known and unknown risk areas.

i. A ***Risk database*** is the primary repository of risks identified as part of the program risk management process. Industry will maintain risk databases for their proposed designs.

j. ***Robust Design Practices*** are those which are characterized by a greater degree of thoroughness and a higher level of intensity aimed at ensuring that engineering disciplines previously underemphasized by the government and underutilized by the contractor, have been applied to the design. A robust design provides a much higher level of confidence that functional performance requirements will be met, applied stresses are well known, and every part will be able to endure those stresses for the life of the product.

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

l. Use of an ***Independent Risk Assessment*** is a tool to help ensure that overlooked risk is identified. The knowledgeable, experienced people selected are independent from the management and execution of the specific program processes and

procedures being reviewed. Prior non-involvement promotes questions and observations not otherwise available from within the program management team.

m. ***Risk Management Training*** will be provided by the program to all program participants. Courses will be updated to reflect changes to the risk management process.

n. DoD 5000 Series Instructions and Notices

o. "Methods and Metrics for Product Success Manual" – ASN RDA

p. McGraw-Hill Technical Guides

- "Design to Reduce Technical Risk"
- "Testing to Verify Design and Manufacturing Readiness"
- "Moving a Design into Production"
- "Design's Impact on Logistics"

q. "Risk Management Guide for DoD Acquisition," January 2000.

APPENDIX H — SAMPLE TECHNICAL ASSESSMENT PROCESS INSTRUCTION

TECHNICAL ASSESSMENT INSTRUCTION XXXX.X

From: Program Manager (PMSXXX)

Subj: PROGRAM TECHNICAL ASSESSMENT PROCESS

Ref: (a) Program Instruction XXXX.X - Mission Readiness Reviews

Encl: (1) Program Assessment Report

1. Purpose. Promulgate the policy, procedures and responsibilities to plan and conduct comprehensive, integrated cost, schedule, and performance (mission/technical) assessments of system designs, products, and associated development efforts.

2. Applicability and Scope. This instruction applies to all program personnel who plan and execute events or actions that the program manager determines are related to program assessments. This instruction provides program management with a continuous appraisal of cost, schedule, and performance (mission/technical) performance.

3. Policy. A formal process shall be used to plan and execute comprehensive, integrated cost, schedule, and performance (mission/technical) assessments critical to system definition and program execution. These assessments will be required throughout the program life or until superseded by a formal source selection process defined in separate correspondence.

4. Definitions.

    a. Focus Areas. Principal divisions of program cost, schedule, and performance (mission/technical) performance assessment. The five focus areas are Technical Design, System Effectiveness, Life Cycle Engineering and Support (LCE&S), Management and Total Cost.

    b. Assessment Areas. Each focus area is further subdivided into three levels of increasingly specific assessment areas, entitled Tiers I, II, and III.

    c. Assessment Criteria. The standards and measures to which Tier I, II, and III assessment areas will be assessed to include Measures of Effectiveness (MOEs), Measures of Performance (MOPs) and Measures of Suitability (MOSs).

d. Functional Area Leader (FAL). The individual assigned responsibility for overall assessment status of a specific aspect of the system design and development effort, including industry efforts and government assessments thereof.

e. Assessment Area Leader (AAL). The individual assigned responsibility for conducting assessments in a specific assessment area.

f. Assessments. Assessments will be performed throughout the program life on the occasion of one or more of the following:

(1) Formal program reviews

(2) Formal technical reviews (system and subsystem reviews)

(3) Informal meetings

(4) Receipt of deliverables which need to be examined

(5) Receipt of analyses or data which require analysis

(6) Demonstrations or tests

(7) Mission Readiness Reviews (MRRs) as appropriate (reference (a))

(8) Major changes in industry team approach/concept since the last program review, if any

(9) Emergence of issues that may affect compliance with CDD, statutory and regulatory requirements, including environmental issues and impacts

(10) Emergence of issues that have the potential to affect a decision to commit significant program resources

(11) Identification of items of potential Navy, Department of Defense, congressional or news media interest.

5. Objectives. Objectives of the program assessments are to:

a. Determine whether the system design can be produced and supported within program cost goals with acceptable risk.

b. Develop relevant expertise with respect to industry's concepts and design methodology.

c. Assess the performance, value and risks associated with industry's designs.

d. Identify, document and monitor risk mitigation of all moderate-to-high performance (mission/technical), cost, schedule and other programmatic risks.

6. Process. These objectives will be attained by implementing the following approach:

a. Define focus areas and supporting assessment areas for Tiers I, II, and III.

b. Define specific assessment criteria for each focus area and assessment area in Tiers I, II, and III.

c. Assess aspects of the system design and development effort, including industry efforts and government assessments thereof, using the assessment criteria in enclosure (1).

d. Document each assessment to the extent that it can stand alone, or reference other sources as necessary. In this regard, it is important that respective assessment area leaders seek and obtain input from other areas as necessary.

e. Produce assessments that support requirements of the program risk management process.

f. Produce assessments that support recommendations to program management or higher authority.

g. Provide insight for program management to use in allocating assessment resources.

7. Assessment Areas. Assessments will be conducted in the following areas:

Technical Design	System Effectiveness	LCE&S	Management	Total Cost
Ship Design	Mission Support	Readiness and Logistics Support	Earned Value Performance	RDT&E
C4I System Design	Survivability	Training	Program Management Performance	Production
TSC	Mobility	SPM		
	Ship's Crew	IDE	Risk Management	Operations and Support
		Modernization and Disposal	Third Party Coordination	Other TOC Impacts
		T&E	Security	
		Personnel and Manpower		

a. The observed performance could be in the form of data, a deliverable, a meeting, a demonstration or a formal review. The assessment should reflect the success potential of the design concept/development plan, as well as the credibility of the team to execute and achieve the concept/plan.

b. Appendices A through E contain a top-level summary of assessment criteria for each area.

c. Each Assessment Area Leader (AAL) will maintain a comprehensive detailed description of each assessment area and its associated criteria. This body of information will constitute the definitive basis of information for conducting technical assessments in each area. A duplicate set of this information will also be maintained by the AAL in the Master Assessment Notebook in the Project Manager's office. Assessment Area Leaders are responsible for maintaining their respective appendices in this master document in addition to their individual files, obtaining Focus Area Leader approval for initial and updated versions throughout the program life.

8. Assessment Reports. Each assessment will be documented in an assessment report. Enclosure (1) is a sample assessment report, which includes a written description for each measure of performance, effectiveness or suitability.

   a. Assessment reports should be snapshot assessments of each area for which the Assessment Area Leader is responsible. Reports should be concise and require only a few minutes for completion in most cases.

   b. Each report should include essential information about who is completing the assessment and what was assessed.

   c. The assessment should characterize performance for the relevant areas observed:

      (1) Summary of superior and deficient aspects of observed performance.

      (2) Discussion of superior or deficient aspects of observed performance that merit Program Manager attention.

9. Risk. Assessment Area Leaders shall report all HIGH and MODERATE risks within their assessment area.

   a. Reports shall include the following:

      (1) Assessment Area Title

      (2) Risk Level (HIGH/MOD)

(3) Short Description which includes the appropriate operational performance requirements (e.g., KPP) or development process (e.g., best practice) not likely to be met

(4) Rationale (e.g., physical cause) explaining risk and risk assessment; and

(5) Status of Mitigation plans (e.g., defined, scheduled, approved, funded). Include fallbacks if appropriate.

b. Risk levels (HIGH/MOD) shall be based upon independent (government) risk assessments using the following definitions and criteria:

(1) The Risk Factor (RF) = Pf * Cf where Pf is the probability of that shortfall occurring and Cf is the consequence of not meeting the appropriate operational performance requirement or development best practice

(2) The Risk Factor thresholds set the boundary values for determining the Risk Level (RL). The Risk Level is HIGH for RF greater than 0.X. A HIGH Risk Level indicates the need for Program Manager attention to avoid serious impact to the program. The Risk Level is MODERATE for RF greater than 0.Y and less than or equal to 0.X. A MODERATE Risk Level indicates significant impact to the program is possible without special management attention.

(3) The following scoring criteria shall be used to estimate Pf and Cf:

(a) For all risk events that reference operational performance requirements use Table 1 for Pf scoring criteria and Table 2 for Cf scoring criteria.

(b) For all risk events that are related to development best practices use Table 3 for Pf scoring criteria and Table 4 for Cf scoring criteria.

9. Responsibilities.

a. Project Manager.

(1) Designate special assessments to be conducted, when indicated.

(2) When required, make final determination of assessments conducted by program personnel.

b. Focus Area Leaders.

(1) Review and endorse assessments conducted by program personnel.

(2) Assign additional assessments to be conducted, as required.

c. System Assessment and Review (SAR) Panel.

(1) Review completed assessments, as requested.

(2) Recommend additional assessments to the Focus Area Leaders or Program Manager, as appropriate.

d. Functional Area Leaders.

(1) Conduct assessments in their specific areas of responsibility in direct support of Assessment Area Leaders as delineated in paragraph 7.

(2) Formulate formal or informal recommendations to Department Heads when indicated by technical assessment results.

(3) Coordinate with other Functional Area Leaders as necessary to ensure that assessments present a clear and complete characterization of the issues being examined.

e. Assessment Area Leaders.

(1) Conduct and report assessments, as directed, in accordance with this instruction.

(2) Formulate formal or informal recommendations to Focus Area Leaders when indicated by assessment results.

(3) Coordinate with other Assessment Area Leaders, as necessary, to ensure that assessments present a clear and complete characterization of the issues being examined.

11. Action. All program personnel shall review, implement, and comply with the provisions of this instruction. Recommendations for change will be submitted to the cognizant Focus Area Leader or Program Manager, as appropriate.

Distribution:

Appendices:

A. TECHNICAL DESIGN ASSESSMENT CRITERIA
   1. Ship Design Assessment Criteria
   2. C4I System Design Assessment Criteria
   3. TSC Assessment Criteria

B. SYSTEM EFFECTIVENESS ASSESSMENT CRITERIA
   1. Mission Support Assessment Criteria
   2. Survivability Assessment Criteria
   3. Mobility Assessment Criteria
   4. Ship's Crew Assessment Criteria

C. LIFE CYCLE ENGINEERING AND SUPPORT ASSESSMENT CRITERIA
   1. Readiness and Logistic Support Assessment Criteria
   2. Training Assessment Criteria
   3. Personnel and Manpower Assessment Criteria
   4. SPM / IDE Assessment Criteria
   5. Modernization and Disposal Assessment Criteria
   6. Test & Evaluation Assessment Criteria

D. MANAGEMENT ASSESSMENT CRITERIA
   1. Earned Value Performance Assessment Criteria
   2. Program Management Performance Assessment Criteria
   3. Risk Management Assessment Criteria
   4. Third Party Coordination Assessment Criteria
   5. Security Assessment Criteria

E. TOTAL COST ASSESSMENT CRITERIA
   1. RDT&E Assessment Criteria
   2. Production Assessment Criteria
   3. Operations and Support Assessment Criteria
   4. Other TOC Impacts Assessment Criteria

Tables:

Competition Sensitive (when filled in)

Program Assessment Report

Date of Assessment _____
Assessment Leader _____
Organization/Code _____
Phone _____
Industry POC _____
Industry POC Organization _____
Industry POC Phone _____
Program FAL _____

Function _____
MOE/MOP/MOS _____

Risk Level:

Description of Risk:

Risk Mitigation Plans:

Proposed Actions:

Other Recommendations for Program Focus Area Leader/Project Manager:

Competition Sensitive (when filled in) **Enclosure (1)**

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I — QUALITY ASSURANCE CHECKLIST

Government Team Assessment Questions	**Yes**	**No**	**Comments**
1. Risk Assessment			
a) ***Tier Structure - Focus Area and up to nine lower tiers***. Are the columns complete to at least Tier II? Are decompositions complete? Are Tier II roll-ups performed?			
b) ***Scenario – The operational context for system employment***. Are Threat and Physical Environment specified? DRM OPSIT ID provided? Concept of Operations (CONOPS) specified? Are Defended Assets listed? Are External Resources listed?			
c) ***Metric –*** Are metrics clear, discrete, measurable attributes that can be used to evaluate the tier elements?			
d) ***KPP*** – Is the risk related to a KPP, ORD requirement, or neither?			
e) ***Req/Scen Refs - Reference for required metric value (threshold).*** Is the reference provided?			
f) ***Metric Utility – Utility of the required metric value (threshold), how much weight should be put on meeting this threshold.*** Is the rating (H, M, or L) provided and realistic?			
g) ***Estimate (Normalized, Lower and Upper Bounds)*** – *Normalized estimate on a –1 to 2 scale, with Threshold=0 and Objective=1.* Is the normalized value provided, and is it realistic?			
h) ***Estimate Uncertainty*** – Is an uncertainty range provided?			
i) ***P_f (and Rationale) – Probability of failure. Use tables. Provide rationale.*** Is P_f provided? Is rationale provided? Does the rationale match table guidance?			
j) ***C_f (and Rationale) – Consequence of failure. Use tables. Provide rationale.*** Is C_f provided? Is rationale provided? Does the rationale match table guidance?			
k) ***R_f – [Calculated. Risk Factor = P_f x C_f ,*** ***Low (Green) 0.2 <Med (Yellow) <0.6 High (Red)*** Is a value provided? Do estimate and risk factor agree? (An estimate above the objective value should not be high risk.)			

l) ***Previous R_f – For trend calculation (If Previous/Present R_fs are the same, why isn't risk being reduced?)***
Is previous R_f provided?

m) Last Update – Date of last update

n) Risk Title – Short title for Risk ID

o) ***Risk Description – Concise statement for summary reports compiled from other column entries. "Expected value for <metric> may not be met (P_f=xx), because of <high uncertainty> due to <incomplete testing, HW maturity, SW complexity,…>. Consequence (C_f=xx) includes <loss of assets, mission degradation,…>."***

Is description satisfactory, and can it support decision making?

p) ***Analysis Source - Primary data source supporting assessment. Government study, industry deliverable, best judgment, etc.***
Is the source defined and credible?

2. Risk Mitigation
   a) ***Summary - General description of mitigation plan.***
   Is the plan appropriate for the risk being mitigated?
   Will it mitigate the risk?
   Is there a clearly defined end-condition?
   Is the description complete?
   Is there a clear relationship between the mitigation and risk?
   Is the mitigation plan realistic (cost, schedule, technical)?
   Is it linked to actual Design Test events?
   Are there milestones that have clear metrics for tracking progress?

   b) ***Cost Exposure - Additional Cost adjustments required to mitigate risk.***
   Is there a cost listed (in $K)?
   Is the cost realistic?

   c) ***Schedule Exposure - Additional Schedule adjustments required to mitigate risk.***
   Is the schedule adjustment listed (in Months)?

   d) ***Resource Status - Degree to which mitigation task resources have been programmed. Ranges from "Proposed" to "Approved" to "Funded" to "Funded and Scheduled"***
   Is resource status listed?

   e) ***Fallback Options -***
   Is there a contingency plan if the Risk is not acted upon, or if the mitigation plan is not completely successful?
   Is the contingency plan fully described, including required government and industry actions?

Are performance, cost, and schedule impacts of the contingency plan discussed?

f) ***Post Mitigation P_f*** –
Is Post-mitigation P_f provided?
Is it consistent with Table guidance?
Is it realistic, given the mitigation plan?

g) ***Post Mitigation C_f***
Is Post-mitigation C_f provided?
Is it consistent with Table guidance?
Is it realistic, given the mitigation plan?

h) ***Post Mit-Rf - [Calculated. Risk Factor = P_f x C_f ,***
Low (Green) 0.2 <Med (Yellow) <0.6 High (Red)
Is a value provided?

i) ***Completion Date - Completion date of the mitigation effort.***
Is a date provided?

j) ***Event -***
Is an event identified?

k) ***Trend -***
Is a trend identified?
Is the trend correct?

l) ***Acceptable - Yes or No***
Is the risk reduction effort satisfactory?

m) ***Explanation -***
Is an explanation provided?

n) ***Recommendation -***
Are recommend Government Actions and/or Fall-Back Options identified?

o) ***Cost Risk (and Rationale) - Quantify in $K additional costs if risk remains unmitigated.***
Is the Cost Risk identified?
Is a rationale provided?

p) ***Schedule Risk (and Rationale) – Quantify in months schedule delays if risk is unmitigated.***
Is the schedule risk identified?
Is a rationale provided?

COMMENTS

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J — SAMPLE LOOKUP TABLES

Operational Performance Requirements Scoring Guidance for Consequence of Failure – Effectiveness and Suitability

P_f	General	HW	SW	HSI	Support Infrastructure	CONOPS
1.0	High P_f. Fraction of estimated performance distribution that falls below the required (expected, baseline) value. Applies to operational metrics of effectiveness (technical performance), and suitability (e.g., Op Cost, Response Time, Availability). Distribution accounts for estimation uncertainty (e.g., from unaccredited M&S, high sensitivities to environment, lack of testing, variance from Best Practices). See further examples of uncertainties in other columns. Range of integration inherent in the distribution (e.g., over OPSIT sets) shall be described. Accounts for redundancy in design for function; rationale describes dependency.	High uncertainty due to theoretical design based on advanced research. Low technology maturity. Requires technology breakthrough.	High uncertainty due to theoretical S/W concepts beyond known practice. Development of new approach &/or language.	High uncertainty due to low model fidelity, lack of validation. New expectations; breakthrough needed to make workload and retention credible.	High uncertainty due to theoretical technology or processes required for support structure, SE, training, facilities, support staff, or PHS&T.	Integration into Fleet/Joint tactics, doctrine NA. New approach; Culture changes needed.
0.9		High uncertainty due to new theoretical design. Application of leading edge concepts. Significant research required.	High uncertainty due to new complex S/W, new approach, new language. new unproven apps. Extremely large scale integration.	High uncertainty due to new unproven apps.	High uncertainty due to new support structure, support equipment, training, facilities, support staff, or PHS&T	
0.8		High uncertainty due to all new complex design with many stringent rqmts &/or major integration of many new HW elements. Concept untested, not verified.	High uncertainty due to all new S/W development; beyond experience base. Large integration of new or existing SW.	High uncertainty due to all new; beyond experience base.	High uncertainty due to extensive changes to existing support structure; mostly new SE, training, facilities, staff, or PHS&T	
0.7	Med P_f. Fraction of estimated performance distribution that falls below the required (expected, baseline) value. Applies to operational metrics of effectiveness (technical performance), and suitability (e.g., Op Cost, Response Time, Availability). Distribution accounts for estimation uncertainty (e.g., from unaccredited M&S, high sensitivities to environment, lack of testing, variance from Best Practices). See further examples of uncertainties in other columns. Range of integration inherent in the distribution (e.g., over OPSIT sets) shall be described. Accounts for redundancy in design for function; rationale describes dependency.	Uncertainty of new design or moderately improved existing design &/or major integration of many HW elements. Concept untested; predicting M&S not validated for this use.	Uncertainty of extensive changes in S/W development approach & application. Moderate integration of new or existing SW. M&S not validated for intended use.	Uncertainty of extensive changes in approach & application. Moderate integration of new or existing programs. M&S not validated for intended use.	Uncertainty of moderate changes to existing support structure; mostly new SE, training, facilities, staff, or PHS&T	
0.6		Uncertainty of major design change; significant modifications &/or moderate integration of HW elements. Feasibilty and M&S proven only by analogy, studies and/or concept verification. Sim environment not accredited.	Uncertainty of major modification of approach, conversion from similar SW, expanded to new application. Some Integration needed. M&S verified by analogy, no direct validation.	Uncertainty of major modification of approach, conversion from similar methods, expanded to new application. M&S verified by analogy, no direct validation.	Uncertainty of minor changes to existing support structure;mostly new SE, training, facilities, staff, or PHS&T	
0.5		Uncertainty of redesign or moderate modifications. Integration is primarily of internal functional elements. Some feasibility studies and initial testing. Predicting M&S verified for use.	Uncertainty of moderate modification & tailoring of existing SW; close link of developer to design, integrator. M&S verified only.	Uncertainty of moderate modification & tailoring of existing capability; M&S verified only. Workload reach; retention marginal.	Uncertainty of existing support structure;mostly new SE; minor resource shortfalls	Some coordination with Fleet/Joint still needed -- synthesis probable; successful experimentation with lessons being worked.

Operational Performance Requirements Scoring Guidance for Consequence of Failure – Effectiveness and Suitability — Continued

P_f	General	HW	SW	HSI	Support Infrastructure	CONOPS
0.4	Low P_f. Fraction of estimated performance distribution that falls below the required (expected, baseline) value. Applies to operational metrics of effectiveness (technical performance), and suitability (e.g., Op Cost, Response Time, Availability). Distribution accounts for estimation uncertainty (e.g., from unaccredited M&S, high sensitivities to environment, lack of testing, variance from Best Practices). See further examples of uncertainties in other columns. Range of integration inherent in the distribution (e.g., over OPSIT sets) shall be described. Accounts for redundancy in design for function; rationale describes dependency.	Low uncertainty of existing proven components; recombined or minor mods in function. Predicting M&S validated in similar application.	Low uncertainty of slightly modified SW &/or combining of existing functions with minor integration. Developer did design, will integrate. Validation in legacy similar application.	Low uncertainty of slightly modified method &/or combining of existing functions with minor changes. Validation in legacy similar application.	Low uncertainty of existing support structure; some new SE; minor resource shortfalls	
0.3		Low uncertainty of existing proven components, repackaged and/or minor usage variation. Predicting M&S validated in sim environment. Sim environment validated for use.	Low uncertainty of some modification of existing S/W approach with minimal integration impacts. Developer did design/integration. Validated in sim environment.	Low uncertainty of some modification of existing approach with minimal changes. M&S validated in sim environment.	Low uncertainty of existing support structure; some modifications to existing support equipment; minor resource shortfalls	
0.2		High confidence of functional proven H/W. Mods in form only. Minor usage variation. Predicting M&S validated in op environment. Sim environment validated for use.	High confidence of minor revision and checkout of existing software. No impacts on integration tests. Validated in most of op environment.	High confidence of minor revision and checkout of existing capability. Validated in most of op environment.	High confidence of existing support structure; minor modifications to existing support equipment	
0.1		High confidence of functional, fully tested hardware and validated M&S. Hardware will meet the form, fit, & functional rqmts. of the application	High confidence of existing, checked out SW. Integrated, verified, validated in operational environment.	High confidence of existing, checked out capability. Integrated, verified, validated in operational environment (capability fully demo'd). Workload, retention meet QoL objective.	High confidence of all existing support elements meet program requirements	Fully compliant with Fleet/Joint CONOPs; demo'd
0.0	No failure expected: proven, validated solution in expected operational environment; stable, robust capability.					

Development Best Practices Scoring Guidance for Consequence of Failure – Effectiveness and Suitability

C_f	General Mission Impact	Devel Effectiveness	Development Cost	Development Schedule
1.0	High Impact if unmitigated: High Program sensitivity to process variance given all other processes followed. Score may reflect magnitude of shortfall within the P_f range. Sources of Program impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Wrong problem solved -- unaddressed requirements/scenarios threaten program hold or termination. Significant contribution to product uncertainty (and Operational P_f). Inability to trace, monitor, justify, prioritize, and control pgm causes OIPT failure.	Program hold or termination due to significant failure to meet KPP threshold.	Deployment delay opens threat window.
0.9		Wrong problem solved -- extra capability threatens program viability via mismanaged resources. Or unexpected capability deficit threatens loss of assets.		
0.8		Stovepipe management threatens redesign at integration, or significant capability loss. System design limits operational evaluation -- inadequate insight to meet accountability to user and oversight. OT or LFT&E failure. Environmental impact.		
0.7	Med Impact if unmitigated: Medium Program sensitivity to process variance given all other processes followed. Score may reflect magnitude of shortfall within the P_f range. Sources of Program impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Short view solution hides LCC or seriously limits capability. Limited insight causes unintended risk exposure. Reduced ability to maintain confidence in system having frequent upgrades. Inability to pace rapid threat and technology change. Data rights provide inadeuate insight to support program management	<20% increase in NRE cost to program. Budget overrun surprises may lead to T&E shortcuts.	Need to renegotiate Milestone Events. Critical path violation significantly disrupts subcontractor tasking.
0.6		Timelines preclude quality product. Team pushed beyond best design practices.		
0.5		Lack of direction / Lexicon causes significant inefficiencies, loss of innovation opportunity; test consolidations missed. Gov't accountability to user and ability to manage FSC weakened by limited in-house technical capability.		
0.4	Low Impact if unmitigated: Low Program sensitivity to process variance given all other processes followed. Score may reflect magnitude of shortfall within the P_f range. Sources of Program impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Inadequate tools slow development, reduce attention to integration dependencies -- time for innovation inadequate.	<10% increase in NRE cost to program.	Readjustment of intermediate review schedules.
0.3		Some Degraded Insight/Control. Missed innovation opportunities. Inefficiency and errors from mis-communications.	Lost LCC savings from SPM/M&S reuse	
0.2		Retention probem degrades program continuity	<5% increase in NRE cost to program.	
0.1		Minor degradation of insight and control		
0.0	No Consequence to Program or MIssion			

Operational Performance Requirements Scoring Guidance for Probability of Failure
Effectiveness and Suitability

C_f	General Mission Impact	Op Effectiveness	Op Cost	Op Response	Op Availability	Crew Size	Interop
1.0	High Impact if unmitigated: Mission sensitivity to threshold deviation given all other thresholds met. Score may reflect magnitude of shortfall within the P_f range. Sources of mission impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Loss of Assets; Inability to act due to likelihood of loss; program termination due to KPP, COI, or Exit Criteria failure.	Program hold or termination due to significant failure to meet KPP threshold.	Significant contribution to Susceptibility due to slow reaction time.	NA	Program hold or termination due to significant failure to meet primary KPP threshold.	NA
0.9		Significant mission failure; Inability to act due to likelihood of failure					
0.8		Mission failure; Inability to act due to likelihood of failure					
0.7	Med Impact if unmitigated: Mission sensitivity to threshold deviation given all other thresholds met, or if a second worst case additional function fails. Score may reflect magnitude of shortfall within the P_f range. Sources of mission impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Significant mission degradation; Loss of Assets given worst case single additional function failure. Associated employment and programmatic impacts.	<25% increase in O&S cost to program.	Significant mission degradation due to slow reaction time	Significant mission degradation due to low availability	Contribution to increased operating costs due to minor variance from KPP threshold.	Significant mission degradation due to data limitations and weak deconfliction coordination.
0.6		Moderate mission degradation.					
0.5		Significant mission degradation given worst case single additional function failure.					Limited mission set due to inability for combined operations.
0.4	Low Impact if unmitigated: Mission sensitivity to threshold deviation given all other thresholds met, or if a second worst case additional function fails. Score may reflect magnitude of shortfall within the P_f range. Sources of mission impact due to various Effectiveness and Suitability weaknesses are illustrated in the other columns.	Some mission degradation.	<10% increase in O&S cost to program.	Loss of op tempo due to slow reaction time.	Increased inventory requirements and O&S cost burden to offset reliability shortfall.	Contribution to increased operating costs due to minor variance from KPP threshold, but has offsets in other areas.	
0.3		Significant coupling to other metrics types; Moderate mission degradation given worst case single additional function failure.					Significant wastage from redundant engagements.
0.2		Significant reduction in usability or efficiency. Some mission degradation given worst case single additional function failure.	<5% increase in O&S cost to program.				
0.1		Minor reduction in usability or efficiency.					
0.0	No Consequence to Mission or Program						

Development Best Practices Scoring Guidance for Probability of Failure Effectiveness and Suitability

P_f	General	Management	Requirements	Design	Production	Eval (Perf/V&V/Risk)
1.0	Indicates high degree of deviation from Best Practices. Use 0-1 scale to grade answers to Best Practice questions in each process area (see other columns for general guidance) as seen applied in your Functional Area.	No principals identified; limited experience in relevant project areas; plans and procedures for critical processes not available. Team skills and integration not matched to problem. R&R and common lexicon, management tools do not support integration. Data, risk, configurations not captured or managed.	Unknown Rqmt or similar Rqmts not known to have been implemented or documented. No systematically developed statement of requirements of any type exists. Specs will not support design or serve as evaluation reference.	Design not traceable to requirements. Segment designs not integrable. No trades or CAIV considered. Role of M&S ill-defined. Life Cycle issues of tech insertion, testability, COTS/OSA, disposal not addressed. Design tools (incl SPM) not matched to system complexity.	No known capability or technology to produce product.	Process does not trace to requirements and relevant scenarios. Is not justified or prioritized by risk assessments. Sim and physical data collection not integrated to support/leverage M&S use. M&S V&V NA. Does not cover life cycle trend detection. Does not provide for error source isolation. Inadequate attention to integration and test consolidations. Resources not identified. Schedule/resources do not account for test failures.
0.9		No principals identified; limited experience in major relevant project areas; some plans and procedures for critical processes not available.	Uninvestigated Rqmt or major elements of rqmt beyond scope of previous systems. Only functional or performance requirements defined. Specs will not support design or serve as evaluation reference.		Theoretical manufacturing concepts researched but requires significant R&D to develop processes.	
0.8		Few principals identified; limited experience in major relevant project areas; some plans and procedures for critical processes not available.	Undocumented Rqmt or significant deficiencies in meeting requirements. Few major requirements defined; current practices and methods would result in significant performance deficiencies. Specs will not support design or serve as evaluation reference.		Conceptual manufacturing processes identified. Significant investment to develop capability.	
0.7	Indicates some degree of deviation from Best Practices. Use 0-1 scale to grade answers to Best Practice questions in each process area (see other columns for general guidance) as seen applied in your Functional Area.	Some principals identified; limited experience in major relevant project areas; plans and procedures for critical processes must be validated. R&R and common lexicon, management tools partially supporting data sharing for integration. Data, risk, configurations partially captured and used in decision making.	Questionable Rqmt or moderate deficiencies in meeting all requirements. Most major requirements defined; current practices and methods would result in significant performance deficiencies. Spec provides ambiguous or partial references for design/eval.	Design partially traceable to requirements. Segment designs coordinated, but not optimally integrable. A few major trades considered; some risk linkage; CAIV constraints incompletely addressed. M&S used inconsistently without program level guidance to support/represent design. Life Cycle issues of tech insertion, testability, COTS/OSA, disposal treated superficially. Design tools (incl SPM) partially effective in capturing and controlling design.	New manufacturing process to industry. Major investment to establish capability & develop experience.	Process does not fully cover requirements and relevant scenarios. Plan linked to risk assessments, but not driven by them. Sim and physical data collection addressed separately; M&S V&V effort under scoped. Life cycle trend detection addresses only reliability (not performance or technology insertion). Only provides for isolation of major faults. Integration shortcuts; limited test consolidations. Resources not fully identified and committed to. Schedule/resources success oriented.
0.6		Some principals identified; experienced in most major relevant project areas; plans and procedures for critical processes must be validated.	Conflicting or unsure of Rqmt or expanded Rqmt from previously developed systems. Major requirements defined; current practices and methods would result in significant performance deficiencies. Spec provides ambiguous or partial references for design/eval.		Partially new or modified manufacturing processes to industry & no in house experience.	
0.5		Most principals identified; experienced in most major relevant project areas; most plans and procedures for critical processes validated.	Documented & understood Rqmts with minor deficiencies. Major requirements defined; current practices and methods would result in minor performance deficiencies. Spec provides ambiguous or partial references for design/eval.		Proven Manufacturing processes but no in house experience.	

Development Best Practices Scoring Guidance for Probability of Failure – Effectiveness and Suitability — Continued

P_f	General	Management	Requirements	Design	Production	Eval (Perf/V&V/Risk)
0.4	Indicates low degree of deviation from Best Practices. Use 0-1 scale to grade answers to Best Practice questions in each process area (see other columns for general guidance) as seen applied in your Functional Area.	Management principals identified; experienced in major relevant project areas; plans and procedures for critical processes validated.	Requirement similar to previously developed systems but with little margin. Major requirements defined; current practices and methods should provide minimum margin based on analysis. Spec provides minimal support as design/eval reference.	Design clearly traceable to requirements. Segment designs fully integrated with perf/CAIV/risk trades. Role of M&S optimized for LC payoff. Life Cycle issues of tech insertion, testability, COTS/OSA, disposal fully addressed. Design tools (incl SPM) used to capture and manage design complexity.	Proven Manufacturing processes but newly established capability.	Process explicitly covers requirements and relevant scenarios. Test Plans justified and prioritized by risk assessments. Sim and physical data collection fully integrated to support/leverage M&S use. M&S accredited for T&E use. Life cycle engineering data collection integral to design and support plan. Methods effectively isolate errors sources for mitigation.Integration testing thorough. High level of test and cert consolidations. Resources fully budgeted and account for test failures.
0.3		Management organization largely defined and experienced in major relevant project areas; plans and procedures for critical processes validated.	Requirement similar to previously developed systems with moderate margin. Major requirements defined; current practices and methods should provide minimum margin based on outcomes of similar projects. Spec provides adequate support as design/eval reference.		Proven Manufacturing processes used at least twice by design agent.	
0.2		Management organization well defined and experienced in most relevant project areas; plans and procedures mostly validated.	Requirements well within the scope of previously developed systems with moderate margin. Requirements fully defined; current practices and methods should provide acceptable margin based on outcomes of numerous similar projects. Spec provides good support as design/eval reference.		Proven Manufacturing processes used occasionally by design agent.	
0.1		Management organization well defined and experienced in all relevant project areas; plans and procedures fully validated. R&R, common lexicon, management tools ensure optimum integration. Data, risk, configurations all captured, managed, and used in decision support.	Requirements well within the scope of previously developed systems with significant margin. Requirements fully defined; current practices and methods should provide significant margin based on outcomes of numerous similar projects. Spec provides excellent support as design/eval reference.		NDI off the shelf manufacturing processes which have been used often.	
0.0	No failure expected: proven process of Best Practices tailored to the acquisition environment; continuous improvement implemented					

APPENDIX K — DEVELOPMENT FUNCTIONS – SAMPLE QUESTIONS TO ASSESS PROGRESS AGAINST BEST PRACTICES

BEST PRACTICE CRITERIA
MANAGEMENT:
Senior Level: 1. Is there convincing evidence that top-level corporate management is committed to program success? 2. Is the management team comprised of participating representatives from all pertinent disciplines (design, manufacturing, logistics, etc.), and are they empowered to act? 3. Is the management team experienced in systems of identical or similar complexity? 4. Is the Program Manager experienced in planning, controlling, and exercising continuous improvement on a contract(s) of similar scope and complexity? Does the PM have experience in controlling cost, schedule, and technical disciplines in an integrated and balanced manner? 5. Is the Program Manager authorized to commit the team's resources? What additional approvals and what management thresholds must the PM obtain in the team's corporate structure?
PLANNING: 1. Is there a Project Management Plan, Project Master Plan, or equivalent? 2. Does it include critical elements such as organization, lines of communication, levels of responsibility and authority, program monitoring and control, communications plans for interacting with the Navy (design reviews/major milestones), over-arching schedules, etc? 3. Are planning tools such as PERT and Critical Path networks included in the team's planning regime? 4. Does the process encourage or allow proactive behavior and reward those who are engaged in forecasting problems and taking appropriate mitigation actions?
MONITORING AND CONTROLLING: 1. Does the schedule include a comprehensive formal review process to monitor and control progress on a regular basis? 2. Are there procedures and organizational structures in place to facilitate "ad hoc" or "in process" reviews? 3. Does the information technology infrastructure proposed support the control and monitoring of the program in an efficient manner? Does it leverage management tool technology without adding risk to the program? Has the approach been proven on other programs of similar data/engineering complexity? Does the system provide a collaborative work and information-sharing environment with all program stakeholders? 4. Does the team's management have a plan to accommodate third party dependencies if they are required?

5. Does the subcontractor management plan (or actual subcontracts) provide incentives, collaborative features, and safeguards that ensure excellent performance standards?

BEST PRACTICE CRITERIA

IMPROVEMENT:

1. Has the team been trained and/or have experience in IPPD, IPT, commercial business processes, and outgrowths of Acquisition Reform that can lead to continuous improvement, innovative thinking, and lower costs?

2. Has an independent agent certified the team's improvement processes? (This refers to ISO certification, SEI ratings, etc.)

SYSTEMS ENGINEERING:

Requirements:

1. Is there clear evidence that requirements are understood beginning with the mission profile (performance, maintainability, reliability, safety, environmental, etc.)?

2. Is there a workable traceability tool set and associated business process to track requirements to the design products? Are preliminary design efforts traceable to a functional baseline?

3. Are requirements allocated and verified at the lowest possible level? Is there evidence that the team's management structure understands the program objectives and discrete requirements?

4. Is there a process and schedule to conduct trade studies on an iterative basis to evaluate alternative configurations relative to requirements?

Design:

1. Has a clear design policy been defined and communicated to all team members? Does it include the latter stages of the ship/system life cycle? Are systems engineering principles, including integration, central to the overall design process?

2. Is the design team comprised of experienced personnel who can draw upon lessons learned in programs of similar complexity?

3. Does the design process accommodate changes in disciplined fashion? Can the process be partitioned to accommodate technology insertion or higher risk scenarios? Does the Configuration Management Plan support the baseline control as well as a disciplined design change process?

4. Is there a robust menu of design analyses and diagnostic processes including cost analysis, criticality analysis, reliability analysis, hazard analysis, etc. to improve and lend credibility to design team performance?

5. Is the design review process well understood and defined so that it can be executed collaboratively and effectively with the Navy?

Production:

1. Is the production team experienced with identical or similar systems?

2. Is the production infrastructure in place (including software, hardware, integration, and testing)? Are facilities and capital assets available to accommodate the magnitude of the project?

3. Have production personnel been involved/integrated in the design process? Is there evidence that the team's processes will accommodate long lead time items, complex integration, and other production challenges?

4. Is the plan to transition from design to production executable?

5. Does the quality control/quality management system have sufficient rigor to lower the Navy's risk to appropriate levels? (ISO 9001, IEEE, SEI standards apply.)

BEST PRACTICE CRITERIA

Evaluation:

1. Has the team developed a comprehensive test program?

2. Does it take advantage of modeling and simulation and other cost reduction testability alternatives?

3. Does the plan include the appropriate infrastructure (facilities, equipment, etc.) to conduct the test program? Does it cover all certification and safety requirements that the government must validate or ultimately approve?

4. Are there innovations in the test program that are advantageous from a cost and schedule perspective over conventional programs?

5. Is the test program directly traceable to performance requirements/objectives including integration and total ship engineering?

6. To what degree has the team made use of soft analyses to validate performance?

7. Is the team's risk management process comprised of appropriate rigor including disciplined analysis, continuous monitoring, validation from outside experts, etc?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] DoD 5000 Series Instructions and Notices. DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003. Last accessed May 31, 2008, at: https://akss.dau.mil/dag/DoD5000.asp?view=document&doc=2.

[2] DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003. Last accessed May 31, 2008, at: https://akss.dau.mil/dag/DoD5000.asp?view=document&doc=2.

[3] DoD 4245.7-Manual—"Transition from Development to Production." September 1985.

[4] "Methods and Metrics for Product Success Manual." ASN RDA. July 1994.

[5] NAVSO P-6071—"Best Practices: How to Avoid Surprises in the World's Most Complicated Technical Process," Willis J. Willoughby Jr., publisher. March 1986.

[6] *Risk Management Guide for DoD Acquisitions*, Sixth Edition, Ft. Belvoir, VA: Defense Systems Management College Press. March 1998.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3 David F. Matthews
   Naval Postgraduate School
   Monterey, California

4. Mike Persson
   NAVAIR 4.1G
   PAX River NAS, Maryland

5. Edouard Kujawski
   Naval Postgraduate School
   Monterey, California