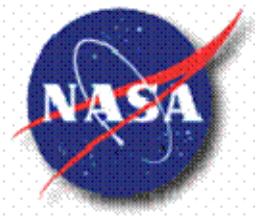


National Aeronautics and
Space Administration

ESMD-RMP-04.06 Rev 2
EFFECTIVE DATE: ***August 16, 2007***

Exploration Systems Mission Directorate
NASA HQ
Washington, DC 20546

Exploration Systems

Risk Management Plan

Submitted By:

Original Signed by David Lengyel

16 AUGUST '07

Directorate Integration Office, Risk & Knowledge Management Officer
David Lengyel

Date

Approved By:

Original Signed by Scott Horowitz

8/17/07

for Associate Administrator
Scott Horowitz

Date

Concurred to by the Exploration Systems Mission Directorate Program Management Council *August 16, 2007.*

DOCUMENT HISTORY LOG

Document Version	Effective Date	Description
1.0	April 27, 2006	Baseline Document
1.1	May 15, 2006	Updated hyperlinks that have changed
2.0	May 1, 2007	• Clarified language throughout the document • Updated references list to reflect current content and approach • Added explanation of risk "escalation" and presented the Top Risk Reporting process • Updated ESMD scoring scheme for ease of use and to better align with the Constellation Program (CxP) and Orion scoring schemes • Emphasized and added detail to the risk management process including description of handling strategy, risk status, and risk category • De-emphasized risk tool discussion and eliminated the Active Risk Manage (ARM) appendix • Defined process for KBR identification and processing • Added discussion of wikis and ESMD's Vignette Risk & Knowledge Management (R&KM) Portal • Eliminated Risk Mgt Team (RMT) and added detailed discussion of and charters for the ESMD Risk Management Working Group (RMWG) and ESMD "HQ Only" RMWG • Refined risk management roles and responsibilities to reflect current processes, including detailed breakout of responsibilities for the ESMD Risk Management Officer (RMO) and ESMD/HQ Divisions and Offices • Included discussion of Transition Control Board (TCB) and Joint Integration Control Board (JICB) activities • Added discussion of the ESMD cost threat process • Added discussion of Risk-Informed Decision Making • Updated risk reporting requirements to reflect current process • Added discussion of Top Risk Reporting (TRR) process, including reporting structure, reviewing risks, escalation, TRR out-of-board process, reporting • Defined process for transferring risks • Added discussion of the risk management Assurance Process Map • Included ESMD's Risk Breakdown Structure • Updated definitions for clarity and better alignment with ESMD Performing Organization RMPs • Replaced Risk Management Team (RMT) charter with charters for the ESMD RMWG and the ESMD "HQ Only" RMWG • Updated Tailorable Risk Management Process Appendix

Table of Contents

Figures and Tables

Foreword

The Exploration System Mission Directorate (ESMD) Risk Management Plan (RMP) describes how ESMD manages risks across the Directorate. It provides guidance and requirements for ESMD/Headquarters (HQ) Divisions and Offices and Center performing organizations charged with conducting risk management activities for work under ESMD purview. It encourages open communication of risks across the Directorate using the Continuous Risk Management (CRM) process, and defines the functional requirements for documenting and reporting risks. This RMP also provides guidance for integrating knowledge management with risk management processes, and describes roles and responsibilities for implementing risk management within the ESMD.

1 Introduction

1.1 Purpose and Scope

The Exploration System Mission Directorate (ESMD) Risk Management Plan (RMP) defines the ESMD organizational and process approach to risk management, given the risk management requirements and guidance included in Agency documents NPR 7120.5 and NPR 8000.4.

The ESMD RMP:

- Provides policies, requirements, guidelines, and a common framework for identifying, analyzing, communicating, and managing risks for ESMD and its performing organizations;
- Establishes internal and external ESMD relationships for managing risk, including the coupling of Knowledge Management (KM) with risk management systems to capture and preserve "lessons learned;"
- Defines common processes, metrics, and standards for executing integrated risk management and KM practices across the Directorate; and
- Defines Risk Management interfaces between ESMD and: (1) the Space Operations Mission Directorate (SOMD), and (2) Agency Institutional organizations.

1.2 References

The following items are referenced in the text of this document:

1. Continuous Risk Management Guidebook – Software Engineering Institute, Carnegie Mellon University, 1996. NTIS#: AD-A319533KKG, DTIC#: AD-A319 533\6\XAB
2. NPR 7120.5 – NASA Procedural Requirement, NASA Program and Project Management Processes and Requirements
3. NPR 8000.4 - NASA Procedural Requirement, Risk Management Procedural Requirements
4. NASA Cost Estimating Handbook

The following documents are not specifically discussed in this document, but are applicable to ESMD risk management:

5. NPR 8705.2 – Human-Rating Requirements for Space Systems
6. NPR 8705.5 – Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

7. NPR 8715.3 – NASA General Safety Program Requirements
8. NPR 8715.5 – Range Safety Program
9. NPR 9501.3 – Earned Value Management Implementation on NASA Contracts

2 ESMD Risk Management Approach

ESMD/HQ functions based on a "corporate model." In this context, ESMD/HQ provides direction, establishes ESMD risk management policy, and provides oversight to performing organizations. All programs are responsible for providing infrastructure, staffing, and funding to support risk management; developing and maintaining their risk management plans; and complying with all ESMD/HQ policies and guidance.

A Risk Management Officer (RMO) role shall be assigned at each ESMD/HQ Division and Office and at each ESMD Program and Project, to facilitate the implementation of the RMP within their organization. This does not abrogate the responsibility or accountability of a Program Manager to ensure that all stakeholders or "customers" are integrated into their risk management processes.

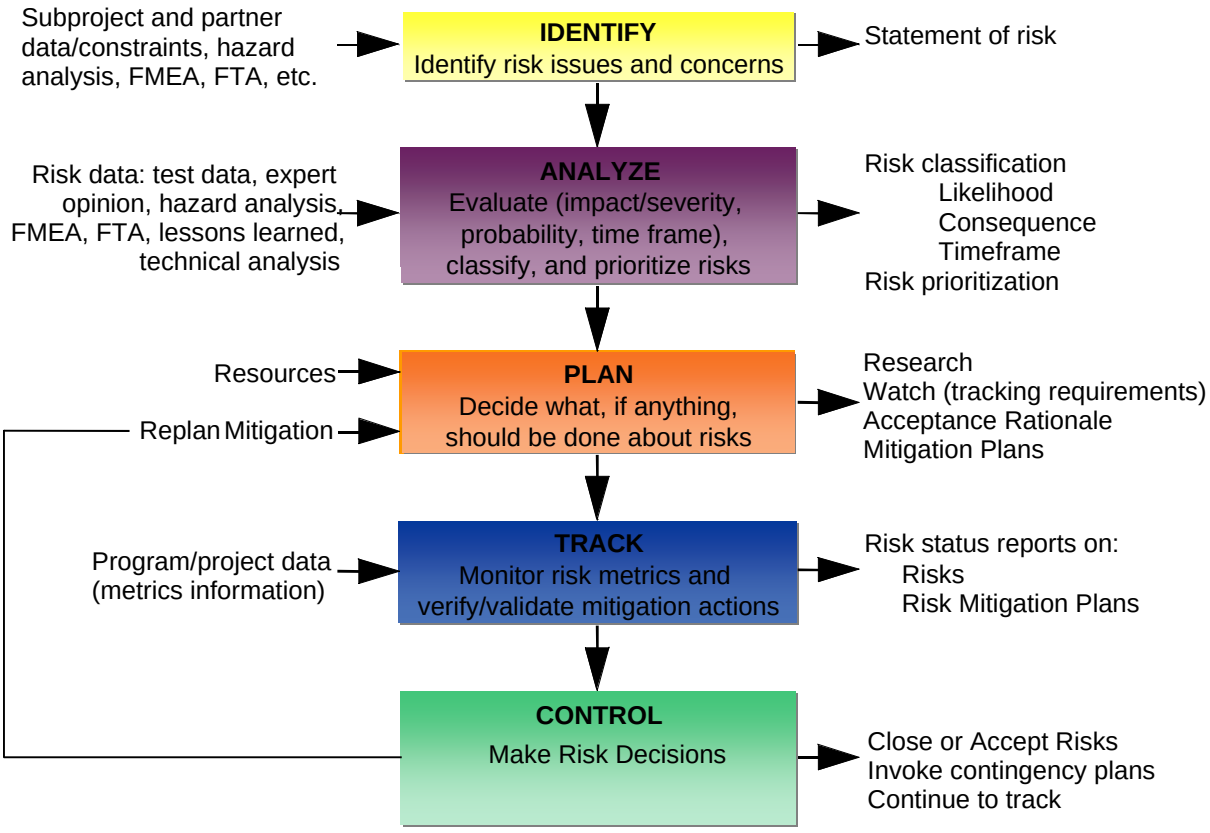
2.1 Continuous Risk Management (CRM) Process

ESMD shall implement the Continuous Risk Management (CRM) process as described in NPR 8000.4 and NPR 7120.5C, including appropriate CRM-complementing processes such as Risk-Based Acquisition Management (R-BAM) and Risk-Based Decision Support, throughout the organization. The CRM process shown in Figure 1 is a continuous, iterative process that identifies, analyzes, plans, tracks, controls, communicates, and documents risk through all life cycle phases of an organization's product developments. The standard terminology specified in Appendix A shall be used by performing organizations to satisfy ESMD reporting requirements.

Figure 1. CRM Process

CRM principles shall be incorporated throughout ESMD as part of performing organizations' risk management plans and processes. Each level shall follow the risk management steps shown in Figure 1 and Figure 2. Performing organizations shall identify and manage risks at

the lowest level possible. Risks shall be reported to their parent organizational level of the ESMD organizational structure (see section 5.2). Performing organizations shall communicate risks horizontally and vertically throughout ESMD.



FMEA – Failure Modes and Effects Analysis
FTA – Fault Tree Analysis

Figure 2. Continuous Risk Management Process Flow

2.1.1 Risk Characterization and Scoring

Risks are characterized primarily by:

- ID Number
- Risk Title
- Risk Owner
- Condition & Consequence (i.e., risk statement). The structure of the risk statement is, "Given that <a specific condition exists> there is a possibility that <a specific consequence may occur>. Consequences are scored against the four standard "Impact Categories" defined in the ESMD Risk Scoring Scheme: cost, schedule, performance (technical), and safety.

Additional attributes are used to characterize a risk such as its categorization in a Risk Breakdown Structure (RBS), Escalation level, Context, and Status. These risk attributes are used to sort, search, and report on risk data.

All ESMD organizations shall use the 5x5 Probability–Impact Diagram (PID), shown in Figure 3, to score their risks. Red risks are termed "High", Yellow as "Moderate", and Green as "Low". A probability (P) of between 1 and 5 and an impact (I) of between 1 and 5 maps to a risk score in the PID. ESMD has biased the PID color scheme with "Impact" having a slightly larger effect than "Probability" on the overall score.

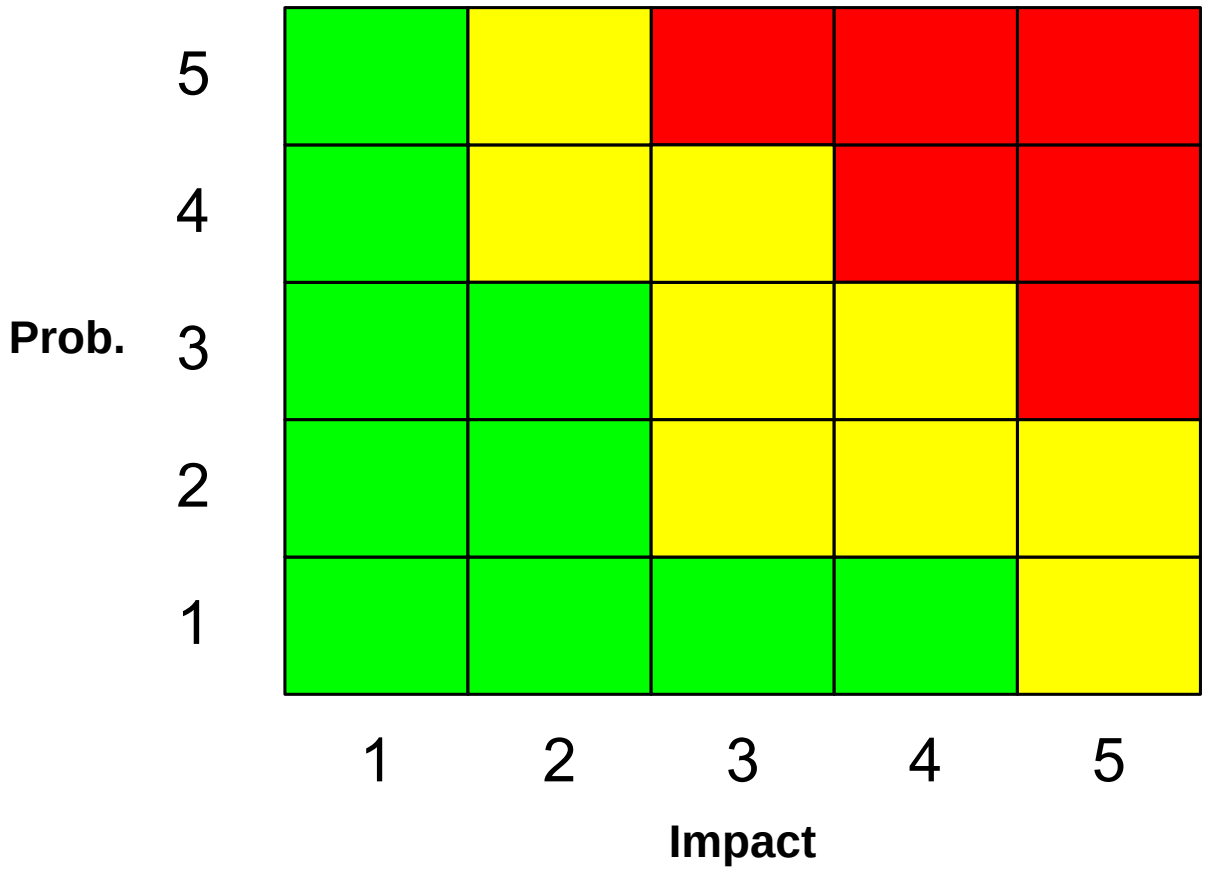


Figure 3. Probability-Impact Diagram (PID)

Probabilities and Impacts may be scored on a qualitative and/or quantitative basis. Risks at each organizational level shall be assessed for their impact in the following four categories:

- Safety
- Cost
- Schedule
- Performance (e.g., technical impacts, managerial aspects, mission impacts, risk integration, management decision-making)

A Scorecard has been defined by ESMD to correlate Risk Qualitative and Quantitative descriptions to both Probability and Impact values. Table 1 and Table 2 show this Scorecard. The ESMD scorecard provides a common reference framework that enables risk data comparison across all Directorate programs. From this scoring scheme, performing organizations shall develop a scoring scheme description to the level of detail necessary to adequately map risk to the ESMD 5x5 matrix.

Table 1. ESMD Probability Scoring

Probability Rating	Ordinal Value	Description
Very Low	1	Qualitative: Very unlikely to occur, management not required in most cases. Strong Controls in Place Quantitative: <=E-5 (for risks with primary impact on Safety) or 1%<P<= 20% (for risks with primary impact on Cost, Schedule, or Performance)
Low	2	Qualitative: Not likely to occur, management not required in all cases. Controls have minor limitations/uncertainties. Quantitative: <=E-4 (for risks with primary impact on Safety) or 20%<P<= 40% (for risks with primary impact on Cost, Schedule, or Performance)
Moderate	3	Qualitative: May occur, management required in some cases. Controls exist with some uncertainties. Quantitative: <=E-3 (for risks with primary impact on Safety) or 40%<P<= 60% (for risks with primary impact on Cost, Schedule, or Performance)
High	4	Qualitative: Highly likely to occur, most cases require management attention. Controls have significant uncertainties. Quantitative: <=E-2 (for risks with primary impact on Safety) or 60%<P<= 80% (for risks with primary impact on Cost, Schedule, or Performance)
Very High	5	Qualitative: Nearly certain to occur, requires immediate management attention. Controls have little or no effect. Quantitative: <=E-1 (for risks with primary impact on Safety) or P>80% (for risks with primary impact on Cost, Schedule, or Performance)

Table 2. ESMD Impact Scoring

Impact		**1 Very Low**	**2 Low**	**3 Moderate**	**4 High**	**5 Very High**
SAFETY	**Personnel** (Crew, ground, or public)	Minor injury requiring first aid treatment	Moderate injury, illness or incapacitation	Severe injury, illness or incapacitation	Permanent disabling injury	Death
	Facilities, Equipment, or Other Assets	Minor damage to Non-Critical ground facilities or systems	Major damage to Non-Critical ground facilities or systems	Minor damage to Flight assets or Critical ground facilities or systems. Loss of Non-Critical ground facilities or systems	Major damage to Flight assets or Critical ground facilities or systems	Loss of Flight assets (vehicle) or critical ground facilities or systems
	Environment	Negligible OSHA/EPA violation – non-reportable.	Minor reportable OSHA/EPA violation.	Moderate OSHA/EPA violation which requires immediate remediation.	Major OSHA/EPA violation causing temporary stoppage.	Serious or repeat OSHA/EPA violations which may result in termination of program.

Impact		**1** **Very Low**	**2** **Low**	**3** **Moderate**	**4** **High**	**5** **Very High**
PERFORMANCE (Mission Success)	**Requirements**	Negligible impact to requirements/ design margins	Small Impact to requirements/design margins	Moderate impact to requirements/design margins	Major impact to requirements/design margins	Technical goals not achievable with existing engineering capabilities/ technologies
	Operations	Negligible impact to mission objectives/ operations	Minor impact to operations – workarounds available	Moderate impact to operations – workarounds available	Major impact to operations – workaround not available	Unable to achieve major mission objective
	Supportability	Temporary usage loss or capability to maintain a non-flight critical asset	Permanent usage loss or capability to maintain a non-flight critical asset	Temporary usage loss or capability to maintain major element(s) of flight vehicle or ground facility	Permanent usage loss or capability to maintain major element(s) of flight vehicle or ground facility	Inability to support further flight operations

Impact	**1** **Very Low**	**2** **Low**	**3** **Moderate**	**4** **High**	**5** **Very High**
Cost	≤$100K	>$100K but ≤$1M	>$1M but ≤$10M	>$10M but ≤$50M	>$50M
Schedule	<1 month delay to major program milestone (SRR, PDR, CDR, SAR)	1-3 month delay to major program milestone (SRR, PDR, CDR, SAR)	> 3-6 month delay to major program milestone (SRR, PDR, CDR, SAR)	6-9 month delay to major program milestone (SRR, PDR, CDR, SAR)	>9 month delay to major program milestone or cannot meet major program milestones (SRR, PDR, CDR, SAR)

2.1.2 Managing Risks

Once a risk has been identified, analyzed, and characterized as described previously, a plan for how to manage risk reduction is developed. The management (or handling) phase of the CRM paradigm includes planning, tracking, and controlling elements. The CRM planning element includes assignment of responsibility for overall risk handling, and a determination of approach.

- When a potential risk is identified, it is initially defined as a candidate risk. This status is used while the risk is being evaluated and a decision is being made as to how significant the risk actually is, who the most appropriate risk owner is, and what strategy should be employed in mitigation.
- Risk ownership should be assigned to the organization and person best able to define and implement mitigation efforts. Visibility and support for significant risks are achieved through escalation in the Top Risk Reporting Process.
- Candidate risks become Approved risks with the concurrence of the governing Risk Review Board, once sufficient information and analysis is available, and a handling strategy is selected.

2.1.2.1 Handling Strategy

The risk owner reviews the technical aspects of the approved risk and recommends a plan of action to their management (at the level that the risk is being managed). The recommendation will be one of the following:

- Accept – risks in which the impacts (consequences) are tolerable should the risk actually be realized. Accepted risks will be reviewed periodically to ensure conditions/assumptions have not changed requiring the risk to be "reopened".
- Mitigate – risks whose likelihood of consequence will be reduced by taking proactive steps.
- Research – risks that need more information/analysis before a decision can be made to mitigate or accept (a future reassessment date needs to be specified to determine further action).
- Watch – risks in which the impacts (consequences) are tolerable should the risk actually be realized, given the current environment / circumstances. But, the impacts may be intolerable if the current environment / circumstances change. However, risks with a handling strategy of "Watch" must be reviewed on a clearly defined and regular basis.

If the choice is to mitigate the risk, the risk owner will develop and document a high level mitigation plan. This plan is documented in the ESMD risk management tool. Each plan may have several tasks that need to be performed by different owners in different organizations. Detailed mitigation actions are then created and documented in the ESMD risk management tool. The plan owner will implement the mitigation plan and oversee that all the mitigation

actions are completed until the risk reaches an acceptable limit, or is eliminated. At that time, the owner will recommend "closure" of the risk to the appropriate level of management.

It is the goal of ESMD to reduce risks to the lowest level possible within the allocated resources. When choosing to mitigate a risk, some common criteria should be considered when developing the mitigation plan approach, including:

- Cost
  - Is the mitigation plan within the current funded budget?
  - How much does each mitigating option cost?
  - Is the mitigation going to cost more than the actual cost of the risk impact?
- Schedule
  - Does the mitigating option fit into current schedules?
  - What is the impact to the schedule for each mitigation option?
  - Does the risk affect the critical path?
- Confidence of successful completion
  - What is the confidence level for completion of each mitigation option?
- Amount of risk reduced
  - What is the remaining risk level at the completion of the mitigation plan (residual risk)?

Detailed risk data is captured in the ESMD risk management tool. Such data should be reviewed and updated in the ESMD risk management tool on at least a monthly basis. However, updates are recommended on a more frequent basis as the need arises in order to ensure that all stakeholders are aware of changes affecting the risk. Periodic updates should include a re-assessment of the defined mitigation plan to ensure that risk reduction efforts are on track and that changes are not needed.

If a candidate risk is disapproved, a clear, concise rationale for rejection, including dissenting opinions, will be documented within the ESMD risk management tool.

2.1.2.2 Risk Status

The following risk statuses are available:

- APPROVED
  - Approved risks have been reviewed by the governing Risk Review Board and have been determined to be legitimate risks to be managed.
- CLOSED
  - Closed risks will no longer be actively mitigated or monitored. Risks that have been reduced to a level where the remaining risk is considered negligible and further risk reduction activity is deemed unnecessary may be closed.
  - Closed risks should be re-evaluated if new knowledge is gained that may require the risk to be re-opened or a new risk generated. Also, risks that have been incorporated or combined with a new risk may be closed.

- Closure rationale must be defined, approved, and documented in the ESMD risk management tool.
- Approval from the owning organization, affected stakeholders, and the highest level of escalation is required to close an open risk. For example, the Program Manager must approve the closure of Top Program Risks.
- The risk owner may propose the risk to the ESMD RMWG for consideration as a possible a Knowledge Based Risk (KBR) before closing a risk (see section 2.2.1).
- A risk that has been incorporated into a new risk for clarification can be closed; however, the closure rationale must reference the new risk. In addition, the new risk must reference the risk that was closed to ensure configuration management.
- To close a risk, the closure rationale must have concurrence by the governing Risk Review Board.

- REJECTED
  - Rejected risks have been reviewed by the governing Risk Review Board and have been determined to be unnecessary.
  - Risks may be rejected for many reasons. For example, because another risk already exists that addresses the issue. Existing risks may be modified to capture the issue identified in the rejected risk.
  - Rejected risks are stored in the ESMD risk management tool for reference. Risks are not deleted from the ESMD risk management tool.

2.1.2.3 Risk Category

A risk may be associated with one or more Risk Categories. The risk category is a Risk Breakdown Structure (RBS), which is analogous to a Work Breakdown Structure in that it is a hierarchical way to categorize risks and support their integrated assessment.

The RBS provides the taxonomy needed to ensure consistent and comprehensive risk identification and management. The RBS provides a consistent hierarchical structure for reviewing related risks across the ESMD risk portfolio. Reviewing risks in a particular RBS category can be used to coordinate similar or duplicative mitigation efforts and to identify gaps in risk identification.

ESMD's risk categories are defined in Appendix C.

2.1.3 Risk Associations

Risks shall be organized and reported on within a hierarchical, organization and work breakdown structure using the ESMD risk management tool. This is necessary to support the integration of Systems Engineering and Integrated Master Schedule (IMS) tools, which will facilitate integrated risk, requirements, cost, and schedule analyses. These integrations will

support the association of: (1) risks with their related requirements, and (2) risk mitigation activities with their related IMS / WBS elements.

2.2 Knowledge Management Integration

ESMD risk management shall include the integration of knowledge management and risk management processes into the program life cycle. Designing a complex architecture of hardware, software, ground and space-based assets to return to the Moon and then on to Mars will require an effective strategy to generate, capture and distribute knowledge. Risk Management Officers, who already use lessons learned as a source of information for risk identification, are in a unique position within the organization to effectively perform these functions.

2.2.1 Knowledge-Based Risks

Knowledge-Based Risks (KBRs) are documented in the ESMD risk management tool to provide RMOs and other users throughout ESMD, easy access to useful risk identification, assessment, and management information. In addition to conveying lessons learned, KBRs are intended to fill "knowledge gaps" in risk management and other related communities. This provides an “Expert Locator” functionality for RMOs and other users – someone to contact with experience in managing a particular risk. Some KBRs will be linked to “video nuggets,” which are 3 to 5 minute videos of Subject Matter Experts explaining the lessons learned associated with the identification, context, and mitigation of those risks.

2.2.2 "Pause and Learn" (PaL) Events

Pause and Learn (PaL) events are based on the Army After-Action Reviews process. The idea behind the PaL process is to create a learning event at selected critical events in the life cycle of a program. End of program reflections are good but are too infrequent for the organization to learn from in a timely manner. PaLs must be a fundamental part of every program and should be built into the program process and schedule. The basic premise is that learning occurs through ongoing conversation and information sharing. Risk Management Officers shall facilitate these events and share the knowledge gained, as appropriate, vertically and horizontally across the organization. A checklist for conducting a PaL event is included in Appendix D along with a flowchart of critical process steps.

2.2.3 Risk and Knowledge Management Community of Practice

The Risk and Knowledge Management Community of Practice (CoP) serves as a tool for all RMOs to discuss topics of concern within the operating community and to facilitate and leverage best practices. Key event/meeting information can also be shared on the CoP. The community can be accessed via PBMA In addition to regular telecons, the CoP will also collaborate through periodic face-to-face meetings.

2.2.4 Wikis

Wikis are web-based tools that provide a collaborative group authoring capability. Wiki technology, along with other organizational and individual behavioral shifts, will provide the way forward in enhancing ESMD efficiency and effectiveness. Wikis are highly flexible, powerful, web-based environments that allow authorized community members to collaborate in the development of narrative "pages" representing the "knowledge or truth" on a given topic (as defined by the community of collaborators).

ESMD uses the "Confluence" by Atlassian as its wiki engine. Several CoPs and offices are using Wikis to communicate and share information in the areas of Constellation software development, information technology, and other communities. A robust training capability is being developed to support personnel to stand up new wikis for collaborative purposes

2.2.5 ESMD R&KM Portal

The NASA ESMD Vignette Portal software creates a centrally located Web presence for programs, which is secure, easily accessible by users, has a consistent look and feel, and has tools for content management. ESMD Risk and Knowledge Management Office Portal leverages the NASA Vignette Portal as a host the complete set of references for risk and knowledge management activity within NASA ESMD.

3 ESMD Risk Management Roles and Responsibilities

Each ESMD performing organization shall implement the CRM process as described in NPR 7120.5, NPR 8000.4, and Section 2.1. Each performing organization shall develop and implement its own risk management plan that references and complements this ESMD RMP. The scope and detail of each plan should be tailored based on the performing organization's degree of risk management activity and number of reporting subordinate levels. The RMPs describe how the performing organization will implement risk management, including specific organizational structures, processes, tools, metrics, risk scoring criteria, and risk impact categories not explicitly discussed in the ESMD RMP.

3.1 ESMD Associate Administrator Responsibilities

The ESMD Associate Administrator (AA) has overall responsibility for establishing ESMD risk management policy. The following ESMD AA responsibilities are delegated to the Directorate Integration Office (DIO):

- Establish and provide risk management policy, guidance, and templates to programs where necessary
- Establish ESMD policy coupling risk management and knowledge management processes/data repositories
- Perform strategic risk management planning
- Ensure risks are identified for all program life cycle phases defined in NPR 7120.5
- Assess program risk management processes for effectiveness and compliance with requirements (e.g., NPR 7120.5, NPR 8000.4, ESMD RMP)
- Ensure performing organization compliance with R-BAM
- Ensure integration of risks between ESMD and SOMD
- Support the risk management activities as directed by the Transition Control Board and the Joint Integrated Control Board
- Maintain a Directorate Top Risk List (may include risks from Directorate Divisions, Offices, and Performing Organizations)
- Review performing organizations' metrics to ensure that relevant parameters regarding their risk activities are tracked and reported
- Support the Top Risk Reporting (TRR) Process
    - Review the ESMD Top Risk List as proposed by the Directorate divisions / offices, programs, and projects, and modify as needed
    - Evaluate the effectiveness of the mitigation actions
    - Prioritize risks, as needed

- Provide resources to mitigate risks, as needed

3.2 ESMD Risk Management Officer (RMO) Responsibilities

The ESMD Risk Management Officer (RMO) responsibilities include:

- Lead the Risk Management Working Group (RMWG)
- Lead effort to integrate risk management and knowledge management
- Facilitate PaL events and share the knowledge gained, as appropriate, vertically and horizontally across the organization
- Ensure that accurate risk data is collected, archived, and reported to Agency senior management
- Review performing organization risk management practices, procedures, and data for best practices and integration opportunities
- Conduct risk management process audits of ESMD Directorate and Level 2 organizations
- Facilitate horizontal (across organizations) and vertical (higher and lower level organizations) risk integration
- Lead effort to integrate risks and requirements
- Lead effort to integrate risks and integrated master schedule (IMS) data
- Propose changes to the Top Directorate Risk List to the ESMD AA
- Facilitate integration of risks between ESMD and SOMD
- Maintain configuration control of all data in the ESMD risk management tool
- Manage configuration of the ESMD risk management tool
- Provide ESMD-specific training on CRM, ESMD risk reporting, and the ESMD risk management tool
- Support the Top Risk Reporting (TRR) Process

3.3 ESMD Division and Office Responsibilities

The ESMD Division and Office responsibilities include:

- Perform strategic risk management planning
- Provide resources to mitigate risks, as needed.
- Ensure that accurate risk data is collected, archived, and reported to the ESMD RMWG
- Collaborate on joint mitigation plans/tasks with other organizations as necessary

- Support the risk management activities associated with the Transition Control Board and the Joint Integrated Control Board, as needed
- Ensure horizontal (across organizations) and vertical (higher and lower level organizations) risk integration
- Conduct monthly risk reviews/assessments to identify and review candidate risk items and risks. In addition, oversee the overall mitigation plans and ensure mitigation tasks are on track.
- Maintain a Division / Office Top Risk List
- Participate in the Top Risk Review during the Quarterly Program Management Review (QPMR)
- Participate in Division / Office risk forums to develop Division / Office Top Risk Lists and identify risks to be escalated.
- Participate in the RMWG.

3.4 Performing Organization Responsibilities

Performing organizations shall create risk forums / boards per their RMP, as needed to manage risk. Performing organization responsibilities include:

- Develop a risk management infrastructure with implementing organizations, procedures, and tools
- Assure that adequate resources are available to mitigate risks
- Collaborate on joint mitigation plans/tasks with other organizations as necessary
- Conduct risk reviews/assessments to identify and review candidate risk items and risks. In addition, oversee the overall mitigation plans and ensure mitigation tasks are on track.
- Assure that risk management is appropriately addressed in the acquisition strategy in terms of the statement of work, evaluation criteria and incentives (R-BAM)
- Work risk management issues (horizontally and vertically) and perform risk analyses
- Support the TRR process
    - Review subordinate (lower level) performing organizations' escalated risks and review risks identified by the current level performing organization, to determine the Top Risk List for the current level performing organization
- Maintain tracking between parent risks and their child risks
- Assign ownership for each risk
- Maintain the performing organization's Top Risk List

- Ensure the integration of risk management processes with appropriate knowledge management processes

3.5 Risk Management Officer (RMO)

Each performing organization shall assign an individual to serve as its Risk Management Officer (RMO). Responsibilities of the RMO include the following:

- Implement, maintain, and enforce the performing organization's risk management plan and CRM process
- Lead the performing organization's risk management team
- Facilitate all risk management activities within the performing organization
- Ensure horizontal and vertical integration of risks is conducted
- Maintain cognizance of all risk management issues for subordinate organizational levels, as appropriate, and serve as the point of contact for risk issues elevated from subordinate performing organizations
- Review and ensure the effectiveness of the governing risk management process
- Advise and support higher level managers in making decisions on significant risk issues (including subordinate and common level risk issues, as appropriate), risk management resource investments, and in reporting up to the next higher organizational level
- Ensure applicable personnel within the performing organization are provided adequate risk management training to conduct their risk management activities
- Ensure integration of risk and knowledge management processes

4 ESMD – SOMD Transition Interfaces

Because Orion / ARES-I will replace Shuttle and will provide crew transportation functions for the International Space Station, a coordination activity has been initiated to transition these assets efficiently. At the Directorate level, two boards have been created to support this transition: (1) the Joint Integrated Control Board (JICB) and (2) the Transition Control Board (TCB).

All ESMD performing organizations shall ensure that they have a viable working relationship with the appropriate Space Operations counterparts to identify and manage inter-Directorate transition risks. They shall document the nature of such interactions in their respective Risk Management Plans.

4.1 Joint Integration Control Board (JICB)

The Joint Integration Control Board (JICB) is "strategic" a decision-making forum for the Space Operations Mission Directorate (SOMD) and the Exploration Systems Mission Directorate (ESMD). Its purpose is to provide integrated, strategic direction and decision-making for the three Human Space Flight (HSF) programs (Space Shuttle Program, International Space Station Program, and the Constellation Program).

With respect to risk management, the JICB is responsible for coordinating, reviewing, and approving transition risks that are escalated to the JICB.

Transition risks, ESMD- or SOMD-owned, may be escalated to the JICB using the following general criteria:

- Risks that cannot be mitigated at the performing organization's level, including requests for additional funding
- Risks for which the performing organization desires a decision to be made by both ESMD and SOMD Associate Administrators
- Risks that require integration with other Mission or Mission Support Directorate Organizations
- Risks that are of substantial significance and demand broader awareness by the JICB

4.2 Transition Control Board (TCB)

The Transition Control Board (TCB) is a "tactical" decision-making forum for the Space Operations Mission Directorate (SOMD) and the Exploration Systems Mission Directorate (ESMD) to perform program transitional planning as Directorate programs move through their respective life cycles with associated changes to their individual requirements. Headquarters Institutions and Management (IMO), Safety and Mission Assurance (SMA) and the Office of the Chief Engineer (OCE) are also TCB members.

The purpose of the TCB is to communicate and coordinate Shuttle to Constellation transition planning in areas such as resources, assets, and infrastructure. One key TCB focus area related to risk management is to evaluate risks in the ability of Shuttle and Constellation programs to effectively transition assets, activities, capabilities, and contracts.

5 Risk Management Process Details

5.1 Risk Management Processes

All performing organizations shall establish, document, and implement a risk management process. This section defines risk management process requirements, including requirements for implementing the ESMD Cost Threat process, Earned Value Management (EVM), Risk-Based Acquisition Management (R-BAM), Risk-Based Design and Decision Support processes, and a Risk Breakdown Structure.

5.1.1 Tailorable Process Flow for Performing Organizations

A tailorable risk management process is included in Appendix B. This tailorable process describes a generic approach to performing risk management.

Each performing organization's risk management process shall include provisions for:

- Compliance with CRM
- Capability for all employees to propose a candidate risk
- An appeals process for rejected risks
- Support of risk escalation and Top Risk Reviews
- Capture of cost threat data
- EVM reporting on risk management / mitigation activities
- Self-audit of the risk process, at least annually
- Supporting integration of risk management and KM (see section 2.2)
- Facilitation of "pause and learn" events within programs (see Appendix D)

The process shown in Appendix B may be used by all ESMD programs for performing risk management.

5.1.2 ESMD Cost Threat Process

Cost threats, in the context of risk management, are risk mitigation costs that are not included in the current Directorate Integrated Master Schedule (IMS), and therefore, may impact Directorate reserves. Cost threats may result from newly defined mitigation activities, or from mitigation activities that may exceed planned costs.

The ESMD Resource Management Office will work with ESMD Risk Owners to ensure that all cost threats are identified and integrated into a total Directorate cost risk assessment.

Developing a complete cost threat assessment relies upon the active participation of all ESMD divisions and offices. ESMD divisions and offices will evaluate their activities / risks to identify cost threats, including potential cost threats evolving from changes to implementation plans and requirements. The ESMD Resource Management Office is responsible for identifying any additional directorate level cost threats. The ESMD Resource Management Office exercises an integration role in reviewing all cost threats, and works with the ESMD divisions and offices to define accurate cost threat information to develop an integrated cost risk assessment.

5.1.3 Application of Earned Value Management (EVM)

All programs shall identify meaningful, measurable, and relevant risk mitigation activities. These activities and milestones shall be included in the program integrated master schedule (IMS) and shall be tracked with respect to cost and schedule performance against milestone accomplishment throughout the active program implementation period. The IMS shall be updated to reflect any changes in the risk mitigation plan / activities.

EVM shall be used to assess the mitigation progress with respect to planned cost and schedule. The rationale for this requirement is that all risk mitigation activities ultimately involve use of program resources (e.g., personnel, schedule, budget). EVM reporting relies on the accuracy of the cost and schedule data used as inputs. So, performing organizations must employ a rigorous approach for estimating and monitoring costs.

Performing organizations must analyze significant variances from the plan, forecast impacts, and develop an estimate at completion based on performance data and work to be performed.

5.1.4 Application of Risk-Based Acquisition Management (R-BAM)

ESMD and its performing organizations shall apply the principles of Risk-Based Acquisition Management (R-BAM). This requires that the principles of CRM be formally utilized in the program life cycle of a procurement scenario and further that active involvement of the acquisition team begins early in the CRM process. Risks and mitigations are actively addressed throughout the remainder of the acquisition process. This process results in acquisition decisions that are made based on documented, risk-based criteria. From the NASA PBMA R-BAM website note that:

> *Risk-Based Acquisition Management (R-BAM) seeks to integrate risk management principles (including safety, security, health, cost, schedule, technical, damage to the environment, and unintended technology transfer) throughout the entire acquisition process. R-BAM will identify significant risk areas associated with a procurement and enables acquisition team resources to be focused on mitigating these risks. R-BAM is a key NASA acquisition initiative.*

R-BAM principles apply throughout the acquisition phases, including:

- *Requirements Development,*
- *Acquisition Strategy Planning,*
- *Contract Type Selection,*
- *Fee Incentive Planning,*
- *Solicitation Development,*
- *Source Selection,*
- *Contractor Surveillance, and*
- *Other Post-Award Acquisition Management.*

5.1.5 Application of Risk-Informed Decision Making

The intent of the ESMD risk management plan is to establish Risk-Informed Decision Making (RIDM) practices within ESMD and associated performing organizations. RIDM does not imply a broad new set of milestones, processes and tools. Rather, RIDM implies a more effective and comprehensive use of risk assessment to improve the quality and consistency of directorate, program decision making. For example, RIDM should be implemented as a significant element of the following program processes:

- Risk-Informed Design

  Many NASA programs have adopted a cross-discipline iterative design paradigm that begins with a high level evaluation of the operational mission that the program has been chartered to perform, and iteratively evaluates and improves on the mission architecture and operations so that they more effectively meet the mission need within cost and schedule goals. The application of risk assessment as a part of this iterative process allows early risk insights to be incorporated in design and planning. Further, the questions raised by these assessments indicate areas where additional test and analysis are needed to clarify design vulnerabilities. The use of functional risk modeling techniques based on a systematic evaluation of the proposed mission timeline can provide a more systematic way to identify significant vulnerabilities as well as a bridge between traditional hazard analysis and probabilistic risk assessments.

- Risk Assessments at Program Boards / Decision Forums

  While design represents a continuous and iterative decision-making application, programs are called upon to make many discrete decisions that arise during the day-to-day operation of the program. Experience indicates that programs can easily fall into the trap of making these decisions without adequately addressing the risks

associated with the selected action. It is important that decisions brought forward address traditional decision criteria such as cost, schedule, and technical performance – but also address risk. Risks associated with the cost, schedule, and technical performance criteria as well as safety and mission success must be considered when presenting a case for decision to program managers. And the risks associated with all options for action, as well as the "no action" case should be considered.

- Continuous Risk Management

  Programs will implement a Continuous Risk Management process aimed at identifying, analyzing, planning, tracking, controlling, communicating and documenting risks. This process is complimentary to those mentioned above as residual risks arising from both the design and decision processes will be managed using CRM.

- Flight / Test Readiness Reviews

  During flight and test readiness reviews, a review of residual technical risks related to safety and mission success are conducted to ensure informed risk acceptance prior to a decision to proceed.

Effective RIDM depends on the conduct of risk analysis. There are many different risk analysis methodologies and tools associated with different applications (cost, schedule, technical, safety, etc). Applying the most appropriate method and tool to each decision application is a critical decision. The ESMD RMWG can provide guidance to RMOs on the method and tool selection. However, these selections will be somewhat application specific.

The complexity of the analysis is another significant factor to be considered when developing risk analysis to support critical decisions. For example, early design analyses will be less complex generally due to the lack of design definition. Greater complexity generally demands better understanding of the systems and environments to be assessed and higher pedigree for the supporting data. It is recommended that the following considerations be taken into account when planning and executing a risk analysis aimed at supporting a critical decision.

- Availability of data: In some cases historical data is available to support a more rigorous assessment of likelihood of occurrence. Given the long history of NASA operations, much historical data will be available to inform risk analysts. However, if data is scarce or unavailable, a lower granularity assessment may be required. In all cases, clarity in communicating the level of uncertainty that exists in the analysis is paramount to making a credible and defensible decision.

- Expected value of more information: If the investment required to define a more rigorous estimate of risk likelihood is significant but the benefit of that increased accuracy is considered minimal, then it may be determined that resources are best applied to other risks. Conversely, in some cases, significantly improved risk insight may be gained through additional analysis and the investment of time and resources

may be deemed necessary. Furthermore, the program may decide to invest in additional testing to provide the needed insight.

- Significance of the risk: Does the significance of the risk justify the initiation of a more rigorous study? There are many potential risks that ESMD organizations face, and prudence dictates that resources are best applied to the more pressing risks.

5.1.6 Application of a Risk Breakdown Structure (RBS)

A Risk Breakdown Structure (RBS) is analogous to a Work Breakdown Structure, in that it is a hierarchical way to categorize risks and support their assessment, communication, and management. The RBS provides the taxonomy needed to ensure consistent and comprehensive risk identification and management. In the risk identification process, it may be used as a checklist to ensure that all categories of risks and risk sources have been considered. In the risk reporting process, the RBS provides a consistent hierarchical structure for summarizing risks for use in oversight, budgeting, planning, and reporting risks to program decision makers. A baseline RBS structure is shown in Appendix C. The RBS may be expanded or edited to support ESMD activities as needed.

Review and assessment of the risks by Category can help to identify additional risks, recognize risk trends, identify associated / linked / duplicated risks, compare risks across programs, and provide lessons learned for future programs.

5.2 Risk Reporting and Metrics

This section specifies the risk reporting to be provided by performing organizations, describes risk management metrics to be developed and managed by performing organizations as specified in the performing organization risk management plans, and presents risk escalation requirements.

5.2.1 Risk Reporting

Performing organization risk management processes shall support visibility and communication of risks to the next higher management level. This communication will be aided by performing organization risk review and reporting processes.

Each level of performing organization shall review its sublevel performing organization risk data, and track it along with risks originating at their own level, to produce an accurate view of the risk posture at their level and to track progress towards overall risk reduction.

ESMD and its performing organizations shall provide all of their identified risks to ESMD/HQ by entering them in the ESMD-provided risk tool.

Programs shall report top risks to the ESMD RMWG, monthly. Programs shall report top risks to the ESMD AA during their quarterly program management reviews.

5.2.2 Risk Management Metrics

Risk management metrics shall be developed and used for the following purposes:

- Risk management process improvement,
- Trending and identification of new risks,
- Support of periodic audits and reviews,
- Monitoring effectiveness of individual mitigation plans, and
- Long-term program planning.

Metrics that measure and track the effectiveness of the implementation of risk management shall be established by performing organizations. For example, metrics can be used to measure the time it takes for a risk to get from its source to the right destination (i.e., to the appropriate decision-maker – that is, that the risk is escalated to the appropriate level), whether all risks are being captured by the system, or whether there is sufficient representation of risks from all appropriate functional areas. Other metrics could include whether mitigation plans are being followed (through the use of detailed statistics). The base measures are direct measures on the process itself. The derived measures are obtained by applying some algorithm to the base measures to provide trending data for corrective action analysis.

Metrics may include the following types of information (non-inclusive list):

- Staleness of risk data
- Change in number of risks between reporting periods
    - Quantity of new risks created
    - Quantity of risks closed
- Status / effectiveness of mitigation plans
- Number of plans which are underperforming the proposed mitigations (e.g., behind schedule, over budget)
- EVMS
    - Cost Efficiency (CPI) for mitigation activities
    - Schedule Efficiency (SPI) for mitigation activities
- Quantity and degree of coordination of Risks by Risk Category

5.2.3 Top Risk Reporting Process

The Top Risk Reporting (TRR) Process describes how ESMD Divisions / Offices and performing organizations will address risks, which have been escalated by lower level organizations. This process includes Directorate and program risks related to Safety, Technical Performance, Cost, and Schedule objectives.

The TRR process supports risk communication by raising the awareness and visibility of risks to potential Directorate and program stakeholders.

The Risk Management Working Group (RMWG) shall review all ESMD risks prior to the QPMR and will develop a proposed ESMD Top Risk List for review by the ESMD AA. Top ESMD Top Directorate Risks (TDRs) shall be reviewed by the ESMD AA on a quarterly basis, including a review of mitigation progress and of newly identified threats that could impact ESMD's ability to meet safety, technical performance, cost, and schedule goals and objectives.

The following processes will occur within each level of the hierarchy:

- Designate top risks, and designate risks to be escalated for inclusion in the next higher management level's Top Risk List, in the applicable risk management database.
- Participate in the top risk review for the next higher level organization.
- The TRR Process will culminate in a review of the ESMD Top Risk List and Program Top Risk Lists during the Quarterly Program Management Review (QPMR).
- Identify relationships (i.e., associations and parent / child) among risks within the division / program, with risks identified by other organizations within the level ("horizontally"), and with risks identified by the next higher and lower level organizations ("vertically").

5.2.3.1 Risk Reporting Structure

Figure 4 depicts the ESMD Top Risk Reporting structure. All Level 1 and Level 2 organizations and programs develop a Top Risk List, which includes the most critical risks from their organization / program and its subordinate programs / projects. They provide / present their Top Risk Lists to the ESMD RMWG (for information only) and subsequently present them to the ESMD AA during the QPMR.

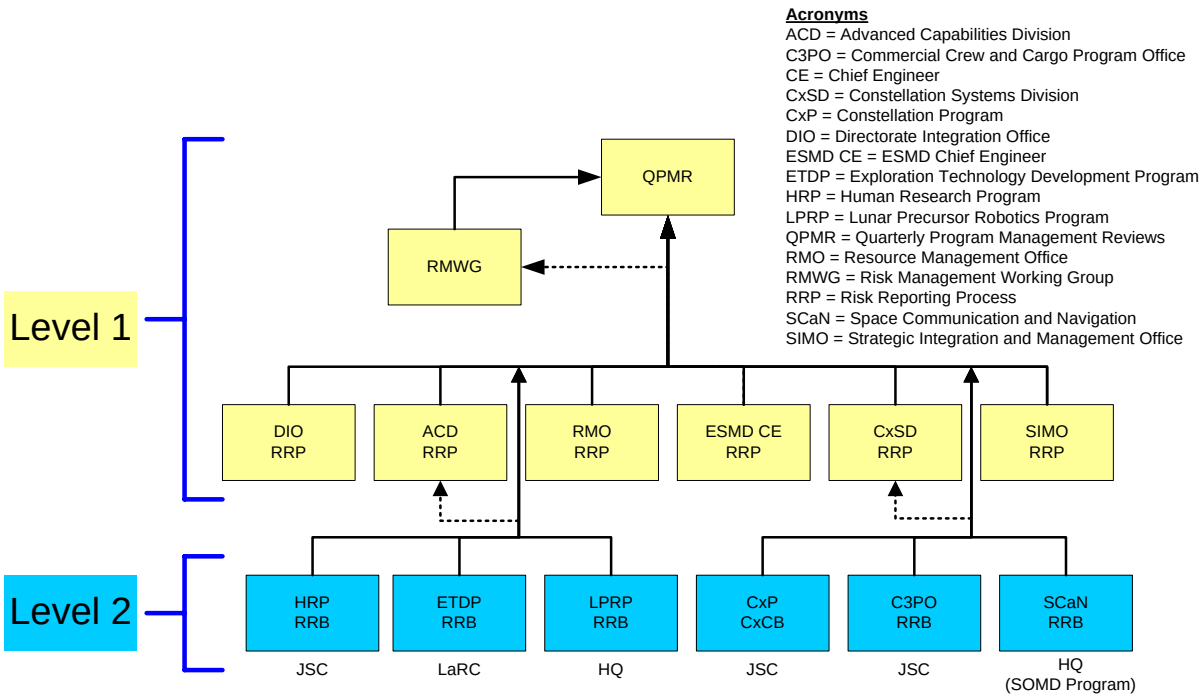


Figure 4. ESMD Top Risk Reporting Structure

In addition to the formal reporting to the RMWG and the QPMR, the Human Research Program (HRP), the Exploration Technology Development Program (ETDP), the Lunar Precursor Robotics Program (LPRP) provide their Top Risk Lists to the Advanced Capabilities Division (ACD). The Constellation Systems Program (CxP), the Commercial Crew and Cargo Program Office (C3PO), and the Space Communication and Navigation (SCaN) program provide their Top Risk Lists to the Constellation Systems Division (CxD).

5.2.3.2 Risk Review Considerations

The RMWG develops the draft ESMD Top Risk List and provides it to the ESMD AA for review and approval. They also provide recommendations for action regarding the ESMD Division / Office and performing organization Top Risk Lists.

At each level of the TRR process, risk information is discussed and decisions are made to manage the risks. Questions to be answered during the status review may include:

- What is the technical basis of the risk assessment?
- Does the risk assessment and risk information adequately convey the significance of the risk to potential program stakeholders?
- Is the mitigation plan on schedule?
- Are the tasks being completed within applicable constraints?

- Has the risk likelihood or consequence changed?
- Are adequate mitigation resources available?
- Are additional measures required to manage the risk?
- Are contingency plans required in order to establish a fallback in the event that risk mitigation is unsuccessful?
- Is the risk related to any existing risks horizontally or vertically?

5.2.3.3 Escalation

The following approach will be followed to classify and "vertically" communicate the significance of each ESMD risk:

- Program Managers and Division-Level managers will define their top risks in terms of risk significance. This will be determined primarily based on risk likelihood and consequence. However, other factors such as time remaining for action may be considered. The RMWG will develop the ESMD Top Risk List.
- Risks are escalated to the next level if:
    - Resources are needed to mitigate the risk.
    - Decisions are needed by the next level of management.
    - Integration with other ESMD organizations or programs is needed (risk owners should work with the ESMD Directorate Integration Office to determine if there are integration impacts).
    - The significance of the risk requires broader awareness throughout the program.
- Risk escalation is a mechanism for prioritizing and reporting risks to the next higher level of management. Escalation can be initiated by the Program Manager "proposing" risks to be included in the next higher level Top Risk list or the next higher level organization "pulling up" subordinate risks to be included in their Top Risk List. Top Risk Lists are identified based on the significance of the risk, which takes into account likelihood, consequence, timeframe, and other factors defined by the Program Manager.
    - Any individual risk can be escalated to multiple levels, simultaneously, above the level at which it is owned. Note that risk escalation and risk ownership are two different parameters. Risk ownership typically remains at the action level and the owner is ultimately responsible for coordination and resolution/mitigation. So, a Top Project Risk (TProjR) may also be a Top Program Risk (TPR) and a Top Directorate Risk (TDR). The RMWG will propose a Top Directorate Risk List based on a review of top division and program risks.

Top risks from the ESMD Divisions, Offices, and Programs are considered for inclusion in the Top Directorate Risk List, which is briefed to the ESMD AA for approval. Each ESMD Division, Office, and Program will hold their own internal risk review to manage their risks and to establish their Top Risk List.

Figure 5 shows the top risks at each level. Note that proposed Top Risks for the next higher management level ("escalated risks") are on the Top Risk List for the current level.

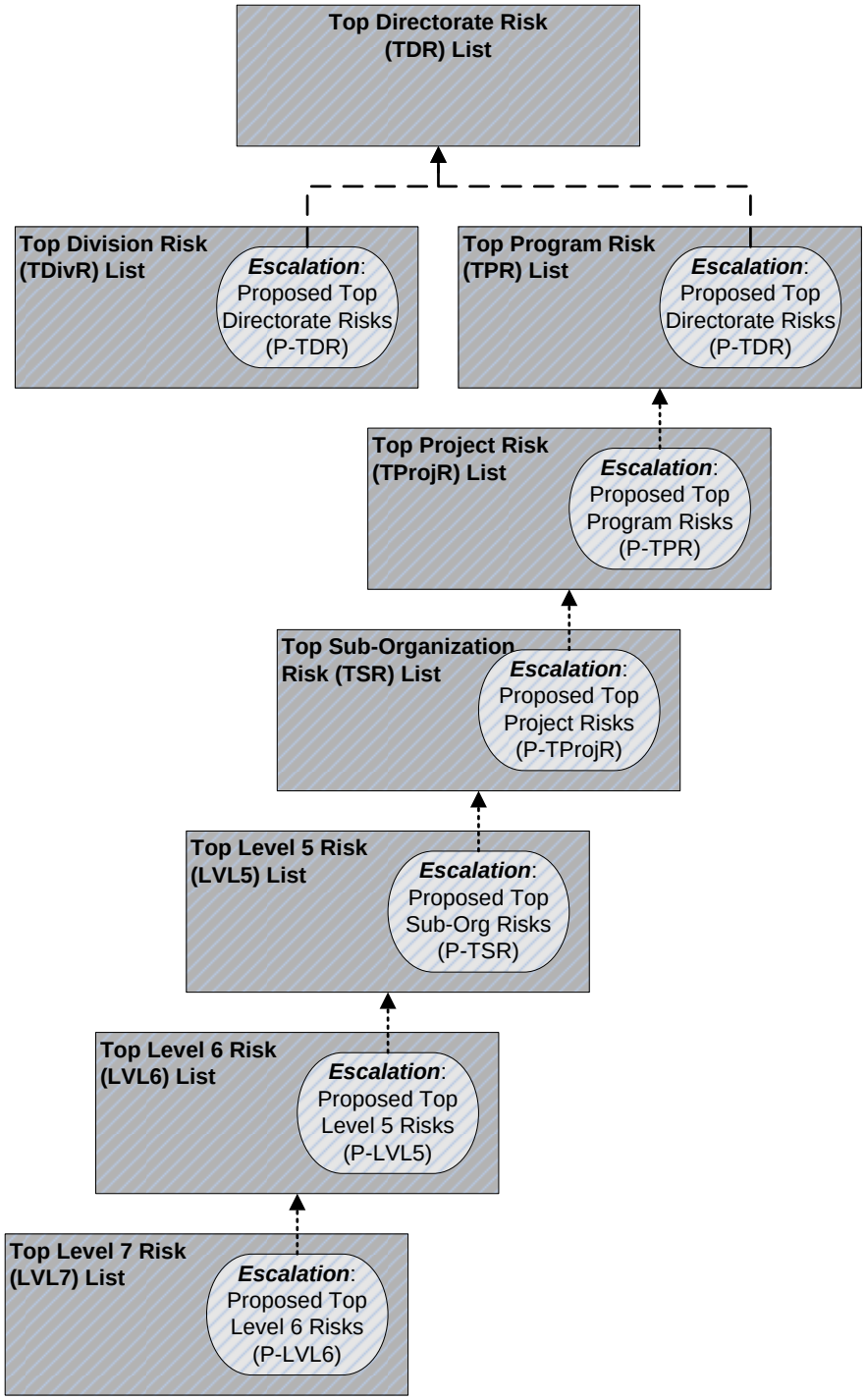


Figure 5. Top Risk Identification and Escalation Flow

5.2.3.4 ESMD Top Risk Review Out-of-Council Process

To ensure that the ESMD AA is kept aware of the Directorate's Top Risk List / risk posture, ESMD has developed a process to make critical changes to the Directorate Top Risk List between QPMRs.

The ESMD Management Decision Forum (MDF) is used to adjudicate proposed changes to the Directorate Top Risk List. The MDF is chartered to resolve single context Level 1 issues that are too narrowly focused for the Directorate Program Management Council (DPMC). The MDF provides a forum tailored for these programmatic issues, convenes when necessary, and adjudicates in an advise/decision format.

Significant changes that may be addressed by the MDF include:

- ***De-escalation*** from TDR status due to significant improvement in risk
- ***Escalation*** requested to TDR for time critical risks that are getting worse
- ***Acceptance or Closure*** of TDRs

When a significant change occurs that must be addressed by the MDF, the RMO responsible for the risk provides a description of the risk and the rationale for its need for immediate review and action. The ESMD RMO requests that the MDF Executive Secretary schedule an MDF meeting to review and discuss the risk.

If the risk change is approved, the ESMD RMO communicates the approval to the responsible RMO, who works with the Risk Owner to implement the change in the ESMD risk management tool.

5.2.3.5 Standard Reports for Top Risk Reporting

ESMD Division, Office, and Program Top Risks are reviewed by the ESMD RMWG, monthly. Each ESMD Division, Office, and Program discusses their top risks and associated mitigation plans. These plans should include details on what will be done to mitigate the risk, when it should be accomplished, who is responsible, and the associated cost and schedule impacts. The RMWG will evaluate, integrate, and coordinate the mitigation plans, and track their implementation. To maintain consistency at the RMWG, each reporting organization will provide the following data for each Top Risk:

- Risk summary report with the key risk details, including risk ID, title, owner, risk statement, context, probability score, and score by impact category.
- Detailed mitigation plan and mitigation step data including plan and step owners and descriptions.

5.3 Risk Transfer

Ownership of a risk may be transferred from one NASA organization to another. The current risk owner will coordinate with the "target" organization's RMO. Transfers must be concurred on by the governing Risk Review Board. If an agreement on transferring the risk cannot be accomplished, the issue is brought forward to the next highest Risk Review Board that is part of the current organization and target organization chains of command. Figure 6 shows ESMD's process for transferring risks.

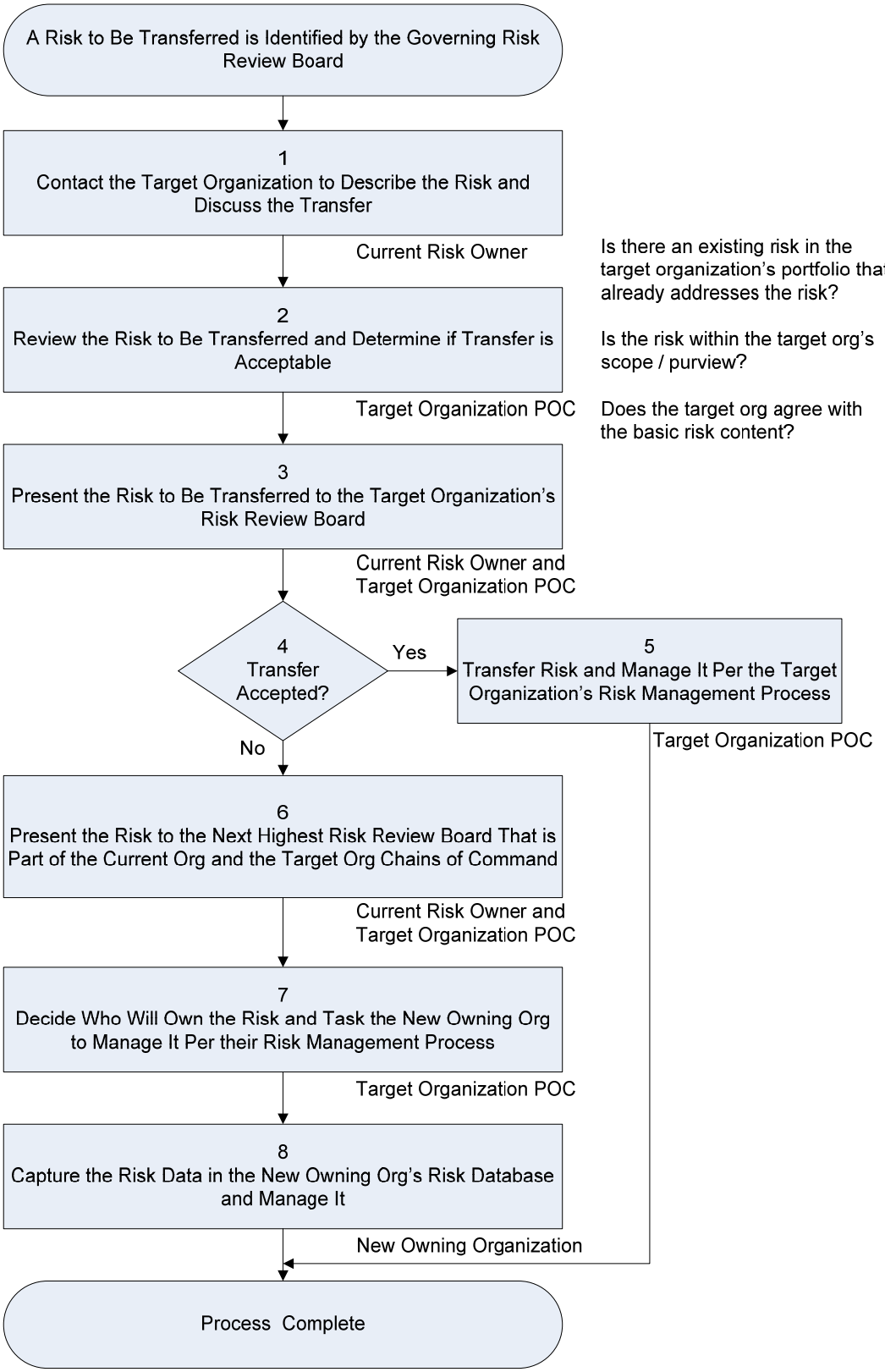


Figure 6. Risk Transfer Process

5.4 Risk Management Training

ESMD risk management training shall include, as a minimum, training on CRM, performing organization risk reporting processes, and the ESMD risk management tool. The ESMD RMO coordinates and provides CRM and risk reporting training to the Directorate, and provides ESMD risk management tool training to level 1 and level 2 users. Performing organizations are responsible for implementing desired training beyond this level of expertise.

5.5 Risk Management Process and Data Reviews

Programs shall conduct internal audits of their program and supporting project risk management processes and data. These audits will:

- Assess and verify the completeness and accuracy of the risk data
- Assess the effectiveness of the internal risk management activities
- Assess compliance with approved risk management plans and processes

In addition to these internal reviews, the ESMD RMO shall periodically review risk management activities conducted by ESMD performing organization.

These reviews shall include:

- Review of all moderate and high risks including risk level trends and accomplishment of the mitigation plan (if applicable).
- Review of the risk management processes and associated data records for adequacy and compliance with Agency / Directorate requirements and
- A review of process metrics selected to manage risks.

5.6 Risk Management Assurance Process Map (APM)

The Risk Management (RM) Assurance Process Map (APM) is a graphical depiction of the key NASA organizations that play a role in ESMD risk management. The risk management APM depicts the following information:

- Program, project, and organization leads and their Risk Management Officers (RMOs),
- Risk review forums,
- Key risk-related documents,
- Chain of command relationships,
- Information flow,

- Risk tool used by the organization.

The risk management APM has an associated spreadsheet that captures:

- Contact information for all individuals shown on the risk management APM,
- Risk Review Board supporting information, and
- Risk Management Plan (RMP) supporting information.

The current version of the APM is available in the Risk & Knowledge Management Project in Windchill.

6 Resource and Schedule Allocation for Risk Management Activities

Based on the corporate management model described in this document, ESMD performing organizations will be responsible for allocating sufficient resources to their own teams, as well as their sub-level and contractual work elements to perform risk management.

ESMD provides all performing organizations with access to the ESMD risk management tool, without funding expenditures required from those organizations. Some training for CRM is provided through SATERN and the ESMD CIO. Beyond these ESMD-provided resources, performing organizations are responsible for funding their risk management tools and CRM activities.

7 Methodology Associated with ESMD Program Re-Scope

In the event of a major program re-scope or cancellation, all program organizations shall create an archive of all risk management data and fully document the current / final risk status and provide it to the ESMD RMO within 60 days of the re-scope / cancellation. Risk reports and supporting risk management documentation shall be created by these organizations for traceability of content and resources and to provide risk management lessons learned for future exploration efforts.

The program organization shall identify risks that will no longer be worked due to the re-scope / cancellation, but will continue to affect other organizations. The program organization shall facilitate the transfer of those risks to suitable Risk Owners in the affected organizations.

The risk data shall be backed up to a format suitable for long term storage and to a format suitable for access by similar continuing NASA programs.

Appendix A. Acronyms and Definitions

A common risk vocabulary is required to maintain consistency throughout ESMD Divisions, Programs, and Projects.

Table 3. Acronyms and Definitions

Word	Definition
AAR	After Action Review. A professional discussion of an event, focused on performance standards, that enables participants to discover for themselves what happened, why it happened, and how to sustain strengths and improve on weaknesses.
Acceptable Risk	Risk reduction action is not being taken to eliminate or reduce this risk. • Controls and acceptance rationale have been defined to justify continuation without further preventive or mitigation action. • Periodic reviews of accepted risks will be conducted to ensure that acceptance rationale is still appropriate and complete and to ensure that controls are still in place. • Accepted risks could potentially be re–opened or closed based on progress reviews.
Active Risk Manager (ARM)	ARM is the web-based software application tool created and licensed by Strategic Thought, LLC, and used by all ESMD organizational elements to report data associated with their risk management activities.
Burn-Down Chart	Use the term "Waterfall Chart" (see definition, below) instead of "Burn-Down chart"
Business Area	In the context of the ESMD risk management tool, this represents a hierarchal breakdown of project definition typically based upon work, process, and organizational elements.
Candidate Risk	A potential risk that has been identified and is pending adjudication by the governing risk review body.
CIO	Chief Information Officer
Closed Risk	A validated risk that is no longer a risk to the program. For example, a risk related to a given procurement may, at the discretion of the Risk Review Board, be closed after the procurement is complete.

Word	Definition
Common Risk	Risks which are present on multiple related programs. Common risks warrant special attention as they may indicate important trends or may merit integrated risk control measures which could be better dealt with if the risk is transferred or integrated mitigation plans are developed rather than having each program and project deal with them on an individual basis.
Community of Practice	A group of professionals informally bound to one another through exposure to a common class of problems, common pursuit of solutions, and thereby themselves embodying a store of knowledge.
Consequence	An assessment of the credible, potential impact / result(s) of a risk. It is the part of the risk statement that focuses on the intermediate and long-term impact of a risk and describes the key, negative outcome(s) of the current conditions.
Continuous Cost-Risk Management (CCRM)	A multi-step approach to cost estimating and project cost management that seeks to integrate the various project management activities that involve cost and cost risk. CCRM encompasses the following: cost-effectiveness trades (where CAIV is a subset), detailed project definitions (CADRe development) and probabilistic, risk-based Life Cycle Cost Estimates (project cost S-curve) documented in the CADRe; disciplined cost and schedule rebaselining; Earned Value Management for continuous management and reporting of risky WBS elements; periodic updates of the CADRe for continual reassessment of project cost performance; and end-of-project data collection and storage in the One NASA Cost Engineering (ONCE) database for cost analysis improvement. CCRM emphasizes that the high-risk elements in the WBS most likely to cause adverse cost and schedule impacts are the common focus of these activities.
Continuous Risk Management (CRM)	The process that identifies risks; analyzes their impact and prioritizes them; develops and carries out plans for risk mitigation or acceptance; tracks risk and the implementation of plans; supports informed, timely, and effective decisions to control risks and mitigation plans; and assures that risk information is communicated and documented.

Word	Definition
Cost Threat	Money that is required to mitigate a risk that is not in the current project's budget. The dollars needed become liens against the Program Manager's reserves and are tracked until a decision is made to fund the mitigation activity or accept the risk.
ESMD	Exploration System Mission Directorate
Earned Value Management (EVM)	A tool for measuring and assessing project performance through the integration of technical scope with schedule and cost objectives during the execution of the project. EVM provides quantification of technical progress, enabling management to gain insight to project status and project completion costs and schedules. Two essential characteristics of successful EVM are EVM system data integrity and carefully targeted monthly EVM data analyses (i.e., risky WBS elements).
Effect	The effect(s) which may occur as a result of a risk impacting. For example, if the risk is "Bridge Collapse", effects of this (as well as the direct impact of the collapse) could be "Road Closures", "Train Delays", etc.
Fallback Plan	A fallback plan is a type of Response designed to provide risk reduction or limitation when the primary mitigating actions have failed (i.e., a risk is realized / becomes a problem). For example, if a mitigating plan was designed to avoid stress fractures, but this had failed and stress fractures occurred, a Fallback response might be "Fit strengthening brackets".
Fault Tree Analysis (FTA)	"..an analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the context of its environment and operation to find all realistic ways in which the undesired event (top event) can occur. The fault tree itself is a graphic model of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event." Ref: Fault Tree Handbook with Aerospace Applications. NASA, August, 2002
ICE	Integrated Collaborative Environment

Word	Definition
Impact	An impact is the effect of a risk on a particular activity within a business folder. The Impact is the (positive or negative) effect that a risk has on a business activity, and a given risk may have multiple impacts. For example, the risk might be "Failure of subcontractor". This might have multiple impacts on different activities within a business folder, each with a different cost and time impact and probability.
Impact Category	When a risk impacts, its effects may be felt in various ways - cost, time, etc. These are known as the Impact Categories. The impact categories used by ESMD are Safety, Performance, Cost and Schedule.
Impact Group	The group, department or organization which would be impacted by a risk. You can configure the possible values of Impact Group to reflect the structure of your business.
Integrated Baseline Review (IBR)	An IBR is a formal project-level review that includes total project (contracted as well as in-house NASA) efforts. It is conducted jointly with personnel responsible for the efforts. Specifically, an IBR verifies that the technical content of the performance measurement baseline is consistent with the contract scope, work breakdown structure, and actual budget and schedule; ensures that effort personnel have identified all risks and are aware of their responsibilities for their management; ensures that there is a logical sequence of effort planned consistent with the contract schedule; ensures the disciplined implementation of all project Earned Value Management Systems (EVMS); establishes a forum through which the Program Manager and the technical staff gain a sense of ownership of the cost/schedule management process; and establishes the baseline for the life of the contract.
Integrated Master Schedule	An IMS includes a baseline master schedule and derivative schedules which provide the framework for time phasing and coordinating all project efforts into a master plan to ensure that objectives are accomplished within program or project commitments.
Integrated Risk	Risks which exist uniquely due to potential complications which arise from the way various performing organizations are integrated.
Interface Risk	Risks that exist at the interfaces of performing organizations.

Word	Definition
IPT	Integrated Product Team. IPTs are composed of representatives from all appropriate functional disciplines working together with a team leader to identify and resolve issues, and to make sound and timely decisions for a specific topic, process, or product.
Issue	An undesirable event that has occurred or will occur and its occurrence cannot be stopped / directly controlled.
Knowledge Management (KM)	Capturing, organizing, and storing knowledge and experiences of individual workers and groups within an organization and making this information available to others in the organization.
Lesson Learned	Lesson Learned — The significant knowledge or understanding gained through past or current Programs that is documented and collected to benefit current and future Programs.
Level 0	NASA Agency
Level I	NASA Headquarters and ESMD
Level II	ESMD Programs (e.g., Constellation Program, Human Research Program)
Level III	ESMD Projects (e.g., Orion, ARES)
Lien	Any claim or charge against resources that must be paid.
Likelihood	The probability that a risk will occur.
Margin	The allowances carried in budget, projected schedules, and technical performance parameters (e.g., weight, power, or memory) to account for uncertainties and risks. Margin allocations are baselined in the formulation process, based on assessments of risks, and are typically consumed as the program proceeds through the life cycle.
MDF	Management Decision Forum. The ESMD MDF resolves single context Level 1 issues that are too narrowly focused for the Directorate Program Management Council (DPMC) . The MDF provides a forum tailored for these programmatic issues, convenes when necessary, and adjudicates in an advise/decision format.

Word	Definition
Mitigation	Taking action to reduce the severity of a risk, either by reducing the probability of it occurring, or by reducing the level of impact if it does occur, or both.
Mitigation Plan	A plan which you put in place to mitigate a risk impact. The plan consists of a number of Responses, and can act to mitigate more than one risk impact. For example, a mitigating plan which involves staff training or safety initiatives could act to mitigate a number of risks within your organization.
NPD	NASA Policy Directive. NPDs are policy statements that describe what is required by NASA management to achieve NASA's vision, mission, and external mandates and who is responsible for carrying out those requirements.
NPR	NASA Procedural Requirements. NPRs provide Agency requirements to implement NASA policy as delineated in an associated NPD.
Open Risk	A risk that has not been closed or accepted.
Opportunity	A Risk which would have a positive effect on your project or organization; for example a supplier making an early delivery.
OSMA	Office of Safety and Mission Assurance
Pause and Learn	A concept for formalizing learning from ESMD projects/programs that is modeled after the Army After Action Review (AAR) system. While the AAR was developed to learn from training exercises, the 25 years of experience, theoretical foundations and practical tools make it a valuable source of lessons for ESMD.
Performing Organizations	NASA ESMD programs, projects, and all levels of sub-project organizations.
Probabilistic Risk Assessment	A systematic, logical, and comprehensive tool to assess risk (likelihood of unwanted consequences) for the purpose of 1) characterizing and improving system performance and mission success, 2) increasing safety in design, operation and upgrade, and 3) saving money in design, manufacturing or assembly, and operation.
Probability	The likelihood of a risk impact occurring.

Word	Definition
Problem	An adverse situation that exists now. A problem is a risk that has already occurred. Reactive management is necessary to deal with a problem. Risk management is concerned with avoiding or reducing the adverse effects of future events.
R&T	Research and Technology
Research	Research is the investigation of an identified risk until there is enough information to know if the risk ownership is still assigned properly, and what to do about the risk (e.g., accept the risk, watch the risk, or mitigate the risk).
Retired Risk	See "closed risk"
Risk	The combination of (1) the probability that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough; and (2) the consequences, impact, or severity of the undesired event were it to occur.
Risk Acceptance (Accepted Risk)	The determination that the consequences of an identified risk, should they occur, are acceptable without further mitigation. No further resources are expended in managing this risk.
Risk Analysis	The process of examining risks in detail to determine the extent of the risks, how they relate to each other, and which ones are the most important. This process covers an evaluation of all identified risks to estimate the likelihood of occurrence, consequence of occurrence, timeframe when mitigation actions are needed. Analyzing risk has three basic activities: • Evaluating attributes of risk • Classifying the risks • Prioritizing (ranking) risks
Risk Assessment	An evaluation of the likelihood and consequence of a risk occurring.
Risk-Based Acquisition Management (R-BAM)	R-BAM is a NASA Headquarters initiative aimed at highlighting risk as a core acquisition concern during the acquisition lifecycle phases. R-BAM integrates the analysis of programmatic risk with the formulation of acquisition strategies by overlaying the CRM Process onto the acquisition process.

Word	Definition
Risk Category	A Risk Breakdown Structure (RBS) used to group risks to support gap analysis and identification of integration opportunities.
Risk Escalation	The process of raising risk visibility by reporting the risk to a higher level in the organization. This is done either to raise the awareness and visibility of a risk, calling attention to adverse changes in consequence, likelihood of occurrence or timeframe, or to request resources needed to handle the risk at a lower level. Escalated risks are captured on the organizations Top Risk List. Top Risk Lists are defined for the following levels: • Top Directorate Risks (TDRs) • Top Division Risks (TDivR) • Top Program Risks (TPRs) • Top Project Risks (TProjR) • Top Sub-Organization Risks (TSR) • Top Level 5 Risks (LVL5R) • Top Level 6 Risks (LVL6R) • Top Level 7 Risks (LVL7R)
Risk List	A complete set of all active, validated risks.
Risk Management (RM)	An organized, systematic decision making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving program goals.
Risk Management Officer (RMO)	The RMO is the individual responsible for implementing and maintaining an organizational element's risk management plan and Continuous Risk Management process and for advising senior managers on significant risk issues (including subordinate level risks), risk management resource investment decisions, and reporting required risk details to the next higher organizational level.

Word	Definition
Risk Management Plan (RMP)	A Risk Management Plan (RMP) is the document that formally defines and establishes an organization's approach to conducting risk management including the organization's risk management strategy; organizational structure, relationships, and responsibilities for managing risk; guidelines and policies regarding processes, metrics and tools for executing and communicating an integrated risk management methodology; and the risk management resource investments required.
Risk Management Working Group	ESMD group that provides risk management oversight to ESMD divisions, offices, and performing organizations/
Risk Owner	The individual to whom the risk is assigned for purposes of responsibility and accountability.
Risk Score	A numeric representation of the overall risk severity, taking into account both the risk impact and the probability of that impact occurring.
Risk Statement	A single descriptive statement that defines the condition of the risk and its consequence. This includes: • A statement of the current conditions that may lead to an undesired consequence • A description of the undesired consequence
Risk Transfer	The reallocation process that identifies a person / organization that can more appropriately own / mitigate the risk using the approved resources.
Risk Watch List	A list of validated risks for which no immediate action required. The trends and behavior of risk indicators for these risks are tracked, surveyed, or watched over time.
SE&I	Systems Engineering and Integration
Summary Risk	A risk which has been created to represent a grouping or aggregation of related, lower level Detail Risks.
Threat	A Risk which would have a negative effect on your project or organization; for example a supplier making a late delivery.
Top Directorate Risks (TDRs)	Risks that are deemed by the ESMD AA to have the greatest significance/impact to ESMD.
Top Division Risks (TDivR)	Risks that are deemed by the ESMD Division Leads to have the greatest significance/impact to their Division.

Word	Definition
Top-N Risks	The vital high and moderate risks that must be mitigated or frequently reviewed based on resource constraints. The number of Top-N risks will vary over time and from one organizational element to another.
Top Program Risks (TPRs)	Risks that are deemed by the Program Manager to have the greatest significance/impact to the program. TPRs significantly affect program safety, technical performance, cost or schedule goals.
Top Project Risks (TProjR)	Risks that are deemed by the Project Manager to have the greatest significance/impact to the project. TProjRs significantly affect project Safety, Technical Performance, Cost or Schedule goals.
Top Risk List	A set of risks that have been escalated from one organizational level to the next higher level.
Top Sub-Organization Risks (TSR)	Risks that are deemed by the Sub-Organization Manager to have the greatest significance/impact to the sub-organization. TSRs significantly affect system safety, technical performance, cost or schedule goals.
TPM	Technical Performance Measure. Technical Performance Measures are part of the Technical Performance Measurement analysis and control technique that is used to: • Project the probable performance of a selected technical parameter over a period of time, • Record the actual performance observed of the selected parameter, and • Through comparison of actual vs. projected performance, assist the manager in decision-making.
Validated Risk	A candidate risk, which has been determined to be a legitimate, open risk by the Risk Review Board. Synonymous with “Approved Risk”.
Watch	The monitoring of an identified risk and its attributes for early warning of critical changes in consequences, likelihood, timeframe, or other aspects.

Word	Definition
Waterfall Chart	During risk mitigation you will typically identify a sequence of responses, and a target risk level which you want to achieve following completion of these responses. However, you may also wish to set a target risk level to be achieved on completion of each individual response, allowing you to track progress towards your goal. The Waterfall Chart provides a graphical view of progress against this plan. The vertical axis is the overall risk score, and the horizontal axis is time. The chart shows how the overall risk score changes (or is intended to change) over time.
WBS	Work Breakdown Structure

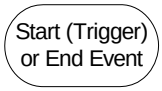
Appendix B. Tailorable Risk Management Process

B.1. Flowchart

This flowchart is intended to convey a generic process for ESMD performing organizations to execute key risk management activities. A narrative discussion of each process step is also provided. ESMD performing organizations may tailor this process to fit the nuances and structure of their particular organization. The flowcharts depict the following risk management activities, which are executed on a recurring basis:

- Identify and Document a Risk
- Plan & Execute a Risk Review Board Meeting
- Conduct Risk Audits

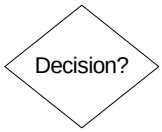
LEGEND



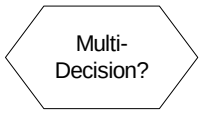
Represents the beginning or end of a process

Actionee

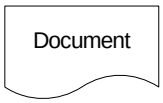
Action to be taken by the actionee (always a verb phrase)



Directs the process flow in one of two possible directions based on a decision



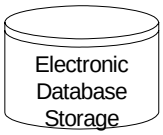
Directs the process flow in one of many possible directions based on a decision



When shown entering a process step from the left, this is a document input to the process.

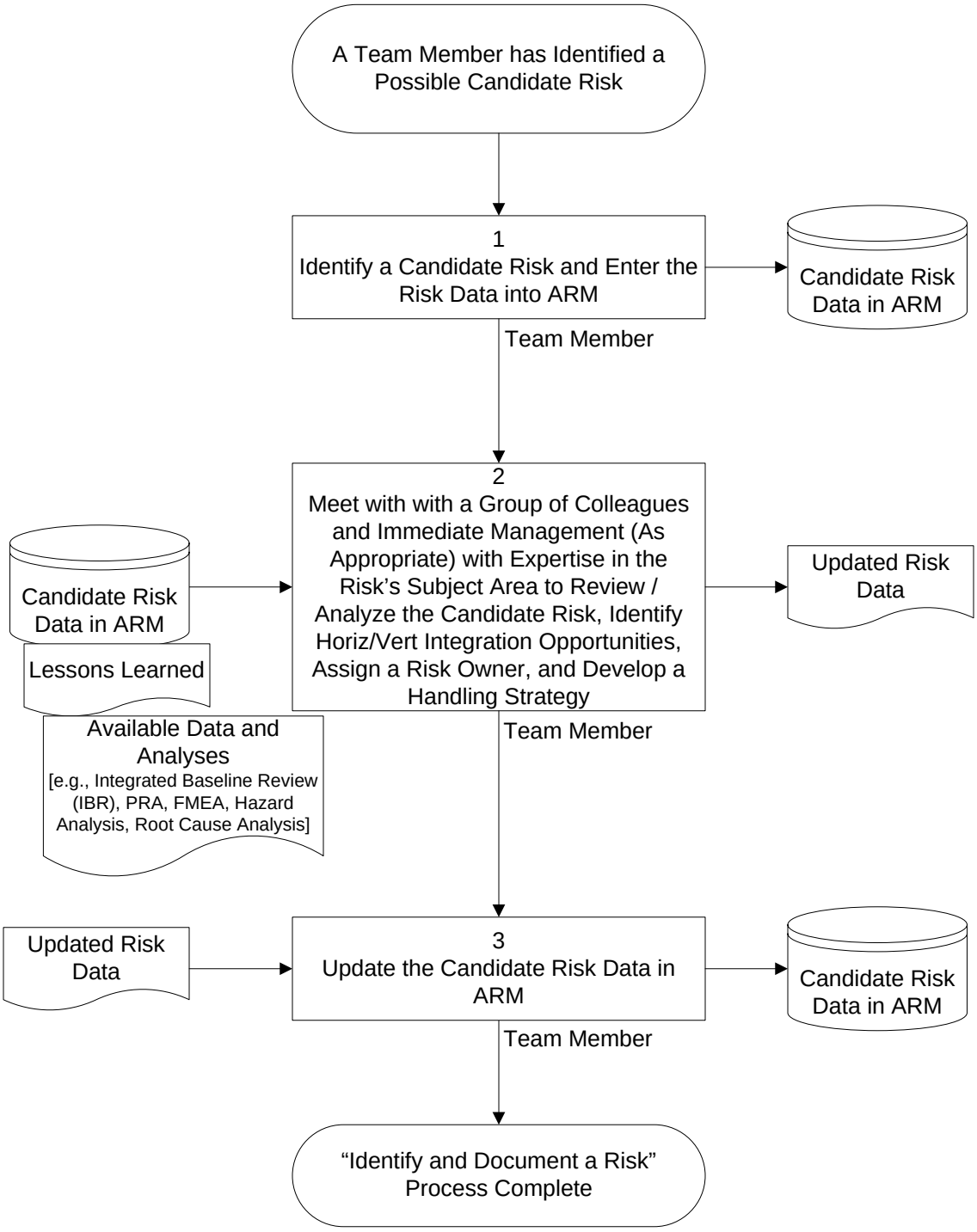
When shown exiting a process step from the right, this is a document that is an output.

Represents continuation of the flowchart on another page. The destination page has a like-numbered "receiving" off-page connector.

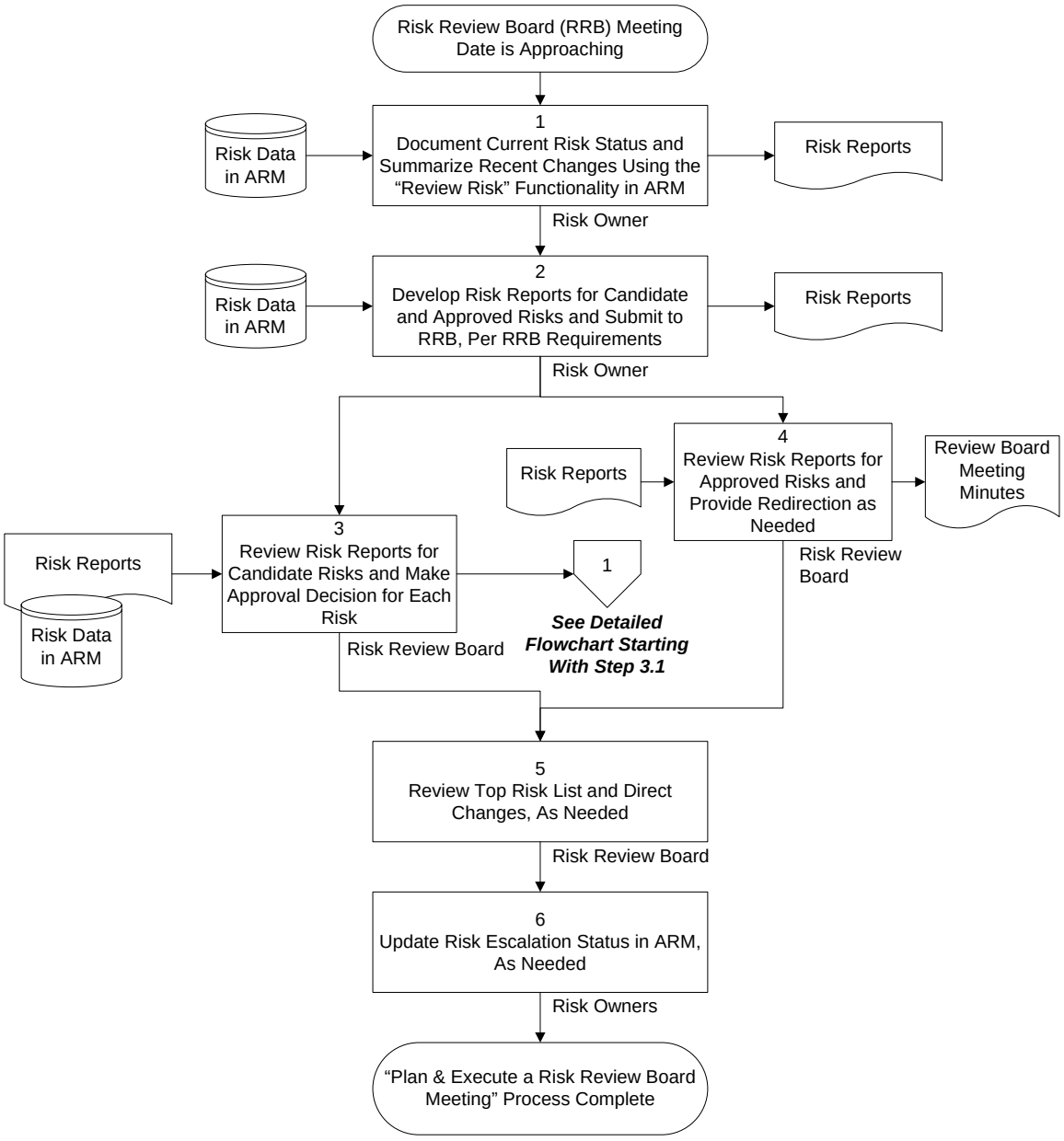


Represents an electronic database

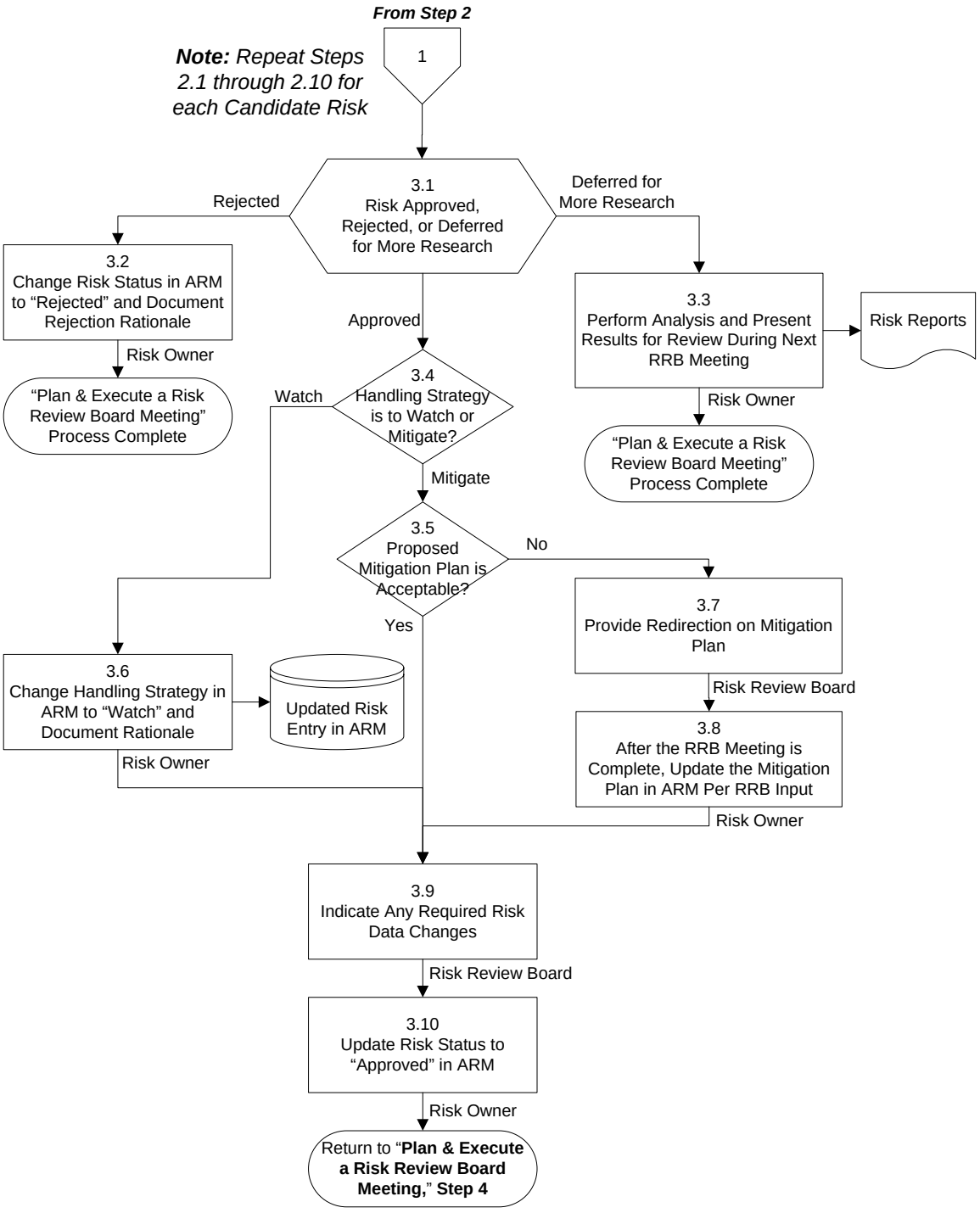
Tailorable Risk Management Process
(Identify and Document a Risk)



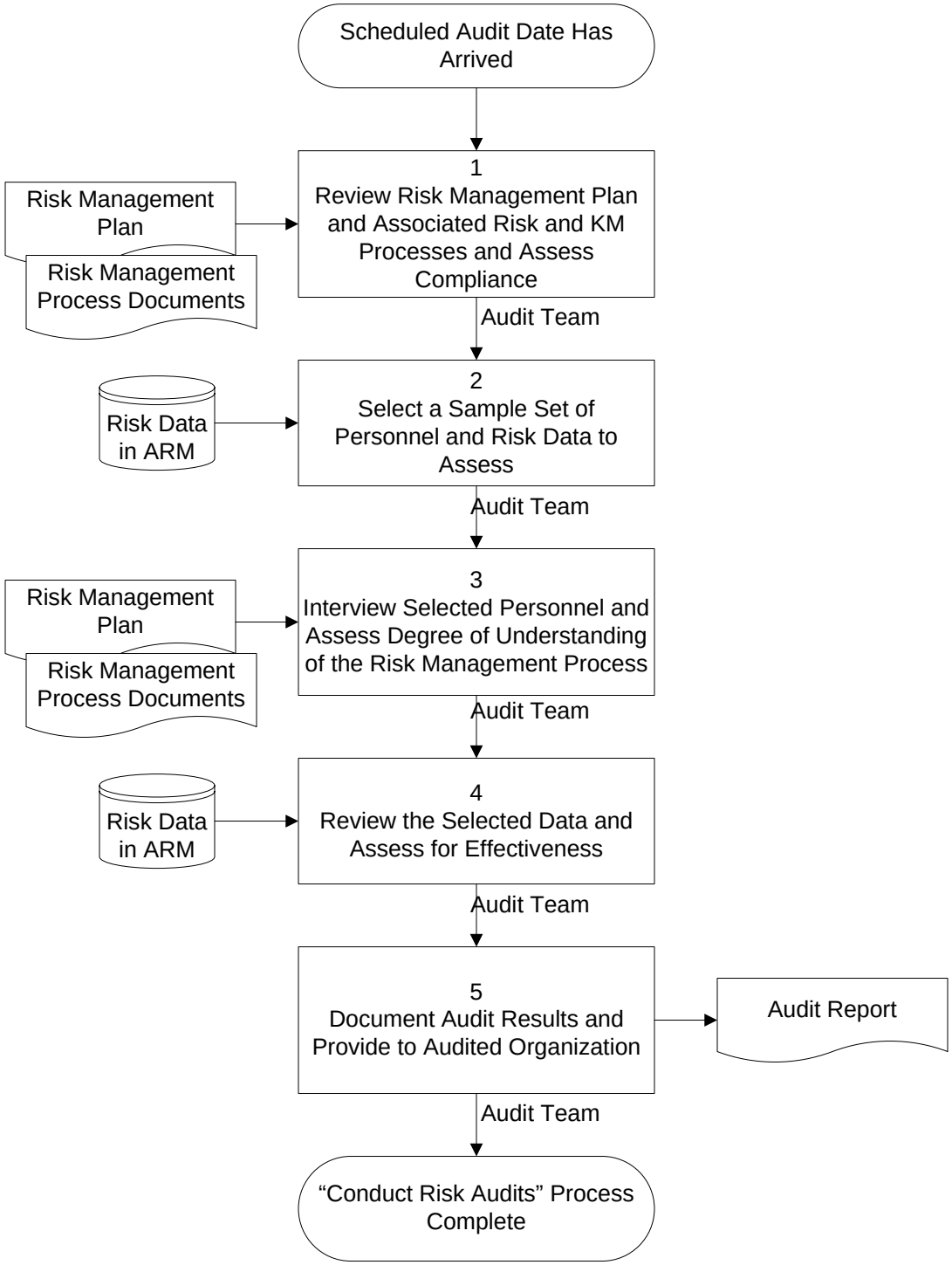
Tailorable Risk Management Process
(Plan & Execute a Risk Review Board Meeting)



Tailorable Risk Management Process
(Review Candidate Risks)



Tailorable Risk Management Process
(Conduct Risk Audits)



B.2. Procedure Qualification – All Referenced to Notional Flowchart

Table 4. "Identify and Document a Risk" Procedure

Ref #	Actionee	Activity Description
1	Team Member	Identify a candidate risk based on all available data and analyses. Team members at all levels are encouraged to identify candidate risks. This step typically includes a review and assessment of available data, and a preliminary scoring of risk likelihood and impact on the standard 5x5 probability–impact diagram. The Team Member populates the data fields in ARM.
2	Team Member	The Team Member meets with a group of colleagues and immediate management (as appropriate) with expertise in the risk's subject area to review / analyze the candidate risk, identify horizontal / vertical integration opportunities, assign a risk owner, and develop a handling strategy. This group ensures that: • The risk statement is focused on the risk's root cause • The context provides as much relevant info as possible to allow readers to understand the risk • The risk score is appropriate and the scoring description / rationale is sufficient • The handling strategy and associated plan details are appropriate and complete. Note that more extensive mitigation planning detail may be populated after the Risk Review Board has approved the risk. • All ARM data fields are populated completely and correctly
3	Team Member	Update the Candidate Risk in ARM. Note that this may have been completed "real-time" during Step 2.

Table 5. "Plan & Execute a Risk Review Board Meeting" Procedure

Ref #	Actionee	Activity Description
1	Risk Owner	Document current risk status and summarize recent changes using the "Review Risk" functionality in ARM. On the "Risk" tab, select "File--Review Risk" and enter the information in the text block.
2	Risk Owner	Develop risk reports for candidate and approved risks and submit to the RRB. The required risk report format(s) are defined by the RRB. The reports typically specify the Risk ID, status, risk statement, context, score, mitigation plan and steps, the current implementation status / progress, and any planned adjustments to allow the mitigation to be completed on schedule.
3	Risk Review Board	Review the Risk Reports and make an approval decision for each candidate risk. Review similar risks, horizontally and vertically, to assess the uniqueness of the risk and consider whether the risk is already addressed by an existing similar risk to capture the intent. Determine if appropriate parent/child relationships to other risks have been identified.
3.1	Risk Review Board	If the Review Board rejected the risk, go to Step 2.2. If they approved the risk, go to Step 2.4. If they deferred the risk for more research, go to Step 2.3.
3.2	Risk Review Board	Change Risk Status in ARM to "Rejected" and Document Rejection Rationale. When the Risk Status is changed in ARM, a window appears to capture the rationale for the rejection.
3.3	Risk Review Board	Perform analysis as directed by the Review Board, and present results for review during next RRB meeting.
3.4	Risk Review Board	If the Risk Review Board elects to mitigate the Risk, go to Step 2.5. If they elect to Watch the risk, go to Step 2.6.
3.5	Risk Review Board	If the proposed mitigation plan is acceptable, go to Step 2.9. If not, go to Step 2.7.

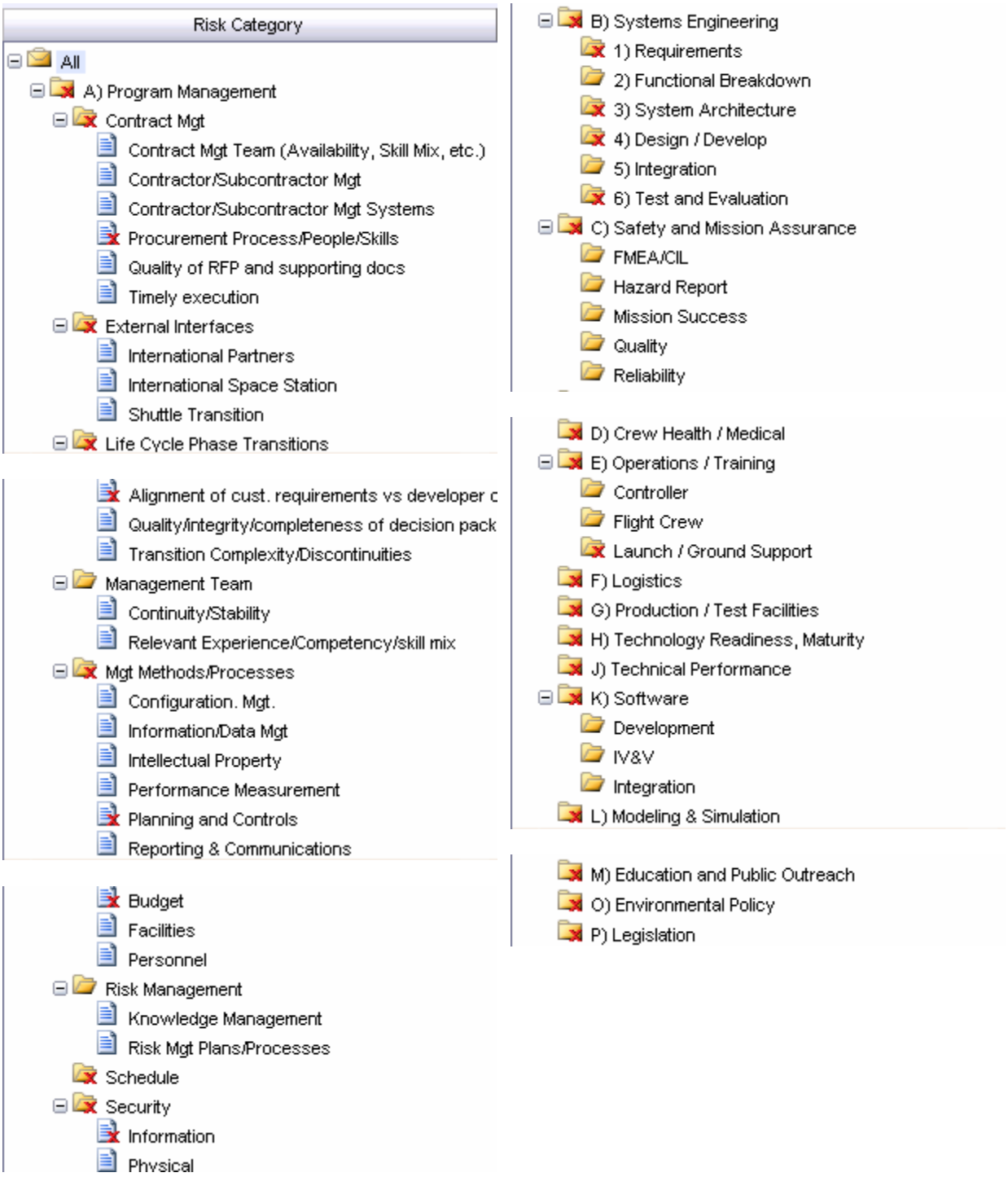
Ref #	Actionee	Activity Description
3.6	Risk Review Board	Change handling strategy in ARM to "watch" and document rationale. On the "Risk" tab, select "File--Review Risk" and enter the information in the text block.
3.7	Risk Review Board	Provide redirection on Mitigation Plan. This review may drive a reallocation of resources to mitigate the risk, a change in approach to addressing the risk, or any other programmatic or technical changes deemed necessary by the Risk Review Board.
3.8	Risk Owner	After the RRB meeting is complete, update the mitigation plan in ARM per RRB input. Use the "Review Risk" functionality in ARM to indicate the changes and note that the changes were directed by the RRB meeting on the specified date.
3.9	Risk Review Board	Indicate any required risk data changes.
3.10	Risk Owner	Update Risk Status to "Approved" in ARM. When prompted to enter the reason for the status change, indicate that the approval was a result of the RRB meeting on the specified date.
4	Risk Review Board	Review the Risk Reports and provide redirection, as needed. This review may drive a reallocation of resources to mitigate the risk, a change in approach to addressing the risk, or any other programmatic or technical changes deemed necessary by the RRB.
5	Risk Review Board	Review the Top Risk List and direct changes, as needed. To remove a risk from the Top Risk List, approval must be provided by the highest level organization to which the risk is currently escalated.
6	Risk Owners	Update Risk Escalation Status in ARM, As Needed

Table 6. "Conduct Risk Audits" Procedure

Ref #	Actionee	Activity Description
1	Audit Team	Review the governing Risk Management Plan and associated risk and KM processes, and assess compliance of the organization with these documents.

2	Audit Team	Select a sample set of personnel and risk data to assess. This sample may be selected based on one or more ARM Risk Categories or other areas of interest to the Audit Team.
3	Audit Team	Interview selected personnel and assess degree of understanding of the risk management process. This may be driven by a questionnaire or face-to-face interviews.
4	Audit Team	Review the selected data and assess for effectiveness. This may include an assessment of: • Risk staleness (how long since the most recent update) • Timeliness of mitigation activities • Horizontal / vertical integration with other risks • Maturity of key data (e.g., risk statement, context, mitigation plan, mitigation steps)
5	Audit Team	Document audit results and provide to audited organization.

Appendix C. Risk Breakdown Structure



Appendix D. Pause and Learn (PaL) Process

Lessons from 25 Years of Army After Action Reviews

An AAR is "…a professional discussion of an event, focused on performance standards, that enables **soldiers to discover for themselves** what happened, why it happened, and how to sustain strengths and improve on weaknesses"

A Leader's Guide to After-Action Reviews, 1993 p 1.

The Army learned from years of experience with AAR that much of the value in the AAR exercise comes from several key design parameters. First, the focus of the AAR is specific to 1) What happened (events), 2) Why did it happen (cause), 3) How can we improve (action). Second, the AAR is a participant discussion. AAR's replaced traditional top-down lecture critiques. What was valuable about AAR's was the voice of the team members themselves offering up their views and ideas. Third, the AAR is close to the action in time, space and personnel. Fourth, the AAR does not function as a career review. It is a non-attribution team review of what happened. The team members participate because they feel free to speak.

Finally, the AAR is part of the overall process whether it be a training exercise, a simulation or a field operation. The action is not complete until the AAR has been conducted. The AAR is a fundamental part of the process built into the project. The AAR method replaced sterile lecture type critiques delivered by judges often some time after the end of the events. The participants were not energized and sometimes defensive about these reviews. While many teams and groups at NASA meet and discuss events after they happen, NASA has no formal process to guide the meaningful collection of learnings in the way AAR's function.

Based on the AAR experience, a PaL in ESMD is designed to specifically focus on:
1. What happened – events
2. Why did it happen – cause
3. How can we improve – action

A PAL session in ESMD should be:

1. A non-attribution participant discussion
2. The voice of the team members offering views and ideas in a safe space
3. Close to the action in time, space, and personnel
4. Conducted immediately after an event, milestone, or review step
5. A fundamental part of every project, built into the project process and schedule

Implementing PaL in the Exploration Systems Mission Directorate

The idea behind the PaL process is to create a learning event at selected critical events in the life of a project. End-of-project reflections are good but are too infrequent for the organization to learn in a timely manner. Also, much intermediate learning is lost between concept and launch. PaL meetings are intended to be integrated into the project life cycle at key points as a natural part of the process. PaL meetings are structured and facilitated by specialists who are not project members for two reasons: first, to intrude as little as possible into the time of the project team; second, to be objective and facilitate open communication.

1. Scheduling – A series of PaL meetings should be scheduled at key project events or milestones as part of the initial project planning and scheduling process. Though ad hoc PaL meetings can be effective, those that are planned in advance seem to be the most productive. Some administrative effort is required for planning, notification, and technical preparation.

2. Pre-meeting interviews – Prior to the PaL, the facilitator will meet briefly with project management and team members to make introductions, gather preliminary information, and establish the objectives for the PaL meeting. Initially, the objectives may be driven primarily by the project lead, but could be defined by any participant. Though insights often arise from discussions outside the scope of the objectives, the objectives provide a framework for discussion.

3. The PaL meeting – The substantive part of the PaL process is the meeting itself, where participants can develop networks and relationships, share information, communicate openly, and identify and magnify key learning opportunities. PaL meetings often explore:

- Tasks and goals that were to be accomplished
- What tasks and goals were actually accomplished
- If it were done over again - what should be kept the same, what should be improved and how

Conducting a PaL: Roles and Responsibilities

One of the key designs of the PaL is minimal intrusion into project work time. To maintain this, the roles of the participants and the supporting staff who conducts the PaL are clearly laid out here. The facilitator does not need to be from outside NASA but should be objective relative to the team holding the PaL. Outside facilitators seem to work well if they have sufficient technical expertise to follow the discussions. It is important that everyone understand their role and responsibility toward making PaLs successful and useful.

PaL Project Attendees Need to:

Make the time to hold the event when scheduled.
You will be asked to re-state portions of an activity in your own words
Explore alternative courses of action
Handle discovery of errors positively

Follow-up on needed actions that you have identified *for yourself*
The PaL is not intended as an action-assignment forum
The team may agree on an action or improvement for themselves
Likewise, you may have actions you identify for your own improvement

PaL Supporting Staff Need to:

Gather attendees: some projects already hold debrief or talk down sessions
Moderator reviews events
Encourage participation
Summarize key events
Have junior leaders re-state portions of their part of an activity
Do not lecture or critique
Ask why certain actions were taken
Ask how they reacted to situations
Ask when actions were initiated
Exchange "war stories"
Relate events to subsequent result
Explore alternative courses of action
Handle discovery of errors positively
Summarize Follow-up on needed actions if any as team actions

Footnote: (1) The PaL process documented in this appendix was copied from the pioneering effort of Dr. Ed Rogers, Chief Knowledge Officer, Goddard Space Flight Center. It was subsequently edited by one of Dr. Roger's assistants, Paul Cox, Knowledge Management Analyst.

Appendix E. ESMD Risk Management Training

ESMD offers the risk management related courses shown in the table below.

Course Title	Key Content
ESMD's Approach for Implementing CRM (~90 minutes)	• Introduces CRM and explains why and how ESMD implements it • Describes the CRM process • Explains how CRM relates to Earned Value Management (EVM) and Knowledge Management (KM)
ESMD Approach to Risk Reporting (~30 minutes)	• Describes the Risk Reporting Process • Provides instruction on when and how to escalate a risk
ESMD's Active Risk Manager (ARM) Software Tool (~90 minutes)	• Describes ARM functionality • Demonstrates how ARM supports horizontal and vertical risk integration • Demonstrates how ARM can be used for communication and reporting

For additional information regarding ESMD risk management training, please contact Dave Lengyel at dlengyel@nasa.gov.

Appendix F. ESMD RMWG Charter

F.1. PURPOSE

This charter establishes the ESMD Risk Management Working Group (RMWG) and its scope, membership, functions, operations, responsibilities, and constraints.

F.2. SCOPE

The RMWG supports the development and coordination of consistent risk management (RM) policy, practice, and tools among ESMD programs, projects, and organizations. The goal of the RMWG is to ensure that risks affecting ESMD activities are proactively identified, accurately characterized, fully communicated to all stakeholders, and acted upon appropriately.

F.3. MEMBERSHIP

The membership of the ESMD RMWG is composed of:

- The ESMD Risk Manager, who is the ESMD RMWG Chair.
- Level I Organization/Project/Program risk management focal points.
- Level II Organization/Project/Program risk management focal points.
- Other members that may be selected or invited by the ESMD Risk Manager, as needed.

F.4. FUNCTIONS

The ESMD RMWG will:

- Develop and pre-coordinates policies, processes, standards, and tools, to support the practice of effective risk identification, analysis, planning, tracking, and control in ESMD programs, projects, and organizations. The RMWG monitors and discusses ESMD risk management practice to ensure compliance with NASA defined policy.
- Coordinate the resolution of issues regarding Directorate and program risks, such as risk ownership and mitigation action.
- Identify relationships (associated risks and parent/child relationships) among Level I and Level II risks, and informs parties to coordinate mitigation activities, as required.
- Review all Level I and Level II top risks prior to the Quarterly Program Management Review (QPMR) to ensure that all significant risks have been identified and fully defined with current progress documented in the risk mitigation plan.

- Provide the ESMD Deputy Associate Administrator with regular risk assessments regarding compliance with and effectiveness of defined risk management policy and practice across ESMD activities.
- Develop the ESMD Top Risk List for review by the ESMD AA.

F.5. OPERATIONS

The ESMD RMWG operates in the following manner:

- Meetings are held on a regular basis and the meeting dates and agendas are established and distributed by the ESMD Risk Manager.
- Meetings are documented and action items are assigned and tracked to resolution by the ESMD Risk Manager.
- The ESMD RMWG uses consensus as the means of making decisions. In the event that consensus cannot be reached, the ESMD Risk Manager makes a decision based upon the facts presented and input from the RMWG members.

F.6. RESPONSIBILITIES

Responsibilities for the RMWG Chair and RMWG Members include the following:

F.6.1. The ESMD Risk Manager, as the ESMD RMWG Chair, will:

- Establish and manage the activities of the RMWG in accordance with the functions set forth in this charter.
- Review Directorate and program processes to ensure rigor and consistency with risk management policies and requirements.
- Define the ESMD Top Risk List and present it to the ESMD AA.
- Schedule meetings, establish agendas, and assign actions.
- Coordinate with other organizations, programs, and projects as needed, to resolve issues.
- Identify information exchange interfaces among the Directorate and Programs.
- Create ad hoc subgroups, as required, to perform activities defined in this charter.
- Communicate ESMD RMWG concerns, recommendations, and issues to ESMD Management.
- Approve KBRs for inclusion in the risk management database.
- Lead the development of the ESMD Top Risk List.
- Lead RMWG horizontal / vertical risk integration activities.

F.6.2. The ESMD RMWG members will:

- Understand NASA and ESMD-specific risk management processes, as well as those processes and standards unique to their respective organizations.
- Establish processes for deployment of risk management policies and training within their organization.
- Review and assess the technical adequacy of ESMD Top Risks prepared by their organization.
- Provide any requested assistance to other Directorate / program organizations in identifying, planning, tracking, and controlling risks when they are an affected stakeholder.
- Provide recommendations for improving risk assessment and management approaches for ESMD.
- Maintain cognizance of ESMD Top Risks and their impact on ESMD Technical and Programmatic goals.
- Resolve technical issues referred to the ESMD RMWG for decision from ESMD management or program representatives.
- Provide evaluations of proposed changes to risk management policies and practices.
- Communicate ESMD RMWG activities such as changes in ESMD policies and procedures to their organization's management.
- Participate in ESMD RMWG subgroups, as needed, to address specific issues defined by the ESMD RMWG.
- Review, evaluate, and propose KBRs for inclusion in the risk management database.
- Support the development of the ESMD Top Risk List.
- Identify opportunities for horizontal / vertical risk integration, and facilitate the integration.
- Research and evaluate risk management tools and support their effective implementation.

F.7. CONSTRAINTS

ESMD RMWG's responsibilities do not include the management of risks for ESMD programs. The RMWG is a communication and facilitation forum.

Appendix G. ESMD "HQ Only" RMWG Charter

G.1. PURPOSE

This charter establishes the ESMD "HQ Only" RMWG and its scope, membership, functions, operations, responsibilities, and constraints.

G.2. SCOPE

The ESMD "HQ Only" RMWG supports the development and coordination of consistent risk management (RM) policy, practice, and tools among ESMD divisions and offices. The goal of the ESMD "HQ Only" RMWG is to ensure that risks owned by ESMD Divisions and Offices are proactively identified, accurately characterized, fully communicated to all stakeholders, and acted upon appropriately.

G.3. MEMBERSHIP

The membership of the ESMD "HQ Only" RMWG is composed of:

- The DIO Manager is the ESMD "HQ Only" RMWG Chair.
- The ESMD Risk Manager, who is the ESMD "HQ Only" RMWG Executive Secretary.
- Other members that may be selected or invited by the ESMD Risk Manager, as needed.

G.4. FUNCTIONS

The ESMD "HQ Only" RMWG will:

- Review and approve level I candidate risks
- Coordinate the resolution of issues regarding Directorate risks, such as risk ownership and mitigation action.
- Identify relationships (associated risks and parent/child relationships) between Level I risks and all other NASA risks, and inform parties to coordinate mitigation activities, as required.
- Review all Level I risks prior to the ESMD RMWG to ensure that all significant risks have been identified and fully defined with current progress documented in the risk mitigation plan.
- Review all Level I "Accepted" and "Watch" risks, periodically (at least annually).

G.5. OPERATIONS

The ESMD "HQ Only" RMWG operates in the following manner:

- Meetings are held on a regular basis and the meeting dates and agendas are established and distributed by the ESMD Risk Manager.
- Meetings are documented and action items are assigned and tracked to resolution by the ESMD Risk Manager.
- The ESMD RMWG uses consensus as the means of making decisions. In the event that consensus cannot be reached, the ESMD "HQ Only" RMWG Chair makes a decision based upon the facts presented and input from the RMWG members.

G.6. RESPONSIBILITIES

Responsibilities for the ESMD "HQ Only" RMWG Chair and ESMD "HQ Only" RMWG Members include the following:

G.6.1. The ESMD DIO as the ESMD RMWG Chair, will:

- Establish and manage the activities of the RMWG in accordance with the functions set forth in this charter.
- Review Directorate risk processes to ensure rigor and consistency with risk management policies and requirements.
- Approve Directorate-level candidate risks.
- Schedule meetings, establish agendas, and assign actions.
- Coordinate with other organizations, programs, and projects as needed, to resolve issues.
- Identify inter- and intra- Directorate information exchange interfaces
- Communicate Directorate risk concerns, recommendations, and issues to ESMD Management.

G.6.2. The ESMD RMWG members will:

- Understand ESMD HQ-specific risk management processes, as well as those processes and standards unique to their respective organizations.
- Establish processes for deployment of risk management policies and training within their organization.
- Review and assess the technical adequacy of ESMD Division / Office Top Risks prepared by their organization.
- Provide any requested assistance to other Directorate / program organizations in identifying, planning, tracking, and controlling risks when they are an affected stakeholder.
- Provide recommendations for improving risk assessment and management approaches for ESMD.

- Resolve technical issues referred to the ESMD "HQ Only" RMWG for decision from ESMD management or program representatives.
- Communicate ESMD "HQ Only" RMWG activities such as changes in ESMD policies and procedures to their organization's management.
- Identify opportunities for horizontal / vertical risk integration, and facilitate the integration.

G.7. CONSTRAINTS

ESMD "HQ Only" RMWG's responsibilities do not include the management of risks for ESMD programs. The ESMD "HQ Only" RMWG is a Directorate / HQ level risk review board.