SPACE ENVIRONMENT TECHNOLOGIES

Space Research *Space Operations* *Space Standards*

DRAFT
Risk Management Process Plan
Command Media

Written by:	Reviewed by:	Reviewed by:
__ Electronically Signed _	___Electronically Signed__	_____
XXXX	Tyrone Jackson	James E. French
Approved by:	Approved by:	Approved by:
_____	_____	_____
S. Dave Bouwer	Rian Shelley	W. Kent Tobiska

ORGANIZATIONAL MISSION ASSURANCE STANDARD: TIER 1

Risk Management Process Plan

SET ™

Revision: 0 Release: 05-06-2011 Effective: 05-06-2011

STANDARD

OBJECTIVE

This Standard defines SET's approach for implementing a Risk Management Process, and describes the roles and responsibilities of the Project Manager (PM), project personnel, major subcontractors, and the customer. Each identified risk is documented, assessed, tracked, and updated in a project Risk Database that complies with the risk metrics defined in this Standard.

APPLICABILITY

This Standard applies to all present and future SET sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a Risk Management Process Plan has been contractually imposed.

Table of Contents

FIGURES

TABLES

1 INTRODUCTION

The SET Project Manager (PM) is required to establish and implement a Risk Management Process to identify risks early, assess their impacts, and execute feasible and effective mitigation or control plans as an integral part of the System Engineering process. The PM is the owner of the Risk Management Process, and as such, is responsible for its administration and improvement.

The Project Risk Management Board (PRMB) is required to review all risk submittals on behalf of the PM to verify the designated Risk Owner and the initial Risk Classification. Each risk is classified as Low, Moderate, Serious, or High. The Risk Classification is based on the likelihood and consequence metrics defined in Tables 1, 2 and 3. Low Risks are reported to the Chief Engineer for adjudication. Moderate Risks are reported to the PM for adjudication. Serious and High risks are reported to the PM, who then reports them to the customer for collaborative adjudication.

The designated Risk Owner is required to coordinate the performance of an initial risk assessment to determine if the risk is actionable and can be mitigated, i.e., burned down. A practical mitigation plan is developed for each actionable risk. Non-actionable risks cannot be mitigated and are classified as residual risks that must be accepted by the appropriate authority. The goal is to identify all significant residual risks early enough to control their likelihood of occurrence, if practical. A practical control plan is developed for each significant residual risk, with the appropriate risk acceptance authority determined by the contractual requirements, this Standard, or the PRMB, in that order of precedence.

Each major subcontractor is required to have a Risk Management Process that is consistent with this Standard. At a minimum, the major subcontractor must report the significant risks associated with their deliverables using data products that comply with the risk metrics defined in this Standard. Each SET project coordinates its risk management activities with those of its major subcontractors to avoid duplication in effort, while ensuring that customer unique impacts are identified and managed by the appropriate process. This coordination occurs at multiple levels, e.g., between subject matter experts at the subcontractor and at SET, between Risk Owners at the subcontractor and at SET, and between Mission Assurance Leads at the subcontractor and at SET.

1.1 Scope

This Standard provides the PM with the risk management criteria needed to make informed decisions regarding uncertain future events that could threaten the ability of the system to meet its technical, performance, safety, cost, and schedule requirements. This Standard addresses risk reporting requirements placed on the project by the customer and/or by applicable government policies/regulations. This Standard meets the government's requirements for Operational Risk Management (ORM), as set forth in DoD and Air Force policies, regulations, and instructions.

1.2 Purpose

The purpose of risk management is to prevent, reduce, or control future impacts of unfavorable events as opposed to reacting to unwanted events that have already occurred. The typical SET software development project is exceedingly complex, and hundreds of potential problems can impact program execution at any time. Thorough mitigation of every plausible risk is beyond the project's available resources and is therefore impractical. Hence, effective risk management requires a process to determine which risks are actionable, e.g., can be mitigated, and which risks are non-actionable or residual, e.g., cannot be mitigated, but be controlled (if identified early enough), watched, or transferred, and must be accepted by the appropriate authority.

An effective risk management process must start from the ground up with participation from all levels of the SET project. Therefore, the project's risk identification process starts with the activities of each subject matter expert. Also, proper risk identification and mitigation must also have the full support of the management chain for success. To ensure this the PM is held accountable for proper risk handling and responsible for residual risks deemed acceptable.

1.3 Application

This Standard defines a risk management process that is structured, continuous, proactive, and focuses on early identification and mitigation or control of significant risks. Any High, Serious, or Moderate Risks identified by this process are considered Significant Risks, and are handled accordingly.

2 REFERENCES

2.1 Normative References

The following reference documents of the issue in effect on the date on invitation for bid or request for proposal form a part of this Standard to the extent specified:

AIAA S-102.1 Mission Assurance Management

1) AIAA S-102.0.1 (Draft) Mission Assurance Program (MAP) General Requirements

2) AIAA S-102.1.1 (Draft) Mission Assurance Program Planning (MAPP) Requirements

3) AIAA S-102.1.2 (Draft) Subcontractor and Supplier Mission Assurance Management Requirements

4) AIAA S-102.1.3 (Draft) Mission Assurance Working Group (MAWG) Requirements

5) AIAA S-102.1.4 (Released) Failure Reporting, Analysis and Corrective Action System (FRACAS) Requirements

6) AIAA S-102.1.5 (Released) Failure Review Board (FRB) Requirements

7) AIAA S-102.1.6 (Draft) Critical Item Risk Management (CIRM) Requirements

8) AIAA S-102.1.7 (Draft) Project Mission Assurance Database System Requirements

9) AIAA S-102.1.8 (Draft) Quality Assurance (QA) Requirements

10) AIAA S-102.1.9 (Draft) Configuration Management (CM) Requirements

11) AIAA S-102.1.10 (Draft) Environmental Safety Assurance Requirements

AIAA S-102.2 Mission Assurance Engineering and Analysis

12) AIAA S-102.2.1 (Draft) Functional Diagram Modeling (FDM) Requirements

13) AIAA S-102.2.2 (Released) System Reliability Modeling Requirements

14) AIAA S-102.2.3 (Draft) Component Reliability Predictions Requirements

15) AIAA S-102.2.4 (Released) Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements

16) AIAA S-102.2.5 (Draft) Sneak Circuit Analysis (SCA) Requirements

17) AIAA S-102.2.6 (Draft) Design Concern Analysis (DCA) Requirements

18) AIAA S-102.2.7 (Draft) Finite Element Analysis (FEA) Requirements

19) AIAA S-102.2.8 (Draft) Worst Case Analysis (WCA) Requirements

20) AIAA S-102.2.9 (Draft) Human Error Predictions Requirements

21) AIAA S-102.2.10 (Draft) Environmental Event Survivability Analysis Requirements

22) AIAA S-102.2.11 (Released) Anomaly Detection and Response Analysis Requirements

23) AIAA S-102.2.12 (Draft) Maintainability Predictions Requirements

24) AIAA S-102.2.13 (Draft) Operational Dependability and Availability Modeling Requirements

25) AIAA S-102.2.14 (Draft) Hazard Analysis (HA) Requirements

26) AIAA S-102.2.15 (Draft) Software Component Reliability Predictions Requirements

27) AIAA S-102.2.16 (Draft) Process Failure Mode, Effects, and Criticality Analysis (FMECA) Requirements

28) AIAA S-102.2.17 (Draft) Event Tree Analysis (ETA) Requirements

29) AIAA S-102.2.18 (Draft) Fault Tree Analysis (FTA) Requirements

30) AIAA S-102.2.19 (Draft) Fishbone Analysis Requirements

31) AIAA S-102.2.20 (Draft) Similarity and Allocations Analysis Requirements

32) AIAA S-102-2.21 (Draft) Component Engineering Requirements

33) AIAA S-102.2.22 (Draft) Stress and Damage Simulation Analysis Requirements

AIAA S-102.3 Mission Assurance Testing

34) AIAA S-102.3.1 (Draft) Environmental Stress Screening (ESS) Requirements

35) AIAA S-102.3.2 (Draft) Reliability Development / Growth Testing (RD/GT) Requirements

36) AIAA S-102.3.3 (Draft) Reliability, Maintainability, and Availability Demonstration Testing Requirements

37) AIAA S-102.3.4 (Draft) Reliability Life Testing Requirements

38) AIAA S-102.3.5 (Draft) Design of Experiments Requirements

39) AIAA S-102.3.6 (Draft) Ongoing Reliability Testing (ORT) Requirements

40) AIAA S-102.3.7 (Draft) Product Safety Testing Requirements

2.2 Relationship to Other Corporate Standards

This Standard is a companion to the SET Corporate Standards for the Mission Assurance Program, the System Safety Program, the Reliability, Maintainability, Availability & Dependability (RMAD) Program, and the Quality Assurance (QA) Program.

2.3 Miscellaneous Risk Management References

1. Risk Management Guide for DoD Acquisition, 6th Edition dated 4 August 2006
2. AFPD 90-9, 1 APRIL 2000, Operational Risk Management
3. AFI 90-901, Operational Risk Management
4. DODI 5000.02, “Defense Acquisition System Safety”, 2 December, 2008
5. AFMAN 91-201, 18 October 2001, Explosives Safety Standards

6. AFMAN 99-113, 1 May 1996, Space Systems Test and Evaluation Process Direction and Methodology for Space System Testing
7. AFSPCCL Checklist 9-2, 1 JULY 1999, Safety Programs
8. AFSPCMAN 91-710, V1
9. EWR 127-1, *Range Safety Requirements,* 31 March 1995, Appendix 1B, "System Safety Program Requirements"
10. SMCI 63-1205, Space System Safety Process

3 TERMINOLOGY

3.1 Terms and Definitions

anomaly
apparent problem or failure affecting a configured product, process, or support equipment/facilities that is detected during product verification or operation
NOTE: Anomalies are distinguished from discrepancies, product defects which do not violate project requirements which may or may not be documented in the FRACAS.

acquisition authority
an organization (Government, contractor, or subcontractor) that levies requirements on another organization through a contract or other document

approximation[1]
a value that is nearly but not exactly correct or accurate

audit
an independent examination of accounts and records to assess or verify compliance with specifications, standards, contractual agreements, or other criteria (Ref. IEEE STD 1624-2008)

baseline process
the minimum set of functions that constitute a specific type of process

baseline program
the minimum set of functions that constitute a specific type of program

capability
one or more processes or activities that describe how SR&QA programs are used, treated, or developed within an organization (Ref. IEEE STD 1624-2008)

capability-based mission assurance program
the set of processes that assesses and controls product deficiency risk at one or more predefined capability levels

capability level
measure of the ability of a mission assurance process, as specified by a set of activities, to address the pertinent mission assurance needs of a systems engineering process

capability level growth
a measurable improvement (e.g., an increase in resources, scope of effort, or maturity of input data) in the ability of a mission assurance process to support the mission assurance needs of a systems engineering process

chaos

[1] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

the random occurrence of unpredictable and unrelated events

control
a method used to reduce the consequences, likelihood, or effects of a hazard or failure mode
NOTE: Controls include special procedures, inspections, or tests

credible failure mode or hazard
a failure mode or hazard with a probability of occurrence greater than 1.0E-6, 0.000001, or one in a million

engineering judgment
a properly trained engineer's technical opinion that is based on an evaluation of specific data and personal experience
NOTE: Engineering judgments are a reality that cannot not be avoided when insufficient time, data, or funding are available to perform a detailed quantitative analysis. (See Sections 5.5.1 and 5.5.2 for more information.)

environmental safety assurance
to give appropriate consideration to potential environmental impacts prior to beginning any action that may significantly affect the environment

estimation
a tentative evaluation or rough order magnitude calculation

failure
termination of the ability of a unit to perform its required function
NOTE: A fault may cause a failure.

failure mode
consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

fault[2]
[1] [Software reliability] a manifestation of an error in software; [2] [Hardware reliability] any undesired state of a component or system; [3] [Components] a defect or flaw in a hardware or software component; [4] [Human reliability] procedure (operational or maintenance) or process (manufacture or design) that is improperly followed;
NOTES: [1] An accident may cause a fault; [2] A fault may cause a failure; [3] A fault does not necessarily require failure.

hazard
a condition that is prerequisite to a mishap and a contributor to the effects of the mishap
NOTE: A single point failure mode (SPFM) item is a hazard with respect to its potential to lead directly to loss of a safety-critical or mission-critical system function.

[2] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

maturity level
measure of the degree of accuracy of a data product, as developed using a specified set of input data, in relation to what is considered the best achievable results

method
a formal, well-documented approach for accomplishing a task, activity, or process step governed by decision rules to provide a description of the form or representation of the outputs (C/SE) 1220-1994s

mishap
an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

mission
the purpose and functions of the space system (sensors, transponders, boosters, experiments, etc.) throughout its expected operational lifetime, and controlled reentry or disposal orbit time period. A space system may have multiple missions (e.g., primary mission, ancillary mission, and safety mission)

mission assurance
the program-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal
NOTE: Deficiencies include damaging-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

mission capability
This term encompasses the purpose and functions of the space system (sensors, transponders, etc.) throughout its intended system mean mission duration (the expected life of the space vehicle). (Ref. AFMAN 91-222 SUPL1)

mitigation
(1) a method that eliminates or reduces the consequences, likelihood, or effects of a hazard or failure mode; (2) a hazard control

modeling
act of producing a representation or simulation of one or more items

non-credible failure mode or hazard
a failure mode or hazard with a probability of occurrence equal to or less than 1.0E-6, 0.000001, or one in a million
NOTE: In System Safety Engineering, the qualitative probability values of an improbable hazard and a non-credible hazard are equivalent.

plan
a method for achieving an end

practice
one or more activities that use specified inputs to develop specified work products for achieving specified objectives (Ref. IEEE Standard 1624-2008)

process-based lesson learned
important information created, documented, and retrieved according to a process or procedure descriptor

product-based lesson learned
important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor

program
[1] the managed collection of an organization's practices that is structured to ensure that the customers' requirements and product needs are satisfied (Ref. IEEE Standard 1624-2008); [2] a defined set of managed processes conducing to an end under a single plan
NOTE: A program does not have to consist of related, managed process. Compare with definition of *"system"*.

process
a sequence of tasks, actions, or activities, including the transition criteria for progressing from one to the next, that bring about a result (Ref. IEEE Standard 1624-2008)

NOTE: A process can be unmanaged or managed. An unmanaged or "free" process does not have its inputs or outputs controlled. The rain and melted snow that replenishes a lake is an example of an unmanaged process. A managed or "controlled" process has its inputs and outputs controlled. An electrical power station is an example of a managed process.

quality
a measure of a part's ability to meet the workmanship criteria of the manufacturer
NOTE: Quality levels for parts used by some of the handbook methods are different from quality of the parts. Quality levels are assigned based on the part source and level of screening the part goes through. The concept of quality level comes from the belief that screening improves part quality.

reliability
probability that an item will perform its intended function for a specified interval under stated conditions

requirements creep
customer or product requirements that are identified late in the product development phase

risk
a measure of future uncertainties in achieving project performance goals and objectives within defined technical, safety, performance, cost, and schedule constraints
NOTE: Risk can be associated with all aspects of a project (e.g., threat, technology maturity, supplier capability, design maturation, and performance against the plan), as these aspects relate across the Work Breakdown Structure (WBS) and Integrated Master Schedule (IMS).

risk area
one of five major risk categories: cost, performance, safety, schedule, and technical

(1) cost risk
the ability of the system to achieve the program's life-cycle cost objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used, given that the technical requirements were properly defined.

(2) performance risk
the degree to which the proposed system or process design is capable of meeting the operational requirements, which include reliability, maintainability, dependability, availability, and testability requirements

(3) safety risk
an expression of the possibility/impact of a mishap that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment, in terms of hazard severity categories and hazard probability levels

(4) schedule risk
risk associated with adequacy of the time allocated for performing the defined tasks, e.g., development, production, testing, etc.
NOTE 1: This risk factor includes the effects of programmatic schedule decisions, the inherent errors in the schedule estimating technique used, and external physical constraints.
NOTE 2: The Integrated Master Schedule (IMS) will be analyzed to determine the confidence level of the project's baseline schedule, as well as to identify the top project schedule risk drivers. This requires performing a detailed analysis to identify the schedule risks and to estimate uncertainty as it applies to milestones. This approach uses a quantitative statistical analysis process.

(5) technical risk
The degree to which the technology proposed for the system has been demonstrated as capable of meeting all of the project's objectives

risk type
one of several risk attributes: residual, transferred, assumed, avoided

(1) actionable risk
risk that can be mitigated, i.e., eliminated, reduced, or controlled

(2) residual risk
risk associated with significant failure modes or hazards for which there are no known control measures, incomplete control measures, or no plans to control the failure mode or hazard

risk management
a continuous process that is accomplished throughout the life cycle of a system to:

- Identify and measure the unknowns.
- Develop mitigation options.
- Select, plan, and implement appropriate risk mitigations.
- Track the implementation of risk mitigations to ensure successful risk reduction.

NOTE: Effective risk management relies heavily on detailed risk management planning, early identification and analyses of risks, early implementation of corrective actions, a user-friendly risk tool to continuously track and reassessment open risks, and open communication paths with the appropriate risk acceptance authorities.

risk disposition
one of several different ways to address identified risk

(1) *Transferring risk* is reallocating or sharing the risk among entities or processes; or having someone else take accountability for the risk. Risk can be transferred by:

- Assigning responsibility to the organization that is best suited to minimize the probability of a negative consequence.
- Reallocating performance risk within the design and function of the system; such as having software perform a function electronically that was previously performed by a mechanical, hardware function.
- Using firm-fixed price contracts and warranties to transfer cost risk to the contractor.

NOTE: Firm-fixed price (FFP) contracts place upon the contractor maximum cost risk and full responsibility for all costs and resulting profit or loss. When an FFP contract is used:

- The agreed-upon price is not subject to any adjustment on the basis of the contractor's cost experience in performing the contract.
- There are maximum incentives for the contractor to control costs, and a minimum administrative burden is imposed on the Government.

(2) *Assuming risk* is planning for the potential consequences by:

- Accepting the risk.
- Putting a monitoring process in place.
- Plan for the future (e.g., reserving funds, modifying schedules) if necessary. All unknown or unidentified risks are assumed

(3) *Avoiding risk* is changing the source (element or constraint) that is subjecting the program to risk. Risk may be avoided by:

- Reducing the scope of performance objectives.
- Using materials or processes with proven track records.

- Extending the schedule to increase the probability of success.

(4) *Mitigating risk* is acting to eliminate or control the risk.
   a. *Eliminating risk* removes the source of the risk. Design for minimum Risk (ref. MIL-STD-882C) is risk elimination methodology.
   b. *Controlling or reducing risk* does not remove the source of the risk, but seeks to reduce or limit its effects. Actions that control risk attempt to reduce the probability of occurrence and/or lessen impact, such as:
      a. Incorporate safety devices (ref. MIL-STD-882C).
      b. Provide warning devices (ref. MIL-STD-882C).
      c. Develop procedures and training (ref. MIL-STD-882C).
         i. Material solutions; e.g., personal protective equipment, and preventive maintenance.
         ii. Non-material solutions; e.g., warning, caution, or other form of written or spoken advisory, inspections, product safety testing, reliability life testing, acceptance testing, qualification testing, and ongoing reliability testing.
      d. Coordinate or oversee critical processes
      e. Use multiple contractors.
      f. Use technology or processes to limit risk exposure.

root cause(s)
most fundamental reason(s) an event might or has occurred

root cause analysis
a process for identifying the fundamental cause of an event or failure

safety
freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

safety critical
a term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component

specialty engineering
a subgroup of the engineering processes that make up the Mission Assurance Process
Note: Traditionally, this subgroup includes Reliability, Maintainability, PMP, Survivability, and Supportability.

system
[1] a defined set of related processes
[2] elements of a composite entity, at any level of complexity of personnel, procedures, materials, tools, equipment, facilities, and software, that are used together in an intended

operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement
NOTE: A system that consists of one or more unmanaged processes is susceptible to becoming "unbalanced" and changing over time (e.g., an ecological system). For a system to maintain stability it must be "balanced" and consist only of managed processes.

system safety
the application of engineering management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle (Ref. MIL-STD-882C)

systems engineering
An interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and life-cycle balance set of system product and process solutions that satisfy customer needs. (Ref. MIL-STD-499B Draft)

tailoring
process by which the individual requirements (tasks, sections, paragraphs, words, phrases, or sentences) of a standard are evaluated to determine the extent to which each requirement is most suited for a specific system acquisition and the modification of these requirements, where necessary, to ensure that each tailored document invokes only the minimum needs of the customer

timely
performance of a task, subtask, or effort when planning and execution results in the output being provided with sufficient time for management, if need be, to identify and implement cost-effective action
EXAMPLE: An action that avoids or minimizes schedule delays and cost increases.

validation
the act of determining that a product or process, as constituted, will fulfill its desired purpose

verification
the process of assuring that a product or process, as constituted, complies with the requirements specified for it

3.2 Acronyms

A_O	Availability Analysis
CA	Criticality Analysis
CIRM	Critical Item Risk Management
CN	Criticality Number
DCA	Design Concern Analysis

D_O	Dependability Analysis
ESS	Environmental Stress Screening
ETA	Event Tree Analysis
ETC	Estimate to Complete
FDM	Functional Diagram Modeling
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and corrective Action
FRB	Failure Review Board
FTA	Fault Tree Analysis
HA	Hazard Analysis
HW	Hardware
LLAA	Lessons Learned Approval Authority
LOE	Level of Effort
MAP	Mission Assurance Program
	Mission Assurance Process
MAPP	Mission Assurance Program Plan
	Mission Assurance Program Planning
MAWG	Mission Assurance Working Group
MCLP	Multiple Capability Level Process
PMP	Parts, Materials & Processes
PoF	Physics of Failure
QA	Quality Assurance
R&M	Reliability and Maintainability
RD/GT	Reliability Development/Growth Testing
RMAD	Reliability, Maintainability, and Availability Demonstration
	Reliability, Maintainability, Availability and Dependability
SCA	Sneak Circuit Analysis
SCLP	Single Capability Level Process
SEC	Standards Executive Council

SPFM	Single Point Failure Mode
SR&QA	Safety, Reliability & Quality Assurance
SSP	System Safety Program
SW	Software
TAAF	Test, Analyze and Fix
V&V	Verification & Validation

4 GENERAL REQUIREMENTS

The SET Risk Management Process is structured, continuous, proactive, and focused on early identification and mitigation or control of significant project risks. Risks that are classified as Moderate, Serious, or High are considered to be Significant and are handled accordingly. Significant Risks are managed in accordance with the project's Risk Management Process Plan, which is mandatory for all product development functions, particularly Design, Manufacturing, and Test. Proactive risk management activities which interface formally with the Risk Management Process are an integral part of all mission assurance processes, e.g., Hazard Analysis, FMECA, and Statistical Process Control. The flowchart shown in Figure 1 provides an overview of the SET Risk Management Process. The main steps in this process are Risk Identification, Risk Mitigation, and Risk Control.

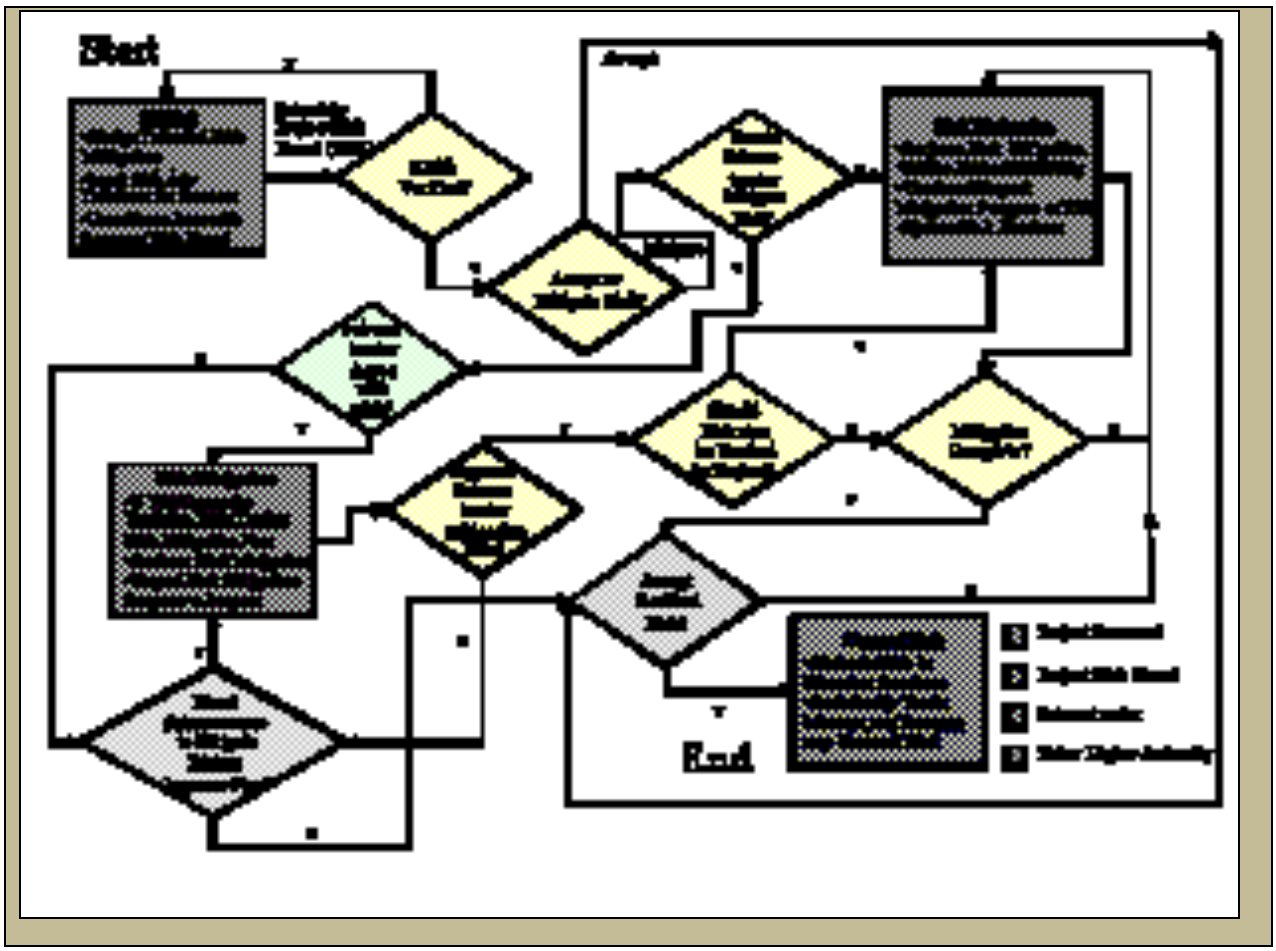

Figure 1: Risk Management Process Flowchart

4.1 Risk Identification

Risk identification is the first and most critical step in the Risk Management Process. Risks cannot be assessed or managed until they are identified and accurately described, preferably using a repeatable procedure[3]. Each identified risk has two components that are assessed separately to determine the risk factor. These components are likelihood (i.e., probability of occurrence) and consequence (i.e., worst-case severity of the end effects). The risk factor represents the degree of uncertainty associated with unwanted technical, performance, safety, cost, or schedule events/conditions. **If there is a zero or one hundred percent likelihood of an event occurring, then there is no risk because there is no uncertainty**. An unwanted event that is certain to occur constitutes an existing problem (i.e., issue), not a risk. Corrective action plans for issues should be generated and implemented separately from the risk mitigation plans described in this Standard.

The project personnel that contribute to product development are the best qualified to identify relevant risks early. The likelihood of unwanted events/conditions occurring during system operation is minimized by identifying and managing Systems Engineering risks early during pre-Design, pre-Manufacture, and the pre-Test. SET's management position is, everyone that is involved in product development is responsible for identifying risks, entering risks in the risk database, and submitting risks to the Project Risk Management Board (PRMB) for disposition.

Beginning with the start of the System Definition phase, and continuing through all subsequent product development phases, the project leads will periodically review the risk submittals that are entered in the project's risk database to identify new risks that affect the Work Breakdown Structure (WBS) budget that they are responsible for managing. They own the risks which affect their piece of the WBS budget. When determining who should own a particular risk, it is important to consider all possible risk sources or pre-requisite conditions. Examples of risk sources include the following:

- Immature technology
- Extreme operating environment (space, desert, etc.)
- New process (design, analysis, production, etc.)
- New design
- High level of design complexity
- Tight tolerance requirements
- New operational requirements (customer needs)
- New mission assurance requirements (safety, reliability, maintainability, dependability, availability, or quality assurance)
- Changing requirements
- Engineering change orders
- Cost and schedule estimating assumptions
- Resource availability (people, materials, facilities, tools, etc.)
- Under-qualified personnel (design, engineering, production, etc.)
- Limited mission assurance capability

[3] For a procedure to be repeatable it must be documented.

The Project Risk Management Board (PRMB) ensures that all Risk Owners receive the necessary support to complete the initial assessment of each new risk. The initial risk assessment is best performed as soon as the risk is identified so that the mitigation strategy trade space can be developed and presented to the PRMB in a timely manner.

4.1.1 Risk Consequence (Severity)

A key aspect of risk identification is the determination of worst case end-effects on the technical, performance, safety, cost, and schedule risk areas, separately. Table 1 provides the risk consequence ratings for these five risk areas. Any sort of cost analysis associated with these risk areas will require the support of the project WBS managers to provide detailed technical and schedule information relevant to each area.

Table 1: Risk Consequence Scales

Consequence						
Rating		1	2	3	4	5
Risk Area	Technical	Project relies on demonstrated/proven applications of legacy or state-of-the-art hardware, software, process, or integration technology	Project relies on unproven applications of legacy hardware, software, process, or integration technology	Project relies on unproven applications of state-of-the-art hardware, software, process, or integration technology	Project relies on development of beyond state-of-the-art hardware, software, process, or integration technology	Project relies on experimental/research hardware, software, process, or integration technology
	Performance	Less than minor inconvenience; < 5% utility loss, e.g., infrequent unplanned downtime	Minor impairment of margin, design life, or secondary missions; 6% to 15% utility loss, e.g., degradation in objectives	Major impairment of margin, design life, or secondary missions; 16% to 45% utility loss, e.g., frequent unplanned downtime with loss of some minor objectives	Severe impairment of margin; 46% to 75% loss of utility, e.g., permanent loss of redundancy, failure to meet key mission objective, early mission termination	System failure during mission leads to early disposal
	Safety	Less than minor injury or less than minor damage to system or environment	Minor injury, minor occupational injury, or minor damage to system or environment	Major injury, major occupational injury, or major damage to system or environment	Severe injury to by-stander, severe occupational injury, or critical damage to system or environment	Death, catastrophic mishap during or after mission prevents proper system disposal, or catastrophic damage to environment
	Schedule	Insignificant or no impact on project schedule	Erode project schedule margin by > 5%	Erode project schedule margin by < 5% or segment margin by > 25%	Erode system schedule margin by < 25%	Delay key milestone date or event, e.g., delay of system delivery
	Cost	< $10K loss	$10K to $50K loss	$50K to $500K loss	$500K to $2M loss	> $2M loss

4.1.2 Risk Likelihood (Quantitative Scales)

For each risk identified, the following question must be answered: "*What is the likelihood the risk will happen*?" Table 2 shows the quantitative scales used to determine the risk likelihood, or probability of occurrence. When determining the likelihood of an event/condition, it is important to estimate the number of occurrences. For example, if a potential problem (risk) exists in a computer network, one must factor in all potential instances of occurrence. For example, the likelihood of the risk occurring on any one of several computers should be considered and the likelihood adjusted accordingly. The determination of a specific probability value must also

define and account for the exposure duration (i.e. length of time potential risk exists). The Risk Owner should choose the highest level of likelihood among technical, performance, safety, cost, and schedule when determining the likelihood rating.

Table 2: Risk Likelihood Quantitative Scales

Likelihood	Rating	Technical Risks	Performance Risks	Safety Risks	Cost / Schedule Risks
	1 - Improbable	< 1%	< .1%	< .0001 %	< 1%
	2 - Remote	1% to 10%	.1% to 1%	.0001% to .1%	1% to 10%
	3 - Occasional	10% to 20%	1% to 10%	.1% to 1%	10% to 20%
	4 - Probable	20% to 30%	10% to 20%	1% to 10%	20% to 30%
	5 - Frequent	> 30%	> 20%	> 10%	> 30%

4.1.3 Risk Likelihood (Qualitative Scales)

The qualitative risk likelihood scales shown in Table 3 should be used for initial risk assessments when the risk source is known and insufficient data is available to develop a quantitative probability of occurrence. Initial safety and performance risk assessments should be periodically updated until high fidelity quantitative risk likelihood data can be fully developed. **Full development of quantitative risk likelihood data for technical, cost and schedule risks may not be practical due to high subjectivity associated with human reliability factors.**

Table 3: Risk Likelihood Qualitative Scales

Likelihood of Failure							
	Risk Area						
	Requirements	Designs	Resources	Procedures	Plans	Analyses	Processes
Frequent (5) (> 30%)	Requirements are not verified by customer, or requirements are not flowed down to subcontractors	New components or assemblies with uncharacterized performance or manufacturability	Critical staffing, facilities, or tools are undefined	New procedures or procedures previously used for an unrelated purpose	Critical program plans and associated metrics are undocumented	No related analytical experience to draw from	Process is undocumented and ad hoc
Probable (4) (> 20% to ≤ 30%)	Requirements are not verified by customer, but identified requirements are flowed down to subcontractors	New components or assemblies with fully characterized performance and manufacturability	Critical staffing facilities, and tools defined, but availability or one or more is undetermined	Major changes to procedures previously used for a related purpose	Critical program plans are fully documented but metrics for completion are partially documented	Experienced with related but less complex analyses	Process is partially documented and partially ad hoc
Occasional (3) (> 10% to ≤ 20%)	RTT documented but is not verified by customer, and identified requirements are flowed down to subcontractors	COTS components and assemblies with major modifications to standardized integration or recommended applications	Critical staffing facilities and tools defined, and availability does not meet needs	Major changes to procedures previously used for a similar purpose	Critical program plans are fully documented but metrics for completion are partially documented	Experienced with similar but less complex analyses	Implementation of process is not consistent with documented approach
Remote (2) (> 1% to ≤ 10%)	RTT documented and Verified by customer, and identified requirements are flowed down to subcontractors	COTS components and assemblies with minor modifications to standardized integration or recommended applications	Critical staffing facilities, and tools defined, and availability barely meets needs	Minor changes to procedures previously used for a similar purpose	Critical program plans and metrics for completion are fully documented	Experienced with similar analyses	Process is fully documented, mature, but only partially implemented
Improbable (1) (≤ 1%)	System Requirements Analysis (SRA) performed, Requirements Trace Tree (RTT) documented and verified by customer, and requirements flowed down.	Commercial off-the-shelf (COTS) components and assemblies with standardized integration or recommended applications	Critical staffing, facilities, and tools defined, and availability exceeds needs	Same procedures used previously for a similar purpose	Critical program plans and metrics for completion are fully documented, and projected to be successfully implemented	Experienced with similar and more complex analyses	Process is fully documented, mature, and fully implemented

Likelihood of Risk	Requirement	Designs	Resource	Procedures	Plans	Analyses	Processes
Frequent (>	Requirements are not verified by customer, or requirements are not flowed down to subcontractors	New components assemblies with uncharacterize performance or manufacturability	Critical facilities, or tools are undefined	New procedures or procedures previously used for an unrelated purpose	Critical program and associated metrics undocumente	No related analytical experience to draw from	Process undocumented and ad hoc
Probable (> 20% to ≤	Requirements are not verified by customer, but identified requirements are flowed down to subcontractors	New components assemblies fully characterized performance manufacturabilit	Critical facilities, and defined, availability of one or more is undetermined	Major to procedures previously used for a related purpose	Critical program and associated metrics partially	Experienced with related but complex	Processes is partially documented partially ad hoc
Occasional (> 10% to ≤	RTT documented but is not verified by customer, and identified requirements are flowed down to subcontractors	COTS components and assemblies with major modifications to standardized integration or recommended applications	Critical facilities and tools defined , availability does not meet	Major to procedures previously used for a similar	Critical program are fully documented metrics for completion partially	Experienced with similar but complex	Implementation process is consistent documented
Remote (> 1% to ≤	RTT documented and Verified by customer, and identified requirements are flowed down to subcontractors	COTS components assemblies with modifications to standardized integration or recommended applications	Critical facilities, and tools defined, availability barely meets	Minor changes procedures previously used for a similar purpose	Critical program plans and metrics for are fully	Experienced with similar analyses	Process is documented, mature, but only partially implemented
Improbable (≤	System Requirements Analysis (SRA) performed, Requirements Trace Tree (RTT) documented and verified by customer, and requirements flowed down	Commercial off-the-(COTS) components assemblies standardized integration or recommended applications	Critical facilities, and tools defined, and availability exceeds needs	Same procedures used previously for a similar purpose	Critical program plans and metrics for are fully documented, and projected to be successfully implemented	Experienced with similar and complex	Process is fully documented, mature, and implemented

4.1.4 Risk Level Assessment

After determining the likelihood and consequence levels, use Figure 2 to obtain the level of risk (Green = LOW, Yellow = MODERATE, Orange = SERIOUS, Red = HIGH) by plugging in the Likelihood and Consequence scores.

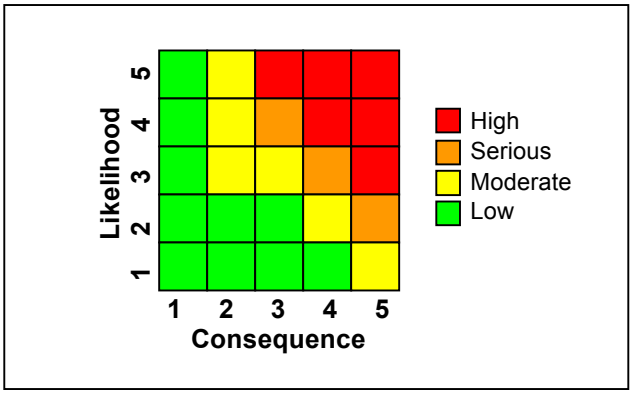

Figure 2: Risk Matrix

4.1.4.1 High Risk

Items classified as red risks are considered primary risk drivers. These risks may involve:

- Death
- Catastrophic system mishap
- Unacceptable technical, schedule, or cost risk
- Catastrophic environmental damage
- >$2M loss

If a risk is determined to be high or series a detailed assessment is required. The types and depth of the assessments will vary from one application to another, as required. A detailed risk assessment should provide:

- Finer resolution of likelihood and consequence estimates
- Ability to expose and rank specific contributions to the risk
- An opportunity to express the uncertainty in these estimates explicitly, and to identify a means of reducing these uncertainties
- An opportunity to break down the likelihood and consequences into their constituents, enabling a better understanding of the composition of the risk and an improved ability to develop mitigation plans.

Detailed risk assessments will be thoroughly documented in the risk database by the Project Risk Management Board (PRMB). Documentation will include the objectives and purpose of the assessment, a statement of scope, the approach, and the results. Documentation will also include an estimated dollar and schedule impact to the project should the risk occur as well as an estimated cost of the mitigation. Should the risk status change the risk item will be reassessed by the Risk Owner and resubmitted to the PRMB.

4.1.4.2 Serious Risk

Items classed as orange are considered serious risks. Serious risks may involve:

- Severe injury
- Adverse effect on interfaces of designated system
- Major system damage
- Critical environmental damage
- Loss between $500K-$2M

Detailed risk assessments will also be thoroughly done by the PRMB for serious level risks. The procedures will be the same as those for high level risks.

4.1.4.3 Moderate Risk

Items classed as yellow are considered Moderate Risks. Moderate risks may involve:

- Minor injury
- Minor impairment of margin, design life, or secondary missions
- Minor environmental damage
- Loss between $50K-$500K

A preliminary risk assessment is required for Moderate Level Risks. The depth of the preliminary risk assessment will be determined by the Risk Owner. All preliminary risk assessments will be thoroughly documented in the risk database by the PRMB. Documentation will include the objectives and purpose of the assessment, a statement of scope, the approach, and the results. Documentation will also include a rough estimate of the dollar and schedule impact to the project should the risk occur as well as a rough estimate of the cost of the mitigation. Should the risk status change the risk item will be reassessed by the Risk Owner and re-submitted to the PRMB.

4.1.4.4 Low Risk

Items classed as green represent a low impact and/or probability of occurrence. Low level risks will be documented and archived in the risk database. No mitigation plans or a risk assessment is required for low risks. However, low level risks should be reviewed at least quarterly to ensure that the risk level has not increased. Should the risk status change the risk item will be reassessed by the Risk Owner and re-submitted to the PRMB.

4.2 Risk Mitigation

Risk mitigation strategies identify tasks that, when implemented, will reduce risk to an acceptable level by: 1) reducing the likelihood of occurrence by shortening the exposure duration and/or other means, and/or 2) reducing the consequence if it occurs. Projects are required to develop mitigation strategies for all High, Serious, and Moderate Risks, on a selective basis.

Each Risk Owner must perform the following tasks:

- Define what work has to be done
- Identify the level of effort in terms of manpower and accomplishment time
- Specify the required material or facilities
- Estimate current risk rating associated with each requirement
- Propose a risk burn-down plan to accomplish each mitigation and estimate a closure date for each step
- Perform a cost-benefit analysis for the proposed risk burn-down plan
- Identify alternative risk burn-down plans with a cost-benefit analysis for each
- Assign a point of contact (POC) for each mitigation step
- Estimate the achievable risk reduction
- Estimate the mitigation induced risk level (target residual risk)
- Track and ensure timely progress of risk burn-down plan execution
- Update status of risk to the Project Risk Management Board (PRMB) when the risk profile changes (i.e. mitigation steps completed, new issues with risk, etc.)
- Verify risk control.

4.2.1 Development and Implementation of Mitigation Plans

Each project should brainstorm potential mitigation options and agree upon one or more options to analyze further. The project should conduct a tradeoff analysis to choose the option that will have the greatest impact keeping in mind the constraint on resources. Factors such as expected risk reduction, likelihood of success, cost of implementation, resource requirements, interdependencies with other program activities, and requirements for external approval or direction should be compared among various mitigation alternatives.

For all risk areas, the following mitigation order of precedence will be applied:

1. Safety
2. Performance
3. Schedule
4. Cost
5. Technical

For system safety risk mitigations, the following technique order of precedence will be followed: (1) design for minimum risk, (2) incorporate safety devices, (3) provide warning devices, and (4) provide procedures and training. Frequently, combinations of these techniques are used. For example, the designer could use engineered safety features, safety devices, and provide training to mitigate a single hazard risk.

After the mitigation plan is coordinated by the Risk Owner, the Project Risk Management Board reviews and concurs with it prior to forwarding it to the Project Manager for review and approval. The approved mitigation plan is then incorporated into project planning and budget projections.

4.2.1.1 Design for Minimum Risk

The designer will attempt to eliminate the risk. If risk elimination is not possible, the designer will attempt to modify/change the design so as to reduce the value of the risk. The types of design modifications/changes include safety factors. A safety factor is the ratio of tensile or yield strength over the maximum allowable stress of the material or the ratio of burst pressure over the maximum allowable working pressure. Safety factors are used usually when a single point failure in the system structure would lead to a safety critical or catastrophic failure. For example, safety factors are usually used in structural design of high pressure containment systems and structural systems in satellites and rockets. Also, they are used in Ground Support Equipment (GSE) such as in hoists

4.2.1.2 Incorporate Safety Devices

The designer will attempt to minimize the risk through engineered safety features. Examples of these features include active devices, i.e., redundant backups (fault tolerance), interlocks, and pressure relief valves. Provisions will be made for periodic functional checks of the devices when applicable.

The fault tolerance method introduces redundant subsystems into the system to increase the probability that if one or more of the redundant subsystems failed the remaining redundant subsystem(s) would still function. As an example, for non-safety critical command and control functions; a system, subsystem, component, or subcomponent will be designed in such a way that requires two or more independent human errors, or requires two or more independent failures, or a combination of independent failure and human error. For safety critical command and control functions; a system, subsystem, component, or subcomponent will be designed that requires at least three independent failures, or three human errors, or a combination of three independent failures and human errors.

4.2.1.3 Incorporate Safety Devices

The designer will attempt to mitigate the risk through the use of fixed, passive protective barriers (e.g. guards, shields, latches, and catches). Provisions will be made for periodic functional checks of safety devices when applicable.

4.2.1.4 Provide Warning Devices

The designer will attempt to use devices to detect the fault condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application will be designed to minimize the probability of incorrect personnel reaction to the signals and will be standardized within like types of systems. Examples of warning devices include chemical sniffers with alarm for high values of the harmful chemical, low oxygen level alarm, warning lights, and computer hazard monitoring and annunciation devices. These devices are of limited value for people with vision and hearing impairments.

4.2.1.5 Provide Procedures and Training

Some Project Managers select procedures and training to mitigate hazard risks. Procedures and training may include formal or informal training, checklists, certification or experience requirements, Personal Protective Equipment (PPE), etc. Without an approved waiver from the appropriate risk acceptance authority, no warning, caution, or other form of written advisory will be used as the only risk reduction method for hazards with Category I or II severity. Tasks and activities that are judged to be safety critical may require certification of personnel proficiency.

Mitigation plans that are developed to limit the severity or likelihood of the identified risks are called Control Plans. These plans are implemented, tracked, and kept in a historical record. Once an identified risk has been successfully controlled to an acceptable level of residual risk, or a residual risk accepted by the appropriate risk acceptance authority, the risk is classified in the project risk database as a "historical" risk and periodically reviewed. These risks are periodically reviewed to verify that the residual risk value has not increased.

Project-wide coordination of Safety, Reliability, and Quality Assurance (SR&QA) tasks is implemented to ensure sufficient SR&QA *Engineering and Evaluation* tasks will be applied early in the product life cycle, enabling early development of initial SR&QA requirements and design criteria. For example, performing functional FMECA to support development of the System Requirement Specification can help avoid *requirements creep*, i.e., customer or product requirements that are identified late in the product development phase.

5 ROLES AND RESPONSIBILITIES

5.1 Risk Acceptance Authority Levels

Each project risk, after completion of the mitigation or control plan, may still have residual risk. Based on the magnitude of that residual risk, the Chief Engineer, Project Manager, or a higher level risk acceptance authority will sign the documented Risk Acceptance Statement. The risk acceptance authorities are as follows:

- High Risk: Customer (High Residual Risk Acceptance Authority)
- Serious Risk: Customer (Serious Residual Risk Acceptance Authority)
- Moderate Risk: Project Manager (PM)
- Low Risk: Chief Engineer

5.2 Project Manager Responsibilities

The PM is ultimately responsible for project risk management. Accordingly, the PM will make the final decision and sign-off on all Moderate Risks that are either mitigated to an acceptable level, or accepted as residual risks with control plans the PRMB concur with. The PM selects the members of the PRMB, which is authorized to report directly to the PM. The PM is also responsible for briefing the status of the Risk Management Process to the customer and the SET enterprise chain of command, as required by the contract and applicable government policies/regulations.

5.3 Chief Engineer Responsibilities

The Chief Engineer is responsible for (1) reviewing all risk submittals, (2) ensuring the risk submittals are properly prepared prior to distribution to the PRMB, and (3) the disposition of all Low Risks with the advice of the PRMB.

5.4 Project Risk Management Board Responsibilities

The Project Risk Management Board advices the Chief Engineer and the PM with regard to appropriateness of mitigation methods proposed by Risk Owners for Low and Moderate Risks, respectively. Individuals considered for appointment to the Project Risk Management Board are trained to thoroughly understand their roles and responsibilities before becoming appointed.

The Project Risk Management Board holds regularly scheduled meetings with the Chief Engineer to review new risk submittals. These meetings are typically held weekly. The new risk submittals are entered in the Risk Database once they are documented by the Risk Owner and approved by the Chief Engineer. Project personnel should be informed in a timely manner of new risks that affect the outputs of systems engineering processes which they participate in.

The PRMB is sanctioned by the PM. However, the PRMB has no authority to make decisions that lead to tasking a project with regard to risk mitigations. The responsibility and authority over Low and Moderate Risks rests with the Chief Engineer and the PM, respectively. The responsibility and authority over Serious and High Risks rests with the customer. Moreover, this authority will not be superseded by a consensus opinion among the PRMB members. Risks that

come to the PRMB will be assessed for validity, accuracy, and categorization. The PRMB will assess whether the Moderate Risks warrant further action, and whether the Risk Owner recommended dispositions are appropriate. The PRMB will report its findings to the PM, who then makes the final disposition decision. If the PM decides a risk should be mitigated and tracked, the applicable Risk Owners will be assigned responsibility for executing an agreed-upon risk burn-down plan.

Furthermore, the PRMB is responsible for prioritizing project risks in accordance with the risk mitigation order of precedence defined in this Standard. This prioritized risk list should also have a cost estimate associated with both risk realization and risk mitigation. The objective of this exercise is to provide the PM a prioritized list of project risks ranked by importance. This list is to help the PM make decisions on which project risks should be funded for mitigation based on the available budget.

The following is a list of the PRMB responsibilities:

- Distribute the PRMB agenda to applicable personnel
- Record and distribute the PRMB meeting minutes to applicable personnel
- Notify project personnel of the next PRMB meeting
- Maintain configuration management of risk submittals (i.e. develop a risk database system)
- Coordinate/implement Risk Owner actions as determined by the PRMB
- Develop and provide risk management training materials to project personnel
- Administer a periodic review of the Risk Management Process Plan and update the risk management training plans accordingly

5.5 Risk Management Software Tool

SET is collaborating with the S-102 Mission Assurance Standards Working Group to collect and evaluate open source automated risk management tools. The goal is to find a web-based tool that is capable of processing and tracking risk submittals and associated mitigation plans written against all five risk areas; cost, performance, safety, schedule, and technical. This effort will continue until SET can provide its Risk Owners with a user-friendly tool that improves the efficiency and lowers the cost of project risk management over time.

6 RISK MANAGEMENT TRAINING

Risk Management training will be provided to all SET project members. The S-102 Mission Assurance Standards Working Group is developing web-based courses which will explain the standards and guides for SR&QA programs and the risk management process. The PRMB will be responsible for tracking which project personnel have been trained.

7 RISK ASSESSMENT EVALUATION CHECKLIST

All Risk Assessments are processes. A good process is one that is clearly defined and repeatable. Typically the better your Risk Assessment process is the better, or more accurate, your results will be. This checklist assists SET projects in establishing an effective Risk Assessment Process or effectively evaluating a Risk Assessment Process. If a question cannot be answered affirmatively, the product stake-holder should carefully examine the situation and take appropriate action.

The following Risk Assessment Checklist is based on the Risk Management Process Flow Diagram illustrated in Figure 1, and may be used for any type of Risk Assessment. The key to performing a proper Risk Assessment lies in a firm understanding and definition of the type of Risk Assessment required.

I. Is Appropriate Risk Assessment Approach Selected?

a. Is the methodology acknowledged for its intended use by the government and industry?

b. Are the required input data available?

c. Is the input data collection approach repeatable?

II. Is Accuracy of Identified Risk Verified?

a. Are all pertinent risk sources identified?

b. Are the proper risk factors collected and input to the risk assessment process?

c. Is the risk exposure or vulnerability/threat output from the risk assessment process

d. Is the methodology properly applied to identify the worst case consequences for all five risk areas, i.e., technology, performance, safety, cost, and schedule risk areas?

e. Is the methodology properly applied to estimate the worst case likelihoods for all five risk areas, i.e., technology, performance, safety, cost, and schedule risk areas?

f. Is the basis of the likelihood rating adequately described?

g. Is the associated risk level of each identified risk (i.e., exposure or vulnerability/threat) output from the risk assessment process?

h. Is the overall risk adequately described?

i. Is residual risk identified in terms of worst case consequence and quantified likelihood?

III: Is An Optimum Risk Mitigation Plan Selected?

a. Are the recommended risk mitigation plans output from the Risk Assessment?

b. Is an appropriate mitigation strategy devised for each outstanding risk?

c. Are the resources required to implement each recommended risk mitigation plan identified?

d. Is the priority of recommended risk mitigation plans based on the risk area order of precedence, risk levels, and available resources (e.g., funds, people, technology), in that order.

e. Is the anticipated reduction in risk exposure or vulnerability to the current threat properly calculated for each recommended risk mitigation plan?

f. Is a cost/benefit analysis performed on each recommended risk mitigation plan?

g. Is a schedule impact analysis performed on each recommended risk mitigation plan?

h. Are maintenance requirements for each recommended risk mitigation plan identified?

i. Does the selected risk mitigation plan come from the list of recommended risk mitigation plans output from the Risk Assessment?

IV: Is Risk Mitigation Tracked From Start Through Closure?

a. Are the teams and individuals who will be responsible for implementing the risk mitigation plan identified?

b. Is the start date and projected end date for implementing the selected risk mitigation plan identified?

c. Are follow-up meetings scheduled to periodically review risk mitigation progress?

d. Is the reduction in risk exposure or vulnerability periodically assessed using quantitative risk assessments methods to verify consistency with anticipated results?

V: Is Residual Risk Properly Accepted?

a. Is appropriate risk acceptance authority identified for category of residual risk identified?

b. Are all collateral material that explains the risk assessment and the conclusions properly archived?

c. Is a presentation prepared that summarizes the residual risk in terms of quantitative risk likelihood metrics, and was it briefed to the appropriate risk acceptance authority?

Are the proper signatures obtained on residual risk acceptance documentation?