MPR 8000.4
REVISION B
EFFECTIVE DATE: March 15, 2021
EXPIRATION DATE: March 15, 2026

MARSHALL PROCEDURAL REQUIREMENTS

CS01

MISSION SUPPORT RISK MANAGEMENT

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Change/ Revalidation/ Canceled)	Document Revision/ Change	Effective Date	Description
Baseline		5/27/2015	The contents of this directive were previously published as IMSC-Plan-8000.4, MSFC Mission Support Risk Management Plan.
Change	1	4/4/2017	On 4/4/17, at the request of the OPRD, administrative changes were made to Appendix H, Reference Documents to reflect the updated document titles of MPR 7120.1, MPR 1410.2, and the FAR.
Revision	A	12/11/2019	Revised SMA Responsibilities, added "Risks and Opportunities" to the RIDM process, added the MSFC Risk Management Scorecard, and did some general cleanup/updates.
Revision	B	3/15/2021	Update to Appendix F, MSFC Risk Management Scorecard, to reflect approved changes at December 14, 2020 IMSC. Revised "Dissenting Opinion" to reflect NPD 1000.0.

TABLE OF CONTENTS

PARAGRAPH

PREFACE

P.1 PURPOSE

This document establishes roles and responsibilities, requirements and a common framework for identifying, analyzing, communicating, and managing Mission Support risks (risks to Center's infrastructure or personnel) identified by the Center Directorates, Offices, and resident Programs and Projects as required by NPR 8000.4.

P.2 APPLICABILITY

a. This MPR applies to Center personnel, programs, projects, and activities, including contractors and resident agencies to the extent specified in their respective contracts or agreements. ("Contractors," for purposes of this paragraph, include contractors, grantees, Cooperative Agreement recipients, Space Act Agreement partners, or other agreement parties.)

b. This MPR applies to the Michoud Assembly Facility.

c. This MPR applies the following: all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. This MPR applies the following: all document citations are assumed to be the latest version unless otherwise noted.

e. This MPR applies to the Office of the Director and all Directorate Level Organizations (DLOs) at MSFC both on and off-site. The DLOs may establish their own risk management plans as long as they meet the requirements specified in this document.

P.3 AUTHORITY

NPR 8000.4, Agency Risk Management Procedural Requirements

P.4 APPLICABLE DOCUMENTS AND FORMS

a. NPD 1000.0, NASA Governance and Strategic Management Handbook

b. NPD 1440.6, NASA Records Management

c. NPD 8700.1, NASA Policy for Safety and Mission Success

c. MWI 7120.6, Program, Project and Institutional Risk Management

d. NRRS 1441.1, NASA Records Retention Schedules

e. STD/MA-RMP, Data Requirements Description (DRD) - Risk Management Plan

P.5 MEASUREMENT/VERIFICATION

Compliance with this document will be measured using risk metrics provided by DLOs to the Center councils. Center organizations required to conduct risk management activities may develop a DLO risk management plan or may choose to adopt this directive as their organization's Risk Management Plan. The plan will describe the risk metrics that will be provided to Center management, and the frequency for risk process validation.

P.6 CANCELLATION

MPR 8000.4A, Mission Support Risk Management, dated December 11, 2019.

Electronic approved by

Steven C. Miley for
Jody Singer
Director

1. RESPONSIBILITIES

1.1 MSFC Associate Director or Designee shall:

1.1.1 Manage the Mission Support Risk Management (RM) process.

1.1.2 Ensure that schedules, new products, and tools are reviewed, and risk management process issues are resolved. The Mission Support Risk Manager (MSRM) coordinates all Mission Support risk activities requested by the Associate Director, MSFC, supporting organizational units and risk review boards and panels.

1.2 Office of Strategic Analysis and Communications (OSAC) or Designee shall:

1.2.1 Provide Electronic Project Online Risk Tool (ePORT) System Administration Support.

1.2.2 Collate inputs to the Center Risk Review Process.

1.2.3 Provide Status Reports to Mission Support Risk Management Working Group (MSRWG).

1.2.4 Provide Status Reports to Center Management.

1.2.5 Staff the MSRM function.

1.3 Safety and Mission Assurance Directorate (SMA) or Designee shall:

1.3.1 Perform the role of SMA Functional Manager as defined in NPD 8700.1.

1.3.2 Provide risk management consultation, facilitation, and training to the MSRM and DLOs.

1.3.3 Ensure that the training material is consistent with the requirements of NPR 8000.4.

1.3.4 Ensure that MWI 7120.6 is maintained.

1.3.5 Ensure that the Data Requirements Description (DRD) for the Risk Management Plan (DRD number: STD/MA-RMP) is maintained.

1.4 MSRM or Designee shall:

1.4.1 Have overall responsibility for implementing the Mission Support RM policy in accordance with NASA policy and NPR 8000.4.

1.4.2 Implement a risk database for tracking mission support risks.

1.4.3 Chair the Mission Support Risk Management Working Group (MSRWG) in support of Center Management.

1.4.4 Lead MSRWG activities utilizing the principles of Continuous Risk Management (CRM) and Risk Informed Decision Making (RIDM) (More details on the RIDM process are listed in Appendix E.)

1.4.5 Approve and maintain Risk Reporting Metrics and Risk Reports.

1.4.6 Coordinate communication with the other Organizational Units and Senior Management.

1.4.7 Ensure personnel are provided adequate Risk Database training.

1.4.8 Provide Mission Support Risk status to appropriate center-level forum.

1.4.9 Propose Top "N" Mission Support Risks.

1.4.10 Recommend acceptance, closure and downgrade of "Center-level" risks.

1.5 Directorate Level Organization (DLO) Management or Designee shall:

1.5.1 Determine which organizational units within their organizations are subject to the risk management requirements in this plan.

1.5.2 Ensure that Continuous Risk Management (CRM) and RIDM processes are implemented and that performance measures defined for the organization are for risk analysis of decision alternatives.

1.5.3 Designate the risk manager(s).

1.5.4 Ensure that the designated risk managers have experience in risk and decision analysis and in the RM process.

1.5.5 Ensure that key decisions of the organization are risk-informed. More details on the RIDM process are listed in Appendix E.

1.5.6 Ensure that risks are identified and analyzed in relation to the performance requirements for major acquisitions of the organization and risk analysis results are used to inform the source selection.

1.5.7 Ensure and concur in the definition of elevation criteria to be applied by DLOs.

1.5.8 Ensure that cross-cutting risks and interdependencies between risks are properly identified as cross-cutting and either managed within the organization or elevated.

1.5.9 Coordinate the management of cross-cutting risks being managed at the Center level with other involved organizations.

1.5.10 Ensure that dissenting opinions arising during risk management decision-making are handled through the dissenting opinion process as defined in Section 3.4 of this document.

1.6 DLO Risk Managers or Designees shall:

1.6.1 Facilitate the implementation of CRM and RIDM.

1.6.2 Ensure that training is provided by SMA to organization-level staff on risk management policies, tools, and processes.

1.6.3 Ensure the development of organization RM plans in compliance with NPR 8000.4. Organizations may choose to:

a. Develop a stand-alone document, which complies with NPR 8000.4, or

b. Adopt this directive as their organization's RM Plan.

1.6.4 Periodically review the RM Plan to ensure it is current.

1.6.5 Coordinate the organization's RM (CRM/RIDM) process with the RM processes of organizational units at levels above and below, including contractors if applicable.

1.6.6 Ensure that risk documentation is maintained in accordance with NPD 1440.6 and NRRS 1441.1, and under formal configuration control, with a capability to identify and readily retrieve the current and all archived versions of risk information and the risk management plans.

1.7 Mission Support Risk Management Working Group (MSRWG)

A body of representatives from each MSFC DLO that is chaired by the MSRM. The MSRWG seeks to ensure consistent implementation of risk management processes. The MSRWG shall:

1.7.1 Aid in improving Center risk management policies, procedures, and tools.

1.7.2 Review risks elevated to the Center Level with respect to Center commitments, resource requests, and potential common solutions.

1.7.3 Review and approve procedures and criteria for prioritizing the Center risks to support Risk-Informed Decision Making. More details on the RIDM process are listed in Appendix E.

1.7.4 Assure the appropriate risk information is provided for each top Center Risk to properly support the recommended alternatives and decision-making process.

1.8 MSFC Employees Implementing Mission Support Risk Management Activities shall:

1.8.1 Continuously and systematically review their respective areas using appropriate methods to identify any event that could adversely affect the achievement of planned performance.

1.8.2 Identify, evaluate, and manage risks in accordance with the requirements specified in this document.

2. MSFC RISK MANAGEMENT

2.1 Overview

MSFC Mission Support risk management integrates risks from various sources to assist with decisions that maximize the efficient allocation of resources to enable MSFC to meet commitments, align with Programs/Projects, and position the Center for future business. The approach used by MSFC for risk management is an integration of RIDM and CRM (Figure 1: NASA Risk Management Paradigm). The purpose of integrating RIDM and CRM into a coherent framework is to foster proactive risk management: to better inform decision making through use of quality risk information, and then to more effectively manage implementation risks using the CRM process, which is focused on the baseline performance requirements emerging from the RIDM process. Within the RIDM process, decisions are made with regard to outcomes of the decision alternatives, taking into account applicable risks and uncertainties; then, as part of the implementation process, CRM is used to manage those risks in order to achieve the performance levels that drove the selection of a particular alternative. Proactive risk management applies to programs, projects, and mission support offices.

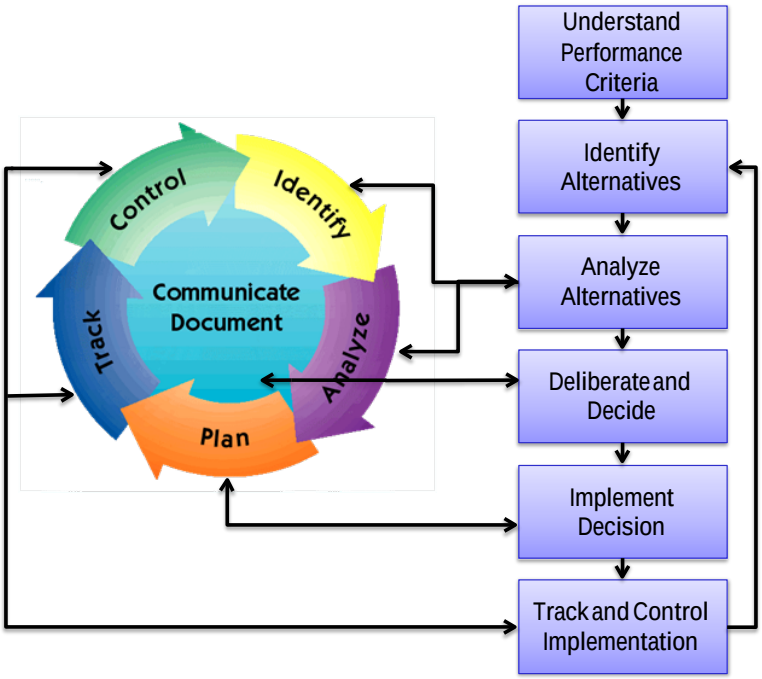


Figure 1: NASA CRM Paradigm

2.2 Risk-Informed Decision Making (RIDM)

2.2.1 Figure 1 shows the interface between CRM and RIDM. The following steps are a Risk-Informed Decision Analysis Process:

a. Identify and understand the performance criteria.

b. Propose and identify decision alternatives, recognizing both risks and opportunities.
c. Perform risk analysis and rank decision alternatives.
d. Deliberate and choose a decision alternative.
e. Implement decision.
f. Track the implementation of the decision.

2.2.2 These steps support good decisions by focusing first on objectives and associated performance criteria, next on developing decision alternatives with those objectives clearly in mind, and then on developing decision alternatives that have been developed under other systems engineering processes. The risk analysis of decision alternatives (step three) not only guides selection of a preferred alternative, but it also relies on the Identify and Analyze steps of CRM. Selection of a preferred alternative is based in part on an understanding of the risks associated with that alternative. Alternative selection is followed immediately by a planning activity in which key implementation aspects are addressed, namely, how the risks are to be handled. The risk handling plans are executed as the decision alternative is implemented, along with risk tracking and control. New risks may also be identified during the planning and implementation of the selected decision alternative. More details on the RIDM process are listed in Appendix E.

2.3 Continuous Risk Management (CRM)

2.3.1 CRM is a widely used technique within NASA, initiated at the beginning and continuing throughout the program life cycle to monitor and control risk. It is an iterative and adaptive process, which promotes the successful handling of risk. Each step of the paradigm builds on the previous step through the feedback of generated information, leading to improved designs and processes. The steps are:

a. Identify: State the risk in terms of condition and consequence(s); capture the context of the risk (e.g., what, when, where, how and why).

b. Analyze: Estimate the probability and consequence components of the risk through analysis, including uncertainty in the probabilities and consequences and, as appropriate, estimate aggregate risks.

c. Plan: Assign responsibility, determine approach (research, accept, mitigate, or watch); if risk will be mitigated, define mitigation level (e.g., action item list or more detailed task plan) and goal; execute plan.

d. Track: Acquire/update, compile, analyze, and organize risk data; report tracking results; and verify and validate mitigation actions.

e. Control: Analyze tracking results, decide how to proceed (re-plan, close the risk, invoke contingency plans, continue tracking); execute the control decisions.

f. Communicate and Document: Document supporting information for each key element in a system organized to track details, plans, progress, and risk decisions.

2.3.2 In addition to being identified through a process life cycle, risks may be identified during the analysis of alternatives or during the planning and implementation of the chosen alternatives. Hence, the risk management process is continuous: proactively seeking out and managing risks to success through the end of the mission, project, or process.

3. RISK MANAGEMENT PROCESSES

MSFC requirements flow down from NPR 8000.4. In the context of mission execution, risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements. The performance shortfalls may be related to institutional support for mission execution or related to any one or more of the following mission execution domains:

a. Safety
b. Technical / Performance / Mission Success
c. Cost
d. Schedule

3.1 Continuous Risk Management (CRM)

3.1.1 Potential Risk Sources

There are numerous sources that should be considered when identifying risks. The following list represents examples of potential sources of risk:

a. Inadequate facilities and infrastructure
b. Inadequate information technology
c. Delayed acquisition
d. Ineffective communication with stakeholders
e. Unrealistic schedule estimates or allocation
f. Operational hazards
g. Issues, hazards, and vulnerabilities that could adversely affect the program's technical effort
h. Unrealistic cost estimates or budget allocation
i. Inadequate staffing or skills
j. Uncertain or inadequate contractor capability
k. Uncertain or inadequate vendor capability
l. Insufficient production capacity

3.1.2 Risk Identification

Risks shall be identified by an examination of the Center's performance criteria relative to the sources of risk to include the following:

a. Identify contributors to risk (shortfalls in performance relative to the baseline performance requirements). Sometimes the relationship between an identified risk and performance measures is indirect, but risks within the proper scope of CRM are addressed precisely because they may affect one or more performance measures.

b. Identify risks by drafting a risk statement or scenario that summarizes the events leading to degraded performance with respect to one or more performance measures.

c. Provide/prepare a risk context that describes the circumstances, contributing factors, uncertainty, range of possible consequences, and related issues (such as what, where, when, how, and why).

Note: Appendix I includes a taxonomy-based questionnaire to assist with the identification of potential risks.

3.1.3 Risk Analysis

Risks shall be analyzed for determination of likelihood of occurrence and significance of consequence. The risk assessment steps are as follows:

a. Evaluate the background information that forms the basis of the analysis and reduces the uncertainty regarding the potential risk event or situation.

b. Identify significant consequences to the MSFC performance criteria that may result from the risk event.

c. Select one or more assessment methodologies for each consequence identified.

d. Assess likelihood and consequence of the risk, along with the duration of time until action needs to be taken (timeframe).

e. Aggregate risks that impact the same performance criteria and assess the aggregate impact, when possible.

f. Prioritize risks based upon their likelihood, consequence, and timeframe.

3.1.4 Risk Communication and Documentation

The following risk information required for decision-making shall be provided by DLO Risk Managers and include the following:

a. Risk statement or scenario
b. Risk context
c. Risk likelihood, consequence, and timeframe
d. Criteria required for closure or acceptance
e. Estimated Completion Date (ECD)
f. Current status
g. Handling strategy overview

3.1.4.1 Risk likelihood and consequence is summarized using the MSFC RM Scorecard, given in Appendix F. The scorecard provides ordinal scales for likelihood, consequence, and timeframe. After risk analysis is completed, levels on the ordinal scales are selected. A risk severity of high, moderate, or low is determined based on the chosen levels for likelihood and consequence.

3.1.4.2 The Center and its DLOs will use the ePORT to document and communicate risk data. A description of each risk, likelihood and consequence rating determined via the MSFC RM Scorecard (Appendix F), timeframe, and handling plan are entered into this database. MSFC management and DLOs use this database to effectively manage and track each risk and to gain insight into impacts of other organizations' risks. The risk database should be able to produce the necessary reports required for DLO, Center, and Agency management.

3.1.5 Risk Planning

Risks shall be reviewed for technical aspects and the risk owner recommends a plan of action to management. This plan of action is referred to as the handling strategy. A risk owner is designated to manage the execution of the handling strategy. The recommended handling strategy will consist of one of the following:

a. When a decision is made to *accept* a risk, the risk manager shall ensure that each acceptance is clearly documented in the MSFC risk database including the assumptions and conditions (risk acceptability criteria) on which the acceptance is based. Accepted risks are periodically reviewed to ensure that acceptance rationales are still applicable and that controls are still in place. Typically, only low risks are accepted. Acceptance of a high severity Center risk requires concurrence of Center management.

b. When a decision is made to *mitigate* a risk, the risk manager shall ensure that a risk mitigation plan is developed and documented in the risk database (including the appropriate parameters that will be tracked to determine the effectiveness of the mitigation).

c. When a decision is made to *watch* a risk, the risk manager shall ensure that tracking requirements are developed and documented in the risk database. Typically, watched risks have low consequence.

d. When a decision is made to *close* a risk, the risk manager shall ensure that the closure rationale is developed, approval of closure is obtained from the unit manager, and that both rationale and management approval are documented in the risk database. Typically, closed risks have no or low consequence. Appendix G: Mission Support Risk Processes illustrates how Mission Support center-level risks are to be closed.

e. When additional information is needed to make a decision, the risk manager shall ensure that efforts to *research* a risk (obtain additional information) are documented and tracked in the risk database.

f. When dispositions (a), (b), (c), (d), or (e) above cannot be applied, management shall *elevate*

the decision to the organizational unit management at the next higher level and document the action taken in the risk database. Center management elevates/transfers risks to Agency-level organizations. DLOs elevate risks to Center management and/or to mission directorates for MSFC-resident programs. Protocols for risk elevation are provided in Section 3.2.

g. Risks identified by Center management or by stakeholders external to MSFC may be best managed by MSFC DLOs. In these instances, risks shall *delegated* to the appropriate level in the MSFC organization. Protocols for risk delegation are also provided in Section 3.2.

3.1.6 Risk Tracking

3.1.6.1 Risks shall be updated by the owning DLO on a recurring basis to reflect current status:

a. Accepted risks are updated as indicated by the review plan
b. Open risks with a Watch Plan are updated as indicated by the review plan
c. Open risks with Research or Mitigation Plans are reviewed and statused monthly

3.1.6.2 Metrics shall be developed and used to measure the effectiveness of the implementation of the Center risk management process. DLOs are required to present the following metrics to the appropriate governing council or Center-level forum on a regular basis:

a. Metrics revealing the overall risk environment and progress of the risk management process within the DLO, including:

(1) Number of changes to risk severity since last reporting period, by low, medium, and high severity
(2) Number of plans that are underperforming the proposed mitigations
(3) Turnover in the number of top risks

b. Detailed information on the top risks faced by the DLO, including:

(1) List of all Top Risks
(2) Risk likelihood, consequence and timeframe assessment of each risk
(3) Status of mitigation plans for top risks

3.1.7 Risk Control

The risk owner shall utilize the risk control phase of the CRM paradigm to assist in making informed, timely, and effective decisions regarding risks and their mitigation plans. For example, types of decisions may include:

a. Continue as planned – Analysis of tracking data indicates progress is as expected.

b. Re-plan the mitigation – Analysis of tracking data indicates a mid-course correction is required.

c. Invoke a contingency plan – Analysis of tracking data indicates the current plan is inadequate.

d. Close the risk – Analysis of tracking data indicates risks will no longer be actively mitigated or monitored for any of the following scenarios:

(1) Residual risk is considered negligible and further risk reduction activity is deemed unnecessary
(2) Risks that have been incorporated into or combined with a new risk
(3) Risks that have become problems; the problems may spawn new risks
(4) Risks have been transferred to another entity for management

e. Accept the risk – Analysis of tracking data indicates risk reduction actions are not justified to eliminate or reduce the risk and no resources will be expended for one or more of the following scenarios:

(1) Mitigation is not cost effective
(2) Some residual risk may exist, but at an acceptable level
(3) Controls and acceptance rationale have been defined to justify continuation without further preventive or mitigation action.

f. Transfer – Analysis of tracking data indicates a particular risk should be owned by another organization for one or more of the following reasons:

(1) The risk was identified outside of the owning organization
(2) The organizational roles and responsibilities have changed
(3) The control of mitigation resources has changed

In order to transfer a risk, negotiations and mutual agreements between the current risk owner, proposed future risk owner, and other stakeholders is necessary.

3.2 Elevation and Delegation of Center-Level Risks

Risk elevation is another aspect of communicating risk information, but the emphasis is bottom-up instead of top down flow. Risks are typically handled at the lowest feasible level of organization. A risk's elevation reflects the hierarchical level of insight or control of resources needed to effectively handle the risk. Risks meeting any of the following criteria shall be elevated to the Center level:

a. Threatens Center's ability to support assigned projects and is outside the organization's ability to mitigate (e.g., Certification of high pressure systems)

b. Threat to Center's future resources (e.g., ; Base Realignment and Closure (BRAC) competition and/or New Competing Industry to Center workforce)

c. Threat to Center's/Agency's credibility as a government entity and/or compliance with Agency

policies, direction or funds (e.g., Diversity goals; Agency's desire for more consolidation of Center functions)

3.2.1 To elevate a risk to the Center level, the DLO risk manager shall first present the risk to their respective Organizational Risk Review Board (e.g., Safety & Mission Assurance Council [SMAC] or Engineering Management Council [EMC]) and then to the MSRWG for recommendation to be elevated to the Center level.

3.2.2 Risk is presented to Center Management for approval, typically at quarterly Integrated Management System Council (IMSC) Mission Support Risk Management Update. If Center approves the elevation of the risk the MSRM ensures that the Risk is indicated as “IMSC” in the risk database and that the appropriate Center Manager is elected based on the type of risk or the organization owning the risk.

3.2.3 Risk delegation is required as Center management becomes aware of risks that are best handled by mission execution or mission support organizations within the Center. Such risks may be identified by Center personnel, agency management, mission directorates, or by external agents, such as auditors. In these situations, risk ownership is transferred from Center management to the appropriate person. To delegate a risk from the Center-level, the MSRWG determines the appropriate owner. Then the risk is assigned to the owner in the risk database by the MSRM and communicated to the assigned risk owner. (see Appendix G)

3.3 Identification and Handling of Cross-cutting Risks

3.3.1 Risks with impact to multiple organizations are cross-cutting risks. Since each organization is represented on the management councils, it also has the opportunity to hear risks presented by other DLOs and to identify impacts to its own organization. Ownership of the risk shall be decided per one of three criteria:

a. Organization of greatest consequence
b. Organization most capable of reducing the risk
c. Organization with the appropriate decision authority

3.3.2 Based on consideration of these criteria, the affected organizations determine which organization is chiefly responsible for managing the risk and a risk owner shall be assigned from within that organization.

3.3.3 In consultation with the affected organizations, the risk owner shall develop a plan to handle the risk. This involves a prioritization of the requirements at risk and the resources available. Specific steps in the handling plan may be executed by members of every affected organization. If a dispute between affected organizations arises over the proper handling approach, the head of the appropriate management council makes the final determination.

3.4 Dissenting Opinion

Dissenting opinions arising during risk management decision making are handled through the dissenting opinion process as defined in NPD 1000.0. Dissenting opinions related to Mission Support (Institutional) risk will be vetted through the MSRWG and may be elevated to the Center Associate Director for adjudication.

APPENDIX A
DEFINITIONS

Accept: The formal process of justifying and documenting a decision not to mitigate a given risk associated with achieving given objectives or given performance requirements. (See also Risk acceptability criterion).

Aggregate Risk: The cumulative risk associated with a given performance measure, accounting for all significant risk contributors. For example, the total probability of loss of mission is an aggregate risk quantified as the probability of the union of all scenarios leading to loss of mission.

Close: The determination that a risk is no longer cost-effective to track, because (for example) the associated scenario likelihoods are low (e.g., the underlying condition no longer exists), or the associated consequences are low.

Continuous Risk Management: A systematic and iterative process that efficiently identifies, analyzes, plans, tracks, controls, and communicates and documents risks associated with implementation of designs, plans, and processes.

Cross-Cutting Risk: A risk that is generally applicable to multiple mission execution efforts, with attributes and impacts found in multiple levels of the organization or in multiple organizations within the same level.

Deliberation: In the context of this document, the formal or informal process for communication and collective consideration, by stakeholders designated in the Risk Management Plan, of all pertinent information, especially risk information, in order to support the decision-maker.

Dissenting Opinion: A dissenting opinion is a disagreement with a decision or action that an individual judges is of sufficient importance to warrant a specific review and decision by higher-level management.

Elevate: The process of transferring the decision for the management of an identified source of risk to the risk management structure at a higher organizational level.

Key Decisions: Key decisions are those that fall within the purview of each governing council.

Likelihood: A measure of the possibility that a scenario will occur that also accounts for the timeframe in which the events represented in the scenario can occur.

Mission Support Risks: Risks to infrastructure, information technology, resources, personnel, assets, processes, occupational safety, environmental management, or security that affect capabilities and resources necessary for mission success, including Mission Support flexibility to respond to changing mission needs and compliance with external requirements (e.g., Environmental Protection Agency or Occupational Safety and Health Administration regulations).

Mitigate: The modification of a process, system, or activity in order to reduce a risk by reducing its probability, consequence severity, or uncertainty, or by shifting its timeframe.

Organizational Unit: An organization, such as a program, project, Center, Mission Directorate, Mission Support Office, or Center Directorate that is responsible for carrying out a particular activity.

Performance Measure: A metric used to measure the extent to which a system, process, or activity fulfills its intended objectives.

Performance Requirement: The value of a performance measure to be achieved by an organizational unit's work that has been agreed-upon to satisfy the needs of the next higher organizational level.

Research: The investigation of a risk in order to acquire sufficient information to support another disposition; i.e., close, watch, mitigate, accept, or elevate.

Risk: In the context of mission execution, risk is *operationally* defined as a set of triplets: The *scenario*(s) leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, or destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage); The *likelihood*(s) (qualitative or quantitative) of those scenarios; The *consequence*(s) (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur. Uncertainties are included in the evaluation of likelihoods and consequences.

Risk Acceptability Criterion: A rule for determining whether a given organizational unit has the authority to decide to accept a risk.

Risk-Informed Decision Making: A process that uses a diverse set of performance measures (some of which are model-based risk metrics) along with other considerations within a deliberative process to inform decision-making.

Risk Management: Risk management includes RIDM and CRM in an integrated framework. This is done in order to foster proactive risk management, to better inform decision-making through better use of risk information, and then to more effectively manage implementation risks by focusing the CRM process on the baseline performance requirements emerging from the RIDM process.

Risk Owner: The entity, usually a named individual, designated as the lead for overseeing the implementation of the agreed disposition of that risk.

Risk Review Boards: Formally established groups of people assigned specifically to review risk information. Their output is twofold: (1) to improve the management of risk in the area being reviewed and (2) to serve as an input to decision-making bodies in need of risk information.

Safety: In a risk-informed context, safety is an overall condition that provides sufficient assurance that mishaps will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic criteria and risk-informed criteria.

Scenario: A sequence of events, such as an account or synopsis of a projected course of action or events.

Uncertainty: An imperfect state of knowledge or a variability resulting from a variety of factors including, but not limited to, lack of knowledge, applicability of information, physical variation, randomness or stochastic behavior, indeterminacy, judgment, and approximation.

Watch: The monitoring of a risk for early warning of a significant change in its probability, consequences, uncertainty, or timeframe.

APPENDIX B
ACRONYMS

BRAC	Base Realignment and Closure
CMO	Center Management and Operations
CRM	Continuous Risk Management
DLO	Directorate Level Organization
DRD	Data Requirements Description
ECD	Estimated Completion Date
EMC	Engineering Management Council
ePORT	Electronic Project Online Risk Tool
FAR	Federal Acquisition Regulations
IMSC	Integrated Management System Council
MA	Management
MSRM	Mission Support Risk Manager
MSRWG	Mission Support Risk Management Working Group
NRRS	NASA Records Retention Schedules
OSAC	Office of Strategic Analysis and Communications
RIDM	Risk-Informed Decision Making
RM	Risk Management
RMP	Risk Management Plan
SMA	Safety and Mission Assurance
SMAC	Safety and Mission Assurance Council
STD	Standard

APPENDIX C
VERIFICATION MATRIX
(Reserved)

NONE

APPENDIX D
RECORDS

RM records will be maintained in the ePORT Risk Database by the MSRM in accordance with NRRS 1441.1, Schedule 1, Item 26.5.A; destroy when 7 years old.

APPENDIX E
RISK-INFORMED DECISION MAKING (RIDM)

E.1 RIDM

E.1.1 Key Decisions

Center management ensures that key decisions are risk-informed. This occurs during the meetings of the governing councils or other Center-level forum.

E.1.2 Understand Performance Criteria

The performance criteria are identifiable through analysis of MSFC objectives and analysis of performance measures used by MSFC stakeholders to gauge Center performance. Performance criteria are subject to change as priorities change and must be revisited on a regular basis, typically in concert with Agency strategic planning. The acceptable range and scale of the criteria will also change with time. For example, workforce safety metrics should improve with time. Some criteria may not be applicable to a specific decision; however, they should be documented as having been considered.

E.1.3 Identify Alternatives

Almost every decision will involve selection of one alternative from a list of many. To fully identify alternatives, decision alternatives should be brainstormed and the summary names for each alternative should be documented. For complex decisions, a best practice is to perform a literature search to identify options. Reduce the decision options to a reasonable set. While some options will be clearly less desirable than others, documenting that these options were considered remains prudent. The use of mandatory criteria also can help reduce the number of options. A few decisions might only have one alternative. A best practice is to develop a decision matrix even for one option if a major decision is at hand. Sometimes maintaining the status quo—that is, deciding to take no action—should be considered as an alternative.

E.1.4 Analyze Alternatives

E.1.4.1 Numerous techniques are available to analyze decision alternatives, including trade studies, decision matrices, influence diagrams, and the analytical hierarchy process. Regardless of the methods or tools used, results must include:

a. Evaluation of assumptions related to evaluation criteria and of the evidence that supports the assumptions.

b. Evaluation of whether uncertainty in the values for decision alternatives affects the evaluation.

c. Evaluation of the impact of risk on the performance of the decision alternatives.
Risk impact can be factored into the alternative decision in three ways. First, risk can be

considered as an independent performance criteria that is ranked and rated along with other performance criteria. Second, risks to specific performance criteria can be modeled as degradation in that performance criteria. Third, risks can be modeled as degradation in the overall value of the decision alternative.

E.1.4.2 This step in the RIDM process relies on effective execution of the Identify and Analyze steps in the CRM process, presented in Section 3.1.2 and 3.1.3, respectively.

E.1.5 Deliberate and Decide

E.1.5.1 Deliberation is recommended in order to make use of collective wisdom to promote selection of an alternative for implementation. Deliberation may also identify opportunities for improvements that could be realized by the organization. In the case of complex and high-stakes decisions, deliberation may be required to recommend a final round of trade studies or uncertainty reduction efforts. Participants involved in Center-level deliberations are the individual members of the governing councils.

E.1.5.2 To risk-inform the decision-making process, risk information must be effectively documented and communicated. Therefore, this step in the RIDM process relies on effective execution or the Communicate and Document step in the CRM process, presented in Section 3.1.4.

E.1.6 Implement Decision

E.1.6.1 At this point, a single alternative has been selected. The management parameters of the decision are used to update the management baselines; i.e., expected costs are added to budgets, tasks are added to work breakdowns and schedules, and decision risks are added to the risk list. Along with the decision alternative, plans for handling the risks to the alternative must also be determined and implemented. This step in the RIDM process relies on effective execution of the Plan step in the CRM process, presented in Section 3.1.5.

E.1.6.2 As the decision is implemented, new risks may be discovered. In an operational environment, employees may be implementing decisions made long ago and changes in the operational environment introduce new risks. These new risks are managed using the same CRM process, along with the risks identified when the decision was made. Hence, the CRM process is continuous.

E.1.7 Track and Control Implementation

The performance criteria used to select the decision alternative are used to track and control the implementation of the chosen alternative. For example, if cost was a key performance criterion then budget spending is tracked and controlled. Since risk is always a factor in decision- making, risks are tracked and controlled during decision implementation. This step in the RIDM process relies on effective execution of the Track and Control steps in the CRM process, presented in Section 3.1.6 and 3.1.7, respectively.

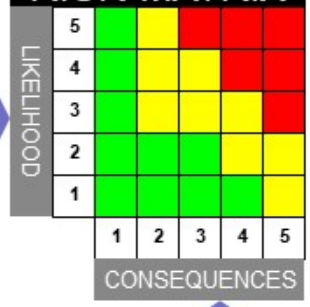
APPENDIX F
MISSION SUPPORT RM SCORECARD (Next Page)

MSFC Risk Scorecard

LIKELIHOOD RATING

Level	Probability	
5	Very Likely	Expected to happen
4	Likely	Could happen. Controls have significant limitations or uncertainties.
3	Possible	Could happen. Controls exist, with some limitations or uncertainties.
2	Unlikely	Not expected to happen. Controls have minor limitations or uncertainties.
1	Highly Unlikely	Extremely remote possibility that it will happen. Strong controls in place.

RISK MATRIX



TIMEFRAME

Near	0 to 6 months
Mid	6 to 12 months
Far	> 12 months

Consequence Rating	Minor	Moderate	Significant	Major	Catastrophic

Level	1	2	3	4	5
SAFETY Health, Safety, Quality & Environment	- First aid incident or damage to minor asset - Release to the environment causing insignificant to no impacts or damage to natural or cultural resources.	- Short-term injury, impairment or incapacitation. Minor damage to major asset or loss of minor asset. Minor OSHA violation - Release to the environment causing moderate impacts or damage to natural or cultural resources or a Regulatory warning.	- Long-term injury, impairment or incapacitation. Significant damage to major asset or loss of major asset. Moderate OSHA violation - Release to the environment causing significant impacts or damage to natural or cultural resources or a violation with minor fine.	- Permanent serious injury, impairment or incapacitation. Loss of major asset. Major OSHA violation -Significant release to the environment causing substantial impacts or damage to natural or cultural resources or a violation with major fine.	- May cause loss of life - Significant release to the environment causing irreparable impacts or damage to natural or cultural resources or violation resulting in loss of environmental permit
Mission Success/ Supportability (Human Capital, Facilities, Infrastructure)	Minor impact to programmatic and technical support, human capital, capability and diversity. Minor impact to facilities and infrastructure	Moderate impact to programmatic and technical support, human capital, capability and diversity. Minor impact to facilities and infrastructure	Significant impact to programmatic and technical support, human capital, capability and diversity. Significant impact to facilities and infrastructure	Major impact to programmatic and technical support, human capital, capability and diversity. Significant impact to facilities and infrastructure	Failure to meet customer requirements. Failure to meet major goal or objective
SCHEDULE	Minor milestone slip < 1 week: Critical Path slip 1 week	Minor milestone slip > 1 week to <1 month: Critical Path slip 1 week -1 month	Major milestone slip > 1 month to <2 months: Critical Path slip 1 - 2 months	Major milestone slip > 2 months: Critical Path slip 2 - 6 months	Cancellation of project due to schedule overruns
COST	$0 to <$500K OR < 2% increase over allocated budget/negligible impact on reserve	$500K to <$1M or 2% to 5% increase over allocated budget/can handle with reserve	$1M to < $2.5M OR 5% to 10% increase over allocated budget/ cannot handle with reserve	$2.5M to < $5M OR 10% to 15% increase over allocated budget/ exceeds reserves	>$5M OR >15% increase over allocated budget/ exceeds reserves

APPENDIX G
MISSION SUPPORT RISK PROCESSES

Figure G-1

Process for Closing/Downgrading Mission Support Risks

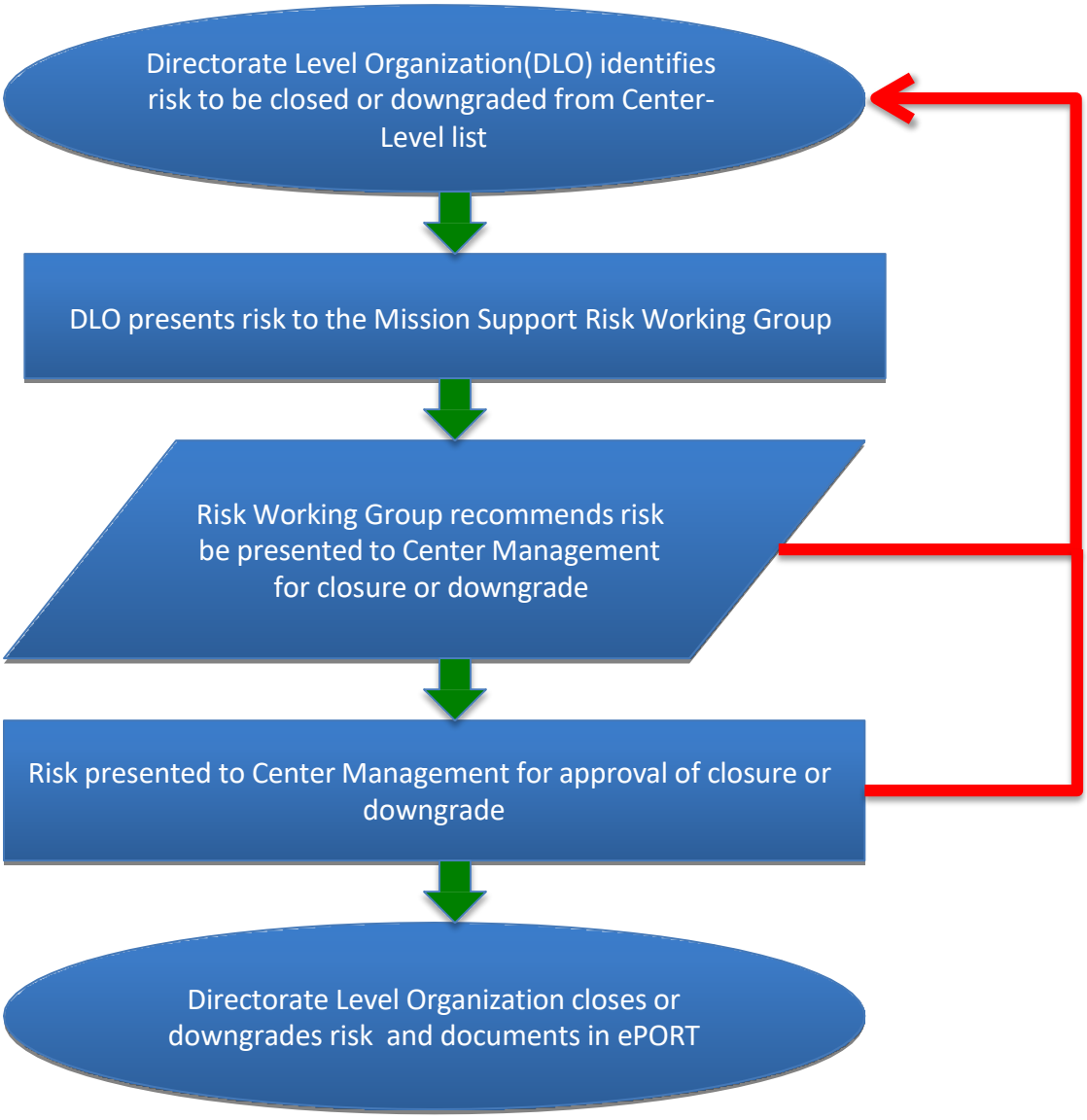


Figure G-2

APPENDIX H
REFERENCE DOCUMENTS

H.1 Federal Acquisition Regulation, 48 CFR, ch. 1, pts. 7 and 15
H.2 NASA Federal Acquisition Regulation Supplements, 48 CFR, ch. 18, pts. 1807 and 1815
H.3 NPD 7120.4, NASA Engineering and Program/Project Management Policy
H.4 NPR 1600.1, NASA Security Program Procedural Requirements
H.5 NPR 2810.1, Security of Information Technology
H.6 NPR 7120.8, NASA Research and Technology Program and Project Management Requirements
H.7 NPR 8715.3, NASA General Safety Program Requirements
H.8 MPR 1410.2, Marshall Directives System
H.9 MPR 7120.1, MSFC Engineering and Program/Project Management Requirements

APPENDIX I
RISK IDENTIFIACTION TAXONOMY-BASED QUESTIONAIRE

The taxonomy-based questionnaire is a set of questions, ordered into groups or categories, which may assist in identification of potential risks. The outcome of the exercise provides a general magnitude of risks based on the specific circumstances. Depending on the answers, follow up questions are used to probe relationships and identify risks that would not have been identified otherwise. The questionnaire fosters risk awareness and personnel motivation and involvement.

Risk Source	Questions	Considerations
Requirements	Are there risks that may arise from requirements documentation?	Stability, Completeness, Clarity, Validity, Feasibility
Design	Are there risks in the designs selected to meet requirements?	Functionality, Difficulty, Interface Control, Performance, Testability
DLO Specialties	Are there risks as a result of special attributes of planned Facilities, Equipment, Hardware or Software?	Maintainability, Reliability, Safety, Security, Human Factors
Resources	Are there risks resulting from the resources needed by the Center, Program, or Project to complete the activities?	Schedule, Staff, Budget, Facilities
Interfaces	Are the risks associated with any uncontrollable external interfaces?	Customer, Vendors, Senior Management,
Metrics and/or Trends	Are there metrics and/or trends available which may indicate potential risk situations?	Periodic Reviews
Technology	Are there risks associated with technology that will have technical or performance limitations and endanger the program/project?	Technology is unimproved, new and poorly understood, not easily integrated.
External Context	Are there risks, as a result of external environments, which hinder the organization from achieving its objectives?	External Context can include: - the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; key drivers and trends having impact on the objectives of the organization; and - relationships with, and perceptions and values of external stakeholders.

Internal Context	Are there risks, as a result of internal environments, which hinder the organization from achieving its objectives?	Internal context can include: - governance, organizational structure, roles and accountabilities; - policies, objectives, and the strategies that are in place to achieve them; - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); - information systems, information flows and decision-making processes (both formal and informal); - relationships with, and perceptions and values of, internal stakeholders; - the organization's culture; - standards, guidelines and models adopted by the organization; and - form and extent of contractual relationships.