Space and Missile Systems Center Risk Management Process Guide

Version 2.0 – 5 September 2014

DISTRIBUTION STATEMENT A: Approved for public release; distribution unlimited.

(This page intentionally left blank)

APPROVAL PAGE

Use of the Space and Missile Systems Center (SMC) Risk Management Process Guide is approved for SMC.

THOMAS A. FITZGERALD, SES, DAF
Director, Engineering

5 SEPT 2014
Date

Document Change Record

Version #	Changes	Date
1.0	Initial Risk Management Process Guide document	7 Dec 11
2.0	Document revised per 2014 AFI 63-101/20-101, 2014 AFPAM 63-128, 2012 MIL-STD-882E, and associated SMC tailoring documents. Additional information and updates are also included.	5 Sept 14

For additional information and comments, please contact the document author, Mr. Edmund Conrow, SMC/EN.

Table of Contents

Table of Contents, Continued

1.0 Introduction

Risk management is a key process that can help program personnel to better manage their programs. Effective risk management can assist in better applying scarce resources across a program; help balance cost, performance, schedule, and associated risk; and provide inputs for managing the program on a day-to-day basis. However, risk management is often poorly performed, and ineffective risk management will contribute to program inefficiency or problems, and in the worst case program failure [1] [2].[1]

This document provides guidance to Air Force and support contractor personnel for developing and implementing an effective risk management process on Air Force Space and Missile Systems Center (SMC) programs that is compatible with Air Force requirements and Air Force and DoD guidance.[2] [3] [4] [5] It is not an all-inclusive risk management source but a summary of essential concepts and approaches to assist in developing and implementing the risk management process. Specific organizational implementation characteristics for individual programs, as well as at the Directorate (enterprise) level, such as roles and responsibilities, the number of risk management boards, etc. are not addressed in this guidance document but should exist within the program's risk management plan (RMP) and the Directorate's (enterprise) RMP, Operating Instruction (OI), or equivalent.

Behavioral aspects of risk management implementation are also not addressed in this guidance document. However, together with organizational aspects mentioned above, they are equally

---

[1] For example, "Risk management is *performed* on most programs, but we found that it is mainly for show. Risks are not communicated and the identified risks frequently do not influence program decision making." [1] Of 49 entries involving risk management in a business acquisition lessons learned database, 43 of the cases (88 percent) "described problems with risk management during the business acquisition process as a contributor to program execution problems" [2].

[2] See SMC T-005, "Tailoring of Risk Management Requirements in SMC-S-001 (2013)," [3], 27 January 2014 or more recent for the "Government's requirements and expectations for contractor performance in defense systems acquisition and technology developments" associated with risk management. The material contained in SMC-T-005 will be incorporated into the next edition of SMC-S-001.

[3] Portions of this guidance document may also be helpful to program contractors. However, some material (e.g., the risk analysis scales given in Section 4.1) are potentially unique to the Air Force and their support contractors.

[4] Operational risk management (ORM) is not discussed in this Risk Management Process Guide document. While ORM and life cycle (acquisition) risk management (LCRM) are based on the same general principles, the key elements of LCRM… have been tailored specifically for life cycle management programs. When a system is fielded, some of the program's LCRM risk information may be useful to the risk identification efforts of operators and maintainers. Similarly, operator and maintainer risk management activities can identify risks that should be integrated into the program's LCRM efforts. [4] (pg. 88) For additional information on ORM, see references [5] and [6].

[5] While risk management information is contained in the program Systems Engineering Plan (SEP), this information is typically a highly condensed summary of the Risk Management Plan which is not sufficient to fully describe either the risk management process or its implementation on a given program. On some smaller programs and projects the Risk Management Plan may correspond to the equivalent section in the SEP, Project Management Plan, etc. However, for large-scale programs, a separate Risk Management Plan or Operating Instruction, or equivalent document should exist.

important with process quality in determining a program's overall risk management effectiveness. Simply stated, a suitable risk management process that is poorly implemented will not contribute to program success, but rather lead to program inefficiency and/or problems. Risk management needs both top-down (including the program manager) and bottom-up (from working-level engineers) to be successful. Failure to have program personnel properly engaged in performing risk management may lead to information and charts being generated but not being used as an input to program decision making. [7] (Chapter 3)

Discussions of residual mission assurance risk (e.g., go/no-go preceding launch), residual risk acceptance criteria and authority, and Environment, Safety, and Occupational Health (ESOH) risks are not included in this Risk Management Process Guide . See current Air Force SMC/EN, SMC/Independent Readiness Review Team, SMC/SE, MIL-STD-882C [8], MIL-STD-882D [9], MIL-STD-882E [10], SMC-T-004 [11], SMC Instruction 63-1205 [12] , and Aerospace Corporation President's Review guidance relative to dealing with these types of risks.

1.1 Risk and Risk Management

"A risk is a future event that, if it occurs, may cause a negative outcome or an execution failure in a program within defined performance, schedule, and cost constraints." [4] (pg. 84). Risk can be associated with all aspects of a program (e.g., cost, design maturation, environment, hardware, integration, human interface, schedule, software, supplier capability, technology maturity, threat) as these aspects relate across the work breakdown structure and Integrated Master Schedule (IMS). [13] (pg. 1), [14] , (pg. 5) "Risk addresses the potential variation in the planned approach and its expected outcome." [13] (pg. 1)

A risk can be differentiated from an issue and problem by the following [15]:[6] [7]

---

[6] This material also appears in reference [16] (pp. 873-875) and other sources.

[7] Opportunities and opportunity management are not discussed in this SMC Risk Management Guide, nor in key Air Force documents associated with risk management. All programs and their personnel are encouraged to consider and examine potential opportunities. However, there is typically a finite pool of resources available to allocate for risks and opportunities. Resolving risks is essential to prevent program failure, while opportunities are typically benefits not essential to prevent program failure nor ensure program success. Furthermore, in the probability, consequence, and time-frame framework there is no universal definition for an opportunity, namely: while the probability is > 0, the upper boundary point associated with probability = 1 is ambiguous as there is no clear analog to an issue or problem. There is also a broad range of potential consequence outcomes from negative to less negative to positive (and even better than expected). Finally there is no boundary for time-frame associated with opportunities (e.g., past, present, future) as there is with risks [15] [16] (pp. 873-875). Opportunities are also not the dual, mirror, or mirror image of risks as shown by Kahneman and Tversky [17]. (Daniel Kahneman was awarded the 2002 Nobel Memorial Prize in Economics for this work. His partner, Amos Tversky, was deceased by that time.) The potential benefit of an opportunity is often overstated. More formally, "the positive utility magnitude of improving an expected outcome is considerably less than the negative utility magnitude of failing to meet an expected outcome." [18] While opportunity management is a "useful approach during program definition when a wide range of alternative solutions are being investigated," …"once a program enters into development, its value is generally overstated and is more limited than claimed" [19]. Finally, all candidate opportunities should be thoroughly screened for potential risks, This is rarely stated or considered, yet unanticipated outcomes associated with opportunities all too often lead to risks and problems that were not previously considered [19].

- Risk: 0 < probability < 1, consequence < 0, time-frame in the future
- Issue: probability = 1, , consequence < 0, time-frame in the future[8]
- Problem: probability = 1, , consequence < 0, time-frame is now

A concern is a potential future event for which the cross-functional life cycle risk management (LCRM) team does not have sufficient information to quantify a likelihood or consequence. An example of a concern is “Congress may not fund the full program, and the amount of funding is unclear.” “A concern should be periodically monitored and reevaluated for likelihood and/or consequence.” Once likelihood and consequence can be quantified by the team, a concern may become a risk [4] (pp. 84-85).

While the focus of the risk management process provided in this guidance document is on risks, the process can also be used, with some tailoring associated with time-frame considerations, to address issues and problems.

Risk management is the overarching process that includes the following process steps: planning for risk management (risk management planning), risk identification, risk analysis, risk handling planning and implementation, and risk tracking (monitoring). 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 identification and consequence management.

Risk management is critical to acquisition program success. Addressing risk on programs “helps ensure that program cost, schedule, and performance objectives are achieved at every stage in the life cycle and communicates to stakeholders the process for uncovering, determining the scope of, and managing program uncertainties.” [13] (pg. i) To be effective the risk management process must include, at a minimum, all process steps (mentioned above), be well structured, repeatable, continuous, integrated with appropriate program processes (e.g., program management, systems engineering, cost, scheduling, quality), and documented. Risk management must also be well implemented in the program to be effective: from the program manager to working-level engineers, action officers, and others (top-down), as well as the converse.[9]

---

[8] The 10 July 2014 Air Force Pamphlet 63-128 does not differentiate between an issue and problem, stating that an issue has a likelihood (probability) = 1, consequence > 0, and a past, present, or future time frame [4] (pg. 85).

[9] Top-level management involvement in risk management is absolutely essential not only for potentially enhanced decision making but also to set a positive example for other program personnel [7] (Chapter 3). Risk management involvement at the lowest program levels sets the right management control expectation to implement risk management.

2.0 Risk Management Planning

Risk management planning consists of the up-front activities necessary to develop, implement, and document a successful risk management program. Risk management planning addresses each of the other risk management process steps and how they will be implemented, resulting in an organized and thorough approach to identify, analyze, handle, and monitor risks. It also assigns responsibilities for specific risk management actions, and establishes risk reporting and documentation processes. This information should be included in the RMP.

From Air Force Pamphlet 63-128 [4] (pg. 90), "Risk management planning is the foundation of the life cycle risk management process and key to successful program execution. It links a program's risk management effort to life cycle planning by answering "who, what, where, when, and how" risk management should be performed." Two key outputs of the risk management planning process are the Risk Management Plan (RMP) and risk management training (discussed in Sections 2.4 and 2.5, respectively).

A graphical representation of the risk management process and process flow is given in Figure 2-1. A brief summary of the individual process steps is given in Table 2-1.

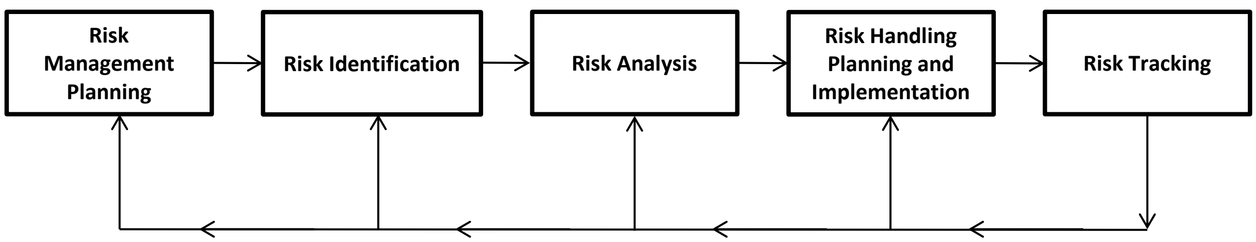


Figure 2-1. Risk Management Process Steps [4] (pg. 90)

Per the 2014 AF Pamphlet 63-128 [4] (pg. 102), the term "risk handling planning and implementation" is the name of the fourth process step shown in Figure 2-1 (above). And the term "risk handling" is generically used in this SMC guidance document instead of "risk handling/mitigation." "Risk handling is the preferred and more encompassing term to recognize that there are potentially multiple options to manage risks. These options include accepting, monitoring, transferring, mitigating (or controlling), and avoiding risks." [4] (pg. 84).[10]

Other key items associated with risk management planning include implementation and organization responsibilities (e.g., the number of risk management boards, their meeting frequency and constituents) (not addressed here), ground rules and assumptions for performing risk management, candidate risk categories, and specific risk management tools used (not addressed here).

[10] Using the term "risk handling" instead of "risk mitigation" recognizes "that most of these options address handling risk in a manner other than mitigating (i.e. eliminating or reducing) it. This also emphasizes that in some cases it may be appropriate to "handle" a risk through acceptance or transferring the risk, for example, rather than mitigation actions that may prove more costly." [4] (pg. 84).

Function/Step	Description
Risk Management Planning	The process of defining the risk management process and its implementation.
Risk Identification	The process of identifying potential risks, their associated root causes (when possible), and initially documenting the risks.
Risk Analysis	The process of examining each identified, approved risk to refine its description (as warranted), determine its probability and consequences to quantify the risk level, and develop prioritization among risks.
Risk Handling (Planning and Implementation)	The process of identifying, evaluating, and selecting risk handling options and developing an implementation approach for the selected option(s) to reduce risks to an acceptable level given program constraints and objectives. It also includes risk handling plan implementation.
Risk Tracking (Monitoring)	The process of systematically tracking and evaluating the actual vs. planned performance of risk handling (mitigation) actions against established metrics, and providing feedback to the other process steps.

Table 2-1. Summary of Risk Management Process Steps

2.1 Ground Rules and Assumptions

Accurate and viable risk management requires ground rules and assumptions that are common across the program and used by its personnel.

Some typical ground rules for risk management relevant to SMC programs include:

- Time Frame: Both probability and impact levels are based upon the status of the item under evaluation *today*, the day of the analysis, and not based upon projected or planned risk handling activities.[11]
- Time of risk event: In order to analyze a risk, the time should be identified at which the risk will hypothetically occur. (This time is often specified during risk analysis on previously approved risks, and is different than the time-frame associated with implementing a risk handling strategy to avert or accept the risk.)
- WBS Level: Hardware and software risk events will be identified to the lowest level possible to specify where the risk event applies.

Some typical assumptions for risk management relevant to SMC programs include:

- Parts for space usage shall be chosen to meet the spacecraft reliability and operational service life requirements.
- Key program milestones shall be derived from the current baseline schedule.

[11] Waterfall/burndown charts developed and used for risk handling and monitoring may make use of prior and current risk scores (and levels) as well as projections of future risk scores (and levels).

2.2 Risk Categories

Risk categories can be broadly categorized in terms of cost, performance, and schedule. This top-level aggregation can be further divided into a number of additional categories and sub-categories. For example, performance can be divided into the ability to meet performance requirements and the potential implementation approach to meeting these requirements. The implementation approach category can be divided into a number of sub-categories, including but not limited to: design/engineering, integration, manufacturing, support (logistics), technology, and threat. Several of the potential implementation sub-categories can also be broken into lower level sub-categories. For example, integration can potentially be divided into: hardware/hardware, hardware/software, software/software, box to system level, architecture level, and system of systems level integration. Likewise, manufacturing can be divided into equipment, facilities, industrial capabilities, materials, and test and evaluation. Additional information is given for several of the potential risk categories [13] (pg. 9), [20] (pp. 9-10), [21] (pp. 9-10): [12]

- **Budget.** The sensitivity of the program to budget variations and reductions and the resultant program turbulence.
- **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 uncertainty and/or 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.
- **Cybersecurity.** Loss of confidentiality, integrity, or availability of information or information systems and considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation[13]. [22] (pg. B-8).
- **Industrial Capabilities.** The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system. (Note: this risk category overlaps somewhat with production/facilities and resource risk categories.)
- **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.
- **Management.** The degree to which program plans, staffing levels, 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.
- **Management processes**. The degree to which the management processes provide effective and integrated technical/schedule/cost planning and baseline change control. Management processes risk includes the ability to establish and maintain valid, accurate,

[12] A classification used for performing integrated baseline reviews includes technical, schedule, cost, resource, and management processes [21] (pg. 9). However, a much larger set of potential risk categories will often exist. The list of risk categories presented here (Section 2.2) is representative but certainly not all inclusive. The constituent risk categories will vary for each program, hence any such list should be program specific and updated as appropriate.

[13] See DoDI 8510.01, 12 March 2014 for the Risk Management Framework (RMF) for DoD Information Technology (IT) [23].

and timely performance data, including data from subcontractors, for early visibility into risks.

- **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 operations and support phase). (Note: this risk category overlaps somewhat with industrial capabilities and resource risk categories.)
- **Resources**. The availability of personnel, facilities, and equipment, when required, to perform the defined tasks needed to execute the program successfully. Resource risk includes the effect of external factors such as loss of availability to competing programs or unexpected downtime that could preclude or otherwise limit the availability of the resources needed to complete planned work. (Note: this risk category overlaps somewhat with industrial capabilities and production/facilities risk categories.)
- **Schedule.** The sufficiency of the time allocated for performing the defined acquisition tasks. This factor includes the effects of programmatic schedule decisions, the inherent uncertainty and/or errors in schedule estimating, and external physical constraints.
- **Spectrum Supportability.** Spectrum supportability determines and documents if adequate spectrum is available to support system operation in DoD, Allied, and Coalition operations. The purpose is to identify and assess an acquisition's potential to affect the required performance of the newly acquired system or other existing systems within the operational electromagnetic environment.
- **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.
- **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.
- **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). (See also the cybersecurity risk category.)

In addition to the risk categories mentioned above, Air Force Instruction 63-101/20-101 [24] (pp. 25-27, pg. 91) calls out, in all but one case with a “shall,” that the following risk categories must be evaluated: programmatic risk, risk-based source selection, schedule risk management, cost risk management, technical risk management, product support risk management (no “shall” call out), ESOH risk management, test and evaluation risk management, operational risk management (ORM), and information assurance. In addition, for each of these risk categories, except for risk-based source selection, the program manager is tasked with specific responsibilities. The reader of this Guide should download the Change 1 (or more recent) version of AFI 63-101/20-101 and familiarize themselves with the relevant content so that it is properly applied on their program.

2.3 Responsibilities

The program risk manager should lead risk management planning activities for the overall program. Risk management planning should cover all aspects of risk management to include identification, analysis, handling (mitigation), and tracking (monitoring) of risk management actions. The risk manager should examine program planning activities to ensure they are consistent with the RMP, and that appropriate revisions to the RMP are made when warranted.

Each contractor and stakeholder is responsible for conducting their own internal risk management planning and associated risk management implementation, and elevating risks that significantly affect overall program cost, performance, or schedule to the program risk manager.

2.4 Documentation and Reporting

The RMP establishes the basic documentation and reporting requirements for performing and implementing the risk management process. Per AF Instruction 63-101/20-101, [24], pg. 42, "The PM shall prepare a Risk Management Plan (RMP) or annex to an overarching RMP for all ACAT programs and potential ACAT programs. The RMP describes the strategy by which the program will coordinate and integrate its risk management efforts to include a description and the responsibilities of the cross-functional risk management Integrated Product Team (IPT)." All participants in the risk management process should identify any additional requirements that might be needed to effectively develop and implement risk management at their level. (If necessary, the RMP should be updated to incorporate these additional requirements.) It may also be necessary for each contractor and stakeholder to develop a RMP to document their specific risk management process.

The RMP or OI should contain key risk management process and organizational implementation information, including: 1) a project summary; 2) appropriate risk management-related ground rules and assumptions; 3) key risk management-related definitions; 4) a list of key references; 5) risk management process steps; 6) inputs, tools and techniques, and outputs per process step; 7) the relationship between risk management and other key processes; 8) relevant risk categories; 9) government and contractor roles and responsibilities; and 10) personnel roles and responsibilities [7] (Chapter 4). However, the specific content of each RMP or OI may vary between Directorates and programs within a given Directorate depending upon organizational and other of considerations.

2.5 Resources and Training

The degree to which all members of the team, both government and contractor, are properly trained will have bearing on the success of the risk management efforts. All members of the program office team should receive, at a minimum, risk management training to provide a basic understanding of the risk management process.[14] Key program personnel with program management or assessment responsibilities should also receive risk management training specific to the risk management tools they will use in their program areas, as well as instruction on the risk management database being used across the program[15]. The program office team should also be familiar with contractor and stakeholder risk management processes and tools because many of the performance (including a variety of technical) risks will be identified and managed by contractors and stakeholders. The risk manager will formulate and maintain the risk management training for use in the program. The training will instruct the program team on the established risk management process and, where appropriate, on the respective contractors' and stakeholders' risk management processes.

2.6 Risk Management Plan Update

The RMP should be updated, as necessary, when a major program re-baselining occurs, or immediately before the beginning of a new acquisition phase (e.g., at completion of the technology design phase and before the start of the production and deployment phase). Particular attention should be given at such times to the adequacy of the risk analysis scales to assist in evaluating risks as the program's main focus shifts, for example, from the handling of "development risk" to the prevention of "mission execution risk." The risk analysis scales (Section 4.1) change in terms of cost consequence of occurrence (see Table 4-3) during the acquisition phase. Pre-launch mission assurance addresses the residual risk to the program and may involve a different set of definitions for probability of occurrence, as well as the mapping of probability and consequence to risk level.[16]

The RMP may also be subject to review and revision on any of the following occasions: 1) whenever the acquisition strategy changes, or there is a major change in program emphasis; 2) in preparation for major program milestones or decision points; 3) in preparation for or immediately following broad scope technical audits and reviews; 4) concurrent with the review and update of other program plans; 5) in preparation of a Program Objective Memorandum (POM) submission; 6) change in segment or system architecture; 7) change in segment or

---

[14] This training should be supplied by the SMC University, the SMC Directorate or Program Office's risk manager and/or support personnel. Acquisition strategy-related risk management training can be supplied by SMC/PID to assist these organizations.

[15] Risk management database is generically used to represent the tool and data storage for the program risk management information. As mentioned in Air Force Instruction 63-101/20-101, Active Risk Manager (ARM) is the "current standard tool to manage program risks" [24] (pg. 25).

[16] This is permitted per Air Force Pamphlet 63-128 [4], Section 12.1.6.1.1, (pg. 88). "12.1.6.1.1. System Safety/Mission Assurance. Mission assurance and system safety risks are assessed and managed using methodologies separate from LCRM." For mission assurance use, the low (green), medium (yellow), and high (red) boundaries in the risk matrix given in Figure 4-1 may be adjusted so that probability values of even 20% are considered nearly certain, thus shifting the risk boundaries towards relatively higher levels. In addition, the consequence of occurrence dimension may in some cases be solely related to performance consequence and not address cost and schedule consequence. See SMC/Independent Readiness Review Team, Aerospace Corporation President's Review and related methodologies for evaluating mission assurance risk. The performance consequence scale given in Table 4-4 of this document is intended for acquisition rather than mission assurance risk management.

architecture contractors; 8) change Air Force mandated risk management policy requirements, etc.

3.0 Risk Identification

Risk identification is the action of examining a program or project to determine ―What can go wrong? [4] (pg. 92) Risk identification involves examining all significant facets of the program to identify potential risks. The program should identify risks via a combination of formalized activities, such as risk identification workshops, and informal activities, including identification of candidate risks by individual program team members and contractor risk management processes. While comprehensive risk identification (e.g., workshops) may be initially performed at the start of a program phase, risk identification itself should be viewed as a continuous activity throughout the life of the program.[17]

3.1 Risk Identification Responsibilities

All program personnel are encouraged to identify candidate risks, both individually and through their corresponding integrated product teams (IPTs) and functional organizations. Limiting risk identification to a subset of program personnel will contribute to "escapes" that come back later in the program as problems. Program personnel involved in the detailed and day-to-day technical, cost, and scheduling aspects of the program may be most aware of the potential risks that need to be managed. Because risks can be associated with all aspects of a program, not just that of the program manager or chief engineer, all personnel, regardless of their organization or role, are encouraged to consider and identify potential risks on a continuous basis.

3.2 Risk Identification Strategy

A structured approach for specifying risk is desirable to avoid vague and/or inconsistent risk statements. A commonly used method derived from hypothesis testing includes a two-part statement in the "If"-"Then" format:

- "If" a possible event (condition) occurs, it will initiate the chain of events/conditions ultimately leading to an adverse program impact.
- "Then" the part of the program or system that will be affected by the risk, and the nature of the outcome (consequence) if the event occurs.

[17] Comprehensive risk identification should also be conducted yearly or following major re-baselining of the program to lessen the chance that potential risks will go undetected and later surface as problems which are much more costly to deal with.

It is important that risks be clearly written in an "If"-“Then” format, characterizing the possible risk event or condition (“If”), and the outcome or consequence(s) (“Then”) in a concise statement. A hypothetical risk statement in "If"-“Then” format follows:

> "If the real-time software design does not meet timing requirements, then the payload integration schedule will slip."

This particular example follows the “If,” “Then” format, clearly states the condition and outcome in easy to understand language, and does not include a potential risk handling strategy or other solution.

Numerous other risk statement formats are possible which use the “If,” “Then” framework, then add one or more additional qualifiers, such as “Because,” “By,” “Due To,” “Resulting In,” etc. These additional qualifiers may be helpful, but can also diminish focus on the “If,” “Then” portion of the statement which are essential for describing the risk.[18]

However, it is beneficial that a single approach is used and followed within a program.

While the enumeration of conditional risks via “If,” “Then,” and related statements is certainly helpful to the success of the program, even the most complete list cannot exhaust all the program uncertainty that will exist. Continued vigilance is required on the part of the program management and engineering staff, the risk manager and other program personnel to identify candidate risks throughout the course of the program.

One or more top-level and one or more lower-level risk identification approaches should be used for comprehensive risk identification. Examples of top-level approaches include WBS, key requirements [7] (Chapter 5), key processes[19] [25], and risk categories (see Section 2.2). Examples of lower-level approaches include affinity; brainstorming; cause/effect diagrams; checklists; critical and near critical path; expert opinion, failure analysis; influence diagrams; ; lessons learned from analogous programs; Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis; and triggers from risk scales [20] (Chapter 5), [7] (Chapter 5), [26] (Chapter 11).[20] Additional attention should be given to candidate risks that occur at relatively high WBS

---

[18] The “If,” “Then,” “Because” statement is no longer recommended. Despite instructions that the “Because,” portion of the statement should be related to the root cause (if known), “Because” was commonly used on one SMC program to further describe the “Then” portion of the statement related to outcome (consequence).

[19] The cited document contains information that can be potentially applied to spacecraft development and production programs. However, it is also out of date, written for non-space programs, and written primarily for programs that may have true rate production (e.g., tactical missiles, aircraft).

[20] Another lower-level approach is the “five whys,” which was originally developed by Toyota founder Sakichi Toyoda. While this approach can be helpful, there is a tendency if not used properly, or if insufficient training exists, to fall back on deductive logic and not identify potential risks and root causes. Mr. Teruyuki Minoura, then managing director of Toyota's global purchasing, urges caution when using this approach. The following is extracted from a statement Mr. Minoura made at the 2003 Automotive Parts System Solution Fair, Tokyo, Japan:

> “When an error occurs, the first thing that needs to be done is fix the error. Minoura recalls that Ohno used to order them to ask the question "Why?" five times over because "that way you'll find the root cause, and if you get rid of that it'll never happen again." However, Minoura emphasizes that on-the-spot observation

levels (e.g., WBS level 1 and 2) and those affecting various types of integration (e.g., hardware/hardware, hardware/software, software/software, box through system level, and system of systems level). All identified risks should be documented with a statement of the risk, including the “If,” “Then,” structure in an appropriate risk management database.

A helpful methodology that combines key processes (top-level approach) coupled with trigger questions (lower level approach) is given in the “Risk Identification, Integration, and Ilities (RI3) Guidebook,” Version 1.2, 15 December 2008 [27] (pp. 23-53). Each of the nine process areas are subdivided into topics, and each topic includes multiple trigger questions. Another source of trigger questions to consider is the “SMC Systems Engineering Primer and Handbook,” Air Force Space and Missile Systems Center, Third Edition, 29 April 2005 [28] (pp. 240-243). The processes, topics, and individual questions can be tailored to the program being examined.

When performing comprehensive, rather than ad hoc risk identification a relevant rule is to use what applies, discard the rest, and review the methodology in-depth prior to holding the risk identification session (or workshop). In other words, focus the top-level approach to the relevant portion(s) of the WBS, key requirements, key processes, and/or risk categories, and apply one or more lower-level approaches against these items before the session (or workshop) takes place. While this does not guarantee that all potential risks will be uncovered, it is typically far more effective than an ad hoc application of one or more lower-level approaches (e.g., brainstorming) by itself.

Finally, whatever methodology is used, recognize that it will almost never identify all of the candidate risks present. One helpful approach to apply following the initial completion of the risk identification activity is to ask one or more negative questions, such as “what have I left out?” Inevitably, this type of “out of the box” thinking will lead to one or more additional candidate risks.

3.3 Risk Identification Documentation

The candidate risk should be documented in the risk management database with at least the following information: title, date identified and updated, “If,” “Then” statement, point of contact (POC), POC IPT manager, linkage to other risks, existing work performed (as part of the baseline program), and associated key requirements (if known). Neither the preliminary risk analysis, the risk handling strategy, nor risk time-frame should be estimated at this occasion, because the resulting information may be uncertain, incorrect, and it may pre-bias a subsequent

---

rather than deduction is the only correct way to answer a "Why?" question. "I'm always struck that the five-why method doesn't seem to be working as well as it should be because there's been a lack of practical training. The reason is that they end up falling back on deduction. Yes, deduction. So when I ask them 'Why?' they reel off five causes as quick as a flash by deduction. Then I ask them five whys again for each of the causes they came up with. The result is that they start falling back on deduction again, and so many causes come back that you end up totally confused as to which of them is important."

"Through real training," Minoura says, "you'll be able to discover dozens of problems and also get to their root causes”…[29]

more thorough analysis. Developing risk analysis or risk handling information at this time will also waste resources should the risk be judged to be a watch list item (or rejected) which may not require this information to be generated. In addition, when the Risk Management Board (RMB) evaluates the candidate risk it may provide or request information to be included (e.g., a new facet of the risk is added) which may lead to additional risk sub-categories being relevant, potential changes to the risk analysis probability and consequence scores, a potential change in the risk level, a potential change to the risk time-frame, and/or potential changes to the desired risk handling strategy.

3.4 Evaluation of Candidate Risks

Once a candidate risk is identified, the risk is first reviewed by the nominator and Risk Manager for completeness and relevance to the program. Adjustments are made to the risk identification documentation (database) as warranted. The risk is then reviewed at the next RMB, where a determination is made as to whether/not the risk will be approved (by the RMB) and who will be assigned or approved as the risk owner (which may/may not be the risk nominator).[21] Potential outcomes from the RMB include, but are not limited to: deferred, pending, need additional information, approved, closed, rejected, management action, engineering process/practice item.[22] (All RMB decisions associated with candidate risks and other actions should be documented and maintained to provide a risk management record for the duration of the program and application to other programs.) In many cases candidate risks will actually be potential management actions or engineering process/practice items that may not rise to the level of a risk but nevertheless need to be dealt with to insure they don't adversely impact the program in the future.[23]

---

[21] For additional information on defining the risk owner's roles and responsibility see the relevant Directorate RMP or OI and reference [30], Appendices B and D.

[22] For an engineering process/practice item, a question may exist as to whether/not an item can be developed, manufactured, tested, whether suitable equipment and facilities exist, etc. The level does not reach that of a risk, but it is sufficient to be noted, along with identifying a POC, a closure plan and an associated closure date. As with a management action, should closure not occur on-time, then the engineering process/practice item can be elevated to a risk.

[23] Candidate risks were evaluated from risk identification activities on three different groups of programs. In the first case, five different programs were examined that represented different customers and/or program contractors. Across the five programs, approximately 2% of the identified candidate risks were mapped to existing program risks, 1% were approved as new risks, and 97% were determined to be management actions, engineering process/practice items, or were closed or rejected. In the second case, a new-start program was similarly evaluated, but a cursory risk identification had been performed just weeks earlier. Approximately 19% of the newly identified candidate risks were mapped to existing program risks, 4% were approved as new risks, and 77% were determined to be management actions, engineering process/practice items, or were closed or rejected. In the third case, two acquisition support programs were evaluated for candidate risks. Approximately 0% of the identified candidate risks were mapped to existing risks, 4% were approved as new risks, 2% were overlapping (duplicate) new risks and 94% were determined to be management actions, engineering process/practice items, or were closed or rejected. The large percentage of candidate risks that were determined to be non-risks in each of the above three cases (from 77% to 97%) suggests that a thorough evaluation of whether an item is a risk vs. a management action, engineering process/practice item, or closed or rejected is necessary to reduce Type 1 (false positive) errors (and potentially wasted resources in dealing with items that are not risks), while at the same time ensuring that Type 2 (false negative) errors are minimized.

For a management action or engineering process/practice item, management needs to take specific steps to resolve the matter.[24] A point of contact (POC) is established along with a brief description of the closure plan and an associated closure date. If the closure date is not (or will not) be met, then the matter can be elevated to a risk, have a formal risk analysis performed and if appropriate a risk handling strategy developed and implemented. While both a management action and engineering process/practice item are placed on a watch list, they must be actively managed (not passively watched) to ensure an acceptable adjudication and preclude a problem from occurring later in the program.

4.0 Risk Analysis

Risk analysis is an evaluation of each identified risk that is approved by the RMB or equivalent to determine possible outcomes, critical process variance from known best practices, the probability of risk events occurring, and the consequences associated with the outcomes.[25] This step involves the use of risk analysis tools and techniques to estimate the probability of the event occurring along with the cost, schedule, and performance consequences, then converting the resulting probability and consequence estimates to a risk level (e.g., Low, Medium, High).

While both qualitative and quantitative risk analysis techniques exist, the risk analysis process illustrated in Air Force [e.g., Air Force Pamphlet 63-128 [4] (Chapter 12)] and Department of Defense (DoD) documentation [e.g., Risk Management Guide for DoD Acquisition [13] (Chapter 4)] relies on ordinal probability of occurrence and consequence of occurrence scales coupled with expert opinion from subject matter experts, and lessons learned from relevant programs for each approved risk. A top-level outline of the risk analysis process includes:

---

[24] A management action follows. A key design requirement document had not been finalized and approved. This prevented finishing code testing and releasing an application specific integrated circuit (ASIC) design to fabrication. The cognizant ASIC design manager elevated the priority of finalizing and approving the requirements document. This permitted code testing to be completed by the desired date to support the design release to ASIC fabrication. (Many simpler examples of management actions exist, such as writing a missing paragraph for a Request For Proposal, a cost account manager signing a notebook page, etc. Of primary importance is to resolve the item in a timely manner to prevent it from becoming a risk, if not issue or problem.)

An engineering process/practice item example follows. Test equipment was needed to support a sensor development. The test equipment was not off-the-shelf, but the supplier had previously built similar units and estimated a six month time-frame for the new unit. The host program did not need the test equipment for two years. Had the program treated the test equipment as a risk, it would have been scored as a medium risk (since it was currently unavailable), but no action would have occurred for more than a year. Instead, the unit was treated as an engineering process/practice item, a POC assigned, and a closure plan developed (along with a closure date), and the item was placed on the program’s watch list. A year later the test equipment was ordered from the supplier following the closure plan and subsequently delivered. Although in this case whether/not the test equipment was treated as an engineering process/practice item or a risk may appear to be a bookkeeping exercise, shifting the procurement to the watch list then taking action at the appropriate time permitted a more efficient resource allocation and focus on more substantial program risks.

[25] A risk analysis should only be performed on approved risks. A risk analysis should not be performed on non-approved risks to preclude wasting resources if the candidate is determined not to be a risk.

- Estimation of probability of occurrence (Section 4.1)
- Estimation of cost, performance, and schedule consequence of occurrence (Section 4.1)
- Determination of the risk level (Section 4.2)
- Estimation of the frequency of occurrence, time-frame, and inter-relationship with other risks (Section 4.3)
- Determination of the risk prioritization given the risk level and other considerations (mentioned above) (Section 4.3)

If likelihood or consequence cannot be reasonably estimated, then it should not be reported as a risk on the 5x5 matrix. It may be separately reported as a concern, as mentioned in Section 1.1, and monitored for change and/or determination of likelihood and consequence [4] (pp. 84-85. The above methodology can be applied to a variety of risk categories. However, cost and schedule risks should be evaluated using a Monte Carlo simulation, as discussed in Section 4.4.

Several other tools and techniques can potentially be used for program risk analyses but are not addressed here. These tools and techniques include, but are not limited to:

- Expert opinion (individual or group). If used in a group setting care should be exercised to avoid "group think" which can bias results. This technique can be used to provide inputs for risk scales and Monte Carlo simulations. It should not be used to directly estimate a risk level (e.g., Low, Medium, High).
- Analysis of relevant historical data and comparison to analogous programs or systems. These techniques can be used to provide inputs for risk scales and Monte Carlo simulations. It should not be used to directly estimate a risk level unless an *exact* match exists with a program risk.
- Uncertainty, sensitivity, and scenario analysis of cost, schedule, and performance (including technical).
- Probabilistic risk assessments, fault tree analysis, failure modes and effects analysis, and similar techniques.. These approaches are typically used in conjunction with some aspects of performance risk analyses, safety analyses, etc.
- Decision analysis (e.g., decision trees, expected monetary value)
- Decision making under uncertainty and risk (e.g., payoff matrices)

Once the risk level has been estimated, the results should be reviewed by the risk POC, risk manager, and appropriate IPT lead before being submitted to the RMB. It is important not to develop a preliminary risk handling strategy at this time because early specification may: 1) bias the selection of the eventual risk handling strategy (option and/or implementation approach), and 2) not have the benefit of RMB feedback which may lead to a change in the risk level, the maximum (dominant) consequence dimension, etc.

4.1 Risk Analysis Scales

An ordinal scale is specified for estimating probability of occurrence for Air Force acquisition programs [e.g., Air Force Instruction 63-101/20-101 (pg. 42) [24], Air Force Pamphlet 63-128

[4] (Table 12.1, pg. 97)].[26] This probability scale is given in Table 4-1 [4] (pg. 97). As shown in Table 4-1, there are five scale levels, from "1" to "5" (lowest to highest likelihood). These levels are defined as Near Certainty, Highly Likely, Likely, Low Likelihood, and Not Likely.[27]

Three ordinal scales are also specified for estimating cost, performance, and schedule consequence of occurrence for Air Force acquisition programs {[24] (pg. 42), [4] (Tables 12.2, 12.3, and 12.4, pp. 97-100)}.[28] The cost, schedule, and performance consequence of occurrence five-level scales contained in Air Force Pamphlet 63-128 [4] (pp. 97-100] are given in Tables 4-2, 4-3, and 4-4, respectively.[29] [30]

[Note: the level coefficients 1 through 5 in the probability scale given in Table 4-1 and the three consequence scales given in Tables 4-2, 4-3, and 4-4 are only ordinal—they have no cardinal meaning and mathematical operations (e.g., averaging) should not be performed on the level values because the results may be erroneous.[31]]

---

[26] Mission assurance and ESOH evaluations are not required to use this scale. Environment, Safety, and Occupational Health evaluations use the mandatory scale given in MIL-STD-882C [8] (pg. 13), in MIL-STD-882D [9] (pg. 19), or the scale in MIL-STD-882E [10] (pg. 11). When using MIL-STD-882E if data is available the quantitative scale should be used [10] (pg. 91) as specified in SMC-T-004 [11] (pp. 8-9).

[27] The subjective probability phrases in Table 4-1 (e.g., likely) coupled with the probability of occurrence ranges in this table (e.g., 41% to 60%) can potentially lead to mis-scoring because analysts that do not agree with the probability value range for a particular phrase may then select a different level that corresponds to a range value they are in closer agreement with. Actual survey results from more than 100 respondents show that far less than 50% of the respondents agree with the probability ranges for highly likely and likely given in Table 4-1 (which were the only two phrases from this table that overlapped with the phrases evaluated in the survey). Despite these limitations, the probability scale given in Table 4-1 must be used by Air Force personnel when conducting acquisition risk analyses.

[28] Mission assurance is not required to use these scales. Environment, Safety, and Occupational Health evaluations use the mandatory scales given in MIL-STD-882C [8] (pg. 13), in MIL-STD-882D [9] (pg. 18), or in MIL-STD-882E [10] (pg. 11).]

[29] Note that the three consequence scales are listing in ascending order (1 being least severe to 5 being most severe), which is the opposite of both convention (descending order) and the probability scale given in Table 4-1. The difference between the ordering of the probability and three consequence scales should be noted and understood when performing a risk analysis.

[30] Each consequence scale given in Tables 4-2 through 4-4 uses different classes of evaluation criteria: cost uses percent increase from the Milestone A or last approved Development or Production cost estimate (this criteria is most applicable for space programs versus Program Acquisition Unit Cost (PAUC) or Average Procurement Unit Cost (APUC), schedule uses a qualitative degree of schedule slip relative to the project or program key milestones, total float, and/or other key dates, and performance (including supportability) uses qualitative technical performance relative to the goal or the level of technical design margins that exist (plus additional criteria that may lead to a performance consequence value = 5). The WBS-level, integration-level, or equivalent that a consequence scale is applied at can have a significant effect on the results. There are, however, no requirements or even universal guidelines as to how the consequence scales should be applied. For example, for schedule consequence, Table 4-2 can be applied to: 1) the IPT-level, 2) segment-level, and 3) the program (system)-level. The preferred approach is for consequence scales to be applied at the program-level but used as necessary at lower levels within the program. The resulting risk levels can then be adjusted as appropriate when elevated to the segment and program-levels. The key is to permit accurate risk comparisons to be made within a program, across programs within a Directorate, and across Directorates within SMC.

[31] See reference [7] (Chapter 6) for additional information on creating and evaluating ordinal probability and consequence scales, and errors that result from assuming that their coefficients are cardinal.

Level	Likelihood (Probability)	Probability of Occurrence
5	Near Certainty	81%-99 %
4	Highly Likely	61%-80%
3	Likely	41%-60%
2	Low Likelihood	21%-40%
1	Not Likely	5%-20%

Table 4-1. Likelihood (Probability) Criteria [4] (pg. 97)

Level	Standard Air Force Consequence Criteria - Schedule
1	Negligible program or project schedule slip
2	Schedule slip, but: Able to meet milestone dates (e.g. A, B, and C) and other key dates (e.g. CDR, FRP, FOC) Does not significantly decrease program total float and Does not impact the critical path to program or project completion date
3	Schedule slip that requires closely monitoring the schedule due to the following: Impacting the ability, but still able to meet milestone dates (e.g. A, B, and C) and/or other key dates (e.g. CDR, FRP, FOC) Significantly decreasing program total float Impacting the critical path to program or project completion date
4	Schedule slip that requires schedule changes due to the following:* Significantly impacting the ability to meet milestone dates (e.g. A, B, and C) and/or other key dates (e.g. CDR, FRP, FOC) Significantly impacting the ability to meet the program or project completion date
5	Schedule slip that requires a major schedule re-baselining due to the following:* Failing to meet milestone dates (e.g. A, B, and C) and/or other key dates (e.g. CDR, FRP, FOC) Failing to meet the program or project completion date
* Exhibit awareness to exceeding Nunn-McCurdy threshold breach for schedule. ***Note:*** Impact varies based on 1) The schedule slip relative to the remaining duration in the program or major milestones; amount of remaining time to work-around the impact; 2) The impact of the slip with respect to key resources.	

Table 4-2. Standard Air Force Consequence Criteria – Schedule [4] (pg. 99)

Level	Standard Air Force Consequence Criteria – Cost (A-B refers to Milestone Designation)
1	For A-B Programs: <1% increase from MS A or last approved Development or Production cost estimate. For Post-B and Other Programs: <1% increase from MS A or last approved Development or Production cost estimate.
2	For A-B Programs: 1% to <3% increase from MS A or last approved Development or Production cost estimate. For Post-B and Other Programs: 1% to <3% increase from MS A or last approved Development or Production cost estimate.
3	For A-B Programs: 3% to <5% increase from MS A or last approved Development or Production cost estimate. For Post-B and Other Programs: 3% to <5% increase in Development or >1.5% increase to Program Acquisition Unit Cost (PAUC) or Average Unit Procurement Cost (APUC) from last approved baseline estimate or >3% increase to PAUC or APUC from original baseline. (1/10 of Nunn-McCurdy 'significant' breach).
4	For A-B Programs: 5% to <10% increase from MS A or last approved Development or Production cost estimate. For Post-B and Other Programs: 5% to <10% increase in Development or >3% increase to PAUC or APUC from last approved baseline estimate or >6% increase to PAUC or APUC from original baseline. (1/5 of Nunn-McCurdy 'significant' breach).
5	For A-B Programs: >10% increase from MS A or last approved Development or Production cost estimate. For Post-B and Other Programs: >10% increase in Development or >5% increase to PAUC or APUC from last approved baseline estimate or >10% increase to PAUC or APUC from original baseline. (1/3 of Nunn-McCurdy 'significant' breach).

Table 4-3. Standard Air Force Consequence Criteria – Cost [4] (pg. 100)

Level	Standard Air Force Consequence Criteria - Performance
1	Minimal consequence to technical performance or supportability but no overall impact to the program success. A successful outcome is not dependent on this issue; the technical performance goals or technical design margins will still be met.
2	Minor reduction in technical performance or supportability, can be tolerated with little impact on program success. Technical performance will be below the goal or technical design margins will be reduced, but within acceptable limits.
3	Moderate shortfall in technical performance or supportability with limited impact on program success. Technical performance will be below the goal, but approaching unacceptable limits; or, technical design margins are significantly reduced and jeopardize achieving the system performance threshold values.
4	Significant degradation in technical performance or major shortfall in supportability with a moderate impact on program success. Technical performance is unacceptably below the goal; or, no technical design margins available and system performance will be below threshold values.
5	Severe degradation in technical performance or supportability; will jeopardize program success; or will cause one of the triggers listed below (**Note 1**)

Note 1: Any root cause that, when evaluated by the cross-functional team, has a likelihood of generating one of the following consequences must be rated at Consequence Level 5 in Performance:

Will not meet Key Performance Parameter (KPP) Threshold
Critical Technology Element (CTE) will not be at Technology Readiness Level (TRL) 4 at MS A
CTE will not be at TRL 6 at MS B
CTE will not be at TRL 7 at MS C
CTE will not be at TRL 8 at the Full-rate Production Decision point
Manufacturing Readiness Level (MRL)* will not be at 8 by MS C
MRL* will not be at 9 by Full-rate Production Decision point
System availability threshold will not be met

* MRLs will be calculated in accordance with the *DOD Manufacturing Readiness Assessment Deskbook.*

Table 4-4. Standard Air Force Consequence Criteria – Performance [4] (pp. 97-98)

4.2 Determining the Risk Level

After estimating the probability of occurrence and consequence of occurrence values (1 through 5 for each), a risk rating can be determined. To provide a consistent and standardized risk analysis, risk ratings are established through the risk matrix given in Figure 4-1 [4], Figure 12.2, pg. 96), which converts the probability of occurrence and consequence of occurrence values to one of three risk levels: low (green), medium (yellow), or high (red).[32] The 5x5 matrix given in

[32] It is possible to map five probability levels and five consequence levels to four or five resulting risk levels, by developing and inserting low-medium and/or medium-high bands. However, the required matrix, given in Figure 4-1 uses three risk levels, which is the number of risk levels commonly used across a variety of DoD and non-DoD programs. Similarly, a wide variety of other risk matrices are possible, and in some cases may even score a cell higher based upon probability than consequence. [See for example, [31]] (pg. 7) for the (probability, consequence)

Figure 4-1 is required per Air Force Instruction 63-101/20-101 [24]) ["shall," pg. 42] and Air Force Pamphlet 63-128 [4] ("required" per Air Force Instruction 63-101/20-101, pg. 87).[33] While there is only a single probability scale (Table 4-1), there are three consequence scales (cost, performance, and schedule in Tables 4-3, 4-4, and 4-2, respectively). Thus for consequence of occurrence the maximum value of cost, performance, and schedule consequence without performing any mathematical operations [4] (pg. 94) should, along with the single probability of occurrence value, be mapped into the risk matrix given in Figure 4-1.

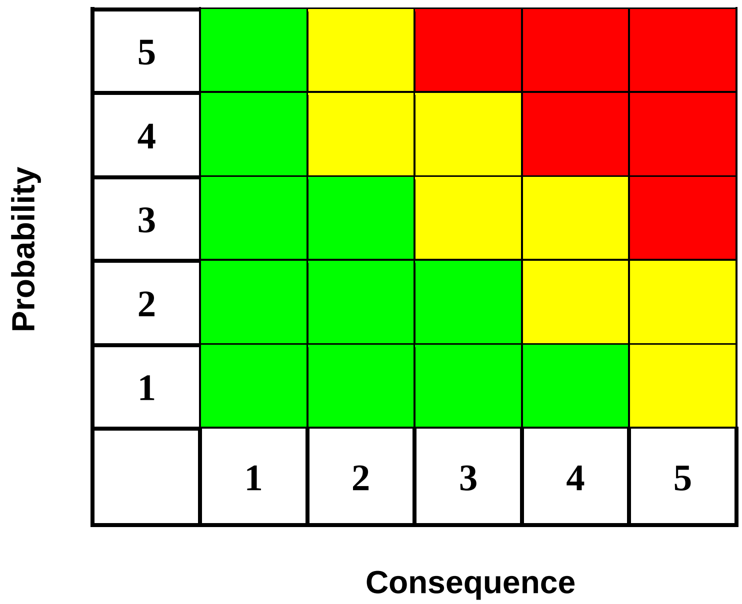


Figure 4-1. Air Force Pamphlet 63-128 Probability:Consequence Risk Matrix [4] (pg. 96)

A second version of the Air Force risk matrix is given in Figure 4-2. The numbers in parentheses contained in Figure 4-2 correspond to the product of the probability of occurrence and the consequence of occurrence values for each cell [except for the value of 7 inserted into the (p = 1, c = 5) cell, as discussed below] and are an addition to the required Air Force risk matrix given in Air Force Pamphlet 63-128 [4] (pg. 96) as shown in Figure 4-1. *These product values are for illustration purposes only.* They should only be used for setting the ordinate range on a waterfall/burndown chart or as an input for prioritizing items within a given risk level (e.g., High). This is because the underlying probability and consequence values are ordinal, not cardinal, and they assume that (p, c) = (c, p) which may not be the case depending upon utility considerations.[34] (See Section 4.3 for additional information on risk prioritization.) Hence, a

---

pair of values (4, 1) versus (1, 4).] However, the required matrix, given in Figure 4-1 should be used by Air Force and support contractor personnel for Air Force applications.

[33] Air Force Instruction 63-101/20-101 [24] (pg. 42) also states: "On the risk matrix, the PM shall plot, and be prepared to discuss, each of the program's identified "high" and moderate risks…."

[34] Note: Cartesian coordinates usually associates the abscissa with the X-axis and ordinate with the Y-axis. This would lead to (x, y) being (c, p). However, for risk analysis a common practice is to designate this pair as (p, c) even though the abscissa is consequence and the ordinate is probability (likelihood). In this Risk Management Process Guide, the Probability:Consequence pair is designated as (p, c) while plotted with the abscissa as the consequence and the ordinate as probability (likelihood).

score of 4 is not necessarily twice the risk of a score of 2 even though both correspond to Low risks, but that the item with a risk score of 4 has a relatively higher level of risk than (holding all else constant) than an item with a risk score of 2.[35]

Probability					
5	(5)	(10)	(15)	(20)	(25)
4	(4)	(8)	(12)	(16)	(20)
3	(3)	(6)	(9)	(12)	(15)
2	(2)	(4)	(6)	(8)	(10)
1	(1)	(2)	(3)	(4)	(7)
	1	2	3	4	5

Consequence

Figure 4-2. Air Force Pamphlet 63-128 Probability:Consequence Risk Matrix with P * C (Product) Values Embedded in Cells

Note from Figures 4-1 and 4-2 that the required standard Air Force 5x5 matrix includes the asymmetric (p = 1, c = 5) yellow vs. (p = 5, c = 1) green color cells. A value of "7," a prime number not found elsewhere in the 5x5 matrix, has been inserted into the Figure 4-2 (p = 1, c = 5) cell vs. a value of "5" for the (p = 5, c = 1) cell. While this does not matter for the representation of risks contained in the 5x5 matrix itself, it is necessary to provide an unambiguous boundary between low (green) and medium (yellow) risk when generating a waterfall/burndown chart. This is because most risk management software does not generate risk vs. time (e.g., waterfall/burndown) charts using information in matrix notation [e.g., (p, c)], but instead use a simple numeric representation. Assigning a value of "7" to this cell creates an unambiguous low/medium boundary when the product of probability and consequence is used, as the highest low risk (green) product is 6 and the lowest medium risk (yellow) product above the (p = 1, c = 5) cell is 8. Assigning a value of "5" to this cell results in an ambiguous green/yellow boundary when plotting a waterfall/burndown chart based upon these values. [Of course, if the cell (p = 1, c = 5) had been specified in the Air Force required 5x5 matrix as low risk (green), then this adjustment would not have been necessary.] Finally, note that this same rationale was used to develop the underlying Probability/Impact Diagram (PID) weights used in the Air Force instantiation of Active Risk Manager (ARM), the "current standard tool to manage

[35] Similarly, a (p, c) score of (2, 4) yielding a product of 8 may be the same, less than, or more than a (p, c) score of (4, 2) yielding a product of 8. This is because the true cardinal coefficients associated with the (p, c) scores are unknown and the integer values are only ordinal placeholders for these undetermined cardinal coefficients.

program risks" [24] (pg. 25). This again was to ensure an unambiguous boundary between low (green) and medium (yellow) risk levels when generating a waterfall/burndown chart.[36]

Under no circumstances should the probability and consequence scores be added together (e.g., to form a range of 2 to 10 from a probability range of 1 to 5 and a consequence range of 1 to 5) because probability and consequence sets are independent of each other.[37] In addition, fractional scale values (e.g., a probability score of 3.4) should never be estimated or placed in a risk matrix or risk handling waterfall/burndown chart because: 1) the scale coefficients themselves (e.g., 1 through 5) are only ordinal, not cardinal; and 2) plotting fractional values into the ordinal 5x5 risk matrix or waterfall/burndown scale is problematic as risks can potentially cross a cell in the matrix or waterfall/burndown value, or even worse cross a risk level boundary (e.g., from Medium to High) in the matrix or waterfall/burndown chart depending upon the specific P and C values if the product of these variables is used. The practice of using fractional probability and/or consequence values is thus both inappropriate and incorrect.

While there are three different consequence scales, the resulting risk level is typically not cost risk, performance risk, or schedule risk (depending upon which consequence scale value is the maximum). Here, the resulting type is specified by the risk under evaluation, and the maximum consequence value is only the impact associated with that risk. For example, if a technology risk is evaluated and the schedule consequence value is the maximum of the three consequence values, then the resulting risk is technology risk, with a maximum impact of schedule. The resulting risk is not schedule risk. This is a common mistake and one that should be avoided.

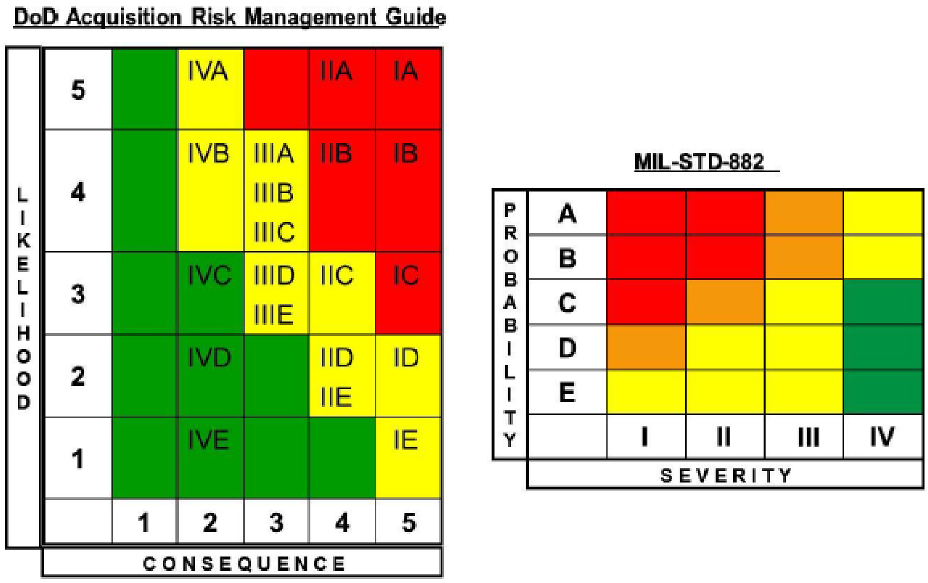
Finally, note that Environment, Safety, and Occupational Health (ESOH) risks shall use the risk mapping representation given in Figure 4-3 to translate cells and risk levels for MIL-STD-882C [8] (pg. A-5), MIL-STD-882D Risk Matrix [9] (pg. 20), and MIL-STD-882E [10] (pg. 12) to the Department of Defense Risk Management Guide Matrix [13] (pg. 11).[38]

---

[36] Note also that a product score of 4 corresponds to three different cells in the Figure 4-2 5x5 matrix: as (p, c) = (4, 1), (1,4), and (2, 2). In addition, the (p, c) product for all other cells in Figure 4-2 that are off- diagonal also represent a pair of product values [except for (p, c) = (1, 5) and (5, 1) because of the use of "7" in the (1, 5) cell]. It is important to designate in ARM as well as in separate documentation the individual (p, c) probability and consequence values for each resulting risk handling activity when developing a waterfall/burndown chart to avoid potential confusion associated with the ARM PID weights that are also the product values given in Figure 4-2. This can be done by inserting a separate column in the listing of risk handling activities on subsequent output with the heading labeled [L, C] or [P, C] and reporting the pair of values [likelihood or probability, consequence] for each activity.

[37] Numerous internal risk matrix scoring methods have been developed and used besides multiplying probability and consequence and presenting (p, c) value pairs. The methodology used to derive the scoring values is never provided. (In some cases the values may be nothing more than unstructured guesses.) In addition, the scoring values are sometimes inconsistent when compared to a corresponding adjacent (matrix) row or column. Using these values for risk ranking, risk handling waterfall/burndown chart development, overall program risk level, or similar purposes may lead to misleading, if not erroneous results.

[38] Specifically, from Air Force Instruction 63-101/20-101 [24] (pg. 42): "Risks identified using MIL STD 882 shall be translated using the translation of MIL-STD-882 Risk Matrix to the OSD Risk Management Guide Matrix in AFPAM 63-128." The Air Force Instruction 63-101/20-101 reference to the translation matrix contained in Air Force Pamphlet 63-128, which is Figure 12.3 [4] (pg. 101), and given in this Risk Management Process Guide document as Figure 4-3. Air Force Pamphlet 63-128 further states in Section 12.1.6.1.1 [4] (pg. 88):



Note: MIL-STD-882E includes probability level "F" for "eliminated" ESOH risks that are "incapable of occurrence." ESOH risks with probability level F should not be translated to the DoD Acquisition Risk Management program risk matrix.

Figure 4-3. Translation of MIL-STD-882 Risk Matrix to the OSD Risk Management Guide Matrix [4] (pg. 101)

4.3 Considerations for Risk Prioritization

While probability of occurrence and consequence of occurrence scores are used to estimate the risk level, additional considerations beyond these two factors may be used to prioritize risks within a particular level (e.g., low, medium, high). The frequency of occurrence, time-frame, and inter-relationship with other risks are examples of other considerations that can be used for risk prioritization [7] (Chapter 6). For frequency of occurrence the question is whether/not the risk can occur more than once. Holding all else constant if a risk can occur more than once it should have a higher prioritization than the another risk of the same (p, c) score that could only occur once. Time-frame represents either the time when the risk will occur if it is not alleviated or the time by which the risk handling strategy must be implemented to prevent the risk from occurring. Neither of these two time-frame definitions are universally correct, but only a single definition

---

"System Safety/Mission Assurance. Mission assurance and system safety risks are assessed and managed using methodologies separate from LCRM. Manage system safety risks by applying MIL-STD-882, the *DoD Standard Practice for System Safety*. All high and serious system safety risks must also be translated and presented in accordance with AFI 63-101/20-101 at all program, technical, and Milestone decision reviews or to support other key decision points. The LCRM 5x5 should display integrated system safety, cost, schedule, and performance risks; this is important because the handling/mitigation of system safety risks can often increase cost, schedule, and performance risks, and vice versa."

should be used for risk prioritization on a particular program. (Each program must thus choose one of the above two time-frame definitions and use it consistently.) Holding all else constant, a risk with a shorter time-frame should have a higher priority than another risk with the same (p, c) score but a longer time-frame. Inter-relationship with other risks corresponds to the degree of overlap of the risk in question with other approved risks. Holding all else constant, the more risks that a particular risk overlaps with at a given risk level, the higher its priority should be.

The prioritization approach should consider the following:

1) Compute the risk factor (risk score), which is Risk Factor = Probability * Consequence_{max}
2) Estimate the frequency of occurrence, time-frame, and inter-relationship with other risks
3) Apply the estimates in 2) as an ordered "tie breaker" should two risks have the same risk score. A structured measure, such as multivoting, decision matrix (matrix diagram, prioritization matrix), and similar methods is preferable to unstructured, subjective rankings (often nothing more than guesses) [32] (pp. 317-324, 383-389, and 391-398). However, results from structured prioritization tools are only as good as the quality of inputs provided. If such techniques are used by uninformed analysts, then the results may have a non-trivial random and/or bias noise term which defeats the value of using the methodologies.

More elaborate applications of combining the risk factor and supplemental criteria can be derived but this is beyond the scope of this Risk Management Process Guide document.

4.4 Cost and Schedule Risk Analyses

Cost and schedule risk analyses should be performed using a Monte Carlo simulation of an approved cost estimate and deterministic schedule network (usually involving most likely cost and schedule estimates, respectively. [39] [40] Performance risk analyses are not addressed here because of their widely varying model structure and complexity.[41] One or more probability

[39] An extensive discussion of performing cost, performance, and schedule Monte Carlo simulations is not included in this Risk Management Process Guide document. See reference [20] (Chapter 5) for an overview of cost and schedule risk analysis simulations. See reference [33] for a detailed treatment of performing cost risk analysis simulations. For additional information on performing Monte Carlo simulations, see reference [34]. For additional information on probability distribution characteristics, see reference [35].

[40] Ideally, a cost and schedule risk analysis can be conducted jointly or the impacts of one variable considered when estimating the other variable. However, the inter-relationship between cost and schedule also involves performance and a variety of constraints, and is far more complex than typically considered or modeled [7] (Chapter 1).

[41] Various types of performance risk analysis are also appropriately analyzed using Monte Carlo simulations, but such a discussion is beyond the scope of this Risk Management Process Guide document. Air Force Pamphlet 63-128 states in Section 12.2.4.5.4.1 [4] (pg. 95):

> "Performance Risk Assessment (PRA). A PRA is a process that uses statistical techniques to quantify the performance impact of the modeled item. PRAs are used to evaluate a wide variety of potential complex risks, including but not limited to predictions of: dynamic stability of control systems, missile accuracy, satellite gap analysis vs. time, and timing closure on application specific integrated circuits (ASICs). Each PRA may have a different model structure and resulting output, depending upon the engineering discipline."

distributions which reflect estimating uncertainty and risk (e.g., technical risk) are then assigned to each relevant cost or schedule activity and outputs are chosen to evaluate probabilistic results (e.g., total development cost or the unit delivery date).[42] The simulation is run until (ideally) a smooth probability density function (PDF, analogous to a histogram) is achieved for the selected outputs. The resulting estimated cost with risk and schedule with risk outputs are evaluated at selected percentiles (e.g., 50th, 80th). The cost with risk at the selected percentile provides an estimate of cost risk coupled with the sum of the most likely estimates. Hence, subtracting the sum of the most likely estimates yields the cost risk estimate at the desired percentile. Likewise, the difference between the estimated schedule item (e.g., delivery date) with risk and the deterministic schedule estimate for that item provides the schedule risk at the desired percentile. In addition, the resulting schedule probabilistic critical path should also be examined to determine the percent of time: 1) the deterministic critical path activities are on the probabilistic critical path and 2) activities not on the deterministic critical path appear on the probabilistic critical path.[43] Cost risk and schedule risk simulations are affected by the probability distributions chosen for selected tasks and the underlying model structures used. For cost risk simulations this usually entails verifying not only the inputs (e.g., labor rate, materials) but how they are entered into the model, verifying that the model subtotals and totals have been correctly specified, etc. It is far easier to accomplish this ahead of time than when actual program simulations have to be performed. Put another way, it is often very difficult to examine simulation output and decide if the underlying model was correctly specified. This problem is all the more complex with schedule risk analyses when the underlying deterministic model can involve 10,000 to 50,000 or more activities. (See Appendix A for some rules of thumb for verifying deterministic schedule quality. These heuristics, or similar ones that may encompass more schedule characteristics, are necessary but not sufficient in and of themselves for verifying schedule quality. See Appendix B for some additional considerations on performing Monte Carlo simulations.)

Three-point estimates are often *required* for performing a schedule risk analysis (SRA) [36] (pg. 26), and in some cases a cost risk analysis. However, any requirement to "force-fit" a specific distribution type on data rather than estimating a potential distribution type from the data may lead to substantial errors. (At a minimum the selection of a specific data type should be identified and documented in the assumptions developed for the simulation.) See Appendix B for additional information.

---

[42] One or more probability distributions are used to model uncertainty and risk for a given element (whether cost or schedule). Thus, for a cost risk example, in the most detailed case one probability distribution could be assigned to cost estimating uncertainty, a second to schedule risk, and a third to technical risk, etc. However, this is often times limited by: 1) the level of knowledge associated with uncertainty and risk, and 2) the capabilities of the tool in performing the modeling. [For example, in some cost risk and schedule risk simulations a single distribution is used to represent estimating uncertainty and all risk components. The resulting single distribution will only approximate the level of estimating uncertainty and risk present. In addition, some commonly used project scheduling software permits only a single "combined" probability distribution to be used without the use of a complex macro implementation (which may not be permitted on government computers due to security considerations), while common spreadsheet software has no such limitation.]

[43] Experience has shown that some schedule risk analysis software used with large-scale schedules containing many thousands of activities and probability distributions may not sometimes properly compute the probabilistic critical path. The probabilistic critical path, along with all other simulation results, should be carefully examined to determine if the information is reasonable or potentially erroneous.

Note: estimating the product of probability of occurrence and cost consequence ("dollarization") may not yield meaningful results because the results are typically derived from : 1) point estimates (not distributions) of both probability of occurrence and cost consequence values, and 2) the quality of the resulting estimate inputs may not be adequate. A more meaningful approach is to perform a cost risk analysis over either a single program cost or all program costs and examine the resulting cost risk dollars at the desired percentile value (as discussed above). While the latter approach can potentially produce more accurate results, the quality of these results as in the "dollarization" case is strongly dependent on the quality of the input cost model and the associated probability distributions encompassing cost estimating uncertainty and cost risk. Finally, this type of analysis should be performed on all three critical dimensions: cost, performance, and schedule. Simply performing the analysis on the cost dimension will lead to incomplete, if not misleading results.

4.5 Documentation

When using probability and consequence scales, document the probability score (and rationale for that score), together with the consequence scores and associated rationale for cost, performance, and schedule consequence in the risk management database. Inputs, assumptions, and results from other risk analyses (e.g., Monte Carlo simulations, decision analyses) should also be documented and included if possible in the risk management database. All other risk analysis results (e.g., sensitivity and uncertainty analyses) should also be documented and stored in an appropriate manner as well.

5.0 Risk Handling

"Risk handling (planning and implementation) is the process that identifies, evaluates, selects options then develops and implements approaches to reduce risk to an acceptable level given program constraints and objectives. This includes the specifics on what should be done, when it should be accomplished, who is responsible, associated available resources, etc." [4] (pg. 102) (As previously mentioned, risk handling is an all-encompassing term whereas risk mitigation is one option of the five available risk handling options.) Risk handling includes specific methods and techniques to deal with known risks and a schedule for accomplishing tasks, identifies who is responsible for the risk area, and provides an estimate of the resources and schedule associated with handling the risk, if any. Risk handling can be applied to a broad list of risk categories (see Section 2.2), and is not solely limited to technical risks.

5.1 Risk Handling Options

The five risk handling options are assumption, avoidance, control (commonly called mitigation), transfer, and monitor. All risk handling options except for assumption and monitor can potentially reduce the probability of occurrence and/or consequence of occurrence.[44] Each option will now be briefly addressed. [Material contained in this sub-section for the assumption, avoidance, control (mitigation), and transfer options is extracted from [20] (Chapters 2, 5).]

5.1.1 Risk Assumption

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

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it occurs. This includes identifying the specific management actions (such as re-testing, additional time for further design activities) that are needed.
- Ensure that necessary administrative actions are taken to identify a management reserve to accomplish those management actions.

5.1.2 Risk Avoidance

Risk avoidance involves a change in the concept, design, requirements, specifications, and/or practices that can reduce the risk to an acceptable level. Simply stated, it eliminates the sources of high and/or medium risk and replaces them with a lower risk solution. The avoidance option can be used to reduce the probability and/or consequence of occurrence terms. Generally, the avoidance option may be done in parallel with the up-front requirements analysis, supported by cost/ requirement trade studies, etc.

5.1.3 Risk Control

Risk control (mitigation) does not attempt to eliminate the source of the risk but seeks to reduce the risk to an acceptable level. The control option monitors and manages the risk by reducing the probability and/or consequence of occurrence terms. This option may add to the cost of a program. However, in many cases the net result is a potential cost and/or schedule reduction vs. if the risk had actually occurred. (In some cases the control option may be necessary even when the resulting benefit/cost ratio is < 1 when the risk must be averted and the other options would

---

[44] In some cases one or more components of the estimated consequence of occurrence term have already been realized or will be realized in the foreseeable future. Here, only the probability of occurrence term can potentially be reduced. Risk analyses should be performed and updated examining both the probability and consequence terms for each risk: 1) prior to developing a risk handling plan (RHP) (Section 4), 2) for each activity contained in the RHP (Section 5.3), 3) as part of risk monitoring the RHP implementation progress and feedback of observed information to the risk analysis process step (Section 6), and 4) throughout the course of the program (both at regularly scheduled intervals, and on an as needed basis).

not yield adequate results.) Examples of control (mitigation) option implementation approaches include, but are not limited to:

- Multiple Development Efforts. Create competing systems in parallel that meet the same performance requirements.
- Alternative Design. Create a backup design option that uses a lower risk approach.
- Trade Studies. Arrive at a balance of engineering requirements in the design of a system.
- Early Prototyping. Build and test prototypes early in the system development.
- Incremental Development. Design with the intent of upgrading system parts in the future.
- Technology Maturation Efforts. Normally, technology maturation is used when the desired technology will replace an existing technology which is available for use in the system.
- Robust Design. This approach, while it could be more costly, uses advanced design and manufacturing techniques that promote quality through design.
- Reviews, Walk-throughs, and Inspections. These three actions can be used to reduce the probability/likelihood and potential consequences/ impacts of risks through timely assessment of actual or planned events.
- Design of Experiments. This engineering tool identifies critical design factors that are sensitive, therefore potentially high risk, to achieve a particular user requirement.
- Open Systems. Carefully selected commercial specifications and standards whose use can result in lower risks.
- Use of Standard Items/Software Reuse. Use of existing and proven hardware and software, where applicable, can substantially reduce risks.
- Use of Mock-ups. The use of mock-ups, especially man-machine interface mock-ups, can be used to conduct early exploration of design options.
- Modeling/Simulation. Modeling and simulation can be used to investigate various design options and system requirement levels.
- Key Parameter Control Boards. The practice of establishing a control board for a parameter may be appropriate when a particular feature (such as system weight) is crucial to achieving the overall program requirements.
- Test, Analyze, and Fix (TAAF). TAAF is the use of a period of dedicated testing to identify and correct deficiencies in a design.
- Demonstration Events. Demonstration events are points in the program (normally tests) that determine if risks are being successfully abated.
- Process Proofing. Similar to Program Metrics, but aimed at manufacturing and support processes which are critical to achieving system requirements. Proofing simulates actual production environments and conditions to insure repeatedly conforming hardware and software.

5.1.4 Risk Transfer

Risk transfer may reallocate risk from one part of the system to another (e.g., between different units, between hardware and software), thereby reducing the overall system risk, or redistributing risks between the Government and the prime contractor or within Government organizations; or between members of the contractor team.[45] It is an integral part of the functional analysis process. In many cases the transfer option is a form of risk sharing and not risk abrogation on the part of the Government, and it may influence cost objectives (e.g., by the use of implementation approaches such as insurance, guarantees, warranties). An example implementation approach is the transfer of a function from hardware implementation to software implementation or vice versa. The avoidance option can be used to reduce the probability and/or consequence of occurrence terms. The effectiveness of risk transfer depends on the use of successful system design techniques. Modularity and functional partitioning are two design techniques that support risk transfer. In some cases, risk transfer may concentrate risk areas in one part of the design. This allows management to focus attention and resources on that area.

5.1.5 Risk Monitor [4] (pg. 102)

Risk monitor takes "no immediate action but watch for changes." (The monitor option does not directly reduce the probability and/or consequence of occurrence terms.) "Recognize what is monitored (i.e., Technical Performance Measures (TPMs) and production rates) and the threshold or trigger event that initiates additional (non-monitoring) handling actions." While the monitor option may be appropriate for relatively short periods of time, it may not be appropriate when risks with complex attributes exist and insufficient time and/or associated resources are available to successfully implement the subsequent handling strategies.[46]

5.2 Developing the Risk Handling Strategy

A risk handling strategy, composed of a risk handling option and an implementation approach, is developed and implemented for all medium and high risks and selected low risks (designated by the RMB) [20] (Chapter 5), [7] (Chapter 7). All five risk handling options (assumption, avoidance, control, transfer, monitor) are evaluated with regards to cost, performance, schedule, and risk, associated trades performed, and the "best" option selected for each risk. For example:

- Can the risk handling strategy be feasibly implemented and still meet the user's needs?
- What is the expected effectiveness of the risk handling strategy in reducing program risk to an acceptable level?
- Is the risk handling strategy affordable in terms of dollars and other resources (e.g., use of critical materials, test facilities, etc.)?
- Is time available to develop and implement the risk handling strategy, and what effect does that have on the overall program schedule?
- What effect does the risk handling strategy have on the system's technical performance?

---

[45] While the transfer option is often used during concept development process it should also be considered throughout the development process (e.g., which side of an interface should an update be applied to prior to qualification testing).

[46] In the worst case when a decision regarding the course of action is made it may not be possible to implement one or more desired risk handling strategies to resolve the risk in a timely manner. This type of situation has occurred on more than one SMC programs.

Given the option chosen, an implementation approach is then selected for each risk again based upon evaluating cost, performance, schedule, and risk, and performing associated trades. Additional trade measures can also be developed, such as a cost/benefit ratio associated with each implementation approach. Similar analyses can also be conducted for schedule and performance.

It is also possible that a risk handling strategy can employ a hybrid method that may include a combination of up to all five risk handling options, and not be solely limited to a single option.

Multiple risk handling strategies can also be developed and performed in parallel for the same risk (or contingent on intermediate progress), as warranted. While the additional risk handling strategy(ies) may have the same (or different) option as the primary strategy, the implementation approach will be different in each case. If the risk handling strategies do not all execute in parallel, then an objective, measureable trigger event needs to be defined for each contingent risk handling strategy that will provide unambiguous evidence that: 1) the contingent strategy should be executed, and 2) when the strategy execution should begin.

5.3 Developing and Documenting the Risk Handling Plan

After a risk handling strategy has been chosen, the risk handling plan (RHP) must be developed and documented. The risk POC is responsible for evaluating and recommending to the RMB the risk handling strategy and the associated RHP that is best suited for a given risk. The final RHP should include the following elements:

- The RHP POC name (typically the risk POC), IPT, IPT Lead name, initial plan date (with an electronic revision sheet for changes).
- A description of the risk to which the RHP applies. The risk handling description should include: what has to be done, the required level of effort, and all assumptions used in developing the handling activities. Specific attention should be paid to risk handling activities that require resources outside the scope of a contract and other RHPs that may be affected.
- A summary of the risk handling option(s) selected and the implementation approach selected, and why the option(s) and approach were selected.
- Detailed RHP activities, including the specific actions that are planned for reducing the level of the risk or eliminating it (when possible). The activities should represent non-baseline work performed on the program (in addition to baseline work), The activities should also be active rather than passive in nature. (For example, attending meetings or holding telecons are often not suitable risk handling activities.) Additional key criteria that should be applied to all risk handling activities and their descriptions include the following, the activity statements should: 1) be objective not subjective; 2) be clearly worded (and not contain acronyms); and 3) have measurable outcomes (see next item for additional information). The results from examining and re-writing hundreds of risk handling activity statements at SMC reveal that far more than 50% violate one or more of the three criteria

mentioned above[47] [48]. Meeting the above criteria is "necessary but not sufficient" as the technical content, programmatic perception, associated resources, etc. must still be satisfactory. However, it is equally clear that poorly written risk handling activity statements can cause confusion and reflect poorly on the program and Directorate in question as reviewed by SMC, other Air Force, and Department of Defense leaders.

- Each risk handling activity should have a specific measurable outcome for assessing whether/not each planned action was successfully completed (also known as "exit criteria"). It is important that measurable criteria be developed for each risk handling activity so that achievement of the activity requirements can be unambiguously determined. (While the criteria may not necessarily be quantitative, it must be specific and measureable.)
- Each risk handling activity should ideally use the Finish-to-Start precedence and be sequential with subsequent activities (e.g., activity "n + 1") not starting prior to completing activity "n".
- Include suitable metrics when possible which will be used as part of risk monitoring to evaluate actual vs. planned progress associated with the implemented RHP . Cost, performance, and schedule metrics, along with risk (generally including both probability and consequence of occurrence) should be selected when possible to track risk handling implementation progress. Typical metrics include cost variance (cost), schedule variation (schedule), and technical performance measurements (TPMs, performance) along with risk level. These metrics should be evaluated at pre-determined times to gauge actual vs. planned progress for each risk handling activity as well as the overall progress in reducing the risk to an acceptable level.

The specific risk handling activities (actions) should include the following information:

- Estimated amount of resources required to execute the specific actions (including but not limited to budget, personnel, capital equipment, procured equipment, facilities and ranges) and a cost estimate
- A proposed schedule for accomplishing the actions [start date, time phasing of significant risk reduction activities, finish date, relationship to significant activities/milestones, appropriate resource loading, and an appropriate precedence (e.g., Finish to Start precedence) and network logic (e.g., appropriate predecessors and successors, and no hard constraints, such as "finish no later than")] should also be developed for each resulting risk handling activity. When possible, risk handling activities should be defined at a level that permits day-to-day execution.

[47] For example, delivering a document is insufficient in and of itself to close a risk handling activity. A key question is did the customer for this document subsequently approve or reject it? And if approved, were there critical liens that would prevent execution of the subsequent ("n + 1") handling activity or re-direction that would modify this activity? The original example statement vs. the questions to that statement illustrate whether/not the activity description has a suitable measurable outcome.

[48] Risk handling activity descriptions provided by program contractors may sometimes be written "as if" they are marketing claims and/or without appropriate justification. This style of risk handling activity statement should be rejected and re-written by the program contractor to make them fact-based, objective, clearly stated, and including a measurable outcome.

- Probability and consequence ratings for the risk upon the start and (successful) completion of each activity
- Possible secondary risk handling plans or contingency plans to handle the risk and the associated triggering milestone/dates for implementing those plans
- Whether each activity is just now being proposed or is already part of the program plan. (Only costs associated with new, unfunded activities should be considered in determining the total cost of the RHP.)
- The risk handling POC assigned to each specific handling activity. (Ideally this is a single POC to ensure accountability, but in some cases for complex risks more than one POC may be needed.)

Upon completing a draft RHP, the plan and its activities should be reviewed by the appropriate IPT Lead and risk manager, then the RMB to determine whether/not it will accomplish the desired risk handling strategy (to the degree that can be foreseen at the time it's prepared), and support resource and other program decisions. Unfocused, non-specific, or inadequately or inefficiently resourced RHPs will generally have little chance of being successfully executed, may waste scarce resources, and may foreclose the ability to reduce the associated risk to an acceptable level in a timely manner.

The POC should work with all stakeholders to coordinate handling efforts. The RHP and subsequent actual vs. planned progress should be documented in the risk management database by the risk POC.

5.4 Integration of Risk Handling Activities with the IMS

It is essential that the risk handling activities be integrated with the program IMS. Ideally, all risk handling activities should be entered into the IMS with an annotation that associates the activities' Task ID to a particular step in the RHP. (It may be permissible to only enter the handling activities for each risk that will potentially lead to a reduction in risk level, or probability or consequence values. However, this is generally not desirable because it may prevent identifying potential shortfalls of precursor activities and their resources that can lead to a slip in the risk reduction date or a decrease in the level of risk reduction that can be achieved.) Assigning handling risk reduction steps to a chargeable activity or activities will not only ensure that the RHP's progress against risk reduction is tracked but that there also is some level of accountability for the plan's progress. The program should use the IMS as well as a waterfall/burndown chart to routinely track actual vs. planned progress of each activity in a RHP. An independent review of all risks within the program risk baseline should occur at each milestone review in addition to occurring at other major program decision points.

From an implementation perspective there are two possible ways to integrate the risk handling activities and the IMS. In the first approach the IMS drives the planned start and finish dates for the activities in each RHP . In the second approach, the start and finish dates for the activities in each RHP drives the IMS. Neither of the two approaches is incorrect, but only one should be selected and used consistently throughout the program. (Using both approaches on the same program will lead to scheduling conflicts.)

5.5 Implementing the Risk Handling Strategy

The final risk handling step is to allocate the resources needed to implement each developed risk handling strategy via its RHP. While this may seem trivial on the surface, it is essential that the RHP be funded and implemented, else risks will not be reduced to the desired level, the "message" sent to program and stakeholder personnel is that the risk management process is a "paper tiger," and the result will be ineffective risk management.

As mentioned in Section 5.3, when a risk handling strategy is implemented, activity "n + 1" should not be started until activity "n" has been successfully completed, unless a precedence method other than Finish-to-Start has been previously approved (and this is the "exception to the rule"). Otherwise, the danger is that hurried and potentially incorrect decisions may be made that an activity is complete in order to start the next activity. (This is all the more problematic when a weak or subjective exit criteria exists for a given activity.) Initiating follow-on activities (e.g., "n + 1") before the current activity (e.g., "n") is complete, or when the current activity is "claimed" to be complete but it actually isn't complete can contribute to problems and inefficiencies occurring if the results associated with the current activity (e.g., "n") later prove contrary or different than anticipated, which may then lead to adjusting the characteristics of one or more follow-on activities (e.g., "n + 1") after they have already started. Similarly, having multiple activities performed at the same time (unless a parallel approach is specifically desired) can lead to potential difficulties. (The above discussion is hardly academic and has contributed to re-baselining actual programs.) This points to the need to carefully examine, if not challenge, information collected for each risk handling activity so that the results are clearly understood and serve as unambiguous inputs for decision makers.

5.6 Charting Risk Handling Results

Actual vs. planned progress of implemented risk handling plans are typically represented by a graphical waterfall/burndown chart—this is a common approach used by both Government and industry on a wide variety of Air Force and other programs. Active Risk Manager generates a waterfall/burndown chart based upon handling activity descriptions, corresponding start and finish dates, risk scores, etc. that are entered by a user. In cases where ARM cannot be used, waterfall/burndown charts can be generated manually with a set of templates or by programming the graphical and database capability contained in Microsoft Excel.[49]

A typical risk handling waterfall/burndown chart shows actual vs. planned risk score (probability times consequence) on the y-axis (ordinate) and time (e.g., month, quarter, year or date) on the x-axis (abscissa). The green (low risk), yellow (medium risk), and red (high risk) waterfall chart boundaries should match the (p, c) boundaries contained in the Air Force risk matrix given in

[49] Both the Air Force and support contractor team, as well as program contractors should be expected to generate waterfall/burndown charts, and other graphical representations of program risks (e.g., a suitably populated 5x5 matrix). This capability should also be explicitly included in Request For Proposals, and subsequent contractual language for both support and program contractors.

Figures 4-1 and 4-2. Since risk scores are commonly derived from ordinal scales, cardinal interpretations between score values should not be attempted (e.g., a probability times consequence risk score of 20 is not twice the risk as a score of 10 because the true cardinal probability and consequence coefficients are unknown). See Section 4.2 for additional information. Also note that the waterfall/burndown graphic results are two-dimensional with actual versus planned values associated with both risk score (or level) and time. Hence, if referring to the results in a text format the risk score (or level) and time must be separately described—having a single text representation of risk handling progress can be confusing and lead to an erroneous interpretation. For example, the actual risk score can be above, on, or below the anticipated value (sometimes represented by an up, sideways, or down arrow, respectively), and time can be behind schedule, on schedule, or ahead of schedule (again, sometimes represented by an up, sideways, or down arrow, respectively). Finally, it should be recognized that a waterfall/burndown chart is not a panacea—its quality is only as good as the information used to populate it.

6.0 Risk Tracking

Risk tracking, commonly called risk monitoring, is the process that systematically tracks and evaluates the performance of risk handling actions against established metrics throughout the acquisition [20] (Chapter 5). Risk tracking is not a problem-solving technique, but rather, a proactive technique to observe the results of risk handling. By monitoring implementation of RHPs at specific intervals (rather than on an ad hoc basis), it feeds back these results, as shown in Figure 2-1, to update RHPs as necessary, re-analyze existing risks, identify new facets of an existing risk, and update risk management planning considerations (e.g., risk categories, ground rules and assumptions) as warranted.

As mentioned in Section 5.3, cost, performance, and schedule metrics should be developed and included in the RHP when possible to track risk handling progress once the strategy is implemented.[50] Note: these metrics are in addition to top-level risk management metrics that are typically collected and reported (e.g., the number of low, medium, and high risks, the number of risks with implemented handling/mitigation plans that are on/ahead/behind plan in schedule and risk level).

6.1 Tracking Risk Handling Plan Activities

Risk tracking involves the following activities:

1. Tracking of the approved RHP and risk handling activity completion criteria.
2. Updating the program risk management database.

[50] As mentioned in Section 5.3, typical metrics include cost variance (cost), schedule variation (schedule), and TPMs (performance) along with risk level.

Tracking RHP activities includes not only monitoring the completion of the defined risk handling activity but also monitoring the risk reduction achieved, if any, by each activity. (This evaluation is typically performed by the risk owner.) The RHP should reflect the anticipated effect that each handling activity should have on reducing the risk to an acceptable level. When implemented, it is important to examine actual vs. planned progress in both completing risk handling activities in terms of schedule as well as risk via the IMS and a waterfall/burndown chart. (For example, did the activity complete behind, on, or ahead of schedule? Was the resulting risk score and level above, on, or below the anticipated value?) Risk owners and their IPT leads should be prepared to discuss at a RMB all risk handling activities that are either late or that lead to an increased, rather than decreased risk level. In addition, risk owners and their IPT leads should be prepared to discuss at a RMB the ability to successfully complete all risk handling activities that are planned to complete within the next two months to determine if any additional resources are needed to enable the activities to close on-time and at the desired risk level.

Any event that causes significant change(s) to the system design, IMS, or acquisition strategy should trigger a re-evaluation of all risks.

6.2 Establishment of Management Indicators (Metrics)

The effectiveness of the risk tracking process may depend on the establishment of a management indicator system (metrics) that provides accurate, timely, and relevant risk information in a clear, easily understood manner (in addition to feedback to the other risk management process steps) [20] (Chapter 5). The metrics selected to monitor program status must adequately portray the true state of risk events and handling activities, otherwise the indicators of risks that are about to become problems will often remain undetected.

Some high-level monitoring techniques that can be adapted to become part of a risk indicator system include, but are not limited to [20] (Chapter 5):

- **Earned Value (EV)**. This uses standard DoD cost/schedule data to evaluate a program's cost and schedule performance in an integrated fashion. As such, it provides a basis to determine if risk handling actions are achieving their forecasted results. (However, variations in actual vs. planned schedule are preferable to schedule variance, since schedule variance is a cost estimate of schedule.)
- **Program Metrics**. These are used for formal, periodic performance assessments of the various development processes, evaluating how well the system development process is achieving its objective.
- **Test and Evaluation (T&E)**. A well-defined (T&E) program is a key element in monitoring the performance of selected risk handling options and developing new risk assessments.

6.2.1 Program Metrics

The program should establish metrics that measure the effectiveness of their implemented risk handling strategies. Additional metrics can be used to examine the overall effectiveness of the risk management process: For example:

1) The number of high, medium, and low risks identified, and how this varies with time.
2) Number of RHPs whose activities are on schedule, behind schedule, and ahead of schedule.
3) Number of RHPs whose activities have a risk level is above, on, or below predictions.
4) Number of high and medium risks with and without implemented plans.
5) Frequency of new risk identification (following comprehensive risk identification).

While high-level metrics that examine the overall risk management process can be helpful, they can also be abused when valid data is not available to support the results. For example, one might consider a program with 10 high risks to be a higher risk program than another program with two high risks. However, a single high risk or even one medium risk that actually occurs can have considerable adverse impact to the program, and thus render the high-level metric comparison meaningless. (Similarly, the number of weeks a RHP activity is behind schedule is not meaningful without knowing how much free slack to the next task and total slack to the completion need exists.) Another example is placing numeric values in the individual cells of the risk matrix (Figure 4-2) beyond the identifier values associated with these cells (e.g., Probability (P) = 5 and Consequence (C) = 5 or P * C = 25 for the upper right hand corner of the matrix). A variety of non-linear schemes can be used to indicate a measure of the program's overall risk level associated with summing (or using a weighted sum) across the total number of risks. However, such measures typically have no statistical or probabilistic basis, which is evident when one realizes that the cells contained in the risk matrix are ordinal (e.g., 1, 2, 3, 4, and 5 for P and C), not cardinal, and adding (or performing other operations on) ordinal numbers does not yield a cardinal result.

7.0 References

[1] Robert Charette, Laura Dwinnell, and John McGarry, "Understanding the Roots of Process Performance Failure," *CROSSTALK: The Journal of Defense Software Engineering*, August 2004, pp. 18-24.

[2] Warren Scheinin, "Start Early and Often: The Need for Persistent Risk Management in the Early Acquisition Phases," Paper to the Aerospace Corporation/Air Force SMC/NASA Seventh National Symposium on Space Systems Engineering & Risk Management Conference, 27-29 February, 2008.

[3] Space and Missile Systems Center, SMC T-005, "Tailoring of Risk Management Requirements in SMC-S-001 (2013)," 27 January 2014.

[4] Department of the Air Force, *Integrated Life Cycle Management*, Air Force Pamphlet 63-128, 10 July 2014.

[5] Department of the Air Force, *Risk Management*, Air Force Instruction 90-802, 11 February 2013.

[6] Department of the Air Force, *Risk Management*, Air Force Instruction 90-802, Air Force Space Command Supplement, 30 July 2013.
[7] Edmund H. Conrow, *Effective Risk Management: Some Keys to Success*, Second Edition, American Institute of Aeronautics and Astronautics, 2003.
[8] Department of Defense, *System Safety Program Requirements*, MIL-STD-882C, 19 January 1993.
[9] Department of Defense, *Standard Practice for System Safety*, MIL-STD-882D, 10 February 2000.
[10] Department of Defense, *Standard Practice for System Safety*, MIL-STD-882E, 11 May 2012.
[11] Air Force Space and Missile Systems Center, *Tailoring Instructions for MIL-STD-882E*, SMC-T-004, 30 November 2012.
[12] Air Force Space and Missile Systems Center, *The SMC System Safety Program*, Space and Missile Systems Center Instruction 63-1205, 28 June 2011.
[13] Department of Defense, *Risk Management Guide for DoD Acquisition*, Sixth Edition, August 2006.
[14] Department of the Air Force, *Life Cycle Risk Management*, Air Force Material Command Pamphlet 63-101, 27 April 2011.
[15] Edmund H. Conrow, "Risk Management for Space Systems." Paper to the Aerospace Corporation/Air Force SMC/NASA Seventh National Symposium on Space Systems Engineering & Risk Management Conference, 27-29 February, 2008.
[16] Harold Kerzner, *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, Eleventh Edition, Wiley, 2013.
[17] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk." *Econometrica.* 47(2), March 1979, pp. 263-292.
[18] "Risk Management." in BKCASE Editorial Board. 2014. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 1.3. R.D. Adcock (EIC). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. Accessed 29 August 2014. www.sebokwiki.org. BKCASE is managed and maintained by the Stevens Institute of Technology Systems Engineering Research Center, the International Council on Systems Engineering, and the Institute of Electrical and Electronics Engineers Computer Society.
[19] Edmund Conrow and Robert Charette, "Opportunity Management: Be Careful What You Ask For." Defense AT&L, March-April 2008, pp. 16-19.
[20] Defense Acquisition University, *Risk Management Guide for DoD Acquisition*, Fifth Edition, Version 2, June 2003.
[21] IBR document pp. 9-10. Department of Defense, *The Program Managers' Guide to the Integrated Baseline Review Process*, April 2003.
[22] National Institute of Standards and Technology, "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST Special Publication 800-37, Revision 1, February 2010.
[23] Department of Defense, DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," 12 March 2014.
[24] Department of the Air Force, *Integrated Life Cycle Management*, Air Force Instruction 63-101/20-101, 7 March 2013 (incorporating through Change 1, 21 March 2014).
[25] Department of Defense, *Transition from Development to Production*, DoD 4245.7-M, September 1985, plus Change 1, 13 February 1989.

[26] Defense Acquisition University, *U. S. Department of Defense Extension to: A Guide to the Project Management Body of Knowledge*, Defense Acquisition University, Version 1, First Edition, June 2003.
[27] Department of the Air Force, *Risk Identification, Integration, and Ilities (RI3) Guidebook*, Version 1.2, 15 December 2008.
[28] Air Force Space and Missile Systems Center; *SMC Systems Engineering Primer and Handbook*, Third Edition, 29 April 2005 (July 2005 Revision).
[29] "The Toyota Production System, The "Thinking" Production System: TPS as a winning strategy for developing people in the global manufacturing environment," Discussion by Mr. Teruyuki Minoura, Toyota's managing director of global purchasing, 2003 Automotive Parts System Solution Fair, Tokyo, Japan, 18 June 2003. Retrieved on 16 August 2014 from: http://www.toyotageorgetown.com/tpsoverview.asp
[30] National Institute of Standards and Technology, "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST 800-37 SP, Revision 1, February 2010.
[31] International Organization for Standardization, "Space systems - Risk Management," ISO 17666, Edition 1, 1 April 2003.
[32] Audrey Dorofee, et al., *Continuous Risk Management Guidebook*, Software Engineering Institute, Carnegie Mellon University, 1996.
[33] Air Force Cost Analysis Agency, *Cost Risk and Uncertainty Analysis Handbook,* April 2007.
[34] Averill M. Law, *Simulation and Modeling*, Fourth Edition, McGraw Hill, 2007.
[35] Merran Evans, Nicholas Hastings, and Brian Peacock, *Statistical Distributions*. Third Edition, New York, NY: Wiley-Interscience, 2000.
[36] OUSD (AT&L) PARCA, DI-MGMT-81861, "Integrated Program Management Report (IPMR)," 6 June 2012.
[37] National Defense Industrial Association (NDIA), Industrial Committee for Program Management (ICPM), Program Planning & Scheduling Subcommittee (PPSS), *Planning & Scheduling Excellence Guide (PASEG)*, Published Release Version 2.0, Public Release, 22 June 2012, pp. 135-136.
[38] National Defense Industrial Association (NDIA), Briefing of the Program Management Systems Committee, Scheduling Working Group, 22 May 2009.
[39] Department of Defense, "Integrated Master Schedule," OUSD(AT&L)ARA/AM(SO), DI-MGMT-81650, 30 March 2005.

Appendix A

Some "Rules of Thumb" Associated with Schedule Quality

Some common "rules of thumb" should be applied to checking a schedule before performing a schedule risk analysis. These schedule checking "rules of thumb" include, but are not limited to: [15], [37], [38]

1) Project tasks should be well specified (e.g., do they accurately describe the project scope?).
2) Project tasks should have reasonable durations and resources applied to them (e.g., are they believable?).
3) The schedule should contain few if any constraints—ideally the initial task can be "start no earlier than," or "start no later than," and all other tasks should be "as soon as possible." (These are known as soft constraints.) Constrained durations or milestones (e.g., "must finish on" or "finish no later than" for a delivery date, known as hard constraints) will often lead to erroneous results whether/not that particular task is being modeled as a potential schedule risk analysis output. (For example, if the task is on the probabilistic critical path then it may affect a number of other "downstream" tasks on this path.) *Even a single "must finish on" or "finish no later than" constraint on a delivery milestone or tasks directly upstream of a delivery milestone on the probabilistic critical path can completely invalidate schedule risk analysis results for the selected milestone.*
4) The schedule should contain few if any open ended tasks other than the initial (start) task and the project complete (finish) task. All other tasks should have one or more predecessors and successors.
5) The schedule should not contain broken schedule logic with either missing dependencies or where downstream tasks are updated but upstream tasks are not updated.
6) The underlying schedule logic should accurately represent how the project will be executed (e.g., not contain out of sequence tasks).
7) The schedule should not contain tasks linked by anything (ideally) other than Finish-to-Start precedence.
8) The schedule should not contain tasks linked with positive or negative lags.
9) The schedule should not contain tasks linked with leads.
10) The schedule should not have forecast dates prior to or actual dates after the current status date.
11) The schedule critical path should not have negative total float.
12) Resource loading should be applied to all tasks other than milestones and summary tasks
13) Schedule tasks should not have large durations (> 2 months), nor large positive float (> 2 months), nor negative float (< 0 days).
14) All tasks should flow up to corresponding summary tasks.
15) Summary tasks should not contain logic linking them to other schedule tasks.
16) The schedule should be regularly updated and current when performing a schedule risk analysis.
17) The schedule risk analysis software as interfaced with the scheduling software performs as expected (e.g., no crashes and unanticipated results with known test cases).

Use the above "rules of thumb," modify and add to them as appropriate for your program. The important thing to remember is that without performing a careful check prior to running a schedule risk analysis, the results may be flawed and adversely affect decisions that are subsequently made. It is far better to correct the underlying schedule errors and limitations than to generate and blindly use erroneous results.

Appendix B

Guidelines for Performing Monte Carlo Simulations

A few simple guidelines are presented here for setting up and running Monte Carlo simulations. More detailed examinations of specific subjects (e.g., cost risk analysis, selecting probability distributions) can be found in the literature [33], [15], [34]).

1) If the entire project file is too large or contains too many subprojects or segmented files to run a schedule risk analysis (SRA), consider creating a single flat file that includes all tasks within a specified number of days of the project's critical path. While 20 work days (one calendar work month) is sometimes used, this number may be too restrictive. Instead try using 60 work days to preclude eliminating potential secondary critical paths from the analysis.[51]

2) Develop a "Rosetta Stone" translation table that shows the fields used for storing risk-related information in the host file; particularly when SRAs are performed. This table should ideally be clearly documented and saved in an file that is easy to access by any potential user. (In some applications this can amount to 10 or more fields that need to be reserved to properly run the simulation.) While this may be unnecessary for standalone or spreadsheet applications, it can be very important for SRAs that rely upon reserved fields contained in the underlying schedule software application. It is both important that the necessary fields for the simulation can be located by the simulation software, and that risk-related information does not over-write fields used to store other critical information associated with either the deterministic or Monte Carlo applications.

3) While "three-point" estimates (e.g., low, most likely, and high) are commonly used for convenience in developing probability distributions (e.g., triangle and beta PERT) for cost and schedule Monte Carlo simulations, the three-point estimate and associated probability distributions are not a panacea and can erroneously misrepresent the potential risk present for a given element. The potential error is that not all data, even continuous data, can be modeled by a three-point estimate. Thus, requiring a three-point estimate "force-fits" a distribution that may be inappropriate and lead to erroneous simulation results.[52]

---

[51] Note also that projects containing a moderate to large number of subprojects or segmented files may prevent some commercial software packages from properly initializing and running the SRA.

[52] Three-point estimates are required per DI-MGMT-81650 [39], Section 2.4.1.23, pg. 5) when performing a schedule risk assessment under the following circumstances:

> "Three-point estimates shall be developed for remaining durations of remaining tasks/activities that meet any of the following criteria: (1) critical path tasks/activities, (2) near-critical path tasks/activities (as specified in the CDRL), (3) high risk tasks/activities in the program's risk management plan. These estimates include the most likely, best case, and worst case durations. They are used by the contractor to perform a probability analysis of key contract completion dates. The criteria for estimated best and worst case durations shall be applied consistently across the entire schedule and documented in the contractor's schedule notes and management plan."

For example, if a subject matter expert says that a particular schedule risk can be modeled as a duration of 0 days for 0 percent probability, 5 days for 20 percent, 8 days for 60 percent, 12 days for 80 percent, and 14 days for 100 percent, how would you model this information? It clearly can't be modeled using a three-point estimate, which requires low, most likely (typically mode), and high values. In this case the most likely value cannot be estimated directly. Attempting to model this data with a three-point estimate by "guessing" a most likely value can lead to considerable error (that varies on a case-by-case basis). Such errors will be present for both triangle and beta PERT distributions, which are common forms of three-point distributions which require low, most likely, and high values. The most appropriate answer in this case is to use a cumulative distribution function (CDF, sometimes known as a general distribution function). Note, however, that many commercial simulation packages do not provide this option.

Finally, at least one commercial simulation package approximates particular continuous distribution types with a three-point estimate (e.g., normal and general beta distributions). The resulting modeled distributions are only approximations performed for computational ease and may introduce errors into the simulation. Because of these considerations, use three-point estimates with caution and do not blindly believe the results. [See item 8) below for additional information.]

4) The number of iterations a simulation should be run depends upon a variety of factors. Two primary considerations are the degree of maturity associated with the simulation and its underlying deterministic model, and the desired use of the resulting output. Immature models may initially be run and the output examined with as little as 25 or even fewer iterations. This should provide insight into potentially abnormal results (outside of the bound of permissible values), interference between the simulation software and the underlying deterministic model, etc. If errors are found with such a small number of iterations they should be fixed to the extent possible before a larger number of iterations are attempted. Next consider a simulation run of 250 to 500 iterations. This may identify other potential errors related to host computer memory usage, memory corruption, etc. that may not appear when a small number of iterations are used. For draft output approximately 500 iterations are desirable to provide sufficient granularity to accurately represent the tails of the resulting modeled output distributions. Otherwise, information near the mean of the output distribution may be acceptable, but results near say the 20^{th} and 80^{th} percentiles or further towards the tails (e.g., 10^{th} and 90^{th} percentiles) may not be accurate and other output characteristics that might exist (e.g., multi modal results) may not be evident. Finally, for final output 500 to 5,000 iterations are desirable to more accurately represent the PDFs and CDFs of selected items. (The number of iterations is sometimes limited by computer throughput, memory, software, time available to run the simulation, and other considerations outside of the underlying model.)

5) Examine the simulation output at the minimum, 20^{th}, 30^{th}, 50^{th}, 70^{th}, 80^{th} and maximum outputs, along with the mean. This should yield sufficient granularity to meet many imposed requirements as well as provide useful insights into the nature of the resulting output. Of course, the above values approximate a CDF that is determined and presented by some simulation packages in either graphical or numeric form. Some simulation packages also contain a "live" percentile estimator that allows the user to input a particular value and the software will then estimate the corresponding percentile for that value (and vice versa).

6) Save the resulting simulation data, both the input and output data, when possible. [In some cases the number of data points may exhaust internal memory (e.g., heap, stack) regardless of how much physical memory exists and cause the simulation software to “crash,” losing all results.] This is particularly important when debugging the simulation and/or before the simulation and its underlying deterministic model is verified. It is not uncommon for errors to appear in the input and/or output data that are represented by substantially “out of family” values. Without collecting the input and output information the debugging job is made all the more difficult because potentially “out of family” values have not been trapped and recorded. Even when the simulation has been verified there is still benefit in collecting the raw output results, namely to permit post-simulation processing (e.g., to estimate a fuller set of statistics than what is built-into the host simulation package, and to verify that the results are effectively uncorrelated with the simulation iteration number). For example, one simulation package provides only percentiles values (in five percentile increments) associated with designated outputs but the simulation data can be used off-line for a variety of additional statistical estimates (e.g., skewness, kurtosis).

7) A key question that should be asked ahead of time is what is the quality and level of technical support available for the simulation being used. While this should be expected for commercial software packages, it is sometimes unavailable (which may be a signal that updates will no longer be made to the software package). Also note whether/not the technical support level of knowledge exceeds what is in the user’s manual (in some cases it doesn’t).

8) Finally, a very important consideration is to challenge the results from *every* simulation-don’t blindly believe them. Many simulations are very complex and the results may indicate errors either directly (e.g., impossible outputs) or indirectly (e.g., the run-time per iteration greatly shortens over the course of the simulation which may not be simply due to a diminishing fixed overhead time to initialize the simulation but more complex factors such as memory corruption). In some cases the change in output values may be very subtle yet point to fundamental simulation or run-time errors, and in the worst case invalid results that are accepted because they weren’t challenged.

Annex A

Acronyms

ACAT	Acquisition Category
AFI	Air Force Instruction
AFPAM	Air Force Pamphlet
APUC	Average Procurement Unit Cost
CDF	Cumulative Distribution Function
CDRL	Contract Data Requirements List
CTE	Critical Technology Element
ESOH	Environment, Safety, and Occupational Health
EV	Earned Value
IMS	Integrated Master Schedule
IPR	Independent Program Review
IPT	Integrated Product Team
KPP	Key Performance Parameter
LCRM	Life Cycle Risk Management
MRL	Manufacturing Readiness Level
OI	Operating Instruction
ORM	Operational Risk Management
PAUC	Program Acquisition Unit Cost
PDF	Probability Density Function
PERT	Program Evaluation Review Technique
POC	Point of Contact
RHP	Risk Handling Plan
RI3	Risk Identification, Integration, and Ilities
RMB	Risk Management Board
RMP	Risk Management Plan
SEP	Systems Engineering Plan
SMC	Space and Missile Systems Center
SWOT	Strengths, Weaknesses, Opportunities, Threats
TAAF	Test, Analyze, and Fix
TPM	Technical Performance Measurements
TRL	Technology Readiness Level
WBS	Work Breakdown Structure