RISK MANAGEMENT GUIDE FOR DOD ACQUISITION

Sixth Edition

(Version 1.0)

August, 2006

Department of Defense

Preface

The Department of Defense (DoD) recognizes that risk management is critical to acquisition program success (see the *Defense Acquisition Guidebook* (DAG), Section 11.4). The purpose of addressing risk on programs is to help ensure program cost, schedule, and performance objectives are achieved at every stage in the life cycle and to communicate to all stakeholders the process for uncovering, determining the scope of, and managing program uncertainties. Since risk can be associated with all aspects of a program, it is important to recognize that risk identification is part of the job of everyone and not just the program manager or systems engineer. That includes the test manager, financial manager, contracting officer, logistician, and every other team member.

The purpose of this guide is to assist DoD and contractor Program Managers (PMs), program offices and Integrated Product Teams (IPTs) in effectively managing program risks during the entire acquisition process, including sustainment. This guide contains baseline information and explanations for a well-structured risk management program. The management concepts and ideas presented here encourage the use of risk-based management practices and suggest a process to address program risks without prescribing specific methods or tools. (Note: this guide does not attempt to address the requirements of DoDI 5000.1 to prevent and manage Environment, Safety, and Occupational Health (ESOH) hazards. The reader should refer to MIL STD 882D, Standard Practice for System Safety, for guidance regarding ESOH hazards).

Since this is a guide, the information presented within is not mandatory to follow, but PMs are encouraged to apply the fundamentals presented here to all acquisition efforts—both large and small—and to all elements of a program (system, subsystem, hardware, and software). Risk management is a fundamental program management tool for effectively managing future uncertainties associated with system acquisition. The practice of risk management draws from many management disciplines including but not limited to program management, systems engineering, earned value management, production planning, quality assurance, logistics, system safety and mishap prevention, and requirements definition in order to establish a methodology that ensures achieving program objectives for cost, schedule, and performance. PMs should tailor their risk management approaches to fit their acquisition program, statutory requirements, and life-cycle phase. The guide should be used in conjunction with related directives, instructions, policy memoranda, or regulations issued to implement mandatory requirements.

This guide has been structured to provide a basic understanding of risk management concepts and processes. It offers clear descriptions and concise explanations of core steps to assist in managing risks in acquisition programs. Its focuses on risk mitigation planning and implementation rather on risk avoidance, transfer, or assumption. The guide is not laid out in chronological order of implementing a risk management program, but rather in a sequence to facilitate understanding of the topic. For example, the discussion on planning / preparation for overall risk management is in Section 8 of the guide to keep it separate from the risk management process. The planning / preparation function deals with planning to execute the risk management process, but is not part of the execution of the process itself.

There are several notable changes of emphasis in this guide from previous versions. These changes reflect lessons learned from application of risk management in DoD programs. Emphasis has been placed on:

- The role and management of future root causes,
- Distinguishing between risk management and issue management,
- Tying risk likelihood to the root cause rather than the consequence,
- Tracking the status of risk mitigation implementation vs. risk tracking, and
- Focusing on event-driven technical reviews to help identify risk areas and the effectiveness of ongoing risk mitigation efforts.

The risk management techniques available in the previous version of this guide and other risk management references can be found on the Defense Acquisition University Community of Practice website at https://acc.dau.mil/rm, where risk managers and other program team personnel can access the additional information when needed. This guide is supplemented by Defense Acquisition University (DAU) Risk Management Continuous Learning Module (key words: "risk management" and course number CLM017).

The Office of the Secretary of Defense (OSD) office of primary responsibility (OPR) for this guide is OUSD(AT&L) Systems and Software Engineering, Enterprise Development (OUSD(AT&L) SSE/ED). This office will develop and coordinate updates to the guide as required, based on policy changes and customer feedback. To provide feedback to the OPR, please e-mail the office at ATL-ED@osd.mil.

Table of Contents

Table of Figures

1. Key Terms, Descriptions, and Principles

1.1. Risk

Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints. Risk can be associated with all aspects of a program (e.g., threat, technology maturity, supplier capability, design maturation, performance against plan,) as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS). Risk addresses the potential variation in the planned approach and its expected outcome. While such variation could include positive as well as negative effects, this guide will only address negative future effects since programs have typically experienced difficulty in this area during the acquisition process.

1.2. Components of Risk

Risks have three components:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at the present time of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to future root causes and their effects.

1.3. Risk versus Issue Management

Risk management is the overarching process that encompasses identification, analysis, mitigation planning, mitigation plan implementation, and tracking. Risk management should begin at the earliest stages of program planning and continue throughout the total life-cycle of the program. Additionally, risk management is most effective if it is fully integrated with the program's systems engineering and program management processes—as a driver and a dependency on those processes for root cause and consequence management. A common misconception, and program office practice, concerning risk management is to identify and track issues (vice risks), and then manage the consequences (vice the root causes). This practice tends to mask true risks, and it serves to track rather than resolve or mitigate risks. This guide focuses on risk mitigation planning and implementation rather on risk avoidance, transfer or assumption.

Note: Risks should not be confused with issues. If a root cause is described in the past tense, the root cause has already occurred, and hence, it is an issue that needs to be resolved, but it is not a risk. While issue management is one of the main functions of PMs, a*n important difference between issue management and risk management is that issue management applies resources to address and resolve current issues or problems, while risk management applies resources to mitigate future potential root causes and their consequences.*

To illustrate the difference between a risk and an issue, consider, for example, a commercial-off-the-shelf (COTS) sourcing decision process. Questions such as the following should be asked and answered prior to the COTS decision:

- *"Is there any assurance the sole source provider of critical COTS components will not discontinue the product during government acquisition and usage?"*
- *"Does the government have a back-up source?"*
- *"Can the government acquire data to facilitate production of the critical components?"*

. These statements lead to the identification of root causes and possible mitigation plans. If a COTS acquisition is decided, and sometime later the manufacturer of a COTS circuit card has informed the XYZ radar builder that the circuit card will be discontinued and no longer available within 10 months, then an *issue* has emerged and with upfront planning the issue might have been prevented. A *risk* is the **likelihood and consequence of future** production schedule delays in radar deliveries if a replacement card cannot be found or developed and made available within 10 months.

If a program is behind schedule on release of engineering drawings to the fabricator, this is not a risk; it is an issue that has already emerged and needs to be resolved. Other examples of issues include failure of components under test or analyses that show a design shortfall. These are program problems that should be handled as issues instead of risks, since their probability of occurrence is 1.0 (certain to occur or has occurred). It should also be noted that issues may have adverse future consequences to the program (as a risk would have).

1.4. Risk Management Objective

PMs have a wide range of supporting data and processes to help them integrate and balance programmatic constraints against risk. The Acquisition Program Baseline (APB) for each program defines the top-level cost, schedule, and technical performance parameters for that program. Additionally, acquisition planning documents such as Life-Cycle Cost Estimates (LCCE), Systems Engineering Plans (SEP), IMS, Integrated Master Plans (IMP), Test and Evaluation Master Plans (TEMP) and Technology Readiness Assessment (TRA) provide detailed cost, schedule, and technical performance measures for program management efforts. Since effective risk management requires a stable and recognized baseline from which to access, mitigate, and manage program risk it is critical that the program use an IMP/IMS. Processes managed by the contractor, such as the IMP, contractor IMS, and Earned Value Management (EVM), provide the PM with additional insight into balancing program requirements and constraints against cost, schedule, or technical risk. The objective of a well-managed risk management program is to provide a repeatable process for balancing cost, schedule, and performance goals within program funding, especially on programs with designs that approach or exceed the state-of-the-art or have tightly constrained or optimistic cost, schedule, and performance goals. Without effective risk management the program office may find itself doing crisis management, a resource-intensive process that is typically constrained by a restricted set of available options. Successful risk management depends on the knowledge gleaned from assessments of all aspects of the program coupled with appropriate mitigations applied to the specific root causes and consequences.

A key concept here is that the government shares the risk with the development, production, or support contractor (if commercial support is chosen), and does not transfer all risks to the contractor. The program office always has a responsibility to the system user to develop a capable and supportable system and can not absolve itself of that responsibility. Therefore, all program risks, whether primarily managed by the program office or by the development/support contractor, are of concern and must be assessed and managed by the program office. Once the

program office has determined which risks and how much of each risk to share with the contractor, it must then assess the total risk assumed by the developing contractor (including subcontractors). The program office and the developer must work from a common risk management process and database. Successful mitigation requires that government and the contractor communicate all program risks for mutual adjudication. Both parties may not always agree on risk likelihoods, and the government PM maintains ultimate approval authority for risk definition and assignment. A common risk database available and open to the government and the contractor is an extremely valuable tool. Risk mitigation involves selection of the option that best provides the balance between performance and cost. Recall that schedule slips generally and directly impact cost. It is also possible that throughout the system life cycle there may be a need for different near-term and long-term mitigation approaches.

An effective risk management process requires a commitment on the part of the PM, the program office and the contractor to be successful. Many impediments exist to risk management implementation, however, the program team must work together to overcome these obstacles. One good example is the natural reluctance to identify real program risks early for fear of jeopardizing support of the program by decision makers. Another example is the lack of sufficient funds to properly implement the risk mitigation process. However, when properly resourced and implemented, the risk management process supports setting and achieving realistic cost, schedule, and performance objectives and provides early identification of risks for special attention and mitigation.

2. Risk Management

2.1. The Risk Management Process

Risk management is a continuous process that is accomplished throughout the life cycle of a system. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination.

Acquisition program risk management is not a stand-alone program office task. It is supported by a number of other program office tasks. In turn, the results of risk management are used to finalize those tasks. Important tasks, which must be integrated as part of the risk management process, include requirements development, logical solution and design solution (systems engineering), schedule development, performance measurement, EVM (when implemented), and cost estimating. Planning a good risk management program integral to the overall program management process ensures risks are handled at the appropriate management level.

Emphasis on risk management coincides with overall DoD efforts to reduce life-cycle costs (LCC) of system acquisitions. New processes, reforms, and initiatives are being implemented with risk management as a key component. It is essential that programs define, implement and document an appropriate risk management and mitigation approach. Risk management should be designed to enhance program management effectiveness and provide PMs with a key tool to reduce LCC, increase program likelihood of success, and assess areas of cost uncertainty.

2.2. The Risk Management Process Model

The risk management process model (see figure 1) includes the following key activities, performed on a continuous basis:

- Risk Identification,
- Risk Analysis,
- Risk Mitigation Planning,
- Risk Mitigation Plan Implementation, and
- Risk Tracking.

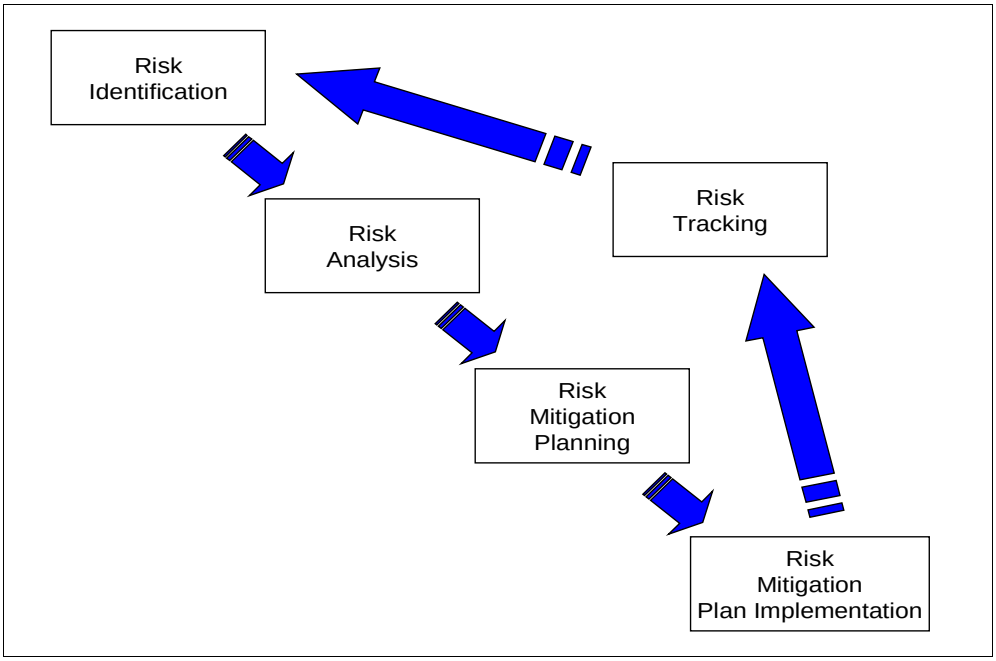

Figure 1. DoD Risk Management Process

Acquisition programs run the gamut from simple to complex procurements and support of mature technologies that are relatively inexpensive to state-of-the-art and beyond programs valued in the multibillions of dollars. Effective risk management approaches generally have consistent characteristics and follow common guidelines regardless of program size. Some characteristics of effective risk management approach are discussed below.

2.3. Characteristics of Successful Risk Management Approaches

Successful acquisition programs will likely have the following risk management characteristics:

- Feasible, stable, and well-understood user requirements, supported by leadership / stakeholders, and integrated with program decisions;
- A close partnership with users, industry, and other stakeholders;
- A planned risk management process integral to the acquisition process, especially to the technical planning (SEP and TEMP) processes, and other program related partnerships;
- Continuous, event-driven technical reviews to help define a program that satisfies the user's needs within acceptable risk;
- Identified risks and completed risk analyses;
- Developed, resourced, and implemented risk mitigation plans;

- Acquisition and support strategies consistent with risk level and risk mitigation plans;
- Established thresholds and criteria for proactively implementing defined risk mitigation plans;
- Continuous and iterative assessment of risks;
- The risk analysis function independent from the PM;
- A defined set of success criteria for performance, schedule, and cost elements; and
- A formally documented risk management process.

To support these efforts, assessments via technical reviews should be performed as early as possible in the life cycle (as soon as performance requirements are developed) to ensure critical performance, schedule, and life-cycle cost risks are addressed, with mitigation actions incorporated into program planning and budget projections. As the award of a contract requiring EVM approaches, preparation and planning should commence for the execution of the Integrated Baseline Review (IBR) process in accordance with the Defense Acquisition Guidebook. Chapter 8 addresses risk planning and Risk Management Plans (RMPs).

2.4. Top-Level Guidelines for Effective Risk Management

- Assess the root causes of program risks and develop strategies to manage these risks during each acquisition phase.
  - Identify as early as possible, and intensively manage those design parameters that critically affect capability, readiness, design cost, or LCC.
  - Use technology demonstrations, modeling and simulation, and aggressive prototyping to reduce risks.
  - Include test and evaluation as part of the risk management process.

- Include industry participation in risk management. Offerors should have a risk approach as part of their proposals as suggested in this guide to identify root causes and develop plans to manage those risks and should include a draft RMP. Additionally, the offerors should identify risks as they perceive them as part of the proposal. This not only helps the government identify risks early, but provides additional insight into the offeror's level of understanding of the program requirements.

- Use a proactive, structured risk assessment and analysis activity to identify and analyze root causes.
  - Use the results of prior event-based systems engineering technical reviews to analyze risks potentially associated with the successful completion of an upcoming review. Reviews should include the status of identified risks.
  - Utilize risk assessment checklists (available for all event-based technical reviews) in preparation for and during the conduct of technical reviews. The DAU Technical Reviews Continuous Learning Module (key words: "technical reviews" and course number CLE003) provides a systematic process and access to checklists for continuously assessing the design maturity, technical risk, and programmatic risk of acquisition programs, and provides links to these checklists.
  - Establish risk mitigation plans and obtain resources against that plan.
  - Provide for periodic risk assessments throughout each program life-cycle phase.

- Establish a series of "risk assessment events," where the effectiveness of risk reduction conducted to date is reviewed. These "risk assessment events" can be held as part of

technical reviews, risk review board meetings, or periodic program reviews. These events should include the systems engineering technical reviews, be tied to the IMP at each level, and have clearly defined entry and exit criteria reviewed during IBRs.

- Include processes as part of risk assessment. This would include the contractor's managerial, development, and manufacturing processes as well as repair processes for the sustainment phase.
- Review the contractor's baseline plans as part of the IBR process which includes joint government/contractor evaluation of the inherent risks in the contractor's integrated earned value baseline (work definition, schedule, and budgets).
- Review the contractor's Schedule Risk Assessment (SRA) when provided as part of the IMS data item (DI-MGMT-81650). Review the realism of the contractor's estimate at completion. Assess the overall likelihood of the contractor achieving the forecasted schedule or final costs against the program's constraints.
- Establish a realistic schedule and funding baseline for the program as early as possible in the program, incorporating not only an acceptable level of risk, but adequate schedule and funding margins.
- Clearly define a set of evaluation criteria for assigning risk ratings (low, moderate, high) for identified root causes.
- Determine the program's approach to risk prioritization, commonly presented in the risk reporting matrix discussed in Section 4.2.

3. Key Activity - Risk Identification

The first key activity in the risk management process is Risk Identification. While in some publications "risk assessment" is used as an umbrella term that includes the primary activities of both risk identification and risk analysis this guide addresses these two critical risk management activities separately in Sections 3 and 4, respectively.

3.1. Purpose

The intent of risk identification is to answer the question "What can go wrong?" by:

- Looking at current and proposed staffing, process, design, supplier, operational employment, resources, dependencies, etc.,
- Monitoring test results especially test failures (readiness results and readiness problems for the sustainment phase),
- Reviewing potential shortfalls against expectations, and
- Analyzing negative trends.

Risk identification is the activity that examines each element of the program to identify associated root causes, begin their documentation, and set the stage for their successful management. Risk identification begins as early as possible in successful programs and continues throughout the program with regular reviews and analyses of Technical Performance Measurements (TPMs), schedule, resource data, life-cycle cost information, EVM data/trends, progress against critical path, technical baseline maturity, safety, operational readiness, and other program information available to program IPT members.

3.2. Tasks

Risk can be associated with all aspects of a program, e.g., operational needs, attributes, constraints, performance parameters including Key Performance Parameters (KPPs), threats, technology, design processes, or WBS elements. Consequently it is important to recognize that risk identification is the responsibility of every member of the IPT, not just the PM or systems engineer.

Examination of a program is accomplished through decomposition into relevant elements or areas. Decomposition may be oriented to requirements, processes, functional areas, technical baselines, or acquisition phases. Another method is to create a WBS as early as possible in a program for a product-oriented decomposition, which is particularly useful in identifying product and some process oriented risks. Other means, such as a process-oriented framework, would be required to sufficiently illuminate process-based root causes, which could be tracked via the WBS structure to view impacts to schedule, resource loading, etc.

To identify risks and their root causes, IPTs should break down program elements to a level where subject matter experts (SMEs) can perform valid identification by WBS or IMS line item number. The information necessary to do this varies according to the life-cycle phase of the program. A program risk assessment checklist is available via the DAU Technical Reviews Continuous Learning Module (key words: "technical reviews;" course number CLE003).

During decomposition, risks can be identified based on prior experience, brainstorming, lessons learned from similar programs, and guidance contained in the program office RMP (see Section 8.2). A structured approach describes each WBS element in terms of sources or areas of risk. MIL-HDBK-881, "Work Breakdown Structures for Defense Materiel Items," serves as the

basis for identifying the first three levels of the program WBS, and developing the contract WBS. The examination of each element and process against each risk area is an exploratory exercise to identify the critical root causes. The investigation may show that risks are inter-related.

WBS product and process elements and industrial engineering, manufacturing and repair processes are often sources of significant root causes. Risks are determined by examining each WBS element and process in terms of causes, sources, or areas of risk. When EVM is applied on a contract it can help identify WBS program elements that are experiencing issues. This information can be used to help prioritize WBS elements that may contain unidentified risks.

3.3. Identification of Root Causes

Program offices should examine their programs and identify root causes by reducing program elements to a level of detail that permits an evaluator to understand the significance of any risk and identify its causes. This is a practical way of addressing the large and diverse number of risks that often occur in acquisition programs. For example, a WBS level 4 or 5 element may be made up of several root causes associated with a specification or function, e.g., potential failure to meet turbine blade vibration requirements for an engine turbine design.

Root causes are identified by examining each WBS product and process element in terms of the sources or areas of risk. Root causes are those potential events that evaluators (after examining scenarios, WBS, or processes) determine would adversely affect the program at any time in its life cycle.

An approach for identifying and compiling a list of root causes is to:

- List WBS product or process elements,
- Examine each in terms of risk sources or areas,
- Determine what could go wrong, and
- Ask “why” multiple times until the source(s) is discovered.

The risk identification activity should be applied early and continuously in the acquisition process, essentially from the time performance and readiness requirements are developed. The program office should develop and employ a formalized risk identification procedure, and all personnel should be responsible for using the procedure to identify risks. Specific opportunities to identify risks (e.g., at event-driven technical reviews) and explore root causes against objective measures (e.g., meeting the entry criteria for an upcoming technical review, requirements stability, technical maturity, software lines of code and reuse ratios, critical paths or near critical paths) should not be overlooked. If technical reviews are schedule, vice event driven, their usefulness as risk assessment tools can be impacted, and the full benefits of risk assessment may not be achieved. The early identification and assessment of critical risks allows for the formulation of risk mitigation approaches and the streamlining of both the program definition and the Request For Proposal (RFP) processes around those critical product and process risks. Risk identification should be done again following any major program change or restructure such as significant schedule adjustment, requirements change, or scope change to the contract.

Typical risk sources include:

- **Threat.** The sensitivity of the program to uncertainty in the threat description, the degree to which the system design would have to change if the threat's parameters

change, or the vulnerability of the program to foreign intelligence collection efforts (sensitivity to threat countermeasure).

- **Requirements.** The sensitivity of the program to uncertainty in the system description and requirements, excluding those caused by threat uncertainty. Requirements include operational needs, attributes, performance and readiness parameters (including KPPs), constraints, technology, design processes, and WBS elements.
- **Technical Baseline.** The ability of the system configuration to achieve the program's engineering objectives based on the available technology, design tools, design maturity, etc. Program uncertainties and the processes associated with the "ilities" (reliability, supportability, maintainability, etc.) must be considered. The system configuration is an agreed-to description (an approved and released document or a set of documents) of the attributes of a product, at a point in time, which serves as a basis for defining change.
- **Test and Evaluation.** The adequacy and capability of the test and evaluation program to assess attainment of significant performance specifications and determine whether the system is operationally effective, operationally suitable, and interoperable.
- **Modeling and Simulation (M&S).** The adequacy and capability of M&S to support all life-cycle phases of a program using verified, validated, and accredited models and simulations.
- **Technology.** The degree to which the technology proposed for the program has demonstrated sufficient maturity to be realistically capable of meeting all of the program's objectives.
- **Logistics.** The ability of the system configuration and associated documentation to achieve the program's logistics objectives based on the system design, maintenance concept, support system design, and availability of support data and resources.
- **Production/Facilities.** The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources (repair resources in the sustainment phase).
- **Concurrency.** The sensitivity of the program to uncertainty resulting from the combining or overlapping of life-cycle phases or activities.
- **Industrial Capabilities.** The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system.
- **Cost.** The ability of the system to achieve the program's life-cycle support objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined and taking into account known and unknown program information).
- **Management.** The degree to which program plans and strategies exist and are realistic and consistent. The government's acquisition and support team should be qualified and sufficiently staffed to manage the program.
- **Schedule.** The sufficiency of the time allocated for performing the defined acquisition tasks. This factor includes the effects of programmatic schedule decisions, the inherent errors in schedule estimating, and external physical constraints.
- **External Factors.** The availability of government resources external to the program office that are required to support the program such as facilities, resources, personnel, government furnished equipment, etc.

- **Budget.** The sensitivity of the program to budget variations and reductions and the resultant program turbulence.
- **Earned Value Management System**. The adequacy of the contractor's EVM process and the realism of the integrated baseline for managing the program.

Developers' engineering and manufacturing processes that historically have caused the most difficulty during the development phases of acquisition programs are frequently termed critical risk processes. These processes include, but are not limited to, design, test and evaluation, production, facilities, logistics, and management. DoD 4245.7-M, *Transition from Development to Production*, describes these processes using templates. The templates are the result of a Defense Science Board task force, composed of government and industry experts who identified engineering processes and control methods to minimize risk in both government and industry.

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

In addition, PMs should address the uncertainty associated with security – an area sometimes overlooked by developers but addressed under the topic of acquisition system protection in the *Defense Acquisition Guidebook* (DAG), as well as in DoDD 5200.1, *DoD Information Security Program*; DoDD 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*; and DoD 5200.1-M, *Acquisition Systems Protection Program*. However, in addition to the guidance given there, PMs must recognize that, in the past, classified programs have experienced difficulty in access, facilities, clearances, and visitor control. Failure to manage these aspects of a classified program could adversely impact schedules. Not only are classified programs at risk, but any program that encompasses Information Assurance is burdened by ever increasing security requirements and certifications. These risks must be identified as early as possible as they affect design, development, test, and certification requirements that will impose schedule challenges to the program.

4. Key Activity - Risk Analysis

4.1. Purpose

The intent of risk analysis is to answer the question "How big is the risk?" by:

- Considering the likelihood of the root cause occurrence;
- Identifying the possible consequences in terms of performance, schedule, and cost; and
- Identifying the risk level using the Risk Reporting Matrix shown in Figure 2.

4.2. Risk Reporting Matrix

Each undesirable event that might affect the success of the program (performance, schedule, and cost) should be identified and assessed as to the likelihood and consequence of occurrence. A standard format for evaluation and reporting of program risk assessment findings facilitates common understanding of program risks at all levels of management. The Risk Reporting Matrix below is typically used to determine the level of risks identified within a program. The level of risk for each root cause is reported as low (green), moderate (yellow), or high (red).

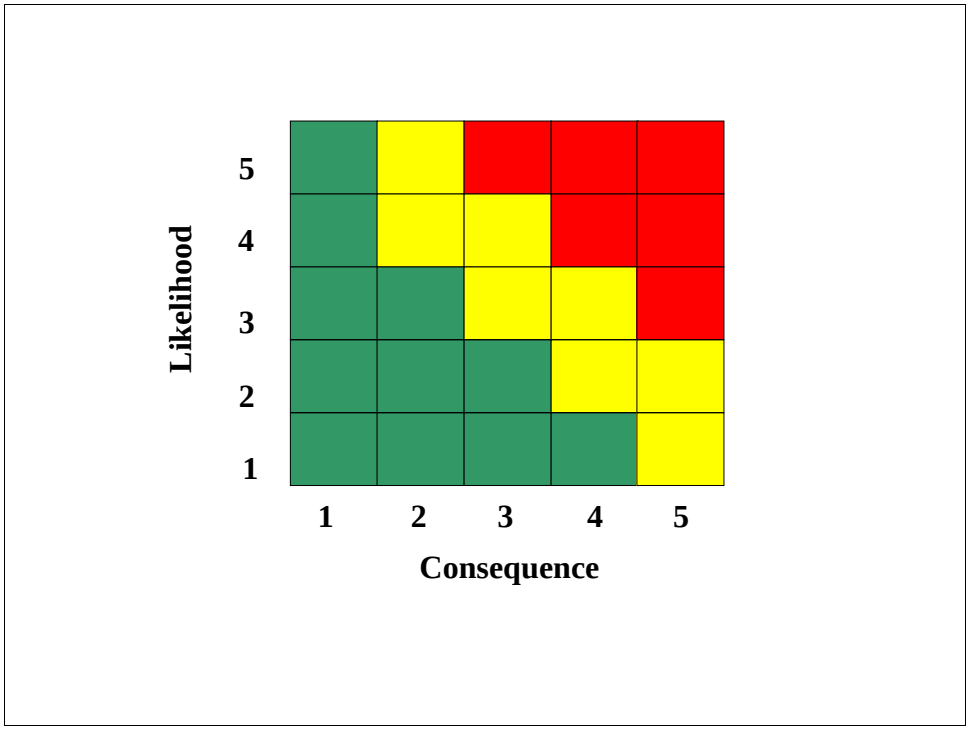

Figure 2. Risk Reporting Matrix

The level of likelihood of each root cause is established utilizing specified criteria (Figure 3). For example, if the root cause has an estimated 50 percent probability of occurring, the corresponding likelihood is Level 3.

Likelihood

Level	Likelihood	Probability of Occurrence
1	Not Likely	~10%
2	Low Likelihood	~30%
3	Likely	~50%
4	Highly Likely	~70%
5	Near Certainty	~90%

Figure 3. Levels of Likelihood Criteria

The level and types of consequences of each risk are established utilizing criteria such as those described in Figure 4. A single consequence scale is not appropriate for all programs, however. Continuing with the prior example of a root cause with a 50 percent probability of occurring, if that same root cause has no impact on performance or cost, but may likely result in a minor schedule slippage that won't impact a key milestone, then the corresponding consequence is a Level 3 for this risk. For clarity it is also classified as a *schedule* risk since its root cause is schedule related.

Consequence

Level	Technical Performance	Schedule	Cost
1	Minimal or no consequence to technical performance	Minimal or no impact	Minimal or no impact
2	Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	Able to meet key dates. **Slip < * month(s)**	Budget increase or unit production cost increases. **< ** (1% of Budget)**
3	Moderate reduction in technical performance or supportability with limited impact on program objectives	Minor schedule slip. Able to meet key milestones with no schedule float. **Slip < * month(s)** **Sub-system slip > * month(s) plus available float.**	Budget increase or unit production cost increase **< ** (5% of Budget)**
4	Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	Program critical path affected. **Slip < * months**	Budget increase or unit production cost increase **< ** (10% of Budget)**
5	Severe degradation in technical performance; Cannot meet KPP or key technical/supportability threshold; will jeopardize program success	Cannot meet key program milestones. **Slip > * months**	Exceeds APB threshold **> ** (10% of Budget)**

Figure 4. Levels and Types of Consequence Criteria

The results for each risk are then plotted in the corresponding single square on the Risk Reporting Matrix. In this example, since the level of likelihood and consequence were both "3," the corresponding schedule risk is reported as "yellow," as shown in Figure 5, using a recommended display method that includes the risk title (where (S) identifies this risk as a schedule risk), risk causal factor, and mitigation approach.

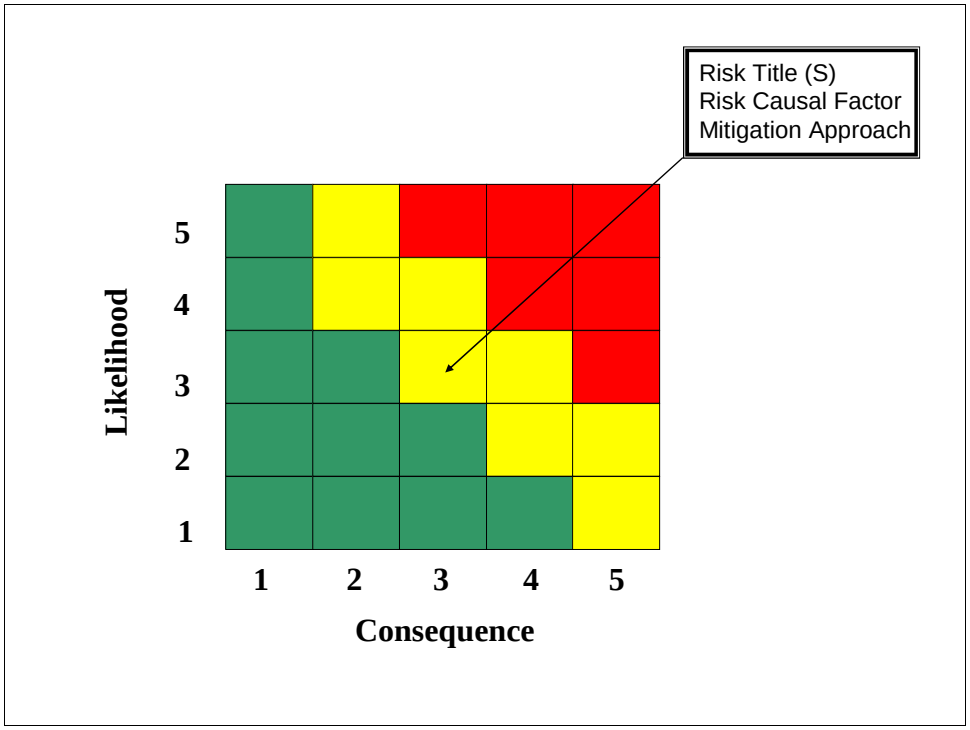

Figure 5. Risk Analysis and Reporting Illustration

4.3. Tasks

Risk analysis is the activity of examining each identified risk to refine the description of the risk, isolate the cause, determine the effects, aid in setting risk mitigation priorities. It refines each risk in terms of its likelihood, its consequence, and its relationship to other risk areas or processes. Analysis begins with a detailed study of the risks that have been identified. The objective is to gather enough information about future risks to judge the root causes, the likelihood, and the consequences if the risk occurs. The frequently used term "risk assessment" includes the distinct activities of risk identification and risk analysis.

Risk analysis sequence of tasks include:

- Develop probability and consequence scales by allocating consequence thresholds against the WBS or other breakout;
- Assign a probability of occurrence to each risk using the criteria presented in Section 4.2;
- Determine consequence in terms of performance (P), schedule (S), and/or cost (C) impact using the criteria presented in Section 4.2; and
- Document the results in the program risk database.

Note: Risk analysis is a snapshot in time and may change significantly during the program. Risk analyses must be periodically re-accomplished to ensure the analysis remains current.

In a WBS approach, risks are identified, assessed, and tracked for individual WBS elements at their respective levels (primarily for impact on cost and schedule performance) and for their resulting effect on the overall product. Since DoD programs are generally established around the

WBS, each product's associated costs and schedule can be readily baselined, and its risk consequence can be measured as a deviation against this baseline. Taking the WBS to successively lower levels will help to assure all required products are identified, along with allocations for cost and schedule performance (as well as operational performance) goals.

Integration of performance, schedule, and cost analyses into a single process provides a final product that starts with well-defined requirements, builds upon a solid technical foundation, develops a realistic program schedule, and documents the resources needed in the program cost estimates. Program root cause identification and analysis integrates the technical performance assessment, schedule assessment, and cost estimates using established risk evaluation techniques. Each of these risk categories (cost, schedule, performance) has activities of primary responsibility, but is provided inputs and support from the other two risk categories. This helps to keep the process integrated and to ensure the consistency of the final product.

The following paragraphs provide relevant questions to ask in assessing performance, schedule, and cost root causes.

4.4. Performance (P) Considerations

Is there an impact to technical performance and to what level? If so, this risk has a performance consequence. These risks generally have associated schedule and cost impacts, but should be carried as a performance risk.

- Operational (e.g., Initial Capabilities Document (ICD), Capability Development Document (CDD), Capability Production Document (CPD), threats, suitability, effectiveness).
- Technical (e.g., SEP, Technology Readiness Levels, specifications, TEMP, technical baselines, standards, materiel readiness)
- Management (e.g., organization, staffing levels, personnel qualifications/experience, funding, management processes, planning, documentation, logistics)

4.5. Schedule (S) Considerations

Is there an impact to schedule performance and to what level? If the risk does not have a first order performance impact, then ask this question. If the risk does impact the critical path, then it impacts both schedule and cost, but should be carried as a schedule risk.

Were any problems that caused schedule slips identified as risks prior to their occurrence? If not, why not? If yes, why didn't the associated mitigation plan succeed? The IPTs should analyze impact of the risk to the IMS and the critical path(s), to include:

- Evaluating baseline schedule inputs (durations and network logic);
- Incorporating technical assessment and schedule uncertainty inputs to the program schedule model;
- Evaluating impacts to program schedule based on technical team assessment;
- Performing schedule analysis on the program IMS, incorporating the potential impact from all contract schedules and associated government activities;
- Quantifying schedule excursions reflecting the effects of cost risks, including resource constraints;

- Providing a government schedule assessment for cost analysis and fiscal year planning, reflecting the technical foundation, activity definition, and inputs from technical and cost areas; and
- Documenting the schedule basis and risk impacts for the risk assessment.
- Projecting an independent forecast of the planned completion dates for major milestones.

4.6. Cost (C) Considerations

Does the risk only impact life-cycle cost? If so, with no performance or schedule impacts, the risk is a cost risk, and may impact estimates and assessments such as:

- Building on technical and schedule assessment results;
- Translating performance and schedule risks into life-cycle cost;
- Deriving life-cycle cost estimates by integrating technical assessment and schedule risk impacts on resources;
- Establishing budgetary requirements consistent with fiscal year planning;
- Determining if the adequacy and phasing of funding supports the technical and acquisition approaches;
- Providing program life-cycle cost excursions from near-term budget execution impacts and external budget changes and constraints; and
- Documenting the cost basis and risk impacts.

NOTE: Cost and funding are not the same. Cost is related to the amount of money required to acquire and sustain a commodity, and funding is the amount of money available to acquire and sustain that commodity.

4.7. Risk Analysis Illustration

The following example illustrates what has been presented in this section with the critical card example used earlier:

The program office has identified a risk in conducting a developmental test.

- The first question to ask is why the test might not be able to be conducted. The answer is that the circuit cards for one component may not be available. In asking the question "why" a second time, the answer is that power conversion circuit cards for one component may not be available in time for system integration to meet the test schedule. The risk causal factor is this availability of power conversion circuit cards. (Alternately, if the power conversion circuit card is no longer in production, then you have a completely different risk that will require a different mitigation plan.) Thus, this is a schedule risk.
- The next question to ask is whether this test is on the critical path or near the critical path. Again, the answer is determined to be "no" because the test has some schedule risk mitigating slack. Therefore the consequence is minimal since it will not likely impact a major milestone. Thus, this risk is reported as shown in Figure 6.

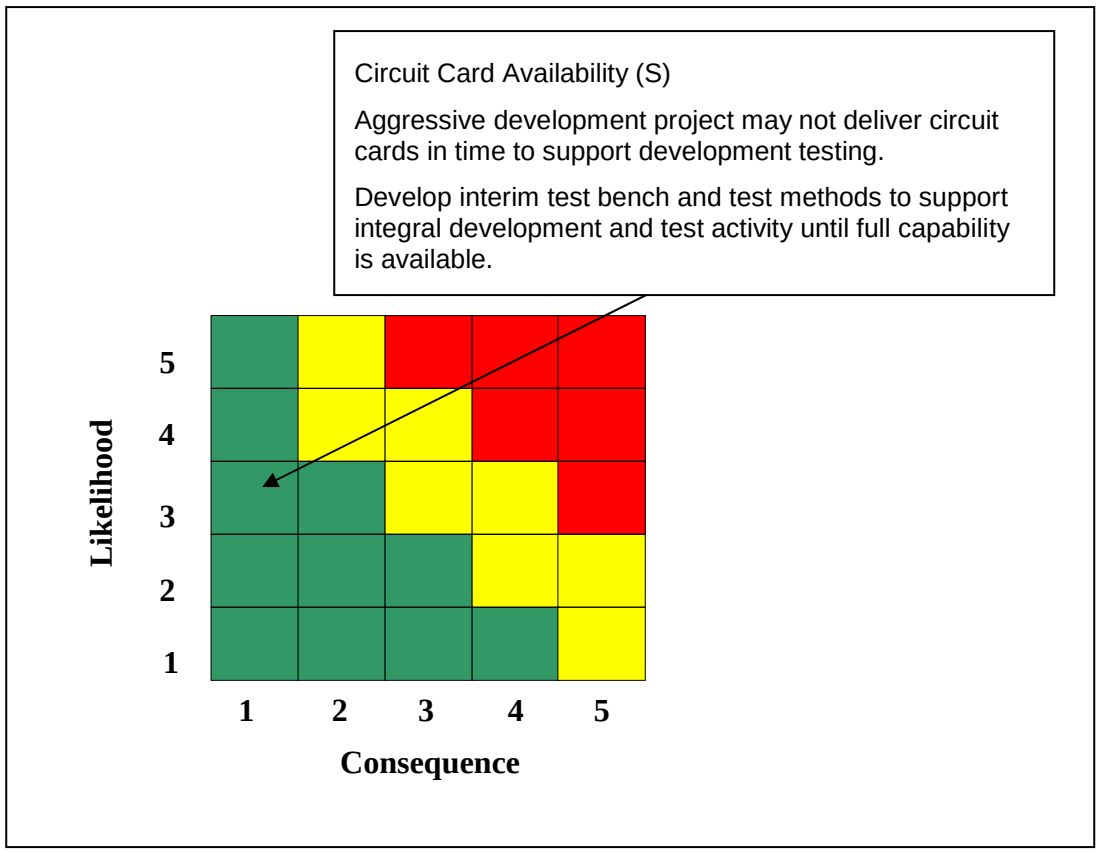

Figure 6. An Example of Risk Reporting

5. Key Activity - Risk Mitigation Planning

5.1. Purpose

The intent of risk mitigation planning is to answer the question *"What is the program approach for addressing this potential unfavorable consequence?"* One or more of these mitigation options may apply:

- Avoiding risk by eliminating the root cause and/or the consequence,
- Controlling the cause or consequence,
- Transferring the risk, and/or
- Assuming the level of risk and continuing on the current program plan.

Risk mitigation planning is the activity that identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. Risk mitigation planning is intended to enable program success. It includes the specifics of **what** should be done, **when** it should be accomplished, **who** is responsible, and the **funding** required to implement the risk mitigation plan. The most appropriate program approach is selected from the mitigation options listed above and documented in a risk mitigation plan.

The level of detail depends on the program life-cycle phase and the nature of the need to be addressed. However, there must be enough detail to allow a general estimate of the effort required and technological capabilities needed based on system complexity.

5.2. Tasks

For each root cause or risk, the type of mitigation must be determined and the details of the mitigation described.

Once alternatives have been analyzed, the selected mitigation option should be incorporated into program planning, either into existing program plans or documented separately as a risk mitigation plan (not to be confused with the risk management plan). The risk mitigation plan needs to be realistic, achievable, measurable, and documented and address the following topics:

- A descriptive title for the identified risk;
- The date of the plan;
- The point of contact responsible for controlling the identified root cause;
- A short description of the risk (including a summary of the performance, schedule, and resource impacts, likelihood of occurrence, consequence, whether the risk is within the control of the program);
- Why the risk exists (root causes leading to the risk);
- The options for mitigation (possible alternatives to alleviate the risk);
- Definition of events and activities intended to reduce the risk, success criteria for each plan event, and subsequent "risk level if successful" values;
- Risk status (discuss briefly);
- The fallback approach (describe the approach and expected decision date for considering implementation);
- A management recommendation (whether budget or time is to be allocated, and whether or not the risk mitigation is incorporated in the estimate at completion or in other program plans);

- Appropriate approval levels (IPT leader, higher-level Product Manager, Systems Engineer, PM); and
- Identified resource needs.

6. Key Activity - Risk Mitigation Plan Implementation

6.1. Purpose

The intent of risk mitigation (plan) execution is to ensure successful risk mitigation occurs. It answers the question *"How can the planned risk mitigation be implemented?"* It:

- Determines what planning, budget, and requirements and contractual changes are needed,
- Provides a coordination vehicle with management and other stakeholders,
- Directs the teams to execute the defined and approved risk mitigation plans,
- Outlines the risk reporting requirements for on-going monitoring, and
- Documents the change history.

6.2. Tasks

Risk assessment (identification and analysis) is accomplished by risk category. Each risk category (e.g., performance, schedule, and cost) includes a core set of assessment tasks and is related to the other two categories. These interrelationships require supportive analysis among areas to ensure the integration of the assessment. Implementing risk mitigation should also be accomplished by risk category, and it is important for this process to be worked through the IPT structure, requiring the IPTs at each WBS level to scrub and endorse the risk mitigations of lower levels. It is important to mitigate risk where possible before passing it up to the next WBS level. In addition, each IPT must communicate potential cost or schedule growth to all levels of management. It is imperative that the Systems Engineer and PM understand and approve the mitigation plan and examine the plan in terms of secondary, unforeseen impacts to other elements of the program outside of the risk owning IPT. As part of this effort, the IPTs should ensure effective mitigation plans are implemented and ongoing results of the risk management process are formally documented and briefed, as appropriate, during program and technical reviews.

When determining that it may be appropriate to lower the consequence of a risk, careful consideration should be given to the justification for doing so, including identifying exactly what about the risk has changed between the time of the original consequence assessment and the current risk state to justify such a reassessment.

7. Key Activity - Risk Tracking

7.1. Purpose

The intent of risk tracking is to ensure successful risk mitigation. It answers the question *"How are things going?"* by:

- Communicating risks to all affected stakeholders,
- Monitoring risk mitigation plans,
- Reviewing regular status updates,
- Displaying risk management dynamics by tracking risk status within the Risk Reporting Matrix (see Section 4.2), and
- Alerting management as to when risk mitigation plans should be implemented or adjusted.

Risk tracking activities are integral to good program management. At a top level, periodic program management reviews and technical reviews provide much of the information used to identify any performance, schedule, readiness, and cost barriers to meeting program objectives and milestones.

Risk tracking documents may include: program metrics, technical reports, earned value reports, watch lists, schedule performance reports, technical review minutes/reports, and critical risk processes reports.

An event's likelihood and consequences may change as the acquisition process proceeds and updated information becomes available. Therefore, throughout the program, a program office should reevaluate known risks on a periodic basis and examine the program for new root causes. Successful risk management programs include timely, specific reporting procedures tied to effective communication among the program team.

7.2. Tasks

Risk tracking is the activity of systematically tracking and evaluating the performance of risk mitigation actions against established metrics throughout the acquisition process. It feeds information back into the other risk activities of identification, analysis, mitigation planning, and mitigation plan implementation as shown in Figure 1.

The key to the tracking activity is to establish a management indicator system over the entire program. The PM uses this indicator system to evaluate the status of the program throughout the life cycle. It should be designed to provide early warning when the likelihood of occurrence or the severity of consequence exceeds pre-established thresholds/limits or is trending toward exceeding pre-set thresholds/limits so timely management actions to mitigate these problems can be taken.

The program office should re-examine risk assessments and risk mitigation approaches concurrently. As the system design matures, more information becomes available to assess the degree of risk inherent in the effort. If the risk changes significantly, the risk mitigation approaches should be adjusted accordingly. If the risks are found to be lower than previously assessed, then specific risk mitigation actions may be reduced or canceled and the funds reprogrammed for other uses. If they are higher, or new root causes are found, appropriate risk mitigation efforts should be implemented.

In addition to reassessing (identifying and analyzing) risks, the program office should look for new risk mitigation options. Alternative technologies may mature, new products may become available in the market place, or may be information found in unexpected places. All of these may be of use to the program office for risk mitigation. A periodic review of developments in the laboratory, and the market place is time well invested for any program.

7.3. Reporting & Documentation

The purpose of risk reporting is to ensure management receives all necessary information to make timely and effective decisions. This allows for coordination of actions by the risk team, allocation of resources, and a consistent, disciplined approach. A primary goal of risk reporting should be to provide the PM with an effective early warning of developing risk.

Risk documentation is the recording, maintaining, and reporting of identifications, analyses, mitigation planning and implementation, and tracking results. Risk tracking should be done as part of technical reviews, risk review board meetings, or periodic program reviews. Documentation includes all plans and reports for the PM and decision authorities and reporting forms that may be internal to the program office. This is consolidated in the Risk Mitigation Plan.

Risk reporting should present standard likelihood and consequence screening criteria, as well as the Risk Reporting Matrix presented in Section 4.2. The details regarding consequences for cost, schedule, and performance should be documented in each Risk Mitigation Plan. The plotted position on the risk reporting matrix should show the PM's current assessment of the risk's likelihood and the estimated severity of its effect on the program if mitigation fails. As risk mitigation succeeds in a program, a yellow or red risk's position on the Risk Reporting Matrix will migrate in successive assessments from its current location toward the green. Each risk description should include three key elements (Figure 6 provides an example):

- A brief description, including both the title and type (P, S or C), of the risk,
- A brief description of the risk root causal factor(s), and
- The planned mitigations, along with critical dates (risk reduction milestones), that address the root cause(s) and effect(s).

8. Planning / Preparation for Risk Management

Risk management is a key element of a PM's executive decision-making. DoD risk management is based on the principles that risk management must be forward-looking, structured, continuous, and informative. The key to successful risk management is early planning, resourcing, and aggressive execution.

Good planning enables an organized, comprehensive, and iterative approach for managing root causes. Networking within government and industry to extract the best ideas, techniques, methods, and information can only help teams seeking to improve their implementation of risk management.

8.1. Risk Planning

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

Risk planning is the detailed formulation of a program of action for the management of root causes. Risk planning, and the resultant plan, should answer the questions: "who, what, where, when, and how." It is the activity to:

- Ensure the principles of this guide are applied to the program;
- Develop and document an organized, comprehensive, and interactive risk management plan;
- Determine the methods to be used to execute a PM's Risk Management Plan (RMP); and
- Plan for adequate resources, including personnel.

Risk planning is iterative, and includes describing and scheduling the tasks for risk identification, risk analysis, risk mitigation planning, resourcing, risk mitigation plan implementation, and risk tracking throughout a program's life cycle. Since contractor abilities to develop and manufacture the system affect program risks, the contractor should be considered a valuable partner in risk planning. The result is the RMP.

8.2. Risk Management Plan

The program office should establish the basic approach and working structure it will use and document that approach it in a RMP. A comprehensive and consistent approach ensures all aspects of the program are examined for risk. The RMP is integral to overall program planning and the program IMP, and/or the SEP, or it may be a stand-alone document, as long as the activities are integrated and consistent.

Planning begins by developing and documenting a risk management strategy. Early efforts establish the purpose and objective, assign responsibilities for specific areas, identify additional technical expertise needed, describe the assessment process and areas to consider, delineate considerations for mitigation planning, define a rating scheme, dictate the reporting and documentation needs, and establish report requirements. This planning should also address evaluation of the capabilities of potential sources as well as early industry involvement. The PM's strategy to manage root causes provides the program team with direction and a basis for planning.

Risk planning consists of the upfront activities needed for a successful risk management program. At the end of each acquisition phase, risk planning is the heart of the preparation for the next phase. Initially formalized during Concept Refinement or other first-phase planning, and updated for each subsequent acquisition phase in all increments of the program, the risk management process should be reflected in the program SEP and in the technology development, acquisition, and support strategies.

These strategies, along with requirement and threat documents, and system and program characteristics, are sources of information for the program office to use in developing the RMP. The RMP tells the government and contractor team how to get from where the program is today to where the PM wants it to be in the future. The key to writing a good plan is to provide the necessary information so the program team knows the goals, objectives, and the program office's risk management process. Although the plan may be specific in some areas, such as the assignment of responsibilities for government and contractor participants and definitions, it may be general in other areas to allow users to choose the most efficient way to proceed. For example, a description of techniques that suggests several methods for evaluators to use to assess risk is appropriate, since every technique may have advantages and disadvantages depending on the situation.

As a program transitions through developmental and operational testing, and then to the end users during sustainment, a program RMP should be structured to identify, assess, and mitigate risks that have a impact on overall program life-cycle cost, schedule, and/or performance. The RMP should also define the overall program approach to capture and manage root causes. Risks that are safety related are outside the scope of this guide and are managed in accordance with MIL-STD-882D as the PM directs.

An example RMP format summary may include:

- Introduction
- Program Summary
- Risk Management Strategy and Process
- Responsible/Executing Organization
- Risk Management Process and Procedures
- Risk Identification
- Risk Analysis
- Risk Mitigation Planning
- Risk Mitigation Implementation
- Risk Tracking

Normally, documentation and reporting procedures are defined as part of the risk management process planning before contract award, but they may be added or modified during contract execution as long as the efforts remain within the scope of the contract or are approved as part of a contract change.

The program office should periodically review the RMP and revise it, if necessary. Events such as these may drive the need to update an existing RMP:

- A change in acquisition strategy,
- Preparation for a milestone decision,
- Results and findings from event–based technical reviews,

- An update of other program plans,
- Preparation for a Program Objective Memorandum submission, or
- A change in support strategy.

8.3. Organizing for Risk Management

In systems engineering, risk management examines all aspects of the program phases as they relate to each other, from conception to disposal. This risk management process integrates design (performance) requirements with other life-cycle issues such as manufacturing, operations, and support.

The PM should establish a risk management process that includes not only risk planning, but risk identification, risk analysis, risk mitigation planning, resourcing, risk mitigation plan implementation, and risk tracking to be integrated and continuously applied throughout the program, including during the design process.

Risk assessment includes identification and analysis of sources of root causes to include performance, schedule, and cost, and is based on such factors as the technology being used and its relationship to design; manufacturing capabilities; potential industry sources; and test and support processes.

In a decentralized program office risk management organization, the program's risk management coordinator may be responsible for risk management planning, and IPTs typically perform the risk assessments. In a centralized program office risk management organization, the program's risk management coordinator may be responsible for risk management planning and perform the risk assessments. In either case, if necessary, the team may be augmented by people from other program areas or outside experts. Section 8.5 elaborates on this for each of the described assessment approaches. Typically, a program-level IPT may conduct a quick-look assessment of the program to identify the need for technical experts (who are not part of the team) and to examine areas that appear most likely to contain risk.

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

8.4. Risk Management Boards

A risk management tool used on many programs is the Risk Management Board (RMB). This board is chartered as the senior program group that evaluates all program risks and their root causes, unfavorable event indications, and planned risk mitigations. In concept, it acts similar to a configuration control board. It is an advisory board to the PM and provides a forum for all

affected parties to discuss their concerns. RMBs can be structured in a variety of ways, but share the following characteristics:

- They should be formally chartered by the PM and have a defined area of responsibility and authority. Note that RMBs may be organized as program office only, program office with other Government offices (such as PEO Systems Engineer, User, Defense Contract Management Agency, test organizations, SMEs), or as combined government-contractor-subcontractor. The structure should be adapted to each program office's needs.
- Working relationships between the board and the program office staff functional support team should be defined.
- The process flow for the RMB should be defined.
- The frequency of the RMB meetings should be often enough to provide a thorough and timely understanding of the risk status, but not too frequent to interfere with the execution of the program plan. Frequency may depend on the phase of the program; e.g., a development program may require monthly RMBs, while a production or support program may hold quarterly RMBs.
- Interfaces with other program office management elements (such as the various working groups and the configuration control board) should be formally defined.

On programs with many significant root causes, the RMB provides an effective vehicle to ensure each root cause is properly and completely addressed during the program life cycle. It is important to remember that successful risk tracking is dependent on the emphasis it receives during the planning process. Further, successful program execution requires the continual tracking of the effectiveness of the risk mitigation plans.

The program management team can assign the risk management responsibility to individual IPTs or to a separate risk management team. In addition, the program office should establish the working structure for risk identification and risk analysis and appoint experienced Government and industry personnel as well as outside help from SMEs, as appropriate.

8.5. Risk Assessment Approaches

For each risk assessment, the program office team must establish how the actual assessment (root cause identification and risk analysis) will be conducted. At least four choices are available:

- Conduct the assessment as part of the normal IPT activity of the program office;
- Establish a program office risk assessment team, as either a temporary ad-hoc team or a permanent organization;
- Establish a Government-industry team; or
- Request an outside team or combined program office-outside team conduct the assessment.

Each approach has its own merits and costs. However, the choices are not mutually exclusive. Program offices could use two or more of these options in combination or for different aspects of the program. An internal effort should always be conducted so that program office personnel are familiar with the risks.

Teams outside the program office may be appropriate if the resources needed to do the assessment are beyond those available from within the program team. First, establish a core risk assessment team if the program team is not already following a disciplined program acquisition process which incorporates risk assessment activities. This team is the core group of individuals who will

conduct the risk assessment and normally includes individuals with expertise in systems engineering, logistics, manufacturing, test, schedule analysis, and cost estimating.

Regardless of the method(s) chosen, the contractor team's input should be solicited and included in the final assessment. If the program is not already on contract, the risk assessment team should also try to gain insight from industry, within the bounds of competitive nondisclosure and protection of proprietary data.

8.6. Risk Management Roles

The following responsibilities are recommended relative to the program risk management process.

8.6.1. Program Executive Officers / Milestone Decision Authorities

- Ensure program acquisition plans and strategies provide for risk management, and that identified risks and their root causes are considered in milestone decisions.
- In conjunction with the program contracting officer, ensure program contract(s) Statement of Objectives, Statements of Work, and Contract Deliverable Requirements Lists include provisions to support a defined program risk management plan and process.
- Periodically review program-level risks.

8.6.2. Program Managers

- Establish, use, and maintain an integrated risk management process. PMs should ensure their integrated risk management process includes all disciplines required to support the life cycle of their system (e.g., systems safety, logistics, systems engineering, producibility, in-service support, contracts, test, earned value management, finance). If the contract is required to comply with ANSI/EIA-748, Earned Value Management Systems, risk management should be an integral part of the Contract Performance Report (CPR) and the associated IMS.
- Develop and maintain a program IMS that incorporates contractor schedules and external Government activities in a single, integrated schedule. Project independent estimates of completion dates for major milestones and assess the probability of maintaining the baseline schedule. Conduct schedule risk analysis as needed and determine the potential impact to the program estimate and approved funding. Review the contractor's schedule risk analysis. Analyze the contractor's monthly IMS submissions, and monitor contractor progress against risk mitigation activities.
- Jointly conduct IBRs with the contractor team to reach mutual understanding of risks inherent in the contractor's baseline plans. Conduct IBRs as necessary throughout the life of the program. The ***Program Managers' Guide to the Integrated Baseline Review Process*** provides details on conducting effective IBRs.
- Analyze earned value information contained in the CPR for identification of emerging risk items or worsening performance trends for known risk items. Assess realism of contractor's projected estimate at completion and adequacy of corrective action plans.

- Synthesize and correlate the status of new and ongoing risk elements in the IMS, CPR, risk mitigation plans, technical status documentation, program status reviews, and other sources of program status.
- Establish a realistic schedule and funding baseline for the program as early as possible in the program, incorporating not only an acceptable level of risk, but adequate schedule and funding margins. Protect the program by budgeting to a conservative estimate with a high probability.
- Ensure the program has a defined RMP, and that risk assessments are conducted per that plan. Ensure the program RMP defines the required relationships with other risk related directives.
- Form a program RMB to include the PM/IPT Leader, Program Risk Management Coordinator, Chief or Lead Systems Engineer, program logistician, budget and financial manager, Prime Contractor PM/Lead Systems Engineer, and other members relevant to the program strategy, phase, and risks.
- Approve appropriate risk mitigation strategies. Include operational users and other stakeholders in the formulation and acceptance of risk mitigation plans.
- Assign responsibility for risk mitigation activities and monitor progress through a formal tracking system.
- Report program risks to appropriate Program Executive Officer (PEO)/PM/Systems Commanders and user personnel prior to Milestone decisions, following significant risk changes, or as requested. Use the Risk Reporting Matrix (see Section 4.2) documented in the program RMP to report program risks.

8.6.3. Integrated Product Team

- Document and implement the RMP, and support the program RMB as required.
- Assess (identify and analyze) risks and their root causes using documented risk assessment criteria. An ongoing/continual risk assessment is highly recommended, and is useful during all phases of a program's life cycle. A tailored program risk assessment should be conducted for each of the applicable technical reviews and for each key program decision point.
- Report risks using the Risk Reporting Matrix documented in the program RMP to report program risks to appropriate PEO/PM/Systems Commander and user personnel.
- Recommend appropriate risk mitigation strategies for each identified root cause, and estimate funding requirements to implement risk mitigation plans. Be prepared to provide required risk mitigation support.
- Implement and obtain user acceptance of risk mitigation in accordance with program guidance from the RMB per the program RMP.

8.6.4. Risk Management Boards

- Evaluate program risk assessments in accordance with the RMP.
- Evaluate and continually assess the program for new root causes, address the status of existing risks, and manage risk mitigation activities. The root causes to be identified and analyzed are those that jeopardize the achievement of significant

program requirements, thresholds, or objectives. Like IPT composition, the RMB is made up of Government program management, industry/contractor, and appropriate Government support personnel.

- Evaluate and prioritize program risks and appropriate risk mitigation strategies for each identified root cause, and estimate funding requirements to implement risk mitigation plans. Be prepared to request required risk mitigation support. Implement and obtain user acceptance of risk mitigation in accordance with program guidance per the program RMP.
- Report risk information, metrics, and trends, using the standard likelihood and consequence matrix format, to appropriate PEO/PM/Systems Commander and user personnel.

8.6.5. Support Activities

- Provide the people, processes, and training to support program risk management activities.
- Designate SMEs and make them available to assist with risk assessments. Upon request of PMs or higher authority, Government support activities should provide personnel to conduct independent risk assessments on specific programs.

8.6.6. Contractor

- Develop an internal risk management program and work jointly with the government program office to develop an overall risk management program.
- Conduct risk identification and analysis during all phases of the program, including proposal development. Develop appropriate risk mitigation strategies and plans.
- Assess impacts of risk during proposal and baseline development. Use projected consequences of high probability risks to help establish the level of management reserve and schedule reserve.
- Jointly conduct IBRs with the Government team to reach mutual understanding of risks inherent in the program baseline plans.
- Conduct schedule risk analyses at key points during all phases of the program, including proposal development.
- Incorporate risk mitigation activities into IMS and program budgets as appropriate.
- Use IMS and EVM information (trends and metrics) to monitor and track newly identified risks and monitor progress against risk plans. Identify new risk items, and report status against risk mitigation plans to company management and the Government program office.
- Assess impact of identified performance, schedule and costs risks to estimate at completion, and include in the estimate as appropriate. Develop a range of estimates (best case, most likely, worst case).
- Synthesize and correlate the status of new and ongoing risk elements in the IMS, CPR, risk mitigation plans, technical status documentation, program status reviews, and other sources of program status.
- Assign responsibility for risk mitigation activities, and monitor progress through a formal tracking system.

- Once risks have been realized (100% probability) and turn into an issue, incorporate the issue into work planning documents, IMS, and earned value budgets, and ensure integration with ongoing work to minimize impacts.

8.7. Training

Getting the program team organized and trained to follow a disciplined, repeatable process for conducting a risk assessment (identification and analysis) is critical, since periodic assessments are needed to support major program decisions during the program life cycle. Experienced teams do not necessarily have to be extensively trained each time an assessment is performed, but a quick review of lessons learned from earlier assessments, combined with abbreviated versions of these suggested steps, could avoid false starts.

The program's risk coordinator, or an outside expert, may train the IPTs, focusing on the program's RMP, risk strategy, definitions, suggested techniques, documentation, and reporting requirements.

A risk assessment training package for the full team (core team plus SMEs) is often very beneficial. This package typically includes the risk assessment process, analysis criteria, documentation requirements, team ground rules, and a program overview. Train the full team together in an integrated manner and the use of a facilitator may be useful.

Appendix A. Applicable References

AT&L Knowledge Sharing System (AKSS) (http://deskbook.dau.mil/jsp/default.jsp)
CIRCULAR NO. A–11 ,PART 7, PLANNING, BUDGETING, ACQUISITION, AND MANAGEMENT OF CAPITAL ASSETS (*http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf*
Continuous Risk Management Guidebook *(http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html)*
Defense Acquisition Guidebook (http://akss.dau.mil/dag/)
Defense Acquisition University Continuous Learning Modules (https://learn.dau.mil/html/clc/Clc.jsp)
DoD 4245.7-M, *Transition from Development to Production* (http://www.dtic.mil/whs/directives/corres/html/42457m.htm)
DoD 5200.1-M, *Acquisition Systems Protection Program* (http://www.dtic.mil/whs/directives/corres/pdf/52001m_0394/p52001m.pdf)
DoDD 5200.1, *DoD Information Security Program* (http://www.dtic.mil/whs/directives/corres/pdf/d52001_121396/d52001p.pdf)
DoDD 5200.39, *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection* (http://www.dtic.mil/whs/directives/corres/pdf/d520039_091097/d520039p.pdf)
DoD Earned Value Management (http://www.acq.osd.mil/pm/)
DoD Earned Value Management Implementation Guide (EVMIG) (http://guidebook.dcma.mil/79/guidebook_process.htm)
MIL STD 882D, Standard Practice for System Safety (https://acc.dau.mil/CommunityBrowser.aspx?id=30309)
MIL-HDBK-881 Work Breakdown Structure Handbook (http://www.acq.osd.mil/pm/currentpolicy/wbs/MIL_HDBK-881A/MILHDBK881A/WebHelp3/MILHDBK881A.htm)
Program Managers' Guide to the Integrated Baseline Review Process (http://www.acq.osd.mil/pm/currentpolicy/IBR_Guide_April_2003.doc)
Risk Management Community of Practice (https://acc.dau.mil/CommunityBrowser.aspx?id=17607)

Appendix B. Acronyms

AKSS	AT&L Knowledge Sharing System
APB	Acquisition Program Baseline
C	Cost
CDD	Capability Development Document
COTS	Commercial-off-the-shelf
CPD	Capability Production Document
CPR	Contract Performance Report
DAG	Defense Acquisition Guidebook
DAU	Defense Acquisition University
DoD	Department of Defense
ESOH	Environment, Safety, and Occupational Health
EVM	Earned Value Management
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IPT	Integrated Product Team
KPP	Key Performance Parameter
LCC	Life-Cycle Cost
LCCE	Life-Cycle Cost Estimate
M&S	Modeling and Simulation
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OUSD(AT&L)	Office of the Undersecretary of Defense for Acquisition, Technology and Logistics
P	Performance
PEO	Program Executive Office or Program Executive Officer
PM	Program Manager
RFP	Request for Proposal
RMB	Risk Management Board
RMP	Risk Management Plan

S	Schedule
SEP	Systems Engineering Plan
SME	Subject Matter Expert
SRA	Schedule Risk Assessment
TEMP	Test and Evaluation Master Plan
TPM	Technical Performance Measure
WBS	Work Breakdown Structure

Appendix C. Definitions

Consequence: The outcome of a future occurrence expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain.

Future Root Cause: The reason, which, if eliminated or corrected, would prevent a potential consequence from occurring. It is the most basic reason for the presence of a risk.

Issue: A problem or consequence which has occurred due to the realization of a root cause. A current issue was likely a risk in the past that was ignored or not successfully mitigated.

Risk: A measure of future uncertainties in achieving program performance goals within defined cost and schedule constraints. It has three components: a future root cause, a likelihood assessed at the present time of that future root cause occurring, and the consequence of that future occurrence.

Risk Analysis: The activity of examining each identified risk to refine the description of the risk, isolate the cause, and determine the effects and aiding in setting risk mitigation priorities. It refines each risk in terms of its likelihood, its consequence, and its relationship to other risk areas or processes.

Risk Identification: The activity that examines each element of the program to identify associated future root causes, begin their documentation, and set the stage for their successful management. Risk identification begins as early as possible in successful programs and continues throughout the life of the program.

Risk Management: An overarching process that encompasses identification, analysis, mitigation planning, mitigation plan implementation, and tracking of future root causes and their consequence.

Risk Management Planning: The activity of developing and documenting an organized, comprehensive, and interactive strategy and methods for identifying and tracking future root causes, developing risk-mitigation plans, performing continuous risk assessments to determine how risks and their root causes have changed, and assigning adequate resources.

Risk Mitigation Plan Implementation: The activity of executing the risk mitigation plan to ensure successful risk mitigation occurs. It determines what planning, budget, and requirements and contractual changes are needed, provides a coordination vehicle with management and other stakeholders, directs the teams to execute the defined and approved risk mitigation plans, outlines the risk reporting requirements for on-going monitoring, and documents the change history.

Risk Mitigation Planning: The activity that identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. It includes the specifics of what should be done, when it should be accomplished, who is responsible, and the funding required to implement the risk mitigation plan.

Risk Tracking: The activity of systematically tracking and evaluating the performance of risk mitigation actions against established metrics throughout the acquisition process and develops further risk mitigation options or executes risk mitigation plans, as appropriate. It feeds

information back into the other risk management activities of identification, analysis, mitigation planning, and mitigation plan implementation.