

Draft

RISK MANAGEMENT PLAN

FOR THE

H-60 AIRBORNE MINE
COUNTERMEASURES Integrated
Product Team (H-60 AMCM IPT)



Version 0.21

14 Dec 98

Draft

Table Of Contents

1	INTRODUCTION	1
1.1	PURPOSE	1
1.2	PROGRAM SUMMARY	1
1.2.1	System Description	1
1.2.2	Acquisition Strategy	1
1.2.3	Program Management Approach	2
1.3	DEFINITIONS	2
1.3.1	Risk	2
1.3.2	Probability of Occurrence (Po)	2
1.3.3	Risk Impact	2
1.3.4	Risk Exposure	3
1.3.5	Impact Time Frame	3
1.3.6	Impact Horizon	3
1.3.7	Templates and Best Practices	4
1.3.8	Critical Program Attributes	4
2	RISK MANAGEMENT APPROACH	5
2.1	GENERAL APPROACH AND STATUS	5
2.2	RISK MANAGEMENT STRATEGY	5
2.3	ORGANIZATION	5
2.3.1	Risk Management Coordinator	6
2.3.2	H-60 AMCM Integrated Product Team (H-60 AMCM IPT)	6
2.3.3	H-60 AMCM Subordinate Teams	7
2.3.4	User Participation	7
2.3.5	Risk Management Training	7
3	RISK MANAGEMENT PROCESS AND PROCEDURES	8
3.1	OVERVIEW	8
3.2	RISK PLANNING	8
3.2.1	Process	8
3.2.2	Procedures	8
3.2.2.1	Responsibilities	8
3.2.2.2	Resource Allocation	9
3.2.2.3	Documentation and Reporting	9
3.2.2.4	Metrics	9
3.2.2.5	Plan Update	9

3.3	RISK ASSESSMENT	9
3.3.1	Baseline Risk Assessment.....	9
3.3.1.1	Define the Key Program Requirements.....	10
3.3.1.2	Risk Identification.....	10
3.3.1.3	Affinity Grouping.....	11
3.3.1.4	Writing Clear Risk Statements	11
3.3.1.5	Identify Time Frame	11
3.3.1.6	Assess Impact.....	12
3.3.1.7	Estimate Probability of Occurrence	12
3.3.1.8	Prioritize Risks	13
3.3.2	Subsequent Assessments.....	13
3.4	RISK HANDLING	14
3.4.1	Risk Handling Options.....	14
3.4.1.1	Risk Avoidance.....	14
3.4.1.2	Risk Transfer.....	15
3.4.1.3	Risk Control	15
3.4.1.4	Risk Assumption.....	17
3.4.2	Choosing the Best Option	18
3.4.3	Procedures.....	19
3.5	RISK MONITORING	19
3.5.1	Process	19
3.5.2	Procedures.....	19
3.5.3	Program Metrics	20
4	<i>RISK MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION..</i>	<i>21</i>
4.1	RISK MANAGEMENT INFORMATION SYSTEM (RMIS)	21
4.2	RISK DOCUMENTATION	21
4.3	REPORTS.....	21
4.3.1	Standard Reports	21
5	<i>ANNEX A – CRITICAL PROGRAM ATTRIBUTES</i>	<i>23</i>
6	<i>ANNEX B – RISK RADAR USERS GUIDE.....</i>	<i>25</i>
7	<i>ANNEX C – PROGRAM METRIC EXAMPLES</i>	<i>43</i>
8	<i>ANNEX D – SAMPLE FORMS.....</i>	<i>44</i>
9	<i>ANNEX E – BORDA VOTING METHOD</i>	<i>47</i>
10	<i>GLOSSARY.....</i>	<i>51</i>

1 INTRODUCTION

1.1 PURPOSE

This Risk Management Plan (RMP) presents the process for implementing proactive risk management as part of the overall management of the H-60 Airborne Mine Countermeasures Mission (H-60 AMCM IPT). Risk management is a program management tool to assess and mitigate events that might adversely impact the program. Successful implementation of risk management will increase the program's likelihood of success. This RMP will:

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

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

This is the initial edition of the Risk Management Plan for the H-60 AMCM IPT. It concentrates on tasks leading to completion of the Phase II and III tow tests, as well as the definition of the capstone requirements for an integrated Organic Airborne Mine Countermeasures system of systems. Subsequent updates to this RMP will shift focus to the later acquisition phases. The PMO Risk Management Coordinator (RMC) has been identified and training of IPT members has commenced.

1.2 PROGRAM SUMMARY

The H-60 AMCM IPT was initiated to address the issues of transitioning AMCM from the MH-53E to the H-60 aircraft in order to meet helicopter type/model/series reduction and resultant cost savings based on the Helo Master Plan. The OAMCM system of systems is based on the need for an integrated organic airborne mine countermeasures system of systems to provide CVBG/ARG commanders with immediately available capabilities necessary for identification of mine threats and neutralization of these threats through avoidance or destruction. The OAMCM mission areas are: (1) Detect, Classify, and Identify; (2) Localize; and (3) Neutralize. The OAMCM program will develop and procure integrated sets of advanced sensors and weapons hosted on H-60 platforms that are organic to the fleet to replace the sensors and weapons hosted on the aging MH-53E platforms (a dedicated force) currently in the inventory. In order to meet force structure objectives, the OAMCM system must reach Initial Operational Capability (IOC) by FY-06.

1.2.1 System Description

The OAMCM system will be affordable, yet capable, taking advantage of technological simplification and advancements. The OAMCM integrated system of systems includes all airborne sensor and weapon subsystems, the integration of the subsystems with the H-60 aircraft, the ship-board systems supporting and controlling the airborne subsystems, and the interfaces between the OAMCM system and the other MCM capabilities organic to the fleet. These integration efforts will provide the OAMCM system with the capability and connectivity to accomplish the broad range of missions defined in the Capstone Requirements Document (CRD).

1.2.2 Acquisition Strategy

The OAMCM program initial strategy is to award a contract to one prime contractor for the integration of sensor and weapons subsystems coincident with successful completion of the Phase II Tow Test. All necessary acquisition approvals and contracting actions in preparation for award will be accomplished during FY99 to permit the integration contract award in the first quarter of FY00 as soon as the Phase II Tow Test is completed. Due to the technical complexity of achieving the performance levels of the

integrated system, the prime will use Government furnished subsystems developed under existing sensor and weapons systems contracts to achieve the initial operational capability.

1.2.3 Program Management Approach

The OAMCM program is presently managed using the IPPD concept, with two subordinate teams (Integrated Test Team and Systems Integration Analysis Team) established to support the tow tests and the requirements definition effort for the integration. The PM chairs the H-60 AMCM IPT that addresses issues not resolved at the lower level teams. The H-60 AMCM IPT and subordinate teams are illustrated in section 2.3 of this RMP.

1.3 DEFINITIONS

1.3.1 Risk

Risk is a measure of the inability to achieve overall program objectives within defined program requirements and constraints and has three components: (1) the *probability* of occurrence, (2) the *impact* of the risk on the program, and (3) the *time horizon* during which the consequences will occur if the risk is not mitigated.

1.3.2 Probability of Occurrence (Po)

The probability of occurrence ranges and definitions used for the H-60 AMCM IPT are given in the following table.

Probability Range	Interpretation
.01 - .10	very unlikely to occur
.11 - .40	unlikely to occur
.41 - .60	may occur about half of the time
.61 - .90	likely to occur
.91 - .99	very likely to occur

1.3.3 Risk Impact

The risk impact categories and definitions used for the H-60 AMCM IPT program are given in the following table.

Impact Category	Definition
Critical (5)	An event that, if it occurred, would cause program failure (inability to achieve minimum acceptable requirements).
Serious (4)	An event that, if it occurred, would cause major cost/schedule increases. Secondary requirements may not be achieved.
Moderate (3)	An event that, if it occurred, would cause moderate cost/schedule increases, but important requirements would still be met.
Minor (2)	An event that, if it occurred, would cause only a small cost/schedule increase. Requirements would still be achieved.
Negligible (1)	An event that, if it occurred, would have no effect on the program.

1.3.4 Risk Exposure

The risk exposure is a value calculated that is the product of probability of occurrence and impact. It is used to compare risks as part of the risk prioritization process. The values range from .01 (very low exposure) to 4.99 (very high exposure). Although there are no specific break points in the risk exposure ranking, those risks with an exposure value of less than or equal to 1.00 are generally considered low risks, those risks with an exposure value between 1.01 and 3.00 are generally considered moderate risks, and those risks with an exposure value between 3.01 and 4.99 are generally considered high risks. The definitions of Low, Moderate, and High are as follows:

- **Low Risk:** Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Actions within the scope of the planned program and normal management attention should result in controlling acceptable risk.
- **Moderate Risk:** May cause some increase in cost, disruption of schedule, or degradation of performance. Special action and management attention may be required to control acceptable risk.
- **High Risk:** Likely to cause significant increase in cost, disruption of schedule, or degradation of performance. Significant additional action and high priority management attention will be required to control acceptable risk.

1.3.5 Impact Time Frame

There are two dates that are specified for each OAMCM risk. The first is the earliest date the risk impact could materialize and the second is the latest date it could materialize. These two dates are used to track when the risk will begin to impact the program and when the risk has been overcome by events.

1.3.6 Impact Horizon

There are three impact horizon periods used for the OAMCM program: near, mid, and far. Near risks are those in which the earliest date of the risk impact is within 180 days of the present date. Mid risks are those

in which the earliest date of risk impact is between 181 and 365 days from the present date. Far risks are those in which the earliest dates of the risk impact are greater than 365 days from the present date.

1.3.7 Templates and Best Practices

A “template” is a disciplined approach for the application of critical engineering and manufacturing processes that are essential to the success of most programs. DoD 4245.7-M, *Transition from Development to Production - Solving the Risk Equation*, provides a number of such templates. The Software Engineering Institute (SEI) System Engineering Capability Maturity Model is another possible template for evaluating program processes.

1.3.8 Critical Program Attributes

Critical Program Attributes are performance, cost, and schedule properties or values that are vital to the success of the program. They are derived from various sources, such as the Acquisition Program Baseline, exit criteria for the next program phase, Key Performance Parameters, test plans, the judgment of program experts, etc. The H-60 AMCM IPT program will track these attributes to determine the progress in achieving the final required value. See Annex A for an initial list of the OAMCM Critical Program Attributes.

2 RISK MANAGEMENT APPROACH

2.1 GENERAL APPROACH AND STATUS

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

The H-60 AMCM IPT will use a centrally developed risk management strategy throughout the acquisition process as well as centralized risk planning, assessment, handling, and monitoring. OAMCM risk management is applicable to all acquisition functional areas.

The results of the initial baseline risk assessment for the program identified potential risks and the Acquisition Strategy being developed will reflect the program’s risk-handling approach. The requirements definition activity that is presently underway and the H-60 Proof of Concept Tow Test are focused on mitigation of the risks identified in the baseline risk assessment.

2.2 RISK MANAGEMENT STRATEGY

The basic risk management strategy is to identify critical risks, both technical and non-technical, and take necessary mitigation action to handle them before they can become problems, causing serious cost, schedule, or performance impacts. This program will make extensive use of modeling and simulation (e.g., Force 21, total ownership cost model), technology demonstrations for candidate subsystems (e.g., RAMICS), and prototype testing (e.g., AQS-20/X tow testing) to handle risk.

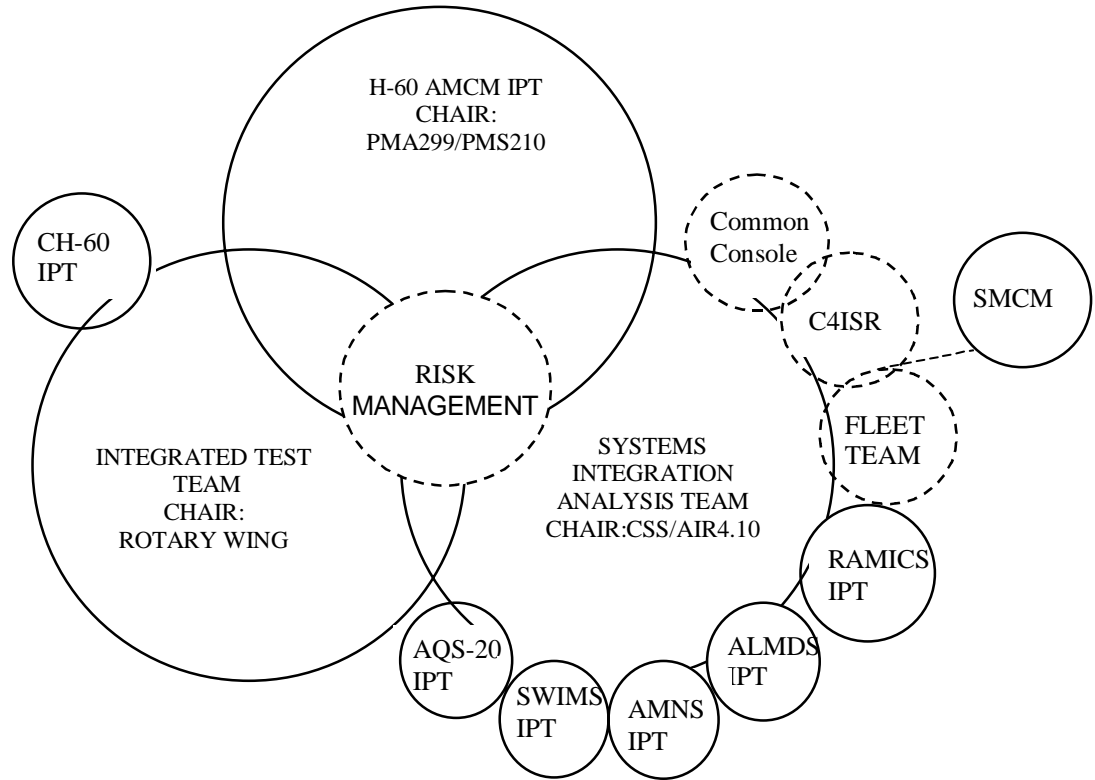
Until an integration contract is awarded, OAMCM risk management will be accomplished using the Program Office’s IPT and subordinate teams (including the users and the sensor system IPTs). After integration contract award, joint Government-Contractor IPTs will accomplish OAMCM risk management activities. The Program Office IPT and subordinate teams are presently using a structured assessment approach to identify and analyze those processes and products that are critical to meeting the program objectives. They are developing risk-handling options to mitigate the risks and monitor the effectiveness of the selected handling options. Key to the success of the risk management effort is the identification of the resources required to implement the developed risk-handling options.

Risk information will be captured by the IPT and subordinate teams and entered into a risk management database using the Risk Radar program from the Software Program Manager’s Network. See Annex B for the Risk Radar User’s Guide. Risk Radar will provide standard reports, and is capable of preparing tailored reports. The RMC will maintain the OAMCM risk databases using the status information provided biweekly, the new risks identified by the IPT and subordinate team members, and the quarterly reassessment process.

Risk information will be a principal topic in all OAMCM program reviews. As new risks are identified, IPT and subordinate team members will complete the OAMCM Candidate Risk Identification Form (See Annex D) and submit it to the Risk Management Coordinator. New risks will be reviewed at the biweekly OAMCM IPT telephone conferences to determine if mitigation action is required prior to the next quarterly update of the Risk Radar database. The goal is to be continuously looking to the future for risks that may adversely impact the program.

2.3 ORGANIZATION

The risk organization for the H-60 AMCM IPT is shown below. This is *not* a separate organization, but rather shows how risk is integrated into the existing IPT organization and shows risk relationships among members of the teams.



OAMCM Risk Management Organization

2.3.1 Risk Management Coordinator

The Risk Management Coordinator (RMC), a systems engineer supporting the program, is the overall coordinator of the Risk Management Program. The Risk Management Coordinator is responsible for:

- Maintaining this Risk Management Plan
- Maintaining the Risk Management Data Base and distributing updates
- Briefing the PM on the status of OAMCM risks
- Tracking efforts to reduce moderate and high risk to acceptable levels
- Providing risk management training
- Facilitating risk assessments and
- Preparing risk briefings, reports, and documents required for Program Reviews

2.3.2 H-60 AMCM Integrated Product Team (H-60 AMCM IPT)

The H-60 AMCM IPT is responsible for complying with the DoD risk management policy and for structuring an efficient and useful OAMCM risk management approach. The Program Manager is the Chair of the H-60 AMCM IPT. The H-60 AMCM IPT membership may be adjusted but is initially as depicted in paragraph 2.3, above.

2.3.3 H-60 AMCM Subordinate Teams

The members of the H-60 AMCM subordinate teams are responsible for implementing risk management tasks per this plan. This includes the following responsibilities:

- Review and recommend to the Program Manager and Risk Management Coordinator changes on the overall risk management approach based on lessons learned.
- Quarterly, or as directed, participate in the update to program risk assessments made during the previous quarter.
- Review and recommend any changes to the risk assessments made and the risk mitigation plans proposed.
- Report new risks to the Risk Management Coordinator via the OAMCM Candidate Risk Identification form
- Ensure that risk is a required topic at each Program Meeting and Design Review.
- Accomplish assigned mitigation tasks and report status/completion of mitigation actions to the Risk Management Coordinator for entry into the database.

2.3.4 User Participation

The users will participate in the OAMCM Risk Management Program through the Fleet Team. The Fleet Team (using the AMCM Candidate Risk Identification form) may identify risks and risk mitigation actions may be assigned to the Fleet Team. All Fleet Team risk identification, tasking, and reporting will be handled through the H-60 AMCM subordinate team member(s) assigned to the Fleet Team.

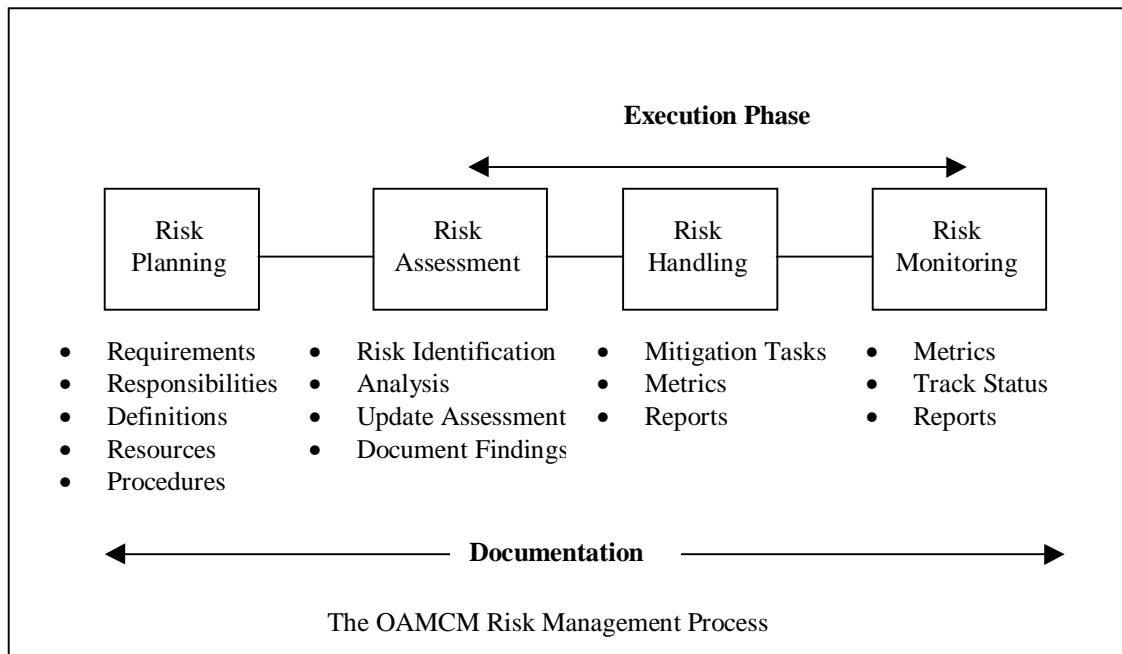
2.3.5 Risk Management Training

The key to the success of the risk efforts is the degree to which all members of the team, both Government and contractor are properly trained. The OAMCM Risk Management Coordinator provided the initial risk management training and will provide additional risk training, if necessary, as part of the quarterly risk assessment meetings or will conduct special sessions at the discretion of the program manager. All members of the team will receive, at minimum, basic risk management training.

3 RISK MANAGEMENT PROCESS AND PROCEDURES

3.1 OVERVIEW

This section describes the H-60 AMCM IPT risk management process and provides an overview of their risk management approach. The Defense Acquisition Deskbook defines risk management as “the act or practice of controlling risk. It includes risk planning, assessing risk areas, developing risk handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program.” Figure 3-1 shows, in general terms, the overall risk management process that will be followed. This process follows DoD and Service policies and guidelines and incorporates ideas found in other sources. Each of the risk management functions shown in figure below is discussed in the following paragraphs, along with specific procedures for executing them.



3.2 RISK PLANNING

3.2.1 Process

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

3.2.2 Procedures

3.2.2.1 Responsibilities

At this stage, the H-60 AMCM IPT is responsible for conducting risk planning, using this RMP as the basis. The planning will cover all aspects of risk management to include assessment, handling options, and monitoring of risk mitigation activities. The Program Risk Management Coordinator will document the initial planning activities in this RMP and make appropriate revisions to this plan when required to reflect significant changes in the program’s risk planning approach. Each person involved in the requirements

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

3.2.2.2 Resource Allocation

Because there are insufficient resources assigned to the program to monitor all potential program risks, the H-60 AMCM IPT will use a risk-based resource allocation process. The H-60 AMCM IPT program manager will allocate personnel, dollar, and schedule resources to monitor and mitigate the most significant risks on the program. The lower level risks will remain on the program's watch list and new risks will be evaluated for potential impact biweekly as they are identified. Following the quarterly reassessment and reprioritization of risks, the program manager may direct a reallocation of resources to manage the current set of program risks.

As part of its planning process, each subordinate team will identify the resources required to implement the risk management and mitigation actions. These resources include time, material, personnel, and cost. If assigned risk mitigation tasks exceed available resources, the subordinate team leaders are responsible for notifying the H-60 AMCM IPT of the impact and an estimate of the additional resources required.

3.2.2.3 Documentation and Reporting

This RMP establishes the basic documentation and reporting requirements for the program. Subordinate team leaders should identify any additional requirements that might be needed to effectively manage risk at their level. Any such additional requirements must not conflict with the basic requirements in this RMP. Additional documentation requirements that can have a beneficial impact on the H-60 AMCM IPT and subordinate teams will be incorporated in subsequent revisions to this RMP.

3.2.2.4 Metrics

Each subordinate team leader shall establish metrics that will measure the effectiveness of their planned risk-handling options. See Annex C for an example of metrics that may be used.

3.2.2.5 Plan Update.

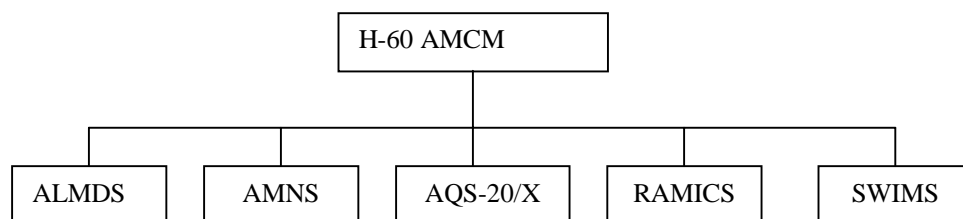
This RMP will be updated, if necessary, on the following occasions: (1) whenever the acquisition strategy changes, or there is a major change in program emphasis; (2) in preparation for major decision points; (3) in preparation for and immediately following major system events listed in the Integrated Master Plan (IMP) and Integrated Master Schedule (IMS); (4) concurrent with the review and update of other program plans; and (5) in preparation for a POM submission.

3.3 RISK ASSESSMENT

The risk assessment process includes the identification of critical risks, which could have an adverse impact on the program, and the analyses of these risks to determine: the consequences, the probability of occurrence, the impact of the consequences on the program, and the time frame during which the consequences are likely to occur. It is the most demanding and time-consuming activity in the risk management process.

3.3.1 Baseline Risk Assessment

The Baseline Risk Assessment is the first risk assessment performed on the program. It is an eight step process that was facilitated by the H-60 AMCM IPT Risk Management Coordinator. The H-60 AMCM IPT and subordinate team members participated in the process over a four day period. A separate risk assessment was accomplished for the OAMCM Integration effort and for each of the five candidate sensor/weapon systems. The following illustrates the structure of the assessment.



3.3.1.1 Define the Key Program Requirements

Defining the key program requirements is the first step in the assessment process. Because the H-60 AMCM IPT is early in the requirements definition phase, all documents, policies, and groups that had an influence on this phase were identified to provide the H-60 AMCM IPT and subordinate team members with a picture of the objectives and constraints for the program. The following were among the documents, policies and groups identified:

- MNS & ORD – H-60R
- MNS – CH-60 ORD
- MCM MNS – 93
- AQS-20 ORD and 20X Draft Chg 1
- AMNS ORD (No H-60)
- ALMDS ORD (With H-60)
- SWIMS ORD Draft (No H-60)
- RAMICS NAPPD ATD (No H-60)
- Proof of Concept Tow Test
- Threat Scenarios
- N-85 letter #2 – Tow test
- N-88 Requirements for Helos
- N-86 Interface
- Mine Warfare Plan
- From The Sea
- Forward From the Sea
- Operational Maneuver from the Sea
- Force 21 Study
- IDA Study
- EXCOM Direction
- Helo Master Plan
- C4ISR Master Plan
- Letter from ASN
- SECDEF Memo
- N-85 letter #1 – Feasibility Study
- MCM Oversight Board

3.3.1.2 Risk Identification.

Risk identification is the second step in the assessment process. The basic process involves searching through the entire OAMCM program to determine those critical risks that would prevent the program from achieving its objectives. All group members participated in a structured brainstorming session to identify risks. Each member was provided with a pad of post-it notes and was given the opportunity to write a single risk on a single sheet. Then the group members were each given a turn to explain one risk to the group and post it on the white board. In the event there were questions in the future, group members were asked to put their initials on the bottom of the post-it for each risk they identified. No risk could be eliminated at this point and no mitigation ideas were introduced. This process continued with each group member identifying and explaining one risk per cycle until all risks had been identified. To minimize duplication, members were asked not to identify a risk a second time if it had already been presented by another group member and posted on the board. The identification of risks was not restricted to technical, cost, and schedule categories. Any risk that had an adverse impact on the program could be identified.

Following are indicators that group members found helpful in identifying and assessing risk:

- Lack of Stability, Clarity, or Understanding of Requirements: Requirements drive the design of the system. Changing or poorly stated requirements guarantees the introduction of performance, cost, and schedule problems.
- Failure to use best practices virtually assures risk. The further the IPT deviates from best practices, the higher the risk.

- Insufficient Resources: People, funds, schedule, and tools are necessary ingredients for successfully implementing a process. If any are inadequate, to include the qualifications of the people, there is risk.
- Test failure may indicate corrective action is necessary. Some corrective actions may not fit available resources, or the schedule, and (for other reasons as well) may contain risk.

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

- Best Judgment: The knowledge and experience of the collective, multi-disciplined Integrated Product Team (IPT) and working group members and the opinion of subject matter experts (SMEs) are the most common sources of risk identification.
- Lessons Learned from similar processes can serve as a baseline for the successful way to achieve requirements. If there is a departure from the successful way, there may be risk.
- DoD 4245.7-M, “Transition from Development to Production,” is often called the
- “Templates” book because it identifies technical risk areas and provides, in “bullet” form, suggestions for avoiding those risks. It focuses on the technical details of product design, test, and production to help managers proactively manage risk. It also includes chapters on Facilities, Logistics, and Management, which make this a useful tool in identifying weak areas of OAMCM planned processes early enough to implement actions needed to avoid adverse consequences.
- The NAVSO P-6071 Best Practices Manual was developed by the Navy to add depth to the Template Book, Dod4245.7-M.
- Critical Program Attributes are metrics that the program office developed to measure progress toward meeting our objectives. Team members, IPTs, functional managers, contractors, etc. may develop their own metrics to support these measurements. The attributes may be specification requirements, contract requirements, or measurable parameters from any agreement or tasking. The idea is to provide a means to measure whether we are on track in achieving our objectives. Some Critical Program Attributes for OAMCM are listed in Annex A.

3.3.1.3 Affinity Grouping

After all risks had been identified, the group was asked to arrange the post-it notes into like categories. There were no predefined categories and no restriction on the number of categories that could be used. The group was given approximately twenty minutes to organize the risks. A name could have been given to each category and this could have been carried into the risk database, but it was not done in this session. This activity grouped similar and related risks and provided the opportunity to combine risks in the next phase of the process. To maintain traceability, a number was assigned to each post-it note and each group had a contiguous set of numbers.

3.3.1.4 Writing Clear Risk Statements

At this point, the group was asked to write a clear risk statement for each numbered. A required format was used. Each risk had to be written in an “IF – THEN” form. The “IF” portion contained the risk or condition and the “THEN” portion contained the consequences to the program if the risk was not mitigated. During this phase, the group was permitted to eliminate or combine risks. If a risk was either combined or eliminated a note was made for that risk number to maintain traceability to the original set of numbers. Those risks that were eliminated or combined were entered into the database and “retired” with an explanation. During this phase, the risk entry form was projected on a screen. When the group concurred with the wording of a risk, it was entered into the database and the group would move to the next numbered risk.

3.3.1.5 Identify Time Frame

After all the risk statements were completed, a time frame was identified for each risk. A calendar date was identified for the earliest date the risk consequence or impact could materialize and the second date was the

latest date that it could materialize. These dates are compared with the present date to determine impact horizon (near, mid, or far) by the Risk Radar program and to identify those risks that have been overcome by events.

3.3.1.6 Assess Impact

After the time frame was identified for each risk, the severity of impact (if no mitigation action is taken) was assessed for that risk using the following scale and definitions. A number from 1 to 5 is entered into the database for each risk. Because it is a required database entry a “1” was entered for eliminated or combined risks before they were “retired”. When agreement could not be reached on the impact, the Program Manager was asked to decide the category.

Impact Category	Definition
Critical (5)	An event that, if it occurred, would cause program failure (inability to achieve minimum acceptable requirements).
Serious (4)	An event that, if it occurred, would cause major cost/schedule increases. Secondary requirements may not be achieved.
Moderate (3)	An event that, if it occurred, would cause moderate cost/schedule increases, but important requirements would still be met.
Minor (2)	An event that, if it occurred, would cause only a small cost/schedule increase. Requirements would still be achieved.
Negligible (1)	An event that, if it occurred, would have no effect on the program.

3.3.1.7 Estimate Probability of Occurrence

After the impact was identified for each risk, the probability of occurrence (if no mitigation action is taken) for that risk was estimated using the following scale and definitions. A number from 1 to 99 is entered into the database for each risk. Because it is a required database entry a “1” was entered for eliminated or combined risks before they were “retired”. When agreement could not be reached for a probability of occurrence, the Program Manager was asked to provide a value.

Probability Range	Interpretation
1–10	very unlikely to occur
11–40	unlikely to occur
41–60	may occur about half of the time
61–90	likely to occur
91–99	very likely to occur

3.3.1.8 Prioritize Risks

All of the risk statements, their time frames, impacts, and probabilities of occurrence were entered into the database. The database was sorted using the Borda sorting algorithm provided in the MITRE Risk Matrix tool. This algorithm sorts all of the risks by probability of occurrence (highest to lowest). It also sorts all of the risks by impact (highest to lowest). It then combines the two lists using the algorithm. The details of the Borda algorithm have been extracted from the MITRE Risk Matrix User’s Guide (Version 2.02) and are included as Annex E.

The Borda algorithm reduced, but did not eliminate ties. When there was a tie in the Borda rank, the tie was broken using the first date in the time frame for a subsequent sort where the early dates were ranked higher than later dates. In the few instances where a tie still occurred, the original risk number order was used.

The resulting ranking was used as the priority ranking for the risks in the Risk Radar database rather than using the default risk exposure calculation.

As a final step, the prioritized set of risks for OAMCM integration and each of the five candidate subsystems was presented to the team to see if the results were reasonable and supportable. The program manager or any member of the team surfaced no exceptions to the resulting rankings.

Had any exceptions been taken, Risk Radar provides the capability to reorder the rankings.

3.3.2 Subsequent Assessments

Risk assessment is an iterative process, with each assessment building on the results of previous assessments. The current baseline assessment is a program office risk assessment done early in the requirements definition phase for the program and prior to the Proof of Concept Tow tests. The program office will accomplish a reassessment of risks quarterly during the months of December, March, June, and September until an integration contract is awarded. Following integration contract award, a joint Government-contractor risk assessment will be performed in conjunction with the post-award Integrated Baseline Review (IBR) and initial partnering workshop.

For the program office, unless otherwise directed in individual tasking, program level risk assessments will be presented at each Program Review meeting and EXCOM briefings and not later than 6 months before the any scheduled Milestone decision. The primary source of information for the next assessment will be the current assessment baseline, and existing documentation such as, Tow test results, Force 21 simulations, changes in the mission scenarios, feedback on the Capstone Requirements Document, industry comments, Fleet Working Group inputs, discussions with MCM subject matter experts, and best practices adopted by the program.

Starting on 15 December 98, the status of risk mitigation actions for all of the OAMCM integration risks will be reviewed and entered into the Risk Radar database. The OAMCM Integration risks will be revisited at every other biweekly meeting. The risks for the five candidate subsystem risks will be reviewed and updates entered into the Risk Radar database at the second H-60 AMCM biweekly meeting in January 99. The subsystem risks will be revisited at every other biweekly meeting.

New risks that have been identified since the last H-60 AMCM biweekly meeting will be added to the “bottom” of the appropriate database and will be discussed at the meetings. Time frame, impact, probability of occurrence will be assigned to all new risks. Mitigation steps for new risks will be added at the discretion of the program manager. **A new prioritization of the risk list will not take place until the quarterly reassessment.**

When the total set of risks is reassessed, the risk statement, time frame, impact, and probability of occurrence will be revisited for each risk based on the events of the previous quarter and the mitigation actions taken to date. The H-60 AMCM IPT or subordinate teams may decide to retire the risk, reword the risk, or change the mitigation steps. The group may also identify new risks during the reassessment and add these risks to the database. Following the reassessment, the risks will be ranked again in a process similar to the initial ranking.

3.4 RISK HANDLING

3.4.1 Risk Handling Options

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

There are essentially four risk-handling techniques, or options:

- (1) **risk avoidance**, which eliminates the sources of high risk and replaces them with a lower risk solution;
- (2) **risk transfer**, which is the reallocation of risk from one part of the system to another, or the reallocation of risks between the Government and the prime contractor or within Government agencies;
- (3) **risk control**, which manages the risk in a manner that reduces the likelihood of its occurrence and/or minimizes the risk's effect on the program; and
- (4) **risk assumption**, which is the acknowledgment of the existence of a particular risk situation and a conscious decision to accept the associated level of risk without engaging in any special efforts to control it.

3.4.1.1 Risk Avoidance

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

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

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

CAIV or Cost/requirement trade studies are used to support operational requirements scrubbing. These trades examine each requirement and determine the cost to achieve various levels of the requirement (e.g., different airspeeds, range, and payloads). The results are then used to determine, with the user, whether a particular requirement level is worth the cost of achieving that level.

3.4.1.2 Risk Transfer

This technique involves the reduction of risk exposure by the reallocation of risk from one part of the system to another or the reallocation of risks between the Government and the prime contractor.

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

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

Following contract award, a joint Government-Contractor risk management program will evolve from this risk management program. As part of that program, joint decisions will be made by the Government and the contractor concerning the allocation of risk and the assignment of risk mitigation actions.

3.4.1.3 Risk Control

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

- **Multiple Development Efforts** — The use of two or more independent design teams (usually two separate contractors, although it could also be done internally) to create a system that meets the same performance requirements. The investigation of alternate sensors or weapons for H-60AMCM as well as a comparison of H-60 AMCM capabilities with other MCM capabilities may result if this approach is used.
- **Backup Choices Available** — Sometimes, a design option may include several risky approaches, of which one or more must come to fruition to successfully meet system requirements. However, if the PM studies the risky approaches, it may be possible to discover a lower risk approach (with a lower performance capability). These lower risk approaches could be used as backups for those cases where the primary approaches fail to mature in time. This option presumes there is some trading room among requirements. Close coordination between the developer and the user is necessary to implement lower capability options. The H-60 AMCM carriage, stream, and recovery studies may fall in this category.
- **Early Prototyping** — The nature of a risk can be evaluated by a prototype of a system (or its critical elements) built and tested early in the system development. The results of the prototype can be factored into the design and manufacturing process requirements. In addition

to full-up systems, prototyping is very useful in software development and in determining a system's man-machine interface requirements. The key to making prototyping successful, as a risk-control tool is to minimize the addition of new requirements to the system after the prototype has been tested (i.e., requirement changes not derived from experience with the prototype). Also, the temptation to use the prototype design and software without doing the necessary follow-on design and coding/ manufacturing analyses should be avoided. Early prototyping of the common console and carriage, stream, and recovery assemblies for H-60 AMCM may result in significant risk reduction on the program.

- **Incremental Development** — Incremental development is when the system design and deployment is completed in steps, relying on preplanned product improvements (P3I) after the system is deployed to achieve the final system capability. Usually, these added capabilities are not included originally because of the high risk that they will not be ready along with the remainder of the system. Hence, development is split, with the high risk portion given more time to mature. The basic system, however, incorporates the provisions necessary to include the add-on capabilities. In P3I, most of the system requirements are achieved by the basic system. In order to accommodate future sensors and changes in the threat, the OAMCM system will be considering a program strategy using incremental development.
- **Technology Maturation Efforts** — Technology maturation is an off-line development effort to bring an element of technology to the necessary level so that it can be successfully incorporated into the system (usually done as part of the technology transition process). Normally, technology maturation is used when the desired technology will replace an existing technology, which is available for use in the system. In those cases, technology maturation efforts are used in conjunction with P3I efforts. However, it can also be used when a critical, but immature, technology is needed. In addition to dedicated efforts conducted by the PMO, Service or DoD-wide technology improvement programs and advanced technology demonstrations by Government laboratories as well as industry should be considered. The RAMICS ATD may be considered a technology maturation effort.
- **Demonstration Events** — Demonstration events are points in the program (normally tests) that are used to determine if risks are being successfully abated. Careful review of the planned development of each risk area will reveal a number of opportunities to verify the effectiveness of the development approach. By including a sequence of demonstration events throughout the development, Integrated Test Team (ITT) can monitor the process and identify when additional efforts are needed. Demonstration events can also be used as information gathering actions, as discussed above, and as part of the risk monitoring process. The Proof of Concept Tow test for the OAMCM program is an example of a demonstration event.
- **Open Systems**—This approach involves the use of widely accepted commercial specifications and standards for selected system interfaces, products, practices and tools. It provides the basis for reduced life-cycle costs, improved performance, and enhanced interoperability, especially for long-life systems with short-life technologies. Properly selected and applied commercial specifications and standards can result in lower risk through increased design flexibility, reduced design time, more predictable performance, and easier product integration, support, and upgrade. However, there are a number of challenges and risks associated with the use of the open systems approach that must be considered prior to implementation. These include such issues as: maturity and acceptability of the standard, and its adequacy for military use; the loss of control over the development of products used in the system; the amount of product testing done to ensure conformance to standards; and the higher configuration management workload required. The H-60 AMCM IPT will be using Open Systems architecture for sensor and weapons integration.
- **Use of Standard Items/Software Reuse** — The use of standard items and software module reuse should be emphasized to the extent possible to minimize development risk. Standard items range from components and assemblies to full-up systems. A careful examination of the proposed system option will often find more opportunities for the use of standard items or existing software modules than first thought. Even when the system must achieve previously

unprecedented requirements, standard items can find uses. A strong program policy emphasizing the use of standard items and software reuse is often the key to taking advantage of this source of risk control. Standard items and software modules have proven characteristics that can reduce risk. However, the PM must be cautious when using standard items in environments and applications for which they were not designed. A misapplied standard item often leads to failure. The H-60 AMCM common console is an example of Standard Item/Software Reuse.

- **Use of Mockups** — The use of mockups, especially man-machine interface mockups, can be used to conduct early exploration of design options. They can assist in resolving design uncertainties and providing users with early views of the final system configuration. Carriage, stream, and recovery and the common console alternatives may involve the use of mockups.
- **Modeling/Simulation** — Modeling and simulation is a useful risk-handling tool because it can provide insights into a system's performance and effectiveness sensitivities. Decision makers can use performance predictions to assess the military worth of the system not only before any physical prototypes are built, but also throughout the system life cycle. The OAMCM total ownership cost model and the Force 21 alternatives study fall in this category.
- **Key Parameter Control Boards** — When a particular parameter (such as system weight) is crucial to achieving the overall program requirements, a control board for that parameter may be appropriate. This board has representatives from all affected technical functions and may be chaired by the PM. It provides management focuses on the parameter and signals the importance of achieving the parameter to the technical community. If staffed properly by all affected disciplines, it can also help avoid sacrificing other program requirements to achieving that requirement (such as cutting screws to location-specific lengths, thereby reducing weight but creating a logistics nightmare). Takeoff gross weights for AMCM missions are prime candidates for a weight control board.

Risk control involves the development of a risk-reduction plan, with risk-reduction actions identified, resourced, and scheduled. The risk reduction plans are identified as specific risk mitigation actions in the OAMCM Risk Radar database. Success criteria for each of the risk-reduction events should also be identified

3.4.1.4 Risk Assumption

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

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

- Identify the resources (time, money, people, etc.) needed to overcome a risk if it materializes. This includes identifying the specific management actions that will be used, for example, redesign, retesting, requirements review, etc.
- Ensure that the necessary administrative actions are taken to quickly implement these management actions, such as contracts for industry expert consultants, arrangements for test facilities, etc.

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

3.4.2 Choosing the Best Option

In determining the "best" overall risk-handling strategy and specific techniques to be adopted, the following general procedures apply. For each identified risk, all potentially applicable techniques should be identified and evaluated, using the following criteria:

- Feasibility of the technique — This addresses the ability to implement the technique and includes an evaluation of the potential impact of the technique in the following areas:
 - Technical considerations, such as testing, manufacturing, and maintainability, caused by design changes resulting from risk-handling techniques.
 - Adequacy of budget and schedule flexibility to apply the technique.
 - Operational issues such as usability (man-machine interfaces), transportability, and mobility.
 - Organizational and resource considerations, e.g., manpower, training and structure.
 - Environmental issues, such as the use of hazardous materials to reduce technical risk.
 - External considerations beyond the immediate scope of the program, such as the impact on other complementary systems or organizations.
- Expected effectiveness of each technique in controlling program risk — The risk-assessment techniques discussed in the previous section, along with other techniques such as trade studies and sensitivity analyses, can be useful in determining this expected effectiveness.
- Cost and schedule implications of the technique — The risk-handling techniques have a broad range of cost implications in terms of dollars, as well as other limited resources, e.g., critical materials and national test facilities. The magnitude of the cost and schedule implications will depend on circumstances and can be assessed using such techniques as cost-benefit analyses and the cost and schedule assessment techniques described in Section 2524.2 of the Defense Acquisition Deskbook. The approval and funding of risk-handling techniques should be part of the trade-off process that establishes and refines the CAIV cost and performance goals.
- Effect on the system's technical performance—The risk-handling techniques may affect the system's capability to achieve the required technical performance objectives. This impact must be clearly understood before adopting a specific technique. As the risk-handling techniques are assessed, the PM should attempt to identify any additional parameters that may become critical to technical performance as a result of implementing them.

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

The results of the evaluation and selection will be included and documented in the Risk Radar database for each risk following completion of the risk assessment (or reassessment) process. The decision on what to do with the risk will be reflected in the Status field in the Risk Radar database for each risk.

- Transfer – used in the status field for risks that are transferred
- Watch – used in the status field for risks that are being assumed
- Mitigate – used in the status field for risks that are being avoided or controlled

For those risks that are being transferred or watched, there will be an entry in the Contingency Plan field in Risk Radar explaining what is being done.

For those risks that are being avoided or controlled, specific mitigation actions, assignees, and due dates will be entered in the Mitigation Plan fields in Risk Radar.

3.4.3 Procedures

The IPT that assessed the risk is responsible for evaluating and recommending to the PM the risk-handling options that are best fitted to the program's circumstances. Once approved, these are included in the program's acquisition strategy or management plans, as appropriate. For each selected handling option, the responsible IPT or subordinate team will develop specific tasks that, when implemented, will handle the risk. The task descriptions should explain what has to be done, the level of effort, and identify necessary resources. It should also provide a proposed schedule to accomplish the actions including the start date, the time phasing of significant risk reduction activities, the completion date, and their relationship to significant Program activities/milestones, and a cost estimate. The description of the handling options should list all assumptions used in the development of the handling tasks. Assumptions should be included in the Risk Radar database. Recommended actions that require resources outside the scope of a contract or official tasking should be clearly identified, and the IPT or subordinate team, the risk area, or other handling plans that may be impacted should be listed. Reducing requirements as a risk avoidance technique will be used only as a last resort, and then only with the participation and approval of the user's representative.

3.5 RISK MONITORING

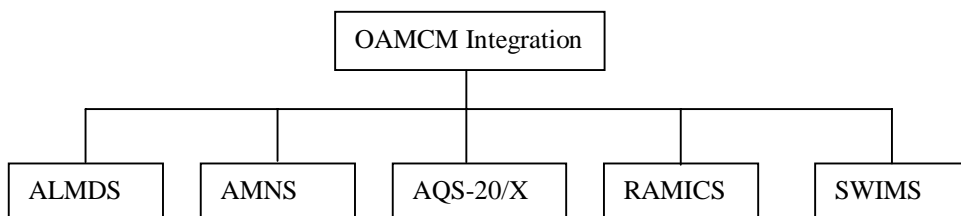
3.5.1 Process

Risk monitoring systematically tracks and evaluates the performance of risk-handling actions. It is part of the PM function and responsibility and will not become a separate discipline. Essentially, it compares predicted results of planned actions with the results actually achieved to determine status and the need for any change in risk-handling actions.

To ensure that significant risks are effectively monitored, risk-handling actions (which include specific events, schedules, and "success" criteria) will be reflected in integrated program planning and scheduling. The detailed information on risk-handling actions and events will be included in the Risk Radar database for each identified risk.

3.5.2 Procedures

The functioning of the IPT is crucial to effective risk monitoring. It is the "front line" for obtaining indications that risk-handling efforts are achieving their desired effects. The IPT and subordinate teams are responsible for monitoring and reporting the effectiveness of the handling actions for the risks assigned. Overall OAMCM risk assessment reports will be prepared by the OAMCM Risk Management Coordinator working with the cognizant IPT or subordinate team leader. A separate Risk Radar database will be maintained for OAMCM Integration and for each of the five candidate subsystems.



At a minimum, the Systems Integration Analysis Team and each subsystem IPT will participate in risk assessments and identify new risks to the OAMCM Risk Management Coordinator using the AMCM Candidate Risk Identification form (see Annex D). The OAMCM Risk Management Coordinator will enter these risks into the Risk Radar database (and rank them quarterly following completion of a reassessment). The coordinator will also track them, using information provided by the appropriate IPT or subordinate team until the risk is recommended for "retirement." The IPT or subordinate team that initially reported the risk retains ownership and cognizance for reporting status and keeping the database current. Ownership means implementing handling plans and providing periodic (every other biweekly meeting) status of the risk and of the handling plans at H-60 AMCM IPT teleconferences. Ownership also includes monitoring

risks that are on the “watch” list in addition to those with mitigation actions. Risk will be made an agenda item at each OAMCM management or design review, providing an opportunity for all concerned to offer suggestions for changes in this Risk Management Plan.

The risk management process is continuous. Information obtained from the monitoring process is fed back for reassessment and evaluations of handling actions. When a risk is no longer significant (due to mitigation actions or other events) it is put into a “Retired File” by the Risk Management Coordinator and it is no longer tracked by the OAMCM PM.

The status of the risks and the effectiveness of the risk-handling actions will be reported to the Risk Management Coordinator:

- Biweekly at the H-60 AMCM IPT teleconference (alternating review of Integration and the subsystem databases)
- When the IPT or subordinate team determines that the status of the risk area has changed significantly (as a minimum when the risk changes from high to moderate to low, or vice versa)
- When requested by the Program Manager.
- The OAMCM Risk Management Coordinator will enter the updates provided at the biweekly teleconferences into the database and will provide the updated database(s) reports to the program participants prior to the next teleconference. The database update reports will be sent to the H-60 AMCM IPT and subordinate team members as MS Word documents via email until a server is established for the program where the IPT members can access and download the updated database reports (in MS Word).

3.5.3 Program Metrics

The effectiveness of the risk-monitoring process can often depend on the establishment of a management indicator system (metrics) that provides accurate, timely, and relevant risk information in a clear easily understood manner. (See Annex C.) The metrics selected to monitor program status must adequately portray the true state of the risks and handling actions. The selection of metrics for monitoring the health of the program is a program management decision and the metrics indicated in Annex C are only examples that could be used, not OAMCM metrics that have been chosen for use.

4 RISK MANAGEMENT INFORMATION SYSTEM AND DOCUMENTATION

The H-60 AMCM IPT will use the Risk Radar database management system as its Risk Management Information System (RMIS). The system will contain all of the information necessary to satisfy the program documentation and reporting requirements.

4.1 RISK MANAGEMENT INFORMATION SYSTEM (RMIS)

The RMIS stores and allows retrieval of risk-related data. It provides data for creating reports and serves as the repository for all current and historical information related to risk. This information will support the creation of risk-related reports. The PMO will use data from the RMIS to create reports for senior management and retrieve data for day-to-day management of the program. The program produces a set of standard reports for periodic reporting and has the ability to create ad hoc reports in response to special queries. See Annex B for a detailed discussion of Risk Radar.

After the initial assessment has been completed, the OAMCM Risk Management Coordinator using the AMCM Candidate Risk Information form (See Annex D) enters data into Risk Radar. This form gives members of the project team, both Government and contractors, a standard format for reporting risk-related information. The form should be used when a potential risk event is identified and will be updated as information becomes available as the assessment, handling, and monitoring functions are executed.

4.2 RISK DOCUMENTATION

All program risk management information will be documented, using the AMCM Candidate Risk Information form as the standard RMIS data entry form.

Current reports (in MS Word) from the six H-60 AMCM risk databases will be posted on the OAMCM server and a current copy can be downloaded at any time to view the current assessment, ranking, status, and handling activities for all OAMCM risks.

4.3 REPORTS

Reports are used to convey information to decision-makers and team members on the status of the program and the effectiveness of the risk management program. Every effort will be made to limit reports to the standard reports available in the Risk Radar program.

4.3.1 Standard Reports

The RMIS will have a set of standard reports. If IPTs or functional managers need additional reports, they should work with the Risk Management Coordinator to create them. Access to the reporting system will be controlled; however, any member of the Government or contractor team may obtain a password to gain **read access** to the reports (in MS Word) on the OAMCM server.

The standard Risk Radar reports are as follows:

Detailed Reports

- Risks by Rank
- Risks by Risk ID
- Retired Risks

Summary Reports

- Risks by Rank
- Risks by Risk ID
- Risks by Title
- Retired Risks

An example of a Risk Radar detailed report and an example of a summary report are contained in Annex D.

5 ANNEX A – CRITICAL PROGRAM ATTRIBUTES

Category	Description	Responsible IPT	Remarks
Performance/Physical	Aircraft Weight		
	System Weight		
	Tow Weight		
	Mission Time		
	Search Rate		
	Clearance Rate		
	Crew Size		
	Data Link Operations		
	Configuration Time		
	Sortie Turnaround Time		
	Distance from Host Ship		
	Navigation Accuracy		
	Probability of Accurate ID		
	Shipboard Space		
	Operational Availability		
	Interoperability – MCM		
	Mission Planning		
	Command and Control		
	Bottom Database		
Cost	Total Ownership Cost / LCC		
	Modifications for H-60		
	System Modifications		
Processes	Requirements Definition		
	Incremental Fielding		

Exit Criteria	Phase II Tow Test		
	Phase III Tow Test		
	CRD Approval		

RISK RADAR USER'S GUIDE

Version 1.1

March 1998

SOFTWARE PROGRAM MANAGERS NETWORK

John E. Moore, Ph.D.

www.spmn.com

riskradr@spmn.com

tel (703) 521-5231

fax (703) 521-2603

Copyright © 1998 Computers & Concepts Associates

Abstract

Risk Radar is a risk management database that helps project managers identify, prioritize, and communicate project risks in a flexible and easy-to-use form. Risk Radar provides standard database functions to add and delete risks, together with specialized functions for prioritizing and retiring project risks. Each risk can have a user-defined risk management plan and a log of historical events. A set of standard short- and long-form reports and viewgraphs can be easily generated to share project risk information with all members of the development team. The number of risks in each probability/impact category by time frame can be displayed graphically, allowing the user to visualize risk priorities and easily uncover increasing levels of detail on specific risks. Risk Radar also provides flexibility in prioritizing risks through automatic sorting and risk-specific movement functions for priority ranking. Risk Radar Version 1.1 runs only on PCs, and requires Microsoft Access 2.0, 95, or 97 for operation.

I. Background

1. Introduction

Risk Radar is a risk management database that is designed to help project managers identify, prioritize, and communicate project risks in a flexible and easy-to-use form. Risk Radar provides standard database functions to add and delete risks, together with specialized functions for prioritizing and retiring project risks. Each risk can have a user-defined risk management plan and a log of historical events. A set of standard short- and long-form reports can be easily generated to share project risk information with all members of the development team. The number of risks in each probability/impact category by time frame can be displayed graphically, which allows the user to visualize risk priorities and easily uncover increasing levels of detail on specific risks. Risk Radar also provides flexibility in prioritizing risks through automatic sorting and risk-specific movement functions for priority ranking.

Risk management is not a hard science, and it requires that the risk manager combine the best known technical information with good professional judgment. A guiding principle in Risk Radar development was to automate functions that clearly benefit the user, but also allow flexibility for individual judgment. For instance, risks can be prioritized automatically by clicking on a button to sort according to risk exposure, but the user also has the flexibility to move risks individually up and down in the priority ranking irrespective of numerical factors. Each risk has a historical events log so that the user can record decisions and events that influence how the risk was managed. A key element of risk management is maintaining the

set of project risks so that the most important risks are prioritized from the perspective of the project team. Risk Radar attempts to facilitate this process to be as simple and straightforward as possible.

Risk Radar is designed with the rationale that the most important part of risk management is to identify the highest-priority risks and to keep attention focused on them as a project evolves over time. Risk management is a dynamic and proactive process that requires continuous vigilance. What is an important risk this month might not be important next month. It is impossible to predict all the risks a project might face in the future, so you shouldn't even try. But you should be watchful for future events or conditions that could be a major threat to your project's success. Risks will pop up, be mitigated, and then hopefully be relegated to a much lower level of concern, and eventually be retired. Other risks will likely step in to replace them. Risk Radar does not discover risks for you; you must do that. But once a risk is identified, Risk Radar allows you to fully describe the risk and prioritize it relative to the other risks your project faces. The key to successful use of Risk Radar is to keep the highest-priority risks at the top of your risk-ranking list and to focus your mitigation efforts on them. With Risk Radar you can describe a risk, set up a risk mitigation plan, prioritize it relative to all the others in the database, and record events and decisions that affect the risk over time. Risk Radar includes a full set of standard short- and long-format reports as well as a viewgraph-formatted report for communicating risk priorities and mitigation efforts to upper management and the entire project team.

To perform the prioritization process, you must make some subjective estimates based on professional judgment of the probability that a risk will occur and its negative impact on the project if it does occur. You assign a probability of between 1 and 99 percent and an impact value of between 1 (for very low) to 5 (for very high) for each risk in Risk Radar. The program then multiplies these numbers together to calculate a risk exposure for the risk. Although we could try to break a risk impact down and quantify all kinds of impacts areas, such as schedule impact in terms of days or cost impact in terms of dollars, in reality the current state of the practice of project risk management does not permit us to quantify these impacts with any degree of accuracy, and adding multiple impact areas adds complexity to the risk management process while providing little quantitative benefit. The 1 to 5 rating system is just that—a subjective rating of the total impact the risk could have on your project. Risk Radar does not presuppose what an impact value of 4 or 5 means to your project. You must come up with the definitions yourself and stick to them. These numbers are, and will continue to be for the foreseeable future, guesses based on past professional experience. Risk Radar uses risk exposure purely as a means to help rank risks relative to one another, but it assumes these numbers have little or no meaning in an absolute sense. In most cases it would be inappropriate to compare risks across projects based solely on numerical factors such as probability, impact, or exposure. The best we can hope for is that numerical risk values will be used consistently by the project team over the life of the project so there is a consistent ranking of risks to keep the most important ones at the top of the ranking list.

Time must also be considered when managing risks. Risks are fundamentally characterized by negative impacts that might occur in the future. Although some risks are tied closely to discrete events, such as a critical piece of software that must be received from a supplier at a particular date, Risk Radar is more general and allows you to identify an impact time frame over which the risk's impact might materialize. As a project draws closer to one of these time frames, this will be calculated by the program and show up as the number of days to the impact time frame and its impact horizon in terms of near-, mid- and far-term for each risk. Is a risk with a risk exposure of 2.5 and a near-term impact horizon more important than a risk with a risk exposure of 4.5 and a far-term impact horizon? Risk Radar will not answer that question, but it will provide **you** with the tools to help you answer that question and keep the most important risks at the top of the priority ranking.

2. How Does Risk Radar Work?

Risk Radar operates in Windows 3.1 or Windows 95, and is a Microsoft (MS) Access database application. You must have MS Access 2.0, 95 or 97 on your computer for it to run. An MS Access database application is identified by a filename with an extension of "MDB,"—for example RISKDB.MDB. An MS Access database application includes all the data tables, application screens, Visual Basic code, and related

material together in one file. Each project will have its own separate Risk Radar database, and therefore its own MS Access database file.

A unique feature of MS Access is that in most cases when you change the data on the screen it is changed at the same time in the underlying database file. This means you do not have the ability to undo changes simply by exiting Risk Radar and opting not to save the changes as is the case with other applications such as MS Excel or MS Word. The word to the wise is that changes to your Risk Radar databases should be made carefully. You should also back your database up frequently, as you would any mission critical data. You should also consider keeping versions of your risk databases stored in backup files at various milestones or at regular intervals so that you can recreate the database in case something untoward happens to your original.

Risk Radar Version 1.1 is currently a single user application that is appropriate for use on a single PC. It does not include the security features that would be required for a network-based application where many users access the same database. Users with advanced experience with MS Access can add their own security features using standard MS Access operations. See the MS Access User's Manual for details.

3. Starting Risk Radar

If you have installed the correct version of Risk Radar (see installation instructions below) and if MS Access has been properly installed on your system, you should be able to click on any Risk Radar database filename (for instance RR11.MDB) in the Windows 3.1 File Manager or Windows Explorer in Windows 95 and it will automatically start MS Access and from there, Risk Radar will automatically start up. Another option is to start MS Access and then use the standard File/Open menu selections to open your Risk Radar MDB file.

Although Risk Radar uses MS Access, in general you do not need to know MS Access to use it. Risk Radar overlays its own screens on top of MS Access to help you manage risks without having to use or learn MS Access. The only exception to this is to print reports for which you use the standard report-printing screens in MS Access. However, the report-printing features of MS Access are very similar to those in other MS Windows applications and should be straightforward to use.

This release package includes two risk database files: an example risk database with example data in it, and an empty risk database with no data in it. To create a new risk database for a project, copy the empty risk database file into a new file with a meaningful name for your project and then start entering data. Use the example risk database to experiment with Risk Radar and explore its functions and reports. The specific files in this release are described below and in the README.TXT file.

Each version of Risk Radar will be released with two copies of the database files to cover MS Access Versions 2.0 and 95. MS Access 95 is also known as MS Access Version 7.0, hence the characters "_7" in MS Access 95-specific files. For instance, the example database in this release converted for use in MS Access 95 is named RR11_7.MDB. If you are using MS Access 97, use the MS Access 95 files as input to the conversion process. Incompatibilities between the MS Access 2.0 and higher versions necessitated programming changes between the MS Access 2.0 and MS Access 95 versions. The MS Access 95 files have been designed to be upwardly compatible with MS Access 97. Unfortunately, you cannot easily convert Risk Radar MS Access Version 2.0 files for use in MS Access 95 or 97.

4. New Features in Risk Radar Version 1.1

Version 1.1 includes the following new features:

- The impact date for each risk has been replaced by an impact time frame defined by the earliest and latest dates during which the impact of a risk might materialize. Another option use the keywords "BOP" for Beginning of Project and "EOP" for End of Project to define time frames that span broad areas of the schedule.

- Risks can be imported from Version 1.0 and Version 1.1 databases. You have the option of viewing the risks to be imported and selecting them one at a time, or you can import all risks from a previous Risk Radar database into an empty database all at once.
- Predefined categories can be set up for the Risk Area, Status, and Control attributes of a risk to make entries in those fields more consistent.
- The Edit Risk Short Form screen has been organized to make the best use of a single screen by using tabs to access selected information.
- Viewgraphs can now be created directly from the reports section.
- Miscellaneous changes and improvements have been made to the internal structure of the database tables and screens.

5. Hardware and Software Requirements

The following minimum configuration is required:

- IBM PC (or compatible) 386DX or better (486DX or better is recommended)
- Mouse
- 8 MB RAM
- VGA Monitor
- Windows 3.1 or higher
- MS Access 2.0 or higher

6. The Software Program Managers Network

Risk Radar was developed by the Software Program Managers Network (SPMN), which was established in 1992 by the Assistant Secretary of the Navy for all Services and OSD agencies. The Network's goal is to identify highly effective practices from industry, government, and academia, and to convey them to software managers and practitioners to improve the cost, schedule, and performance of weapons, command and control, and information systems. These best practices and lessons learned are disseminated through direct satellite broadcasts, the NetFocus newsletter, workshops, symposia, guidebooks, videotapes, and other media. For more information about the SPMN, contact Norm Brown, Executive Director, at tel 703-521-5231, fax 703-521-2603 or E-mail to SPMN@AOL.COM.

7. Disclaimer Notice

This computer software and associated documentation was developed under U.S. Government Contract No. N00039-94-C-0153. The Government has unlimited rights in such software and documentation. Copyright © 1998 Computers & Concepts Associates, a division of Integrated Computer Engineering, Incorporated. All other rights reserved.

Integrated Computer Engineering, Incorporated, makes no warranties, express or implied, including without limitation the implied warranties of merchantability and fitness for a particular purpose. Integrated Computer Engineering, Incorporated, makes no representation or warranty in respect of the use or results from application of the software regarding correctness, accuracy, reliability, or otherwise. Risk of software performance is assumed by the user.

In no event will Integrated Computer Engineering, Incorporated, its directors, officers, employees, or agents be liable for any consequential, incidental, or indirect damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising out of the use or inability to use this software even if Integrated Computer Engineering, Incorporated, had been advised of the possibility of such damages. Integrated Computer Engineering, Incorporated's liability for actual damages for any cause whatsoever, and regardless of the form of the action (whether in contract, tort

(including negligence), product liability or otherwise), is limited to the U.S. Government under Contract No. N00039-94-C-0153.

8. Acknowledgments

Risk Radar was created by John E. Moore, Ph.D., of Computers & Concepts Associates, a division of Integrated Computer Engineering, Incorporated, for the Software Program Managers Network. It was developed in MS Access 2.0 and then converted to MS Access 95 to cover both Windows 3.1 and 95 platforms. We would like to thank the many beta testers and users who provided comments and suggestions to make Risk Radar a successful risk management tool.

II. Installing Risk Radar

Risk Radar is an MS Access database application. You must have MS Access 2.0, 95, or 97 on your computer to use it. Before installing Risk Radar, you must also know which version of MS Access you have. Windows 3.1 systems can only support MS Access 2.0. Although Windows 95 systems typically have MS Access 95 or 97, in some cases MS Access 2.0 might be present instead. The MS Access 95 database files are not compatible with MS Access 2.0. Although MS Access 2.0 files can usually be converted by MS Access 95 or 97, there are minor differences between the two systems that required special programming in Risk Radar. Different sets of files are available in this release for both MS Access 2.0 and 95 to avoid difficulties. The MS Access 95 files are designed to be upwards compatible with MS Access 97. Risk Radar is typically distributed by either an installation floppy disk or from a download file from the Internet. Determine which version of MS Access you have, either 2.0, 95 or 97. If you have MS Access 97, use the instructions for MS Access 95. Once the MS Access 95 files are installed you can use MS Access 97 to convert them. Open the files with MS Access 97 and follow the instructions.

1. Floppy Disk Installation

For installing Risk Radar from an installation floppy disk, perform the following steps:

1. Insert the disk in the 3-1/2 inch drive (either A: or B:).
2. For Windows 3.1, from the Program Manager window click on File and Run. Then enter A:SETUP (or B:SETUP) in the Command Line box. For Windows 95, from the desktop click on Start and Run. Then enter A:SETUP (or B:SETUP) in the Open box.
3. Follow the instructions given by the Setup program. This program will create the directory and sub-directory C:\RISKRADR\V11 on your hard drive. The "V11" stands for Version 1.1. Setup will also ask you which version of Access you have. You will select either 2.0 or 95/97, and it will then copy the appropriate files to your hard drive.

2. Compressed File Installation

As with the floppy disk installation, you must know which version of MS Access you have, either 2.0, 95, or 97. The file RR11.ZIP contains the Risk Radar V1.1 compressed files for use with MS Access 2.0. The file RR11_7.ZIP contains the Risk Radar V1.1 compressed files for use with MS Access 95. Copy the ZIP file from the floppy to a temporary directory on your hard drive. Create a directory C:\RISKRADR\V11 and decompress the .ZIP file into this directory.

3. MS Access 2.0 Risk Radar Files

Once you have installed Risk Radar V1.1 for MS Access 2.0, the files in the C:\RISKRADR\V11 directory should be:

README.TXT	Installation and miscellaneous instructions.
RR11.MDB	The Risk Radar database with example data. This MS Access file requires MS Access 2.0.
RR11NW.MDB	An empty database you can use to create new databases.

USER11.DOC An MS Word 6.0 file containing information about Risk Radar.
PROBREPT.XLS An MS Excel 5.0 workbook for recording comments and problems.

4. MS Access 95 Risk Radar Files

Once you have installed Risk Radar V1.1 for MS Access 95, the files in the C:\RISKRADR\V11 directory should be:

README.TXT Installation instructions.
RR11_7.MDB The Risk Radar database with example data. Equivalent to RR11.MDB above.
RR11NW_7.MDB An empty database you can use to create new databases. Equivalent to RR11NEW.MDB above.
USER11.DOC An MS Word 6.0 file containing information about Risk Radar.
PROBREPT.XLS An MS Excel 5.0 workbook for recording comments and problems.

5. Problem Reporting and Suggestions

Any defects you discover or suggestions for improvement will help make Risk Radar a useful tool for other project managers. Use the Excel workbook PROBREPT.XLS to register problems or suggest improvements. E-mail the file to the address below. Should you encounter problems installing or running Risk Radar, or if you have any questions, contact:

John E. Moore
Software Program Managers Network
(703) 521-5231
riskradr@spmn.com
www.spmn.com

III. Creating a New Risk Radar Database

Version 1.1 requires you to create a new Risk Radar database file for each new project. The file RR11NW.MDB (or RR11NW_7.MDB) is an empty database you can use to create new databases. You must use this as a template to create new databases. If you enter data into RR11NW.MDB itself, it cannot be easily reused again. To create a new database:

1. Use Windows 3.1 File Manager (or Windows 95 Windows Explorer) to make a copy of the file RR11NW.MDB (or RR11NW_7.MDB for MS Access 95) into a new file. For instance, your new file might be called MYPROJECT.MDB.
2. Open the database by double clicking on it in File Manager (or Windows 95 Explorer). MS Access and then Risk Radar will be started automatically by the Windows system.
3. Click on the "Setup Project" button and enter the name of the new project, the number of days to define short-term, mid-term and long-term time frames, etc. Click on "Close." Use the "Edit Risks Long Form" screen to enter new risks into the new database.

IV. General Instructions

1. Automatic Start-up

When you start Risk Radar by using File Manager (Windows 3.1) or Windows Explorer (Windows 95) to open a directory and double clicking on a Risk Radar file (for example RR11.MDB or any Risk Radar file

with the .MDB extension) or by opening a Risk Radar file from within MS Access, the main screen will be displayed automatically. This is your home base from which to access all functions in Risk Radar.

2. Accessing MS Access Functions and Risk Radar Tables

You have access to most of the standard features available in MS Access through the menu bar at the top of the screen. These MS Access features will not be described in this guide unless they are required for running Risk Radar (for example, see the description for printing screens below). If you are interested in exploring MS Access further, you should consult the MS Access User's Guide or one of the many good reference and teaching books on MS Access.

Although the Main Screen prevents you from looking at the underlying database tables, you can close the Main Screen and you will be inside MS Access in its standard database mode. Just click on the close icon (the small box with the "X" in it in the upper right hand corner of the main screen), or click on File and then Close on the menu bar.

3. Printing Screens

Although the Reports portion of Risk Radar provides you with preformatted reports, there might be occasions when you want to print a Risk Radar screen itself for use in a presentation or a report. To print a screen, click on File on the top menu bar and then Print. See the documentation for MS Access for details. Another method of capturing screen images is to press the Print Screen key on your keyboard. This places a BMP-formatted image of the current screen in the MS Windows copy buffer. Then go to another graphics application such as MS Paintbrush and click on Edit and then Paste to paste the image into the application. From there you can print the screen image. See the documentation for Windows and your graphics application for details.

V. Main Screen

The buttons on this screen are your home base from which to input, modify, import, prioritize, display, and generate reports on a project's risks. Click on a button to open screens that will help you perform the appropriate operations. Note: The word "click" in this document means a left mouse button click. If a right mouse button click is meant, it will be called out specifically as a "right mouse click."

Set Up Project Button

The **Set Up Project** screen allows you to set project specific information, such as the title of the project, in one place. When these values have been set once for a project, they will not likely change.

Edit Risks Long Form Button

The **Edit Risks Long Form** screen is the primary screen for editing risks. This screen allows you to add new risks, modify existing risks, delete risks, and retire risks. The screen is called a long form because it requires more than one computer screen to view it all. In this screen, the risk data elements have plenty of room for field descriptions. This screen has buttons that allow you to easily add new risks, delete risks, and retire risks.

Edit Risks Short Form Button

The **Edit Risks Short Form** screen has many functions similar to the long form described above, but presents all of the information for a risk on a single screen without scrolling. This means there is less room for field descriptions. Once you are familiar with the fields on the long form, you will probably use the short form when the data on a risk has to be updated. The major functional difference between this form and the long form is that it does not have buttons to add, delete, and retire risks.

View Risks Button

The **View Risks** screen is a graphical display of risks by risk exposure category and impact time frame. This screen allows you to click on risks to uncover increasing levels of detail.

View Retired Risks Button

The **View Retired Risks** screen provides a simple table of all risks that are no longer considered a threat and have been retired from active risk management. This information might be useful in formulating new risks and for project postmortems.

Prioritize Risks Button

The **Prioritize Risks** screen is a central part of Risk Radar. It provides means for prioritizing risks using automatic sorting buttons, manually moving risks in the priority ranking, and finally renumbering the priority rank of all risks. You will use this screen for prioritizing risks, which is a principal element of risk management.

Reports Button

The **Reports** screen contains a set of predefined reports in both long-form (one risk per page) and short-form (one risk per line) formats that can be generated by clicking a button. You will use this screen to generate reports for upper management and the rest of the project team.

Exit Risk Radar Button

The **Exit Risk Radar** button will exit both the Risk Radar database and MS Access.

VI. Set Up Project Screen

The **Set Up Project** screen allows you to set project specific information, such as the title of the project, in one place. Once these values have been set for a project, they will not likely change. The data entry fields are:

Project Title

Enter the name for the project here. This will be used to identify the project in reports.

Impact Horizon Definitions

The fields shown here define the number of days that will be used to define short term, mid term, and long term for classifying the impact horizon of a risk on this project. See the Edit Risks Long Form screen description for the definition of Impact Horizon.

Risk Area Categories

This list of categories allows you to customize the text options that are available for selection in the Risk Area field to suit the needs of your project or company standards (see the Edit Risks Long Form Screen for a description of the field). The list of categories established here will be available to the user via a drop-down selection list. To add a new category, start typing in the blank line at the bottom of the list. The list will always be presented to the user in alphabetical order. To delete an item, delete all the text including any blank spaces. The text in a category can be changed using standard keyboard and mouse functions. Note that the category selection lists only provide a set of selection options that are inserted into the database as a text string. If you change the text in a category here, it will not be reflected in the previous use of that category in the database, only in new occurrences.

Status Categories

This list of categories allows you to customize the text options that are available for selection in the Status field (see the Edit Risks Long Form Screen for a description of the field). The Status field is important because it is used in the database to determine which risks are active, which are retired, and which have been deleted. The reserved keywords "Retired" and "Deleted" are also used in the database in this field, but they should not be shown to the user in this list because the user might accidentally select one of these without fully knowing the consequences. Adding and deleting categories from the list is the same as that for the Risk Area categories described above.

Control Categories

This list of categories allows you to customize the text options that are available for selection in the Control field (see the Edit Risks Long Form Screen for a description of the field). Adding and deleting categories from the list is the same as that for the Risk Area categories described above.

VII. Edit Risks Long Form Screen

1. Description

This is the primary screen for modifying risks and editing risk records. This screen allows you to add new risks, modify existing risks, delete risks, and retire risks. The screen is called a long form because it provides a description of each field that requires you to scroll down using the right scroll bar to view all input fields. This screen has buttons to add, delete, and retire risks. Fields that should have an input value are marked with a “*.” Input in the other fields is optional. Units or ranges are indicated in parentheses. Features that are common to this screen and many of the others are described in the Common Features section below.

2. Features

Prev. Button

Click on this button to see the previous risk. Risks are ordered for this screen according to their ID. You can also use the standard MS Access record navigation icons at the bottom of the screen for moving among risk records in the database. The left arrow icon, for instance, also moves to the previous risk. The record navigation icons offer more capabilities than the Next and Prev. buttons. See the MS Access user’s guide or click on Help to learn about these features. If you are at the first risk in the database, you will get a warning message when you click this button, and you will be returned to the first risk.

Next Button

Click on this button to see the next risk. The right arrow navigation button at the bottom of the screen performs the same function. If you are at the last risk in the database, clicking on Next will allow you to enter a new risk, which is the same thing as clicking on the Add New Risk button (see below).

Add New Risk Button

Clicking on this button will start the process of adding a new risk to the database. A standard long form risk screen will appear with all fields empty except the ID field and a few others with default values. The ID is set automatically by the database, so you cannot change it. By entering data into any of the other fields, a new risk will be created in the database and a new ID number will be put automatically in the ID field. If you don’t enter any data on this screen, and you either close the form (see the Close button below) or you move to the previous risk (see Prev. button above), a new risk will not be added to the database.

Note that default values will be assigned for Probability, Impact, and Rank. In addition to Title, these are the only fields that absolutely require data in them. The defaults are not “average” values, so you should change them to reflect the actual risk and re-prioritize the overall risk ranking as soon as possible. A value should be in these fields at all times to ensure consistent reporting and displays in Risk Radar.

Delete Risk Button

This button will remove the risk from the list of active risks. A warning message pops up to verify this action. Use this button to remove risks that are poorly formulated or have been replaced by another risk. Consider using the Retire Risk button before using this button. A “deleted” risk record is not actually deleted from the database, but its Status field is given a value of “Deleted,”

which means the record will not show up in the list of active or retired risks. It is possible to restore a deleted risk to either active or retired status, but this requires that you enter into the risk database table itself in MS Access and then change the value in its Status field to one of the status categories in the Set Up Project screen or "Retired."

Retire Risk Button

This button will move the current risk and its mitigation plan and historical events log from the list of active risks to the list of retired risks. The risk is not actually in a separate table, but its Status field is changed to "Retired" which makes it show up on the list of retired risks instead. It is possible to restore a retired risk to active status, but this requires that you enter into the database tables in MS Access, open the table **tblRisk**, and then change the value of the Status field in the appropriate risk record to one of the status categories in the Set Up Project screen, such as "mitigate." See **View Retired Risks Screen** section below for information on viewing retired risks.

Close Button

This button will close this screen and return you to the Main screen. See discussion at the end of this section.

ID Field (Automatic)*

The ID is the unique identifier for a risk. This ID number is set automatically by the system when new risks are added. It cannot be modified. See the discussion above on **Add New Risk Button** for details.

Title Field*

Enter a short title in this field so the risk can be easily identified in tables and reports.

Rank Field

This is the current priority ranking of the risk relative to all other risks. Rank 1 is highest priority, rank 2 next, and so on. Although you can assign a priority ranking here, the **Prioritize Risks** screen described below is designed to help you set this value. New risks are automatically assigned a rank of zero, which will temporarily place them at the top of the priority ranking until the rank is properly assigned. The "Out of" field shows the total number of active risks in the database. The **Prioritize Risks** screen should always be used to maintain the proper rank of risks. If you do not carefully maintain the risk ranking with the **Prioritize Risks** screen, it is possible for more than one risk to have the same rank number or for there to be missing rank numbers or inappropriate rank numbers (i.e. zero).

Description Field

A full description of the risk and its impact on the project can be given here. Do not include information covered in the other fields. Use the Enter key to insert paragraphs to make the text easier to read. Unfortunately, you cannot enter tabs in the text.

Status Field

This shows the current status of this risk in your risk management process. For instance, you may indicate whether it is actively being mitigated, being watched, on hold, etc. The options for the pull-down menu are set in the Set Up Project screen (see above). See the description above for a more detailed discussion of the importance of this field and the reserved keywords that should not be used.

Probability Field (%)*

This contains the current estimate for the probability (in percent) that the risk will occur over the impact time frame (see below). Values from 1% (extremely unlikely) to 99% (almost certain) are valid. This value will be based on professional judgment and past experience—in other words, most of the time it is an educated guess. This value will likely change over time as the risk is actively managed. Note that a risk cannot have a probability of 0% because that would mean the impact of the risk could never materialize, which would by definition mean it is not a risk!

Impact Field (1 to 5)*

This represents the current estimate for the impact the risk will have on the project if it materializes. Like probability above, this will likely be an educated guess. An impact is an undesirable consequence, which would negatively influence your project. The values of 1 to 5 represent a subjective ranking of the impact: 1=very low, 2=low, 3=moderate, 4=high, 5=very high. Since there are many impacts a risk might have on a project, such as greater costs, delayed schedule, reduced quality, and so forth, you should establish guidelines for your particular project for assigning a consistent impact category for different risks and projects. As an example, you might designate that impact costs of less than \$1000 correspond to an impact of 1; \$1,000 to \$10,000 an impact of 2; etc. You will likely change the impact value over time as the risk is actively managed. The primary purpose of the probability and impact numbers are to help rank risks relative to one another. The absolute value of these numbers is not as important as their consistent use over the life of the project.

Risk Exposure Display

This is not a data entry field, but a calculated value, where risk exposure equals probability times impact. Risk exposure is a standard quantitative measure of risk, and is used to compare risks with one another. Because of the limits on the ranges of both probability and impact, risk exposure will have a value between .01 (very low exposure) and 4.99 (very high exposure).

Impact Time Frame Fields*

The first field is the earliest date the risk impact could materialize and the second field is the latest date it could materialize. Dates must be entered in any of the standard formats such as “7/11/97.” Note that the keyword “BOP,” meaning beginning of project, can be placed in the first field and the keyword “EOP,” meaning end of project, can be placed in the second field. These keywords free you from having to assign specific dates for risks that cover these time frames. For instance, to describe a risk that could occur anytime during the life of the project, such as “The project leader might quit,” you would enter “BOP” in the first field and “EOP” in the second.

Days to Impact Time Frame Display

This represents the number of days from the present to the impact time frame (see above). If the earliest and latest dates of the impact time frame are both in the future, this number will be positive and will be the number of days between now and the earliest impact time frame date. If the impact time frame spans the present, this number will be zero. If both the earliest and latest dates of the impact time frame are in the past, the number will be negative and will be the number of days between now and the latest date. An active risk should never have a negative value in this field, which means the risk is in the past and is therefore no longer a threat. Negative numbers mean the risk needs to be examined more closely, either to retire it or change its impact time frame.

Impact Horizon Display

Using the definitions set up in the Set Up Project screen, the program will use the Days to Impact Time Frame value to assign the risk to an impact horizon category. NEAR represents near term, MID represents mid term and FAR represents far term.

Date Identified Field

This is the date the risk was first identified. Only standard date formatted text such as “7/15/97” or “7-Jul-97” is valid as input.

Responsible Person Field

This is the person responsible for tracking or managing the risk.

Program Areas Field

Describe project areas or components that are affected by the risk here. This might include specific products or configuration items that would be impacted if the risk were to materialize.

Affected Phases Field

Describe development phases (such as requirements or design), work packages, or work activity network components that identify which phase would be impacted if the risk were to materialize.

Risk Area Field

Use this field to assign the risk to a risk category. The pull-down menu provides a predefined set of Risk Area categories (see Set Up Project screen above).

Control Field

Use this field to indicate whether the source of the risk is internal or external to your organization. See the Set Up Project screen for setting the categories in the pull-down list.

Contingency Plan Field

The contingency plan is the set of actions that you will take should the risk materialize. If the plan is extensive, this will likely point to another document.

Risk Mitigation Description Field

Use this field to describe the approach or other background information regarding the mitigation efforts that will be taken on the risk. This field can be used in conjunction with the Risk Mitigation Steps Table (see below) to describe the intention of the mitigation efforts and how they will be done.

Risk Mitigation Steps Table

This table allows you to specify steps you wish to take in mitigating the risk. Each step has a:

Step	Number that is user-defined, but you will probably start at 1 and increment upwards.
Title	Short description of the actions to be taken.
Person	The person responsible for carrying out these actions.
Due Date	Date the step should be completed.
Completed?	A check mark to indicate if the step was completed successfully.

The steps in this table are sorted according to step number when you first view this risk. Therefore, you can reorder or insert new steps by changing step numbers, leaving this risk and coming back to it.

Historical Events Log Table

This table allows you to record events about the risk that might be useful in evaluating its importance or in justifying specific actions that were taken. For instance, external events might occur that cause you to change the impact or probability of the risk. This historical log can serve as a repository of thoughts and decisions that affect how the risk was perceived, mitigated, and hopefully retired. Each event has a:

Date	Pertinent date for information, such as the date an event occurred, the date a decision was made, etc.
Person	Person most knowledgeable about the event.
Description	A short description of the event.

The historical events in this table are sorted according to date when you first view this risk.

3. Common Features

The Close button and the record navigation buttons present on this screen are common to many of the other Risk Radar screens.

Close Button

Clicking on this button will close the current screen and return you to the screen it was called from. This button is found in the upper right hand corner. The only exception to this rule is when you are viewing reports that have been generated by MS Access report writer. In that case, the button with a “closing door” icon will close the screen. You can also use the “close window” icon which is one of the three small window-control icons found on most MS Windows screens. Warning! There are two sets of these icons, one for the MS Access window in the far upper right hand corner, and one for the Risk Radar application window just below it. Use the lower one of these sets. If you click on the far upper right “close window” icon, it will close MS Access entirely, not just the current Risk Radar screen.

Icons Record Navigation

At the bottom of many of the screens that display risks is a set of record navigation icons that are standard in MS Access. Although some of these functions are duplicated in the buttons at the top of the screen, advanced users might find these icons useful. The icons provide another means to move through the records of a table being displayed on a screen. The double left arrow moves to the first record in the table. The left arrow moves to the previous record from the present. The number shows the current record number. By changing this number, you can move to any predetermined record directly. The right arrow moves to the next record. The double right arrow moves to the last record.

It is possible to add a new risk in the Edit Risks Long Form and Edit Risks Short Form screens using the record navigation icons. Click on the double right arrow to move to the last record. Then click on the single right arrow and you will get an empty screen with the default values in appropriate fields just as if you had clicked on the Add New Risk button. As soon as you enter data in any of the fields, a new record will be created in the table. If you “navigate” out of the empty screen (left arrow, double left arrow, or close screen) without entering any data, no new record will be created. If you accidentally add a new record, you can remove it using the Delete button.

VIII. Edit Risks Short Form Screen

This screen has the same data fields as the Edit Risks Long Form, only the format is more compact to fit on a single screen for easier viewing and editing. Unfortunately this means less room for on-screen field descriptions. Once you become familiar with the fields and what they mean, you will likely use this screen

for day-to-day updating of risk data. Since the data fields are exactly the same here as in the Edit Risks Long Form, those definitions won't be repeated here.

A major difference between this screen and the Edit Risks Long Form is that it does not have any of the button functions. Use the standard MS Access record navigation icons at the bottom of the screen to step through the risks and even add a new risk. These features were discussed above. You cannot delete or retire a risk from this screen; you must use the Edit Risk Long Form for that. Close this screen by clicking on the "Close Window" icon in its upper right hand corner.

To fit all the information about a risk from the database on one screen, tabs are used at the bottom of the screen to access the Contingency Plan, Risk Mitigation Description, Risk Mitigation Plan, and the Historical Events Log. Click on one of the gray tabs and its information will pop to the front for viewing and editing.

IX. Import Risks Screen

Risks can be imported into a Risk Radar database from other Risk Radar databases. This allows an easy method for migrating risk databases created in a previous version of Risk Radar, or for importing specific risks from another database that might be appropriate for reuse. Enter the full path name for the risk database in the Import Database File Name field. After clicking on the OK button, the program will determine automatically if the import database is in Risk Radar V1.0 or V1.1 format and will display the appropriate import screen.

1. Import Risks from a RR V1.0 Database

This screen displays each risk in the import database in a long-form format. There are two different methods of importing risks, which are described in the descriptions for the **Import This Risk** and **Import All** buttons below. The basic restrictions are that, if the existing database is a new database with no risks in it, you can import all of the risks from the import database simply by clicking on the Import All button. Otherwise you will have to import risks one at a time using the Import This Risk button. The Prev. and Next buttons have the same functions for moving through the risk records as described previously.

Import Active/Retired Risks Pull-Down Selector

Use this pull-down selector to choose between viewing the active risks or the retired risks in the import database.

Import This Risk Button

This button will execute a procedure to import this risk into the database. The warning message describes some of the assumptions that will be made concerning differences in the format of Risk Radar V1.0 and V1.1 databases. The import risk ID will likely not be preserved after it is imported because the program automatically assigns it the next available number in the sequence. If you have a need to track a risk back to its previous database, you should write the message down and record the changed ID numbers in the historical events log.

Import All Button

This button will import all risks, both active and retired, from the import Risk Radar V1.0 database into this V1.1 database. This button is active only if the database is new and without any risks in it. All IDs will be preserved between the import and new databases using this method. To create a new database that is empty, see the section **Creating a New Risk Radar Database** above.

2. Import Risks from a RR V1.1 Database

This screen works identically to the one above with the following exception: when the Import All button is used, all risks, including those that were deleted, are imported into the new database. Otherwise the same restrictions apply:

- The Import All button will only work on a new database.
- You can import risks one at a time from both the active and retired lists but their ID numbers will not be preserved.

IX. View Risks Screen

1. Description

This screen is designed to show you the number of risks in all possible probability/impact combinations, and categorized according to time frame. By clicking on any of the grid cells, you will be given a list of the actual risks in that probability/impact bin; and by clicking on the Risk ID of the displayed risks, you will be given a full description in short-form format. There are six primary elements on the screen:

Legend Box

Describes graphical elements used in the five Probability/Impact grids. The shading increases from white for low-risk exposure, to light gray for medium-risk exposure, to gray for high-risk exposure. The number in each grid cell shows the number of risks in that grid cell category.

Total No. of Risks Grid

Shows the number of risks in each Probability/Impact grid cell category for all active risks, regardless of Date of Impact. The three shaded zones correspond to risk exposure categories of low, medium, and high. The risks that present the lowest risk exposure are in the lower left hand corner. The risks that present the highest risk exposure are in the upper right hand corner.

Impact Time Frame in Past Grid

Displays the same information as the first grid, except only for those risks whose Impact Horizon is completely in the past. These risks should be examined to determine if they are still active, in which case the Impact Time Frame fields should be updated. If the threat of their impact has already passed, then the risks should be retired (see **Edit Risks Long Form Screen** above).

No. of Short-term Risks Grid

Displays the same information as the first grid, except only for those risks whose Impact Horizon is in the short term, as defined in the Project Set Up screen. The risks in this grid most likely present the greatest threat to the project because they are most likely to materialize the soonest. It is likely your mitigation efforts will concentrate on the risks with the highest exposure in this grid first.

No. of Mid-term Risks Grid

Displays the same information as the first grid, except only for those risks whose Impact Horizon is in the mid term, as defined in the Project Set-up screen.

No. of Long-term Risks Grid

Displays the same information as the first grid, except only for those risks whose Impact Horizon is in the mid term, as defined in the Project Set-up screen.

2. Risks Pop-up Screen

By clicking on any of the nonblank grid cells, a screen will pop up listing the risks in that grid cell. This can be used to quickly identify which risks are present in each category.

3. Risk Detail Screen

By clicking on the ID of any of the listed risks in the pop-up, a full screen display in the short-form format will come up, showing all of the risk fields as well as the mitigation plan and historical events tables.

X. View Retired Risks Screen

Retired risks are those that have been removed from the list of active risks and placed in the retired risks list. This screen provides a one-line description along with a few pertinent data fields for each retired risk. See the description of the **Retire Risks** button under the **Edit Risks Long Form Screen** for a detailed discussion.

To see the details about a retired risk, click on its ID, and the **Retired Risk Detail** screen will pop up which shows the risk information in short-form format. You cannot edit this data.

A retired risk is not actually in a separate table, but its Status field has been changed to "Retired" which makes it show up on the list of retired risks instead. It is possible to restore a retired risk to active status, but this requires that you enter into the risk database table itself in MS Access, open the table **tblRisk**, and then change the value of the Status field in the appropriate risk record to one of the status categories in the Set Up Project screen, such as "mitigate."

XII. Prioritize Risks Screen

The key purpose behind any risk management tool is to help you track and mitigate those risks with the greatest threat to your project. Since most projects have limited resources, not all risks can be actively mitigated all the time. The problem is dynamic because the importance of most risks will change over time or be influenced by external forces that are not in your control. What was an important risk one week might be less critical the next or might have been upstaged by other risks. In most organizations, a set number of risks, such as 10 or 20, are actively being mitigated at any one time. It is critical to know what the highest-priority risks are and how they stack up against the others. The Prioritize Risks form is designed to help you make these decisions.

Note that new risks created with the Edit Risks Long Form screen will have a default rank of zero (unless the user changes it) and will thus be shown at the top of the list. Zero is not a valid ranking, but it provides visibility to those risks that have not been fully evaluated and ranked. It is also possible for more than one risk to have the same rank (for instance, if the user edited the rank field and set the number by hand, or if a risk were imported from another database), or for there to be missing rank numbers (which might occur if a risk were retired or deleted). That is not important when first coming into this screen, but you should not exit this screen without making sure all risks are ranked properly and sequentially. The only way to ensure this is to click on the "Renumber Ranking" button after prioritizing the risks on the screen in the order you want (see discussion below). You have a great deal of flexibility in assigning rank and priority in Risk Radar; but it is important that you maintain the ranking of all risks on a regular basis using this screen to ensure there are no zero rank numbers, no missing rank numbers, and no duplicate rank numbers.

When the Prioritize Risks screen first comes up, risks will be presented one to a line, sorted according to rank (shown in blue) with the highest priority at the top. Using this form, you can explore different orderings of the risks by reordering them on the screen, irrespective of their current priority ranking, before committing to a new priority ranking. This screen provides two automatic ordering buttons and a manual method for reordering risks. The screen also allows you to edit values, so you can change values for any of the visible fields here, including probability, impact, and rank. Note that changing values on this screen automatically changes them in the underlying database.

Exposure Button

The **Exposure** button at the top of its column will automatically sort all risks according to their risk exposure. This is the most common way to prioritize risks because the probability and impact numbers are used to quantify the overall risk exposure, which is a single measure of relative risk.

Rank Button

The **Rank** button at the top of its column will automatically sort all risks according to rank. This is the default ordering of risks when the screen first appears. You can also change the rank of a risk by editing its rank field and then clicking on the **Rank** button to move it to a new position. If you have not changed the actual rank numbers of any risks, this button allows you to return the risks to the original order when you started. This can be useful for undoing a series of changes when you might want to explore another prioritization of the risks.

Move Column

Although the risk exposure parameter (which is automatically calculated by Risk Radar by multiplying probability and impact) can help you rank a risk relative to the others, you should keep in mind that this is not a completely objective value and that ranking risks necessarily involves the subjective expert option based on professional experience. While there are other important factors, such as Impact Horizon, that might be important, there could be completely subjective reasons for ranking one risk higher than another, such as “The boss thinks this one is the most important.” There are also likely to be risks that have the same risk exposure, and therefore need to be ranked relative to one another.

The **Move** column allows complete flexibility in ordering the risks. Using this column, you can move individual risks up or down in the list. Place the letter “m” (for MOVE) in the first column of a risk to mark it for movement. Then place the letter “a” (for AFTER) or “b” (for BEFORE) in the first column of another risk where you want it moved. Once the risk has been moved, these letters are automatically erased to be ready for the next move.

Renumber Ranking Button

Once you are satisfied with the new priority of risks represented by their ordering from top to bottom on the screen, their rank can be changed appropriately by clicking on the **Renumber Ranking** button. This will renumber the rank of each risk according to its current order on the screen. Note that once this operation has taken place, the rank cannot be automatically returned to its previous state. This is the only way to ensure that there are no risks with a rank of zero, none with duplicate rank numbers, or that none of the rank numbers is missing.

If you leave this screen without clicking on this button or without changing any of the rank numbers manually, the risks will have the same rank as when you started.

XIII. Reports Screen

1. Description

This screen offers three groups of sample reports. The group titled **Detailed Report** prints out reports with each risk starting on a new page. The group titled **View Graphs** prints out risks in a viewgraph format. The group titled **Summary Report** prints out a much shorter version with each risk on a new line. The risks in these reports are sorted according to the criteria specified, for instance by risk ID or rank.

Clicking on one of these buttons will generate a standard MS Access print preview of the report. If you are satisfied with the report, click on File and then Print (or the printer icon) to send the report to the printer.

2. Exporting Reports to MS Word or MS Excel

There are other options for capturing a report so it can be used in another document or processed further, for instance, as an MS PowerPoint file.

Text Output

If you have the “Generic/Text Only on File” MS Windows printer option selected as the printer in the print window, you can send the text portion of the report to a file in ASCII format. The text can then be formatted or processed further by a variety of applications. Another method is to click on File, then Output To, and then choose the MS-DOS text option.

MS Word or MS Excel Output

To capture a report in MS Word or MS Excel format, click on File, then Output To, which provides a list of options. Choose “Rich Text Format” to save the report in an RTF format file, which can be read by MS Word or another word processor, and which roughly approximates the format of the report on the screen.

To capture the data used in the report, click on File, then Output To, and then select the MS Excel option. The data will be saved in a .XLS file, which can be further processed by MS Excel or other spreadsheets.

7 ANNEX C – PROGRAM METRIC EXAMPLES

Examples of Product-Related Metrics

Engineering	Requirements	Production	Support
Key Design Parameters <ul style="list-style-type: none"> • Weight • Range • Time on Station • Accuracy Design Maturity <ul style="list-style-type: none"> • Open problem reports • Number of ECPs • Drawings released • Failure reports Mission Computer capacity utilization	<ul style="list-style-type: none"> • Requirement stability • Requirement traceability • Threat stability • Mission profile maturity • Requirement validation complete at each requirement level • Requirements prioritized 	<ul style="list-style-type: none"> • Unit Production Cost • Process proofing 	<ul style="list-style-type: none"> • Special tools and test equipment • Support Infrastructure footprint • Manpower estimates

Examples of Process Metrics

Design Requirements	Trade Studies	Design Process	Integrated Test Plan	Failure Reporting System	Manufacturing Plan
Requirements traceability verified Specifications reviewed for definition of all use environments Specifications reviewed for all functional requirements for each mission performed	Alternative configurations examined Test methods selected CAIV implementation	Design requirements stability Producibility analysis conducted Design analyzed for Cost Parts reduction Testability Manufacturing	All developmental tests at system and subsystem level identified Identification of who will do each test (Government, contractor, supplier)	Contractor corporate management involved in failure reporting and corrective action process Responsibility for analysis and corrective action assigned to specific individual with close-out date	Plan documents production methods Plan contains schedule and sequence at prime and subcontractor levels Manufacturing inclusion in design process

Examples of Cost and Schedule Metrics

Cost	Schedule
<ul style="list-style-type: none"> • Cost variance • Cost performance index • Estimate at completion • Management reserve • CAIV targets • Total Ownership Cost 	<ul style="list-style-type: none"> • Establish and maintain IMP and IMS • Schedule variance • Schedule performance index • Design Schedule Performance • Manufacturing Schedule Performance • Test Schedule Performance

8 ANNEX D – SAMPLE FORMS

OAMCM Candidate Risk Identification Form

Date Risk Identified	System	Risk	Time Frame	Impact	Po	Mitigation Action(s)	Point(s) of Contact
Calendar Date of when risk is submitted mm/dd/yy	Integration, RAMICS, ALMDS AMNS, SWIMS, or AQS-20/X	IF [state risk] THEN [consequence]	Impact Start and End Calendar Dates mm/dd/yy	5 – Critical 4 – Serious 3 - Moderate 2 – Minor 1 - Negligible	Percent between 1% and 99%	Recommended Action (One per cell, if multiple mitigation actions are necessary)	Last Name(s) of Recommended Point(s) of Contact for each recommended action

H-60 AMCM Sample Detailed Risk Report

Detailed Report: Risks by Rank

AMCM Integration

Report Dated Oct 27 1998

Risk ID044 *Stable funding for integration, sensor, platform* Ranked 4 out of 35 risks

Description: IF program integration, sensor, platform, and weapon funding is not stable THEN additional costs and schedule delays will be incurred in fielding Organic AMCM

Probability: 99(%)

Exposure: 4.95

Impact: 5(1=low, 5=high)(Prob. x Imp.; .01 = very low, 4.95 = very high)

Impact Time Frame: Sep 15 1998 to: Sep 15 2003

Days to Impact Time Frame: 0

Impact Horizon: NEAR

Date Identified: Sep 17 1998

Responsible Person: Morgan, Blevins, Hunt

Program Area:

Affected Phase:

Risk Area:

Control:

Current Status: Mitigate

Contingency Plan

Mitigation Plan

Step	Description	Person	Due Date	Done?
1	Develop POM input for 00 individually and then cooperatively	Blevins, Hunt, Morgan		
2	Revisit program strategy and ACAT target and develop point paper	Morgan, Hunt		

Historical Events

H-60 AMCM Sample Summary Risk Report

Summary: Risks by Rank

AMNS

Report Dated Oct 28 1998

Rank	ID	Title	%	Prob Impact Expo- Impact			Control	Status
				1-5	sure	Horizon		
1	003	Ordnance handling/mounting/jettison	99	5	4.95	NEAR		Mitigate
2	001	H-60 Integration Direction for AMNS	95	5	4.75	NEAR		Mitigate
3	007	S/W Development - Common Console	95	5	4.75	NEAR		Mitigate
		vs. AMNS						
4	005	AMCM and AMNS IPT Communication	90	4	3.60	NEAR		Mitigate
5	009	A/C Vulnerability - Shallow Water	80	4	3.20	NEAR		Mitigate
		Detonation						
6	008	Common Console Video for AMNS	80	4	3.20	FAR		Mitigate
7	010	AMNS Training	80	4	3.20	FAR		Mitigate
8	002	AMNS Software Data Rights	75	3	2.25	NEAR		Mitigate

9 ANNEX E – BORDA VOTING METHOD

The Borda method is used in the Risk Matrix software application to rank risks from most-to-least critical on the basis of multiple evaluation criteria. This annex describes in detail how the Borda method is applied, using the sample Risk Matrix below as an illustration.

Sample Risk Matrix Chart

Risk No.	Risk	<i>I</i>	<i>P_o</i> %
1.	• Poor design	5	.10
2.	• Algorithm misunderstood • ICD problems	5	.60
3.	• Antenna performance	4	.90
4.	• Wrong power supply ratings • wrong connectors • cosite problems	2	.10
5.	• hard to get pilot consensus	2	.99
6.	• Different Users	4	.60
7.	• Integrated circuit lead time	4	.40

E.1 Background

Borda [2] proposed the following voting method in 1770: Given N candidates, if points of $N - 1$, $N - 2$, . . . , and 0 are assigned to the first-ranked, second-ranked, . . . , and last-ranked candidate in each voter's preference order, then the winning candidate is the one with the greatest total number of points. Instead of voters, suppose that there are multiple criteria. If r_{ik} is the rank of alternative i under criterion k , the Borda count for alternative i is

$$b_i = \sum_k (N - r_{ik})$$

The alternatives are then ordered according to these counts.

The Borda method is an example of a *positional voting method*, which assigns P_j points to a voter's j th-ranked candidate, $j = 1, \dots, N$, and then determines the ranking of the candidates by evaluating the total number of points assigned to each of them. Voting theorists [7, 8, 9] have shown that the Borda

method is the optimal positional voting method with respect to several standards, such as minimizing the number and kinds of voting paradoxes. In addition, if ties are not present in the criteria rankings, Cook and Seiford [10] demonstrated that the Borda method is equivalent to determining the consensus rankings that minimize the sum of the squared deviations from the criteria rankings. The Borda method has been used to rank alternatives in a variety of applications, including a cost and operational effectiveness analysis (COEA) [3] and an aircraft maintenance study [4].

In the Risk Matrix application, let N be the total number of risks, and the index i denote a particular risk. Let the impact assessment be denoted by $k = 1$, and the probability assessment be denoted by $k = 2$. The rest of this section describes how the Borda voting method is implemented in the software application.

E.2 Evaluate Rank of Each Risk with Respect to Impact

Let J be the total number of possible impact assessments. For the original Risk Matrix, Table 2 shows that $J = 5$. Let Q_j be the j th possible impact assessment, which is assumed to be ordered in the following way: Q_j has a higher impact than Q_{j+1} . Let M_j be the number of risks having Q_j as the impact rating. Table E-1 gives the values of Q_j and M_j that are used for our numerical example, where the values of Q_j are determined by Table 2 and the values of M_j are derived from Table 1.

Table E-1. Values of Q_j , M_j , and T_j for Sample Matrix

j	Q_j	M_j	T_j
1	5	2	1.5
2	4	3	4
3	3	0	N/A
4	2	2	6.5
5	1	0	N/A

Let T_j be the rank position for all risks that are given the j th possible impact assessment. How can we evaluate this rank position? The basic approach is to evaluate the rank of a tied alternative as the average of the associated rankings [3, 4, 10]. The following is a key result: if a is the first term in an arithmetic progression, t is the final term, and n is the number of terms, then $(n/2)(a + t)$ is the sum of the n terms. Because there are M_j risks that are tied for positions 1 through M_j , the sum of these rank positions is $(M_j/2)(1 + M_j)$. Thus, the average of this sum is $T_j = (1/2)(1 + M_j)$. Similarly, there are M_2 risks that are

ted for positions M_{j+1} through $M_j + M_2$, so that the average of this sum is $T_2 = (1/2)(2M_1 + 1 + M_2)$. More generally, if $M_j > 0$,

$$T_j = \frac{1}{2} (2C_j + 1 + M_j)$$

where

$$C_j = \sum_{r=1}^{h-1} M_r$$

for $h > 1$ and $C_1 = 0$. The values of T_i are given in Table E-1 for the sample Risk Matrix.

Let r_{ij} be the rank of the i th risk with respect to the impact assessment. If the i th risk has the j th possible impact assessment, then set $r_{ij} = T_j$. The values of r_{ij} are given in Table

E-2 for the sample Risk Matrix.

Table E-2. Borda Points and Count

Risk No.	<i>I</i>	<i>P_o</i>	<i>R_{il}</i>	<i>R_{i2}</i>	Borda Count	Borda Rank
1	5	10%	1.5	6.5	6.0	4
2	4	60	1.5	3.5	9.0	0
3	4	90	4	2	8.0	1
4	2	10	6.5	6.5	1.0	6
5	2	99	6.5	1	6.5	2
6	4	60	4	3.5	6.5	2
7	4	40	4	5	5.0	5

E.3 Evaluate Rank of Each Risk with Respect to Probability of Occurrence

Let H be the total number of possible probability assessments. In the case OAMCM, $H = 5$. (very likely = 1, likely = 2, about half the time = 3, unlikely = 4, and very unlikely =5). Our numerical illustration also uses $H = 5$.

Let P_h be the highest probability associated with the h th possible assessment, and let these probabilities be ordered such that $P_h > P_{h+1}$. Let N_h be the number of risks that are assigned the h th possible probability assessment. Table E-3 shows the values of P_h and N_h that are used for our numerical example, where the values of P_h are determined by (very likely = 1, likely = 2, about half the time = 3, unlikely = 4, and very unlikely =5) and the values of N_h are derived from the sample risk matrix above.

Table E-3. Values of P_h , N_h , and S_h for Sample Matrix

h	P_h	N_h	S_h
1	100%	1	1
2	90	1	2
3	60	2	3.5
4	40	1	5
5	10	2	6.5

Let S_h be the rank position for all risks that are given the h th possible probability assessment. As before, if $N_h > 0$,

$$S_h = \frac{1}{2}(2B_h + 1 + N_h)$$

where

$$B_h = \sum_{r=1}^{h-1} N_r$$

for $h > 1$ and $B_1 = 0$. The values of S_h are given in Table E-3 for the sample Risk Matrix.

Let r_{i2} be the rank of the i th risk respect to the probability of occurrence. If the i th risk has the h th possible assessment, then set $r_{i2} = S_h$. The values of r_{i2} are given in Table E-2 for the sample Risk Matrix.

E.4 Determine Borda Ranking

Let N be the total number of risks, which satisfies

$$N = \sum_{h=1}^H N_h$$

The Borda Count for risk i is computed with

$$b_i = (N - r_{i1}) + (N - r_{i2})$$

The final step is to rank the risks with respect to their Borda Count. In particular, the risk with the highest Borda Count is the most critical, the risk with the second highest count is the next most critical, and so forth. Table E-2 provides both the Borda Count and the implied ranking for the sample problem. The Borda Rank for a given risk is the number of other risks that are more critical than it.

10 GLOSSARY

AMCM Airborne Mine Countermeasures
APB Acquisition Program Baseline
ARG Amphibious Ready Group
CAIV Cost As an Independent Variable
CCDR Contractor Cost Data Reporting
CPM Critical Path Method
CRD Capstone Requirements Document
CVBG Carrier Battle Group
DAD Defense Acquisition Deskbook
DBMS Database Management System
DoD Department of Defense
DT&E Developmental Test and Evaluation
EAC Estimate At Completion
EMD Engineering and Manufacturing Development
EV Earned Value
EXCOM Executive Committee
GAO Government Accounting Office
IBR Integrated Baseline Review
IMP Integrated Master Plan
IMS Integrated Master Schedule
IPPD Integrated Product and Process Development
IPTs Integrated Product Teams
ITT Integrated Test Team
KPPs Key Performance Parameters
LCC Life-Cycle Cost
MDA Milestone Decision Authority
MDAPs Major Defense Acquisition Programs
MIS Management Information System
MNS Mission Need Statement
MS Milestone
OAMCM Organic Airborne Mine Countermeasures
ORD Operational Requirement Document
OT&E Operational Test and Evaluation
PM Program Manager
PMO Program Management Office

PMWS Program Manager's Work Station
POM Program Objective Memorandum
RFP Request for Proposal
RMC Risk Management Coordinator
RMP Risk Management Plan
SEI Software Engineering Institute
SMCM Surface Mine Countermeasures
SME Subject Matter Expert
SOW Statement of Work
SPMN Software Program Managers Network
T&E Test and Evaluation
TEMP Test and Evaluation Master Plan
TPM Technical Performance Measurement