



**NAVY
AERIAL TARGET & DECOY SYSTEMS (PMA-208)
RISK MANAGEMENT PLAN (RMP)**



Version 1.0

18 April 2007





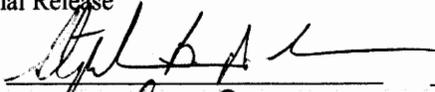
NAVY TARGET & DECOY SYSTEMS (PMA-208) RISK MANAGEMENT PLAN (RMP)

Version 1.0

Original Release Date	Contract Number (If Required)
-----------------------	-------------------------------

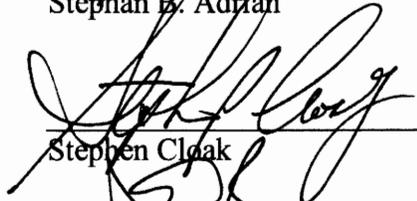
Signatures for Original Release

AUTHOR:


Stephan B. Adrian

PMA-208 Risk Management Administrator
Title

REVIEWED:


Stephen Cloak

PMA-208 Chief Engineer
Title

APPROVAL:


Pat Buckley, CAPT, USN

PMA-208 Program Manager
Title



TABLE OF CONTENTS

1.0	INTRODUCTION	1
1.1	Purpose.....	1
1.2	Scope.....	1
2.0	REFERENCES	1
3.0	PROGRAM OFFICE RESPONSIBILITY	2
3.1	Program Level 2 IPTs and Integrated Product Teams	2
4.0	RISK MANAGEMENT ORGANIZATION/RESPONSIBILITIES	2
4.1	Responsibilities and Authorities	3
4.1.1	Periodicity	3
4.1.2	Program Manager.....	3
4.1.3	Deputy Program Manager (Level 2 IPTL).....	4
4.1.4	PMA-208 Risk Management Administrator	4
4.1.5	Risk Board Members	4
4.1.6	IPT Lead.....	5
4.1.7	APMSE	5
4.1.8	Risk Owner	5
4.1.9	Core Team Members.....	5
5.0	RISK MANAGEMENT PROCESS	5
5.1	Identify	7
5.2	Assess.....	8
5.3	Plan	8
5.4	Control	9
5.5	Communicate and Document.....	9
6.0	RISK MANAGEMENT IMPLEMENTATION.....	9
6.1	Risk Assessment Approach.....	10
6.1.1	Risk Assessment Matrix	10
6.1.2	Assessment Criteria	11
6.2	Risk Management Boards.....	11
6.2.1	Risk Validation	12
6.3	Monitor Items.....	12
6.4	Training.....	12
6.5	Risk Management Integration with Program Management Processes	12
6.5.1	Affordability	12
6.5.2	Work Breakdown Structure	13
6.6	Risk Management Process Implementation.....	13
6.7	Risk Management Database Software Tool.....	13
	APPENDIX A.....	A-1
	APPENDIX B.....	B-1
	APPENDIX C	C-1



LIST OF FIGURES

Figure 1: Typical Program Risk Management Organization.....	3
Figure 2: Risk Management Process.....	7
Figure 3: PMA-208 Risk Management Process.....	10
Figure 4: Risk Assessment Matrix and Legend.....	11



1.0 INTRODUCTION

Risk Management is an organized means of identifying risks and managing the necessary risk mitigation actions. PMA-208 risk management will be accomplished using the “one team” approach of its Government/Contractor Integrated Product Teams (IPTs) and support team structure. This strategy will identify critical areas and risk events, both technical and non-technical, and help determine the necessary actions for mitigation before they cause major performance, schedule, and cost impacts.

The PMA-208 Risk Management Administrator will manage the administrative aspects of the PMA-208 Risk Program. The Integrated Program Teams will manage program risks using information about potential risk events to help set risk mitigation objectives, develop acquisition and management strategies, and identify metrics that allow continuous tracking and assessment of its program/projects status. The PMA-208 risk management process is designed to assist in PMA-208’s decision-making and acquisition control process for achieving success with its target and decoy systems deliveries to the Fleet.

1.1 Purpose

The purpose of this Risk Management Plan (RMP) is to implement a common risk management process within the Navy Aerial Target & Decoy Systems Program Office (PMA-208) that conforms to the guidelines promulgated in the NAVAIR Risk Management Instruction.

The objectives of this RMP are to:

- Define how risk will be managed for the PMA-208 program office.
- Identify who will be responsible for managing risks.
- Define methods for properly assessing risk.
- Establish measures for evaluating risk.
- Define the means for identifying, monitoring, tracking and controlling risk.

The primary objective is to reduce risk to an acceptable level and do so within cost, schedule, and performance constraints.

1.2 Scope

This document provides information on all aspects of implementing risk management. Topics covered include the PMA-208 Program Office’s approach used for assessing risks, risk management responsibilities, the location of the risk management tool, and the reporting of risk data. A brief overview of the risk management process is also included.

2.0 REFERENCES

The following references were used in the preparation of this plan:

- DoD 5000.2 of 12 May 2003
- Risk Management Guide for DoD Acquisition of Aug 2006
- NAVAIR Risk Management Guide



- NAVAIR Risk Assessment Handbook
- NAVAIRINST 5000.21A of 2 Nov 2005
- NAVAIRINST 5100.11A of 28 Nov 2005
- NAVAIRINST 4355.19B of 10 Apr 2006
- PMA-208 Risk Management Database (RMDB) Tool User's Guide, Draft

3.0 PROGRAM OFFICE RESPONSIBILITY

PMA-208 is responsible for the development and procurement of all Navy Aerial Target & Decoy Systems. PMA-208 procures a spectrum of targets and decoys, small to full scale, via a series of programs of record to achieve threat representative targets for Fleet training and system test and evaluation.

3.1 Program Level 2 IPTs and Integrated Product Teams

PMA-208 is comprised of five (5) Level 2 IPTs as follows: Supersonic Targets, Full Scale & Subsonic Targets, Subscale Aerial Targets (SSAT) Development, Control Systems & Common TAAS and Decoys. The Supersonics Targets IPT includes the GQM-163A, AQM-37 and MA-31 programs. The Full Scale & Subsonic Targets IPT includes BQM-34/74E, AST/QF-4 and UAV & Land Targets programs. Each program will establish and maintain their individual Program Risk Charter and Program Risk Criteria. Each of the IPT charters are contained in Appendix C. As applicable, each Risk Management Board (RMB) shall be comprised of a Level II IPT lead Assistant Program Manager for Systems Engineering (APMSE), Assistant Program Manager for Logistics (APML), Business Financial Manager (BFM), Prime Contractor PM/Lead System Engineer, and other members relevant to the program strategy, phase, and risks.

4.0 RISK MANAGEMENT ORGANIZATION/RESPONSIBILITIES

The risk management organization for the PMA-208 Program Office is not a separate entity, but is integrated into the PMA's IPT structure with NAVAIR functional competencies supporting the IPTs as required. Each of the respective IPTs reports to their Level II IPT who then reports to the PM. The PM is responsible for the overall success of the programs/projects within the Program Office in particular managing resources (budget and manpower) and meeting schedule. Figure 1 below depicts a typical program risk management organization.

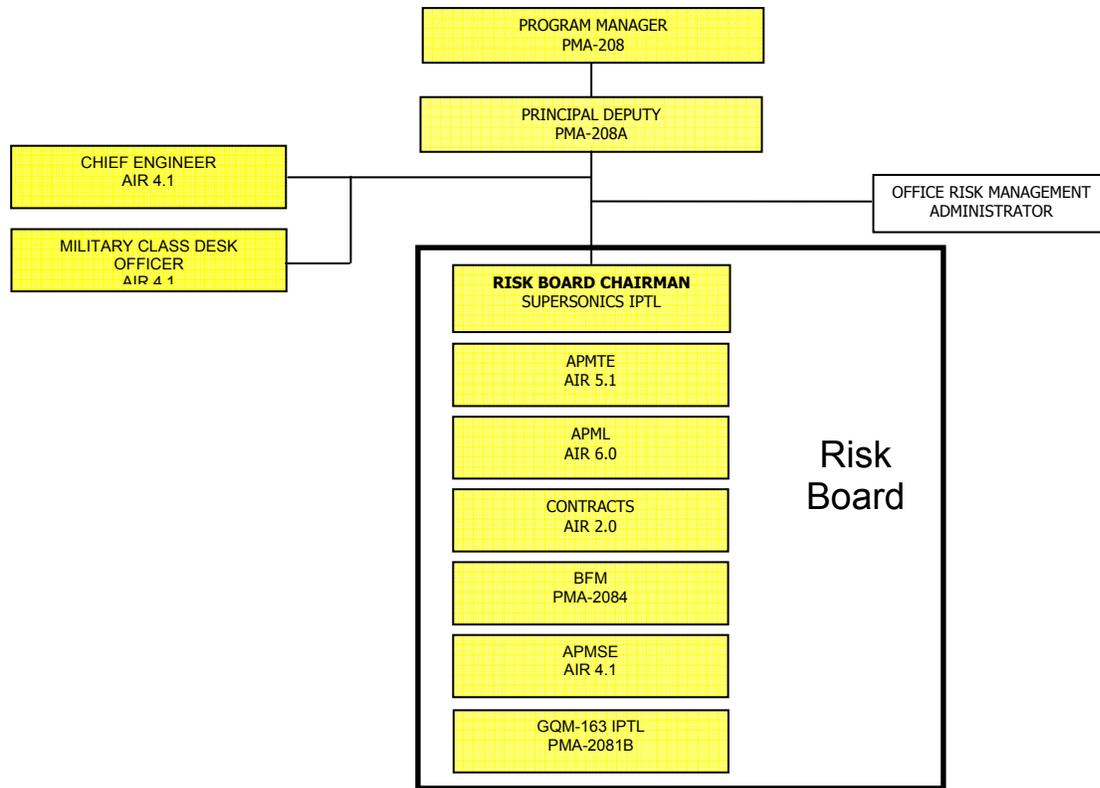


Figure 1: Typical Program Risk Management Organization

4.1 Responsibilities and Authorities

4.1.1 Periodicity

Each project/program team risk board shall convene at least once a month (more if necessary) in order to identify and track risks and risk mitigation progress (understanding that risk mitigation is a normal part of the daily work load). If an IPTL is working with multiple vendors/contractors and sensitive contractor specific issues are discussed during RMBs, convening separate RMBs for each vendor/contractor is an accepted practice. Common sense applies; remember the process is tailorable.

4.1.2 Program Manager

The Targets Program Manager has ultimate responsibility for implementation and performance of the risk management process. Chairmanship of product risk boards is delegated to the Level 2 IPT Leaders. The Program Manager retains the following responsibilities and roles in the risk management process:

- a. Develop a RMP in order to establish and implement an integrated risk management process
- b. Ensure each program IPT establishes defined risk criteria for their program



- c. Approve recommended changes to the RMP
- d. Ensure the formation of a RMB
- e. Report program risks to appropriate PEO/PMA/NAVAIR/Fleet personnel

The Principal Deputy Program Manager maintains the same responsibilities as the Program Manager as described in paragraphs 4.1.2a thru 4.1.2e and shall support the Program Manager as necessary.

4.1.3 Deputy Program Manager (Level 2 IPTL)

The respective Deputy Program Manager (i.e. Supersonics, Subsonics) will chair the RMB for their IPT and report the results to the Program Manager. Additionally, the IPTL has the following responsibilities:

- a. Approve program risk candidates
- b. Approve program risk closure
- c. Obtain and direct resources as necessary to mitigate risks

4.1.4 PMA-208 Risk Management Administrator

The PMA-208 Risk Management Administrator is responsible for managing the risk process and risk tool in use by the individual IPT's Risk Management Teams and Program Office leadership. Additionally, the Risk Management Administrator has the following responsibilities and roles:

- a. Attend the various IPT Program Risk Management Review Board meetings and capture and publish the meeting minutes
- b. Maintain the PMA-208 RMP
- c. Maintain the PMA-208 Risk Management Database (RMDB)
- d. Create the PMA-208 RMDB Tool User's Guide
- e. Facilitate and/or coordinate risk management training with the Program IPT's Program Management Risk Coordinator
- f. Prepare risk briefings, reports, and documents required for program reviews
- g. Prepare/submit monthly status report of all programs to the PMA

4.1.5 Risk Board Members

Each RMB shall be comprised of a Level 2 IPTL, Assistant Program Manager for Systems Engineering, Assistant Program Manager for Logistics, Business Financial Manager, Prime Contractor PM/Lead System Engineer, Vendor/Contractor representative, and other members relevant to the program strategy, phase, and risk assessments/mitigation plan. The board members have the following responsibilities:

- a. Review risk candidates and mitigation plans/assessments
- b. Determine which candidates are valid risks and in need of attention
- c. Provide input to the Chairman as to which valid risks will be actively managed as managed/accepted risks



- d. Provide input to the Chairman as to which valid risks will be actively managed or maintained as managed/monitored items
- e. Review program risk status

4.1.6 IPT Lead

Responsibilities:

- a. Implement the RMP
- b. Establish and maintain their individual Program Risk Charter and Program Risk Criteria
- c. Ensure valid risks are assigned to a risk owner for risk assessment and development of a mitigation plan
- d. Track and status each risk mitigation plan
- e. Maintain currency of risk database

4.1.7 APMSE

The APMSE has the same responsibilities as the IPT Lead as described in paragraphs 4.1.6a thru 4.1.6e and shall support the IPT Lead as necessary.

Additionally:

- a. Is responsible for technical risk management
- b. Will be the primary briefer to the RMB

4.1.8 Risk Owner

When assigned by the IPT Lead the risk owner will be responsible for the following:

- a. Developing the risk likelihood and consequence assessments
- b. Developing the mitigation plan
- c. Implementing the risk mitigation plan
- d. Delegating risks to other individuals or teams as required for assistance in assessing/mitigating assigned risks

4.1.9 Core Team Members

Identify and submit as risk candidates, items that may affect program success. These should be items that have a probability of occurrence that, without specific mitigation actions, will have negative consequences in cost, schedule, or technical areas. Core team members will assist the risk owner in assessing the risk and developing a mitigation plan. The core team members will support the IPT lead and APMSE as needed when presenting the risks to the RMB.

5.0 RISK MANAGEMENT PROCESS

The objective of risk management is to apply a systematic process for identifying, assessing, planning, controlling, communicating, documenting, and reporting program risks and associated risk events. Risk is defined as an undesirable situation or uncertainty that has a realistic and possible likelihood of occurring and that results in an unfavorable consequence if it does occur.



Risk is not a problem. It is an understanding of the level of threat due to potential problems. Each risk has different degrees of technical, schedule, and cost consequences. Risk management occurs continuously throughout the program life cycle and consists of a five-step process (1) Identify, (2) Assess, (3) Plan, (4) Control, and (5) Communicate and Document as shown in Figure 2. Risk management is performed at all levels of the program hierarchy. IPTs or other teams are best able to identify potential risk items at the lowest level within the system where handling those risks can frequently be accomplished with the least impact to the total system.

Key factors for the success of any risk management program include, but are not limited to:

- Garnering management commitment for the use of the risk management program and subsequent risk mitigation process.
- Assigning accountability - putting someone in charge!
- Introducing it early in the program.
- Putting risk management in the statement of work and ensuing contract. For example, in the RFP, require as deliverables, a vendor risk management program that clearly identifies risk likelihood, consequences, and mitigation steps along with an initial assessment of risks. In the Statement of Work (SOW), require as CDRLS monthly participation in NAVAIR IPT risk management boards. When performing a source selection, do not be afraid to use risk management and past performance with Risk management as evaluation factors for award. Award fees for risk management, while a contracting issue, are not out of the realm of possibility. If a team is contracting for In-Service Support, ensure that provisions are made for Operational Risk Management Support.
- Involving and committing your team(s) to the risk management process.
- Focusing on mitigation plans.
- Not carrying risks with un-resourced mitigation steps. If a risk is not important enough to apply resources to its solution, it is not worth carrying.
- Choosing a suitable technology for database access and updates.
- Using technical reviews, checklists, and involving the competencies and your prime contractor (and any sub-contactors when necessary).
- Tailoring the risk program to the project/program; keeping it simple!

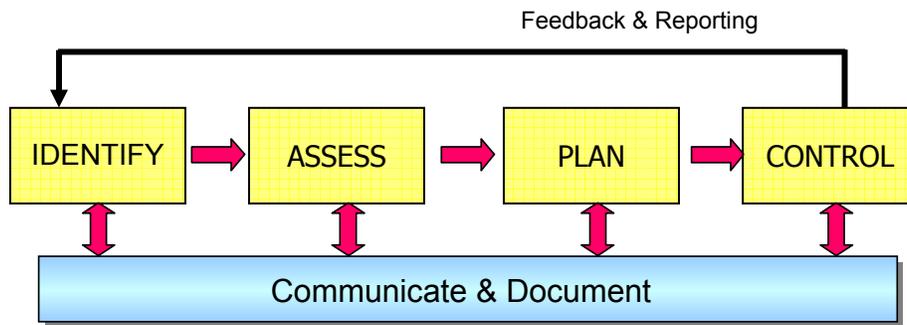


Figure 2: Risk Management Process

5.1 Identify

The first step in the risk management process is identifying risks that would prevent the program/projects from achieving its objectives. This is an activity that encompasses all program personnel to survey the range of potential technical and programmatic problems across the program. Customer and supplier inputs are necessary to ensure thoroughness and completeness in identifying risks. Risk identification is done continually throughout the program life cycle to assure that new risks (technical and programmatic) are addressed. Upon the completion of this step, the potential risk becomes a risk candidate. The following represent a small sample of indicators that may be helpful in identifying and assessing risks:

- Lack of stability, clarity, or understanding of requirements: Requirements drive the design of the system. Changing or poorly stated requirements guarantee the introduction of performance, cost, and schedule problems.
- Failures to use best practices virtually assure 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 qualifications of people, there is risk.
- Test failure may indicate corrective actions are necessary. Some corrective actions may not fit available resources, or the schedule, and (for other reasons as well) contain risk.

Each Program will assess the level of Cost and Schedule risks in accordance with the criteria defined in the individual IPT Risk Management Charters, Attachment 1 (Program Risk Criteria).

After risks have been identified, a clear risk statement is written in an “IF...THEN” format. The “IF” portion contains the risk or condition and the “THEN” portion contains the consequences to the program if the risk is not mitigated. The PMA-208 Program Risk Assessment and Criteria examples are depicted in Appendix B.



5.2 Assess

Once identified, risks are assessed to determine the likelihood of occurring and the consequences of the risks if they do occur. This evaluation provides a basis for prioritizing efforts and allocating resources for managing risk.

To gauge the relative severity of identified risks, risks are rated against predefined likelihood and consequence criteria, as documented in the individual IPT risk management charters. This provides a consistent means for evaluating risks so that objective comparisons of risks can be conducted. Further, depending on the assessment rating, risks can be characterized as high, moderate, or low based on established rating thresholds. Lastly, the criteria provide a means for assessing reductions in likelihood and consequence based on the mitigating actions taken.

The likelihood criteria used to evaluate a particular risk depend on the source of the risk being evaluated. Risk categories, each with a corresponding set of likelihood criteria, are defined for general sources of risk. General risk categories include engineering, management, manufacturing, requirements, support, technology, and others. Risk categories may be expanded to any number of specific areas to provide criteria for evaluating the risk that more accurately reflects the nature of the risk and will be documented in each Program's respectable Risk Management Charter.

Any given risk will have components affecting technical, schedule, or cost performance. Consequence criteria are used to evaluate each risk and categorize it based on which area of consequence has the greatest severity at the time of assessment. For example, technical consequence criteria, assesses the impact of the risk against meeting technical performance goals or requirements or any other area other than schedule or cost. Correspondingly; schedule consequence criteria assesses the impact to meeting schedule, and cost consequence criteria assesses the impact to meeting cost allocations or budgets.

5.3 Plan

This step of the risk management process determines the approaches and plans for mitigating the root cause of the risks. First, the handling approach is determined. Risk handling alternatives consist of avoiding, transferring, assuming, or mitigating a risk. The principal handling approach, however, is mitigation. Risk mitigation alternatives are defined below:

Avoiding Risk – The process of revising component or system designs or plans to eliminate a source of risk. Avoidance includes trading off risk for performance or other capability and is a key activity during requirements analysis. As an example, a lower risk mature technology may be substituted for another higher risk new technology. Simply stated, it eliminates the sources of high or possibly moderate risk and replaces them with a lower risk solution and may be supported by a cost/benefit analysis.

Transferring Risk – The process of reallocating subsystem, component, or interface requirements and responsibilities to other program or product teams to reduce the overall system risk. It effectively moves the risk from one area of design to another where a solution is less risky. Requirements and responsibilities may be transferred to customers, suppliers, or associate contractors.

Assuming Risk – The process of accepting a risk. A risk may be accepted when the likelihood and consequence levels have been reduced to a level that has been determined



as acceptable. Risks may also be assumed if further mitigation exceeds cost or schedule allocations. In this case, efforts would be made to control the conditions that may cause the risk to be realized.

Mitigating Risk – The process of reducing risk likelihood and consequence levels via the systematic completion of mitigation actions. It is the deliberate use of the design process to lower the risk to acceptable levels. When mitigation is selected as the risk handling approach, detailed risk mitigation plans and events are developed.

5.4 Control

This step of the risk management process is associated with monitoring and tracking established action implementation plans. Risk actions are tracked to risk management implementation plans and mitigating steps are determined and implemented. Risks are re-assessed and re-planned as appropriate. Monitoring risk metrics, responding to trigger events, and switching to contingency plans, when needed, are part of controlling risks.

5.5 Communicate and Document

Communicating and documenting risk information at all steps in the process is essential to effectively implementing risk management. The process of reporting and reviewing the status of risk is the principal mechanism for implementing risk management on a program or project. Communicating risks involves presenting the current likelihood and consequence assessment for a particular risk as well as the planned reduction in likelihood and consequence resulting from the completion of mitigation events. Missed, delayed, or failed mitigation events can be identified, and the overall risk status of a particular system, subsystem, or component can be assessed via reporting the status of all risks associated with the item being evaluated. PMA-208 will utilize a risk management software tool to facilitate assessing, communicating, documenting, and reporting risks

6.0 RISK MANAGEMENT IMPLEMENTATION

Figure 3 provides a detailed depiction of the PMA-208 risk management process. The planning phase defines the overall risk management process and how it will be implemented for the PMA-208 Program. This element of the process is recurring and supports the implementation of the other three elements of the risk management process by defining objectives and assigning responsibilities for each of the risk management processes.

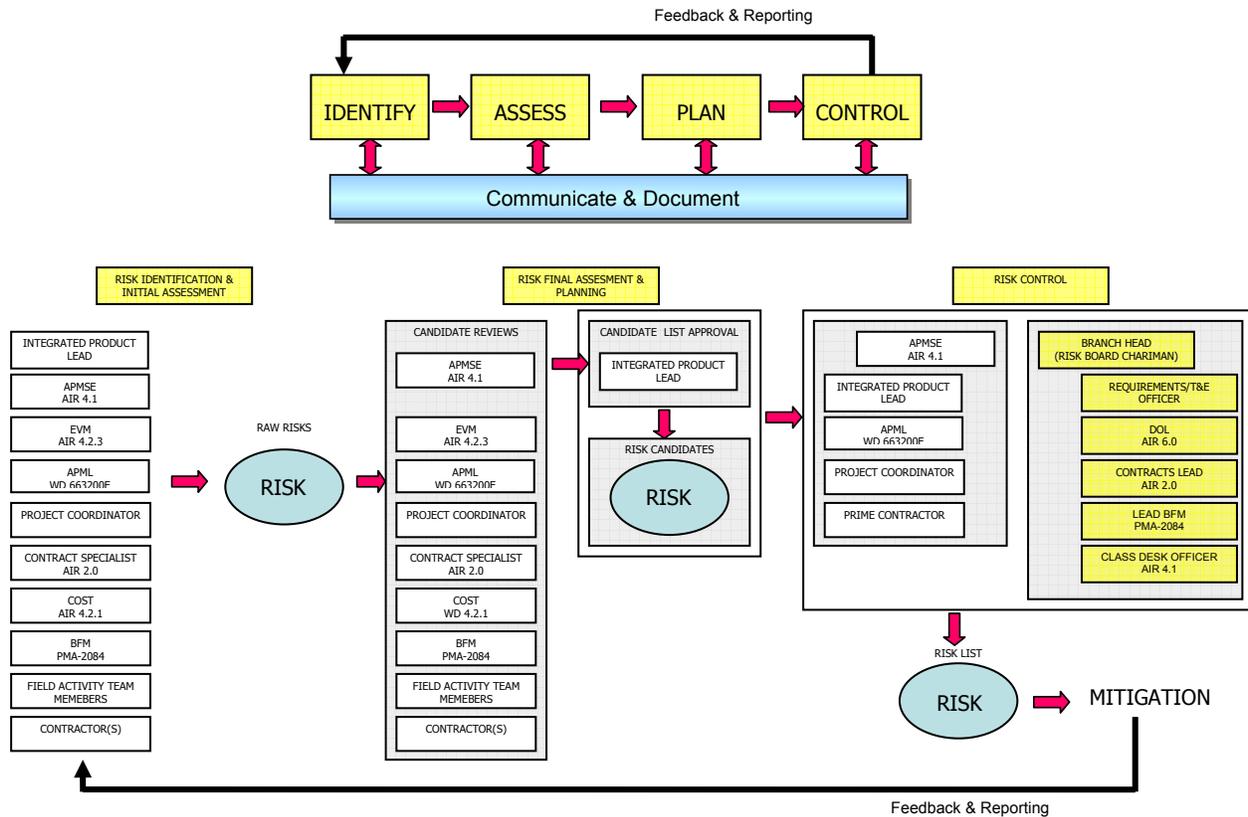


Figure 3: PMA-208 Risk Management Process

6.1 Risk Assessment Approach

The assessment methodology used to evaluate risks employs a 5 by 5 assessment matrix (risk cube) for comparing risks and tables of risk likelihood and consequence criteria.

6.1.1 Risk Assessment Matrix

The 5 by 5 risk assessment matrix provides a graphical representation of risk status. Risks are mapped on the matrix according to their likelihood and consequence assessment. Likelihood is measured on the vertical axis, and consequence is measured on the horizontal axis. Both axes consist of five levels of assessment for a total of 25 likelihood-consequence combinations on the matrix. Green, yellow, and red colored regions on the matrix indicate areas of low, moderate, and high risk, respectively. The 5 by 5 risk assessment matrix is shown in Figure 4.

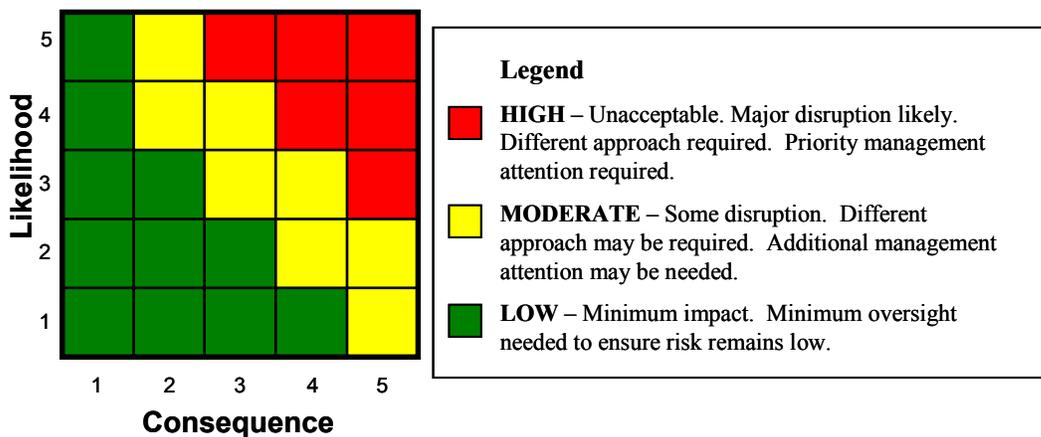


Figure 4: Risk Assessment Matrix and Legend

6.1.2 Assessment Criteria

Likelihood and consequence assessment criteria have been defined for assessing risks. Each set of criteria has five levels of increasing likelihood and consequence severity. Consequence assessment criteria - technical, schedule, and cost measure the impact or seriousness of an event on the success of a product. Each IPT will determine and define their programs risk criteria, which will be included in their Risk Charters.

Mitigation plans for risks that are initially prioritized as “High” may have a contingency plan. Contingency plans ensure that an alternative approach is available to mitigate risks that have a significant likelihood of occurrence and/or severe consequences. If the primary risk mitigation plan is not yielding the required reduction in risk, a contingency plan may be executed. Typically, contingency plans have features that make them less attractive approaches: they cost more, take more effort (time), or involve a degradation of overall performance.

Key to developing contingency plans is determining a decision point or “cutover” date to implement the contingency. This is the date or event by which action must be taken to move to the contingency approach. Determination of the contingency decision date, determined by the risk owner, is based on two factors: the date when the total risk mitigation activity must be complete, and expected reduction results of the primary plan as it relates to the length of time it will take to accomplish the alternative approach (this may be a criterion instead of a date).

Risk mitigation plans with contingency plans will be monitored by the RMBs and the contingency plans will be implemented when the primary mitigation plan is not yielding the required reduction in risk.

6.2 Risk Management Boards

The primary responsibility of the RMBs is to manage the risks on each individual PMA-208 IPT Program. The RMB is composed of both contractor and NAVAIR team members representing all disciplines of the PMA-208 organization. Each IPTs RMB will meet to review new risk candidates, existing risk assessments/ mitigation activities and watch items. Management includes the tracking and evaluation of risks by reporting, feedback on watch list items or action



items, and input on potential developing risks. The RMBs in conjunction with the respective IPTs will approve/disapprove new risk candidates and closure of completed risk.

6.2.1 Risk Validation

Risk validation comes as a function of the Assess stage in the risk management process. With the input from the RMB, risk owners start the assessment process of the risk. Identification looks at sources or drivers for the uncertainty and quantifies risk. Analysis (root cause analysis) includes isolation of the cause for risk and determination of the impact. The RMB validates a risk with the risk owner when the risk is formally accepted and documented. Of primary importance is the fact that Issues – risks that have materialized – are not to be included in the Risk Management Database or any risk reports.

6.3 Monitor Items

The risk review boards manage all risks. Accepted/Monitored Risks are typically low-level risks or items that have the potential to become an active risk (accepted/managed) in the future of the program. Accepted/Monitored Risk statuses are reviewed at each RMB meeting to ensure current status. Each IPT RMB will manage their Accepted/Monitored items.

6.4 Training

Risk training is essential to effectively implement risk management and will be conducted for all PMA-208 personnel. Risk training includes an overview of the methodologies presented in this document as well as an introduction on using the risk management software tool. The PMA-208 Risk Management Administrator will facilitate or coordinate training with each IPTs Program Management Risk Coordinator.

6.5 Risk Management Integration with Program Management Processes

Risk Management and Program Management share common areas of technical, schedule, and cost constraints. Program management defines the technical, schedule, and cost goals and utilizes processes, tools, and resources to achieve the goals. Risk management identifies, assesses, and responds to risks to increase the potential of achieving program goals.

The health of a program is measured by the degree of success in meeting technical, schedule, and cost performance goals. By definition, risks are factors that negatively affect program health. Therefore, there is strong interest in linking the risk process to various other program management processes in order to maintain a healthy program.

Effective linkage of risk management and program management processes and associated tools reduce potential performance deterioration by providing for the right focus and for timely management decisions and actions. Subsequent paragraphs describe the linkages that have been established or are currently being developed. Figure 5 provides a detailed depiction of the Program Management and Risk Management Correlation.

6.5.1 Affordability

All program risks are identified through the risk management process and entered in the PMA-208 RMDB. Ideally, the affordability of the mitigation steps has been built into each individual



IPT Program's Budget Execution Plan. If there is no intention of applying resources to a mitigation step (remember, it is not advisable to carry risks with un-resourced mitigation steps), then the risk is not important enough to carry.

6.5.2 Work Breakdown Structure

The Work Breakdown Structure (WBS) is the framework for program planning, and status reporting. The WBS is often the basis for the product architecture and program IPT organization. Funding and scheduling are also tied to WBS elements.

6.6 Risk Management Process Implementation

All program personnel are responsible for risk management within their respective domains. Accordingly, risks can be identified and assessed by any member of the program team. Once identified, a "candidate" risk is evaluated by the RMB to ensure it is not already being tracked and is a valid risk per the current design and/or process. When the RMB accepts a risk that should be managed, initial assessments and plans are adjusted as required, and the risk is assigned to an owner who is responsible for implementing the plan to control the risk. The individual Risk Management Review Boards conduct the process of accepting a risk and assigning an owner.

Monitoring and tracking a risk that has been accepted is an essential risk management function to ensure that mitigation or other risks handling plans are being implemented and to make decisions associated with the risk. Risk management decisions involve a number of considerations:

- a. Is the risk valid? (Is the risk a risk or is it an issue?)
- b. Is the risk assessment correct?
- c. Is the selected handling approach appropriate based on the current circumstances?
- d. Is the mitigation plan consistent with other program plans?
- e. Is the mitigation plan within the scope of current plans and budgets?
- f. Is the mitigation plan sufficiently developed?
- g. Should the risk be transferred to another team?
- h. Should the risk be elevated or demoted to another level of the risk reporting team structure?
- i. Should the risk be closed?

6.7 Risk Management Database Software Tool

To facilitate the implementation of the risk management process, the PMA-208 program uses a web-based program risk management database software tool. The tool facilitates identifying, assessing, planning, controlling, communicating, documenting, and reporting risks. The PMA-208 Risk Management Database is located at <https://ntrx.navair.navy.mil/riskex/pma208/index>. Each IPT Lead will provide the PMA-208 Risk Management Administrator with a completed Risk Project/Program Setup form detailing which risk management functions will be enabled. Please reference the PMA-208 Risk Management Database User's Guide for direction on how to use the software tool.



APPENDIX A: Acronyms & Definitions

Acronyms

<u>Acronym</u>	<u>Definition</u>
APML	Assistant Program Manager Logistics
APMSE	Assistant Program Manager Systems Engineering
BFM	Budget Financial Manager
DoD	Department of Defense
DoDD	Department of Defense Directive
DOL	Director of Logistics
ICD	Initial Capabilities Document
ID	Identification
IMS	Integrated Master Schedule
IPT	Integrated Product Team
NAVAIR	Naval Air Systems Command
NAVAIRINST	Naval Air Systems Command Instruction
PM	Program Manager
PMA	Program Manager, Air
RMB	Risk Management Board
RMDB	Risk Management Database
RMP	Risk Management Plan
SNTC	System for Naval Target Control
SSAT	Sub Scale Aerial Target
TA/AS	Target Augmentation/Auxiliary Systems
WBS	Work Breakdown Structure

Definitions

<u>Term</u>	<u>Definition</u>
Consequence	A result of an action, process, etc. Consequence factors are defined in each of the individual program/project IPT charters.
Contingency Plan	An alternative approach to mitigate risks that have a significant likelihood of occurrence and/or severe consequences. If the primary risk mitigation plan is not yielding the required reduction in risk, a contingency plan must be available.
Integrated Product Team (IPT)	A multi-discipline, product-focused team composed of both Contractor and Naval Air Systems Command (NAVAIR) personnel, responsible for the development, delivery, and support of a product or element of a product for the Navy Target & Decoys.



<u>Term</u>	<u>Definition</u>
Issue	An event that is certain to occur (or has already occurred) and entails negative consequences. The important difference between an issue and a risk is that issue management is focused toward mitigating current effects, while risk management seeks to mitigate future effects and root causes. An issue and a risk are not necessarily independent or easily distinguished; the review of an issue might reveal a continuing risk from the unresolved root cause of the issue.
Late Mitigations	A summary of risks for the current project that have a mitigation step(s) past the Planned Step <i>completion</i> date. (Reports only available to Risk Management Board (RMB) Members)
Likelihood	The chance or fact that an event will occur. Likelihood factors are defined in each of the individual program/project IPT Charters.
Managed/Accepted	A risk that has been accepted and is being managed by the respective program/projects RMB.
Managed/Monitored	A risk that has been determined to be a possible risk and will be monitored to determine impact to the program by the respective program/project RMB.
Mitigation Plan	A detailed set of steps to accomplish a reduction in risk for a given risk item. Each step is known as a mitigation event. Each event has a defined set of exit criteria which, when accomplished, define the closure of the event. Each event may affect the likelihood and/or consequence of the risk. However, several events may need to take place to produce a reduction in risk level.
Program Manager (PM)	Responsible for integrating and managing all aspects of the program to ensure product integrity and customer satisfaction. Interfaces with upper management and is involved in program issue resolution.
Program Risk Management Coordinator	Each IPT Lead will assign an individual the role of Program Risk Management Coordinator. The assigned will be responsible for coordinating the RMB Meetings, risk management training, maintaining risk statuses in the PMA-208 RMDB, ensuring the RMB Lead and Program IPT Lead are informed of risk status, and coordinating risk management training.
Realized Risk	A risk that is no longer a risk. It is a problem or an issue, which is managed differently than a risk.
Risk	A measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints and has two components: (1) the <i>probability/likelihood</i> of failing to achieve a particular outcome, and (2) the <i>consequence/impacts</i> of failing to achieve that outcome.
Risk Action Plan	The actions to be initiated to reduce or eliminate the likelihood of a risk and/or its consequences should the risk occur.
Risk Assessment	Identifying and analyzing program risks in order to estimate the probability of occurrence and the severity of the impact(s) should the risk materialize as a real problem. Risk assessment increases the chances of meeting cost, technical performance, and schedule objectives.
Risk Candidate	A potential risk. A risk candidate identifies a possible occurrence that would have a negative impact on the program.
Risk Charter	A document setting forth the individual program/project Risk Management Team objective, roles, and responsibilities.



<u>Term</u>	<u>Definition</u>
Risk Event	An event within the program that could result in a problem with the development, production, performance, and/or fielding of the system. Risk events should be defined to a level such that the risk and causes are understandable and can be accurately assessed in terms of probability and consequence. For processes, risk events are assessed in terms of process variance from known best practices and potential consequences of the variance.
Risk Identification	The process of examining each program task to identify potential problems (risks), the impacts of those potential problems, and items/drivers.
Risk Item	An approved risk candidate. Each risk item must have both an event with a finite likelihood of occurrence and a consequence (negative impact) to the program.
Risk Level	A value indicating the likelihood of the risk and the consequences if the risk occurs.
Risk Management	The act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analyzing) risk areas, developing risk-handling options, monitoring risks to determine how risks have changes, and documenting the overall risk management program.
Risk Management Board (RMB)	A group of individuals chartered to review risk assessments and mitigation activities, often from a broader perspective than initially performed by the risk originator.
Risk Management Board (RMB) Lead	An individual assigned by the program IPT Lead responsible for chairing the RMB Meetings.
Risk Management Plan (RMP)	A document identifying a program's methods of identifying, assessing, controlling, and reporting risk on a program.
Risk Mapping	The process of plotting the intersection of the risk likelihood and consequence factors on the 5 by 5 risk matrix.
Risk Monitoring	Systematically tracking and evaluating the performance of risk mitigation plans to determine that risk is managed.
Risk Owner	The person assigned responsibility, authority, and accountability for the management of a risk item. The owner may be a Contractor or a NAVAIR person. In either case, the owner will be teamed with their counterpart. The risk owner manages the whole risk item but other individuals or teams may be assigned responsibility for individual risk events within the mitigation plan.
Risk Reporting	The reporting of risks to affected individuals, teams, management, and the Customer.
Risk Repository	A data repository that contains all risk management data for the program. The risk repository includes the program risk list, risk ownership information, risk assessment information, risk priority ranking information, risk action plans, risk closure criteria, risk status, and other data necessary to perform risk management. The risk repository provides query and report capability to support risk management analysis. It allows for continuous visibility of risk management information.
Team Member	Any person supporting an individual program/project IPT and or the Navy Aerial Target and Decoy Systems Program Office (PMA-208).
Unmitigated Risks	Risks that either have no mitigation plan, or will not be "green" by their impact date. (Reports only available to Risk Board Members).
Valid Risk	Status of a Risk Candidate that is accepted by the Risk Review Board.



<u>Term</u>	<u>Definition</u>
Watch Item	Typically low level risks that will be monitored periodically or items that have the potential to become a risk in the future of the program.
Watch List	Red & Yellow risks within the short/past term impact range.

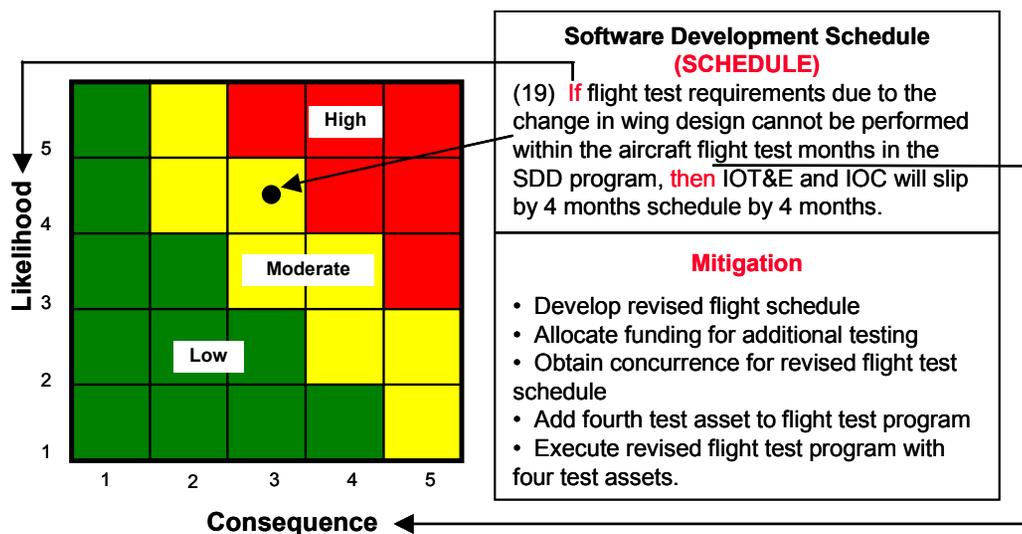


APPENDIX B: PMA-208 PROGRAM RISK ASSESSMENT AND CRITERIA



PMA-208 Program Risk Assessment

- **ALL Risks must be written in the IF, THEN format** (e.g., **if** software development schedule continues to lag behind the FS System schedule, **then** ground and flight testing will be delayed impacting cost and schedule.)
- Insert the Risk Title above the Risk Description along with the category (cost, schedule, performance).
- Insert the Risk Number to the left of the Risk Description.
- List the Mitigation steps below the Risk Description (i.e., after divider line.)
- Mitigation steps must address either likelihood or consequence.
- Mitigation actions must be funded and staffed.
- Draw a line from the risk description text box to the corresponding risk level in the risk cube.
- It is recommended, but not required, to report High risks on one slide and Medium risks on another, not exceeding 5 risks on each slide. Where possible, risks should be “bundled” for briefing purposes.
- Low risks can be reported by listing their risk number, title, and description on a separate slide .



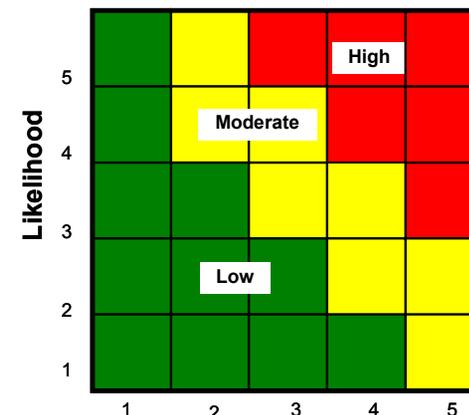
Updated 23 January 2006



PMA-208 Program Risk Criteria

What is the Likelihood the Risk Will Happen?		
Level	Likelihood	Prob of Occurrence -- Your Approach and Process...
1	Not Likely:	... Will effectively avoid or mitigate this risk based on standard practices (~10%)
2	Low Likelihood:	... Have usually mitigated this type of risk with minimal oversight in similar cases (~30%)
3	Likely:	... May mitigate this risk, but workarounds will be required (~50%)
4	Highly Likely:	... Cannot mitigate this risk, but a different approach might (~70%)
5	Near Certainty:	... Cannot mitigate this type of risk; no known processes or workarounds are available (~90%) without mitigation

Likelihood



Consequence

Level	Technical Performance	Schedule	Cost
1	Minimal or no impact (inconvenience or annoyance)	Minimal or no impact	Minimal or no impact
2	Minor technical/supportability shortfall (no impact to KPPs, OPEVAL or COIs – Part III, Pri 4, or Minor Deficiencies)	Additional activities required, able to meet key dates <i>Slip < ? Month(s)</i>	Budget increase or unit production cost increases <i>< ? (1% of Budget)</i>
3	Moderate technical/supportability shortfall (Part II or Pri 3 Deficiencies)	Minor schedule slip, no impact to key milestones <i>Slip < ? Month(s) of critical path.</i> <i>Sub-system slip > ? Month(s)</i>	Budget increase or unit production cost increase <i>< ? (5% of Budget)</i>
4	Major technical/supportability shortfall (Part I*, Pri 2, or Major Deficiencies)	Program critical path affected, all schedule float associated with key milestone exhausted <i>Slip < ? Months</i>	Budget increase or unit production cost increase <i>< ? (10% of Budget)</i>
5	Cannot meet KPP or Key technical/supportability threshold (Part I**, Pri 1, or Severe Deficiencies)	Cannot meet key program milestones <i>Slip > ? Months</i>	Exceeds APBA threshold <i>> ? (10% of Budget)</i>

Consequence

Each program needs to document the schedule and cost consequence criteria in the respective risk management charters and provide that information here.

Updated 23 January 2006



APPENDIX C: Sample Risk Management Board Agenda

The following list offers topics for consideration when convening a monthly risk management board. Please keep in mind that this is provided as a guideline and is not intended to serve as a mandatory agenda.

1. Program Overview
 - a. Key Performance Parameters (KPPs – provided as a reminder for potential APBA breaches)
 - b. Schedule
2. Team Organization
 - a. Government
 - b. Contractor
3. System Overview
 - a. System Requirements
 - b. Constraints
4. Configuration Item Breakout (if under scrutiny for risk)
 - a. Major Physical Interfaces
 - b. Major Functional Interfaces
5. Process Overview (recommended for program in the early stages – first 6 months of life)
 - a. Program Management
 - b. Configuration Management
 - c. Systems Engineering and Trades
 - d. Logistics and Integrated Logistics Analysis Status
6. Requirements Management and Risk Assessments (as applicable to the phase of the program)
 - a. Risk Management
 - b. Software Management/Metrics
 - c. Test Planning (Lab, Ground, Flight)
 - d. Major Facilities/Tools
7. Configuration Item (CI) Review and Risk Assessment
 - a. CI Design Status versus Allocated Requirement
 - b. Performance (KPPs and Derived Requirements)
 - c. Interoperability
 - d. Reliability, FMECA
 - e. Maintainability
 - f. Supportability
 - g. Producibility/Manufacturing Engineering/Qualification Process
 - h. Constraints (weight/Balance/Volume/Power/etc.)
 - i. Physical and Functional Interface Requirements
 - j. Environmental Affects
 - k. EMI/EMC
 - l. Man-Machine Interface
 - m. Parts/Materials Selection
 - n. Built-in Test, Fault Isolation
 - o. Development/Operational Test Status



- p. Logistics Elements
 - 8. Additional Risks
 - 9. Production Risk Assessment
 - 10. OT Risk Assessment
 - 11. System Safety Assessment
 - 12. Risk Summary Activity
 - 13. Risk Reporting Plan
 - 14. Adjourn