**COMPLIANCE IS MANDATORY**



**Responsible Office: Code Q/Safety and Mission Assurance Directorate**

# Subject: GRC Risk Management w/Change 1 (10/01/2024)

## TABLE OF CONTENTS

---

**Distribution: BMS Library**

# PREFACE

## P.1 PURPOSE

a. This GLPR defines the responsibilities, requirements, and a common framework for identifying, analyzing, communicating, and managing institutional and program/project risks, including the interface between Glenn Research Center (GRC), Enterprise Offices and resident Programs/Projects.

b. The goal is to effectively manage Center risks and increase the potential for achieving GRC's goals and objectives by minimizing potential future liabilities for the Center.

## P.2 APPLICABILITY

a. This GLPR is applicable to all organizations at GRC Lewis Field and Neil A. Armstrong Test Facility, and all levels of programs/projects assigned to GRC. Mission support organizations may establish their own implementation plans if they meet the requirements specified in this document. Mission direct organizations engage resident program and project risk management processes in addition to the GRC Risk Management (RM) process. This document does not supersede GRC resident programs that have developed their own Risk Management Plan (RMP).

b. This directive is applicable to documents developed or revised after the effective date of this document.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The term "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. In this directive, all document citations are assumed to be the latest version, unless otherwise noted.

## P.3 AUTHORITY

a. NASA Procedural Requirements (NPR) 8000.4, Agency Risk Management Procedural Requirements

b. NPR 8715.1, NASA Safety and Health Programs

## P.4 APPLICABLE DOCUMENTS AND FORMS

a. Federal Acquisition Regulation (FAR), Parts 7 and 15, and NASA Federal Acquisition Regulation Supplement (NFS), Parts 1807 and 1815

b. NASA Policy Directive (NPD) 1000.5, Policy for NASA Acquisition

c. NPD 1200.1, NASA Internal Control

d. NPR 7120.5, NASA Space Flight Program and Project Management Requirements

e. NPR 7120.7, NASA Information and Institutional Infrastructure Program and Project Management Requirements

f. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

g. NPR 7123.1, NASA Systems Engineering Processes and Requirements

h. GLPR 1280.1, GRC Quality Manual

i. Glenn Charter (GLC)-SMB-FRCWG-8000.4, Functional Risk Coordinators Working Group Charter

j. Glenn Plan (GLP) 1120.1, Technical Authority Implementation Plan

k. Glenn Procedure (GLP)-Q-1280.2, Corrective and Preventive Action

l. Glenn Work Instruction (GLWI)-QB-9980.1, Internal Audit

## P.5 MEASUREMENT/VERIFICATION

a. The Safety and Mission Assurance (SMA) Directorate will monitor compliance to this document through internal and external audits prescribed in GLPR 1280.1. The GRC risk manager will utilize the results of internal assessments to determine the effectiveness of this procedure.

b. The RM is consistent with internal control activities defined in NPD 1200.1.

c. The RM is conducted in accordance with NPR 8000.4.

## P.6 CANCELLATION

This document cancels GLPR 8000.4A, Risk Management w/Change 3 (12/01/2021), dated March 6, 2016.

***Electronic Signature on file.***

Laurence A. Sivic
Associate Director

# CHAPTER 1: Introduction – Risk Management

## 1.1 Overview

1.1.1 Risk Management (RM) is a deliberative, systematic process to analyze and communicate the risk of performance shortfalls. This process involves development of risk handling and mitigation options and implementation of approved strategies to reduce or eliminate the likelihood of occurrence and/or severity of consequence. Risk indicates a potential threat to the ability to meet performance objectives with adverse consequences to health/safety/environment, technical performance, Center/Agency capabilities, cost, or schedule.

1.1.2 The overall RM process includes two key components that are used iteratively: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM). The RIDM component supports decision making at each management tier by applying quantitative and qualitative risk information to achieve requirements. Then, CRM is applied to facilitate implementation of the requirements.

1.1.3 This approach is consistent with the Agency RM procedures and will provide insight to address technical, management, and business challenges and opportunities at the Center

## 1.2 Risk-Informed Decision Making (RIDM)

1.2.1 As prescribed by the Agency Risk Management Procedural Requirements (NPR 8000.4), when a threat is identified, initiate this process to formulate a mitigation strategy using the following steps:

a. **Identify decision alternatives**: Consider challenges and opportunities based on stated objectives.

b. **Analyze alternatives**: Apply subject matter expertise across disciplines as needed to bound risk scenarios, integrate all key drivers and impacts, and consider performance measures.

c. **Select an option**: After a deliberative review *informed* by risk analysis results, select a decision alternative and develop risk mitigation strategies.

1.2.2 This approach is particularly useful when a threat entails high stakes, complexity, uncertainty, multiple attributes or competing objectives, or a diverse range of stakeholders (refer to Chapter 3 for more details).

## 1.3 Continuous Risk Management

1.3.1 As prescribed by NPR 8000.4, implement the mitigation strategy using the following key steps (refer to Chapter 3 for more details):

a. **Identify:** State the risk in terms of an existing condition that may lead to degraded performance and capture the risk context, including key drivers.

b. **Analyze:** Perform quantitative/qualitative assessments to determine risk likelihood (probability) and severity of consequences (impact of degraded performance). Consider the timeframe for action. Consider grouping with similar or related risks and prioritize.

c. **Plan:** Assign a risk owner and develop a mitigation plan (handling strategy). The level of mitigation should be commensurate with the threat complexity and end goal.

d. **Track:** Acquire/update, compile, analyze, and organize risk data and report tracking results. Verify and validate mitigation actions over time.

e. **Control:** Analyze tracking results and decide how to proceed (e.g., re-plan, close the risk, invoke contingency plans, or watch). Execute the risk control decisions.

f. **Communicate and Document:** Report status and request direction or concurrence at the appropriate decision level. Document supporting information to track details, plans, progress, and risk decisions.

1.3.2 Application of RIDM and CRM uses a graded approach, which means the level of risk mitigation and prioritization should be commensurate with the complexity of the risk or severity of consequence if a risk is realized. These factors dictate the rigor applied to make a risk-informed decision (see Figure 1-1).

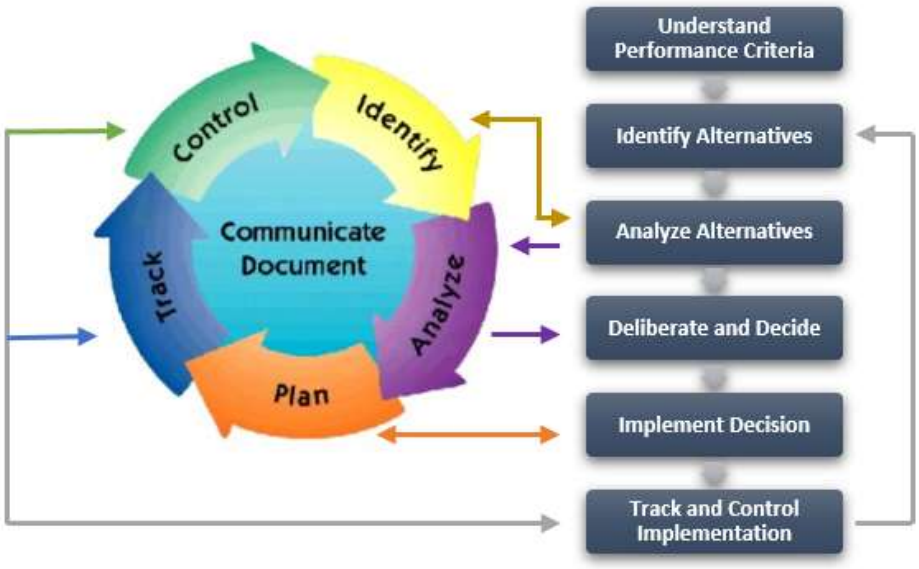



Figure 1-1 RIDM-CRM Risk Management Process Flow

## 1.4 Potential Risk Sources

Potential adverse impacts that affect GRC capabilities and resources necessary for mission success constitute institutional risks. Identify potential risks by reviewing requirements,

products, or services needed to execute a planned mission/process. The following are examples of areas where institutional risks may be identified:

a. Budget/Finance

b. Core Capabilities/Infrastructure – Workforce, Facilities, Information Technology

c. Health, Safety, and Environment (HSE)

d. Security

e. Program/Project Institutional Support

f. Processes/Operations

g. Acquisition

h. Agreements and Commitments (Internal/External Stakeholders)

i. Outreach

j. Knowledge Capture

k. Contractor/Vendor capability

l. Transition Planning

# CHAPTER 2: Responsibilities

## 2.1 Center Director

The Center Director is responsible for the Center RM process. Primary responsibilities shall include:

a. Reviewing recommendations for top Center risks to approve or request further details.

b. Allocating resources using risk-based information

c. Providing final approval on risk closure or risk acceptance rationale for top Center risks. Remain accountable for risk acceptance decisions for GRC institutional activities.

d. Determining escalation of top/Center risks with high safety consequences to NASA Office of Safety and Mission Assurance (OSMA) for resident program/project and institutional risks.

e. Determining top institutional risks which warrants escalation, insight, or awareness to Headquarters/Enterprise offices.

## 2.2 Center Risk Board

The Deputy Center Director and Associate Director co-chair the Center Risk Board. Primary responsibilities shall include:

a. Evaluating escalated risks to determine if a special board meeting is needed.

b. Reviewing recommendations for Center risks to approve or request further details.

c. Allocating resources using risk-based information.

d. Providing final approval on risk closure or risk acceptance rationale for Center risks. Provide Center Director risk acceptance decisions for GRC institutional activities.

e. Providing Center Director recommendations for escalating top/Center risks with high safety consequences to NASA OSMA for resident program/project and institutional risks.

f. Providing Center Director recommendations for top institutional risks which warrants escalation, insight, or awareness to Headquarters/Enterprise offices.

g. Approval of Center Risk Management Working Group (CRMWG) membership.

## 2.3 GRC Governance Councils

The GRC Governance Councils Chairs shall:

a. Provide oversight and review the status of RM efforts.

b. Provide decision points and/or resources to mitigate top risks.

c. Review recommendations for top institutional/resident program/project risks to approve or request further details.

d. Escalate top institutional/resident program/project risks to the Center Risk Board and/or Strategic Advisory Council (SAC), as required.

e. Provide approval on risk acceptance or closure rationale for top Center risks escalated to the governance councils. Escalate to the appropriate decision authority as required.

## 2.4 Safety and Mission Assurance Directorate (SMAD)

The SMAD is the GRC risk management process owner and responsibilities shall include:

a. Developing, maintaining, and improving the GRC RM plan/process/tools.

b. Providing consultation, facilitation, formal RM training (i.e., RIDM, CRM, risk-based acquisition management) and coursework to support implementation of the GRC RM process (refer to section 2.9).

c. Appointing the Center Risk Manager.

d. Utilizing the CRMWG to assist with implementation and improvement of the RM process.

e. Utilizing the SMAD Institutional Safety Authority and Technical Authorities (TAs), to conduct an independent assessment of the safety consequence of each risk escalated to the Center Risk Board.

## 2.5 GRC Directorates

The GRC Directors Of shall implement the RM process to identify and analyze risks to directorate-level performance for risk-inform decision making. Responsibilities shall include:

a. Identifying directorate risk information using procedures in Chapter 3 of this document.

b. Ensuring risks are identified, analyzed, and measured based on documented performance requirement of the owning organization.

c. Assign a properly empowered Directorate Risk Coordinator and participant in the CRMWG which meets membership criteria. (Refer to Appendix I)

d. Communicating Center escalation criteria to their Directorate management team, in coordination with the Directorate Risk Coordinator.

e. Reporting as soon as practical significant high yellow or red risks that are a threat to life, safety, or property without the resources to fix it. (Refer to Appendix D)

f. Maintaining/tracking risks via a database.

g. Defining escalation thresholds to be applied by lower-level organizational units when reporting to the Directorate (refer to Section 3.6.4).

h. Identifying directorate owned cross-cutting risks and interdependencies. Integrate risk discussions with stakeholders and other potential organizations impacted.

i. Coordinating potential cost risks with the resource analyst responsible for the identified function or task area.

j. Coordinating with the Office of Chief Financial Officer (OCFO) to ensure institutional risks are monetized and captured.

k. Coordinating risks with safety-related impacts with the appropriate Center and/or program representative for safety and mission assurance.

l. Ensure assigned personnel within each organization are properly trained in RM.

m. Presenting organizational institutional risk(s) to the Mission Support Council (MSC), the Center Risk Board, and the Strategic Advisory Council (SAC).

n. Ensure risks are identified and managed throughout the acquisition life cycle in accordance with NPR 8000.4 and NPD 1000.5.

o. Ensuring dissenting opinions expressed during risk decision making at each management level are handled through the formal dissent process (refer to paragraph 3.11).

## 2.6 Branch/Division/Offices

The GRC Chiefs shall implement the RM process to identify and analyze institutional risks to organizational-level performance for risk-inform decision making. Responsibilities include:

a. Facilitating risk discussions with organization personnel or risk facilitators. This is an iterative process between the branch and division.

b. Identifying potential risks per directorate and Center guidelines, perform risk analysis using procedures in Chapter 3 of this document.

c. Documenting risk (risk statement, context, mitigation strategy, likelihood, consequence) and capture common risks or trends.

d. Determining if the risk impacts others. Integrate risk discussion with stakeholders and other potential organizations with impact. Utilize existing risk boards for integrating functions across organizations.

e. Immediately report high yellow or red risks that are a threat to life, safety, or property without the resources to fix it, to the Directors Of.

f. Reporting candidate risk(s) and organizational risk summary list to the next management level.

g. Determining if the risk(s) meet reporting criteria per Center or Directorate escalation criteria, report accordingly.

h. Performing continuous risk management within the organization.

## 2.7 Mission Support Enterprise Organizations (MSEO)

The MSEO management shall implement the RM process to identify and analyze to Enterprise-level performance for risk-inform decision making. Responsibilities include:

a. The RM procedure for MSEO organizations to identify Enterprise impacts to the Center:

(1) The local GRC lead for MSEO organization monitors Enterprise portfolio for risks that directly or indirectly impacts the Center.

(2) At a minimum on a quarterly cadence, the local GRC lead for the MSEO organization identifies and compiles relevant enterprise risks.

(3) When Enterprise risk criteria/format differ from GRC, the local GRC lead for MSEO organization translates to GRC criteria/content.

(4) Use local GRC process for risk escalation and awareness to report risk through Center channels. If the risk(s) warrants Center advocacy or awareness the risk report is presented to the Directorate and the Directorate Risk Coordinator.

(5) The GRC will utilize the Agency Baseline Performance Review (BPR) as the preferred forum for risk requiring escalation to Agency leadership.

b. The RM procedure for Center Directorates to identify MSEO Center impacts to the Enterprise:

(1) Facilitate risk discussion with organization personnel.

(2) Identify potential risk per MSEO organization's risk management process.

(3) Document risk (risk statement, context, mitigation strategy, likelihood, consequence)

(4) Local GRC lead for MSEO organization identifies portion of local risk portfolio reported through MSEO channels to Enterprise leadership. If the risk(s) warrants Center advocacy or awareness the risk report is presented to the Directorate and the Directorate Risk Coordinator.

(5) Local GRC Lead for MSEO organization will provide the Center Risk Board awareness of risk(s) submitted through MSEO channels to Enterprise leadership.

(6) When Enterprise MSEO leadership identifies GRC risk for escalation to the Agency leadership the local GRC lead for the MSEO organization will formally notify the Center Risk Board.

(7) The GRC Center leadership will utilize the Agency BPR as the preferred forum to identify significant Center risks and issues to Agency leadership.

c. Perform continuous risk management within the organization.

## 2.8 Center Risk Manager

The Center Risk Manager shall implement the Center RM approach and procedures, including:

a. Establishing, monitoring, analyzing, and implementing this directive in accordance with the NPR 8000.4.

b. Collaborating with Center Risk Board Chairs and Center Management to ensure effective implementation of the Center risk management program.

c. Maintaining the GRC Risk Scorecard for organizations to assess the severity of institutional risks. (See Appendix C)

d. Chairing the GRC Center Risk Management Working Group (CRMWG).

e. Providing Directorate Risk Coordinators with consultation, facilitation, and informal training to support implementation of the GRC RM process. Formal RM training (i.e., RIDM, CRM and risk-based acquisition management) and coursework is provided by the Director, Safety and Mission Assurance via risk facilitators (See Section 2.12).

f. Collaborating with the OCFO to ensure institutional risks are monetized and captured.

g. Collaborating with directorate risk coordinators and resident program/project managers to identify risks or processes with potential cross-cutting impacts.

h. Providing integrated institutional risk data and reporting executive summaries to the MSC/Center Risk Board/SAC.

i. Acquiring the SMAD Institutional Safety Authority and TAs safety consequence assessment for each escalated Center risk.

j. Submitting a quarterly report of escalated Center risks with high safety consequences to NASA OSMA.

## 2.9 Directorate Risk Coordinators

The Directorate Risk Coordinators are appointed by their Directors, and shall perform the following functions:

a. Assuring applicable personnel (both government and support service contractors) within the organizational element are provided proper RM training.

b. Facilitating risk discussions and meetings at the directorate level.

c. Assisting directorate personnel in the development of risk information (identify risks, formulate risk statements, define mitigation plans, etc.).

d. Participating in the CRMWG monthly meetings.

e. Use Center Risk Board presentation templates for reporting center and directorate managed risks.

f. Submitting a status of escalated Directorate/Center risks to the CRMWG and Center Risk Manager to support recommended options and the decision-making process.

## 2.10 GRC Center Risk Management Working Group (CRMWG)

The CRMWG is a body of representatives from each GRC directorate which is chaired by the Center Risk Manager to ensure consistent implementation of the RM processes. The CRMWG shall:

a. Aid in establishing and maintaining current GRC RM policy, procedures, and tools.

b. Review institutional risks with respect to GRC commitments, resource requests, potential solutions, and proposed escalation to the top Center risk level.

c. Collaborate on procedures and criteria for prioritizing the top Center risks to support risk decision making.

d. Assure risk information is provided by the appropriate subject matter expert for each top Center risk to properly support recommended options and the decision-making process.

## 2.11 Resident Program/Project Managers

The risk managers for resident GRC programs/projects collaborate with the Center Risk Manager to identify cross-cutting risks (i.e., bidirectional threats). The program/project risk managers or representatives participate in the GRC CRMWG, as needed to address cross-cutting risks or processes.

## 2.12 Risk Facilitators

A risk facilitator may be needed to support the RM activities by planning, organizing, directing, and providing expertise for CRM implementation within GRC. Duties shall include:

a. Providing ongoing RM consultation and facilitation to assigned GRC programs, projects, and organizations.

b. Ensuring applicable personnel utilize risk-based, decision-making to continuously manage acquisition, safety, technical, and programmatic risks.

c. Assisting with RMPs development and implementation.

d. Assisting with the likelihood, consequences, and timeframe definitions when there is no governing RMP.

e. Ensuring risk statements are written in a “condition; consequence” format.

f. Providing guidance for estimating the risk likelihood, consequences, and timeframe.

g. Reviewing mitigation plans to ensure they will reduce the risk likelihood/consequences.

h. Assuring risk owners track their risks and monitoring risk closures/acceptances.

i. Assuring risk information is documented and maintaining the associated risk list.

j. Reviewing accepted and closed risks minimally every six months to ensure conditions/assumptions have not changed.

k. Assuring applicable personnel are given formal RM training (i.e., RIDM, CRM, risk-based acquisition management) and conducting periodic risk identification forums.

l. Integrating risks internally and externally with the appropriate stakeholders.

m. Assessing the RM process effectiveness for programs/projects/organizations and providing improvement recommendations.

# CHAPTER 3: Risk Management Process

## 3.0 Risk Management

Risk is a potential threat with sufficient information to indicate a negative consequence when measured against a HSE, center capabilities, technical, cost, or schedule performance objective. Risk is also the potential inability to fully implement agreements with NASA stakeholders or partners (commercial, governmental, academic, or international). Resolution requires focused management attention.

## 3.1 Risk Identification

3.1.1 The RM begins with identification of a perceived shortfall against a performance objective, including key drivers and impacts.

3.1.2 Potential risks shall be identified based on a condition, event, or review of requirements, products, and services needed to execute a planned mission or to comply with a Federal mandate. Emphasis is on early identification of potential risks related to: HSE, technical performance, Center capabilities (infrastructure, personnel), and cost or schedule threats. Risks also may be identified when implementing corrective or preventative actions (GLP-Q-1280.2).

3.1.3 Examples of key considerations for a risk include:

a. Funding requirements and priority: Likelihood of budget shortfall and rationale; impact if not funded (e.g., reduced scope, impact to internal/external stakeholders); risk buy-down that would be achieved with full or incremental funding.

b. Cross-cutting risks: A risk-owning organization has primary risk impact but based on potential risk handling/disposition and mitigation timeframe, consequences also may impact one or more NASA organizations or external stakeholders.

c. Center/Agency capabilities: Infrastructure and resources as required for achievement of institutional objectives and Program/Project support requirements.

d. Transition planning: Requirements for changing Agency or Center conditions or objectives.

3.1.4 An identified risk is documented in a risk statement in the following format: “Given the [condition], there is a possibility of [departure] adversely impacting [asset], thereby leading to [consequence].” The condition must be a fact, short and concise.

3.1.5 A candidate risk with information that is insufficient or immature to analyze or define mitigation options, may be captured as a concern. Concerns may be managed internally within existing resources and processes. Concerns need to be watched to determine if they become risks. Once a concern is vetted and more information is available, it may be elevated to a candidate risk.

*Note: A concern is an uneasy state of blended interest, uncertainty, and apprehension. It may be appropriate for organizations to list and discuss concerns as a means of communicating potential candidate risks.*

3.1.6 Once a candidate risk is validated by the governing risk review body, the next activity involves writing the risk context or documenting additional information regarding the circumstances, events, and interrelationships that may affect the risk. The additional information (such as who, what, when, where, how, and why) about the risk ensures that the original intent of the risk can be easily understood by other personnel, particularly after time has passed.

## 3.2. Identification and Handling of Cross-Cutting Risks

3.2.1 Risks with impact to multiple organizations are cross-cutting risks. Branch, Division, Office, and Project Review Board personnel are expected to integrate risk discussion with stakeholders and other potential organizations with impacts, utilizing existing risk boards for integrating functions across organizations. Since each organization is represented on the management councils, there is also an opportunity to hear risks presented and to identify impacts to each organization.

3.2.2 Ownership of the risk should be decided by one of three criteria:

a. Organization most severely impacted by the consequences of risk realization.

b. Organization most capable of reducing the risk.

c. Organization with the appropriate decision authority.

3.2.3 Based on the criteria considerations, the affected organizations determine which organization is chiefly responsible for managing the risk and assign a risk owner from within that organization.

*Note: A risk owner is the entity, usually an individual, designated as the lead overseeing the implementation of the agreed disposition of the risk.*

3.2.4 In consultation with the affected organizations, the risk owner will develop a mitigation plan to handle the risk. This includes prioritizing the requirements at stake and the resources available. All affected organizations may execute specific steps in the handling plan.

## 3.3 Risk Based Acquisition Management

3.3.1 Procurement risks shall be tracked as part of the acquisition approach, which is developed by the procurement team in conjunction with the statement of work that reflects the Government's acquisition approach. Any open risks, at the close of the procurement phase, shall be transferred to the project manager.

3.3.2 Consider procurement risks during the following activities: acquisition, formulation, implementation, strategy/requirements development, solicitation instructions, evaluation of proposals, source selections, surveillance planning, and post-award contract monitoring.

3.3.3 The FAR Parts 7 and 15, and NFS Parts 1807 and 1815, provide acquisition/contract RM requirements; further details are in NPR 8000.4.

## 3.4 Risk Analysis

Risks shall be analyzed to determine likelihood of occurrence and impact to the performance objective. In accordance with RIDM-CRM principles (NPR 8000.4), the risk analysis steps are as follows:

a. **Evaluate risk data**. Identify and assess the impact from each risk contributor, including consideration of any inherent uncertainty.

b. **Perform quantitative and/or qualitative analysis**. Assess risk consequences (degraded performance, loss of function, key milestone slip, personal injury, cost escalation, etc.).

(1) Quantitative risk analyses are preferred and shall be applied to the maximum extent practical. Use of quantified analysis is based on scope of the decision to be made and similarities among suitable alternatives (graded approach).

(2) Select one or more analysis methodologies for each consequence, for example:

(a) Analysis of historical data (similarity).

(b) Probabilistic risk assessments or other quantitative analyses.

(c) Maintenance/repair/replacement cost estimates.

c. **Determine the risk cost threat**. Identify all constraints and thresholds.

(1) Include the cost threat for all applicable fiscal years.

(2) Identify the Most Likely Cost (MLC), i.e., minimum incremental need.

(3) Constrain assessment of risk consequences to the current Planning, Programming, Budgeting, and Execution (PPBE) period to provide a consistent frame of reference.

d. **Determine risk likelihood and severity of consequence(s)**. Map risk assessment results to the descriptions listed on the GRC Risk Scorecard (refer to Appendix C) or to the governing program/project RMP (see Section 3.9).

(1) For example, consider the duration of the risk, available mitigation options, and impact on key stakeholders. Determination of the likelihood rating may be by quantitative or qualitative analysis.

(2) Plot the highest value from the Likelihood (L) and Consequence (C) categories in the 5x5 risk matrix, where the numbers intersect determines the L x C score.

e. **Determine timeframe**. Identify the timeframe to initiate the handling strategy (i.e., near, mid, or long term). Timeframe is used in conjunction with the risk matrix score to determine risk priorities. For institutional risks, refer to the GRC Risk Scorecard in Appendix C.

Programs/projects should use the timeframe designated in the governing RMP or develop timeframe criteria based on the life of the program/project.

*Note: Timeframe is different than the schedule consequence.*

f. **Communicate the risk**. In the appropriate management forum, the risk owner shall periodically review and update risk status, validate new concerns, review progress of mitigation plans, and determine if any risks require escalation to the next level. At the Center level, institutional risks will be reviewed at the MSC and joint CMC/MSC Center Risk Board with Center management.

g. **Immediately report risks that are a threat to life, safety, or property with a high yellow or red score and are without resources to fix it to the Director Of.** The Directors Of have an obligation to report these risks to the Center Director's Office, affected colleagues as soon as practical, and always including the Director of SMA and the Center Risk Manager. (See Appendix D)

(1) Generate email with a synopsis of the situation, the risk itself, and the proposed way forward (i.e., monitoring, mitigation, impact).

(2) If urgent, a text/phone call is an option. Document the discussion or agreement from phone call and submit via email.

h. **Document risks** in a database, including expected likelihood and consequence, scoring and escalation rationale, along with key assumptions.

## 3.5 Risk Documentation

3.5.1 Documentation is crucial to the success of managing risks. This process ensures that RM policies are established, understood, implemented, and maintained. It also develops an audit trail to identify the origin and rationale for all risk-related decisions.

3.5.2 The RM documentation should be readily accessible to the entire team and under configuration control. Types of documentation include the risk database, risk reporting, a RM plan/charter, and the top center risk list.

3.5.3 As risks are identified and mitigation strategies developed, the organization/project shall document the risk with the following information, as a minimum:

a. Risk Title

b. Risk Owner

c. Risk Statement

d. Likelihood x Consequence (L x C) Score and Rationale

e. Risk Description (context)

f. Impact/Consequences

g. Estimated Completion Date (ECD) and Criteria for Risk Closure or Acceptance

h. Current Status

i. Handling Strategy and Task Mitigation Steps with ECD

j. Most Likely Cost Impact, if known

3.5.4 Risks should be classified or grouped based on shared characteristics to help understand the nature of the risks and build cost-effective mitigation plans. Duplicate risks identified can be grouped as either parent-child or an aggregate risk. Risks are considered an aggregate risk when they are related, but not in a parent-child or hierarchy relationship.

a. Parent-child risks - Group the risks hierarchically with a parent risk statement summarizing the children or minor risks. Include the overall mitigation plan and key tasks in the parent risk. Capture the detailed mitigation tasks in the child risks. The context from each child risk is included with the parent risk. Assign the likelihood, consequence, and timeframe attributes to the parent risk. The parent risk cannot be closed until the child risks are closed, accepted, or separated and tracked individually.

b. Aggregate risk - A cumulative risk associated with a given goal, objective, or performance measure, accounting for all significant risk contributors. For example, several organizations have a similar risk on the same topic. An aggregate risk is constructed to include all viewpoints from the risk owners; one risk owner/organization is selected to represent the aggregate risk.

3.5.5 Risk Database

There is no requirement on where risks are maintained. However, for configuration management and for promoting teamwork, the risks shall be in a database, where all team members have access. The Program and Project Assurance Division developed a web-based Risk Management Implementation Tool (RMIT) to implement the NASA CRM process with flexible reporting formats. Resident programs/projects and organizations can use RMIT to manage risks and make risk-informed decisions in an environment tailored to their requirements.

> *Note: Access to RMIT (https://rmit.grc.nasa.gov) is requested via NASA Access Management Systems.*

## 3.6 Planning (Handling Strategy)

3.6.1 Risk planning involves translating risk information into decisions and mitigating actions (both present and future) to implement. Risks are planned in order of importance by those who have the knowledge, expertise, background, and resources to effectively deal with the risks.

3.6.2 The organization/project shall determine a plan of action for each risk, referred to as the handling strategy. Pairing likelihood of occurrence with the highest impact rating yields a relative characterization of severity, a key consideration when selecting a strategy:

a. **High Risk** – Expected to occur with severe impacts, if realized; denoted in the upper right-hand (red) region of the GRC Risk Scorecard.

b. **Moderate Risk** – May occur and impacts would be significant, but not catastrophic; denoted in the middle (yellow) region of the GRC Risk Scorecard.

c. **Low Risk** – Not likely to occur or potential impacts are not expected to be significant; denoted in the lower left-hand (green) region of the GRC Risk Scorecard.

3.6.3 Options for Handling Strategy

The intent of a handling strategy is to minimize the L x C over time. However, the option to "Do Nothing" should be addressed first. Then, the preferred strategy and supporting data are approved at the appropriate management level. Options include:

a. **Research** – Consider and review all pertinent information sources to understand the risk. Research ends when enough information has been gathered to determine the severity of the risk (likelihood and consequences).

b. **Watch** – For risks where circumstances do not warrant immediate mitigation steps, define triggers that indicate the need for action. Include a timeframe for re-evaluation and active mitigation or alternate handling strategies. These risks can be placed on the watch list where each risk should be periodically reassessed every 6 months.

*Note: Risks can be watched if the severity is assessed as low, sufficient mitigation resources are not available, or the cost of mitigation is comparable to recovery costs if the risk were to occur.*

c. **Mitigate** – If "do nothing" is not acceptable, develop a mitigation strategy to measurably reduce the L x C. Specify the mitigation ECDs, resulting L x C score and rationale, and success criteria. The goal is to minimize risks to the lowest practical level within the allocated resources.

*Note: Mitigation plans maximizes opportunity and value by reducing the consequences, reducing the likelihood of occurrence, or shifting the time-interval of when the risk will occur.*

d. **Accept** – If the consequences are tolerable should the risk occur, or no further resources will be expended to mitigate residual risk, a risk owner may recommend ceasing active mitigation to include key assumptions and conditions on which the decision to accept will be based. Periodically assess for changing conditions (minimum of every 6 months).

*Note 1: Refer to section 3.8.1.f for approval authority requirements.*

*Note 2: Accepted risks could potentially be re-opened or closed based on the periodic reviews.*

3.6.4 Risk Escalation

3.6.4.1 Risk owners shall perform due diligence to understand the risk scoring rationale, ranking, and escalation. The decision authority determines if a risk requires escalation to the next level. Reasons for escalation may include:

a. Additional resources are needed to mitigate the risk.

b. Direction or awareness is needed from the next level of management.

c. Transferring the decision/management of a risk to a higher organization level.

d. Emerging risks with the potential of affecting multi-directorates or have Center-level impact.

e. External integration is required (i.e., with other orgs/programs/projects/Centers).

f. The risk has cross-cutting significance with other organizations/stakeholders.

g. Potential risk transfer to another organization.

3.6.4.2 Escalation shall reflect the hierarchical level of insight or control of resources needed throughout the life cycle. Each successive tier in the organization shall review its risks periodically and determine if escalation or de-escalation is required (refer to Figure 3-1). The following levels are defined to support the Center's institutional escalation process:

a. Top/Center Risk – Requires Center management resources or direction to resolve; could have cross-cutting impacts that affect two or more GRC organizations. Top Center risks reside at the SAC, and Center risks reside at the Center Risk Board.

b. Multi-Directorate Risk – Requires coordination between the owning organization/directorate and any affected organizations/directorates. Affects two or more directorates within the Center.

c. Directorate Risk – Requires directorate management direction and/or resources to resolve; affects one or more divisions within the Directorate.

d. Organizational Risk – Requires division management direction and/or resources to resolve; affects one or more sub-organizations.


Figure 3.1 – GRC Institutional Risk Management Hierarchy

3.6.4.3 To escalate or de-escalate, the risk is assessed by the directorate/project that a valid reason exists for the proposed change. The proposed risk is presented to appropriate management level for approval of content, resource requirements, and priority ranking. The review should determine if escalation or de-escalation is required. The risk owner changes the risk level designation in the risk management database. Proposed Center risks are reviewed by the GRC CRMWG (institutional), and project review board (programmatic). As escalated, risk scores may change to reflect the significance of the impact at the next level. (Refer to Appendix E)

3.6.4.4 For Center organizations with top program risks requiring program management direction and resources to resolve, escalate risks via the program's risk review process. Coordinate any cross-cutting risks with all affected Center organizations, including reporting at the CMC for coordination, awareness, or a decision.

3.6.4.5 An independent safety consequence assessment of each escalated Center risk is conducted by the SMAD Institutional Safety Authority and TAs. If the independent assessment identifies different safety consequence scores than the directorate's/project's, no changes will be made to the risk's composite consequence score. The SMAD TA will present the independent assessment at the MSC, Center Risk Board and SAC.

## 3.7 Risk Tracking

3.7.1 Tracking is a process for acquiring, organizing, and analyzing risk data/trends to determine implementation progress and cumulative effects of risk management decisions. Risks identified for mitigation, research, watch, and accept, are tracked to ensure conditions or assumptions did not change, thus requiring reevaluation.

3.7.2 The risk owner shall track risk attributes over the risk life cycle to determine if:

a. Mitigation steps are performed in a timely manner.

b. Steps taken are effectively managing the risk. The owner tracks observable data related to performance measures such as cost/schedule variance or changing conditions.

3.7.3 The organization/project track and update risks on a recurring basis to reflect status and progress and use the results to communicate risk status and information (quantitative or qualitative) as required for effective control and management decisions.

## 3.8 Risk Control

3.8.1 The risk control function is to assess and verify that the mitigation plan is effectively reducing the L x C threat. Based on analysis of tracking data, types of control decisions may include:

a. **Continue as planned** – Progress is satisfactory (as expected).

b. **Re-plan** – Mitigation is not achieving the desired outcome or conditions have changed.

c. **Invoke a contingency plan** – If the current plan proves inadequate, an alternative is developed, approved, and implemented.

*Note: A contingency is reserves, including funding, schedule, technical performance, workforce, and services, allocated to and managed by an organization or program/project manager for the resolution of problems normally encountered to mitigate risks.*

d. **Close** – To close a risk, rationale must be approved at the appropriate management level to demonstrate one of the following:

(1) the risk has been eliminated,

(2) residual risk is negligible such that further steps are unnecessary,

(3) the threat has been subsumed by a new risk,

(4) the risk has become a problem and is now tracked as such.

e. **Transfer** – Transfers generally occur if a risk was identified outside of the primary affected organization or due to a change in either organizational responsibilities or control of resources. Transfers must be mutually agreed upon by the affected parties.

f. **Accept** – To accept a risk requires the risk owner/organization to perform a serial review and approval outlined in the steps below. Utilize existing risk boards for integrating functions across organizations.

(1) Rationale must be approved first by the owning organization and then key stakeholders demonstrating one of the following criterion:

(a) Further mitigation is not cost-effective.

(b) The consequences of an identified risk, should they occur, are acceptable without further mitigation.

(2) Safety/mission success risks require the formally delegated Institutional Safety and/or Technical Authorities (safety, engineering, health, medical) to:

(a) Provide concurrence in the soundness of technical cases in acceptance of risk to safety or mission success.

(b) Concurrence that risk decisions are within the authority of the organizational unit manager.

(c) Concurrence that a risk is acceptable (per NPD 1000.0).

(3) Risk acceptance requires approval from the highest level of escalation (refer to section 3.6.4); provide rationale including objective evidence that the key stakeholders and IA/TAs as required gave their concurrence. Utilize special considerations for determining risk acceptance decision authorities for the following risk types:

(a) *Aggregate risks* – For aggregate risk considerations, the risk acceptability criterion is applied to determine the decision authority to accept individual risks.

(b) *Institutional risks* - Depending on the nature of institutional risks, it can require the Center Director's concurrence. The Center Director is accountable for institutional risk acceptance decisions. The Center Risk Board and CMC chairs will determine when to elevate risk acceptance to the Center Director.

3.8.2 Directorates and projects must review accepted risks periodically (minimum of every 6 months) to ensure conditions/assumptions have not changed. Accepted risks could potentially be re-opened or closed based on the periodic reviews.

3.8.3 Collaboration with GRC organizations is essential for incorporating RM into the Center management decision-making process. Risks are a key input to the process and reflect specific challenges to meeting commitments. Recommendations for resource allocation take into consideration the trade-offs between finite resources and prioritized risks.

## 3.9 Risk Management Plan (RMP)

3.9.1 A RMP formally defines and establishes an organization's approach and strategy for risk management, including organizational structure, relationships, and responsibilities for managing risk; process guidelines/policies, metrics, and tools for executing and communicating an integrated RM methodology.

3.9.2 The RMP may supplement a program plan, as applicable. Programs and projects should follow their governing RM plan. If there is no governing RMP, a plan should be written to meet NPR 8000.4 requirements; the RMP can be included in the project plan or the systems engineering plan (NPR 7120.5; NPR 7120.7; NPR 7120.8; NPR 7123.1).

3.9.3 Directorates and lower-level organizations may establish their own RMP if they meet the intent of this document.

## 3.10 Reports and Recommendations

3.10.1 Relevant risks recommended and prioritized as top/Center risks or proposed Center risks are reviewed at the Center Risk Board (institutional) or Project Review Board and CMC (programmatic). Risks may be referred to the SAC for disposition, as required for decision, resources, or in the case of a dissenting opinion (refer to section 3.11). Summary reports are generated and presented based on risk information in directorate and program risk databases. Recommendations may derive from related Agency, Center, Directorate, and program risk review forums.

## 3.11 Process for Handling Formal Dissent

Resolution for dissenting opinions of any nature (e.g., programmatic, safety, engineering, acquisition, accounting, etc.) are handled per GLP 1120.1 when an individual deems it to be of

sufficient importance to warrant a specific review and decision by higher-level management. An open discussion occurs in an environment of integrity and trust with no suppression or retribution. Elevation of a formal dissent is performed at the discretion of the dissenting party. If the dissenting party is not satisfied with the process or the review outcome, he/she can appeal to the next level of authority (refer to Appendix F).

# Appendix A: Definitions

**Aggregate Risk**. The cumulative risk associated with a given goal, objective, or performance measure accounting for all significant risk contributors. For example, several organizations have a similar risk on the same topic. A risk is then constructed to include all risk owners' viewpoints, and one risk owner/organization is selected to represent the aggregate risk.

**Candidate Risk**. A potential risk that has been identified and is pending adjudication by the affected programmatic or institutional authority. Once validated, it becomes a formal risk.

**Close**. A validated risk that is no longer a risk to the organization or program/project. The risk is no longer cost-effective to track because the likelihood is low, or the associated consequence is low.

**Concern**. A candidate risk with insufficient or immature information to analyze or define mitigation options.

**Contingency**. A provision for an unpredictable future event or circumstance, designed to help effectively resolve or decrease risk impacts. Reserves, including funding, schedule, performance, workforce, and services, allocated to and managed by an organization or Program/Project Manager.

**Continuous Risk Management (CRM)**. A systematic and iterative process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risks supporting informed decision-making.

**Cross-cutting Risk**. A risk with impact to multiple levels of an organization or in multiple organizations at the same level.

**Elevation.** 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.

**Emerging Risk**. Risks that an organization knows exist but are not well understood. Risks that meet the criterion of potentially affecting multi-directorates or having a Center-level impact are escalated to the Center Risk Board or CMC for awareness.

**Center Risk Management Working Group (CRMWG)**. A body of representatives from each GRC directorate, chaired by the Center Risk Manager, who seek to ensure consistent implementation of the CRM and risk management processes.

**Graded Approach.** Application of risk management processes at a level of detail and rigor that adds value without unnecessary expenditure of the organizational unit's resources. The resources and depth of analysis are commensurate with the stakes and complexity of the risk scenarios being addressed. *For example, the level of rigor needed in risk analysis to demonstrate satisfaction of safety-related performance requirements depends on specific characteristics of the situation: how stringent the requirements are, complexity and diversity of*

*hazards, and estimated uncertainties compared to operating margin. Both RIDM and CRM are formulated to allow for this.*

**Institutional Risks**. Potential shortfall against a performance objective related to infrastructure, information technology, resources, personnel, assets, processes, health, safety, environmental management or security that affect capabilities and resources necessary for mission success, including institutional flexibility to respond to changing mission needs and compliance with internal and external requirements (e.g., Environmental Protection Agency, Occupational Safety and Health Administration regulations).

**Mitigate**. Action(s) taken to eliminate or reduce the risk by reducing the consequences, likelihood, or delaying the projected time of occurrence (i.e. to allow time to mitigate, or beyond a time that impacts the tasks being performed). A mitigation plan documents the actions required to eliminate or reduce the risk and the supporting information such as actionees, estimated/actual completion dates, and success criteria.

**Parent-Child Risks**. Risks are grouped hierarchically with an overall top (parent) risk statement which summarizes the children or minor risks. The mitigation plan includes the key tasks entered in the parent risk, while detailed mitigation tasks are captured in the child risks.

**Problem**. An adverse situation that currently exists. A known problem may be a realized risk.

**Realized Risk.** An adverse situation that currently exists; there is no opportunity for avoidance. Contingency plans may be instituted to minimize the impact of the consequence. A realized risk may also be known as a problem.

**Research**. The investigation of a risk until there is enough information to support another disposition (i.e., close, watch, mitigate, accept or elevate).

**Residual Risk**. The risk remaining after all the mitigation steps have been implemented. The amount of remaining residual risk determines if it remains open, is accepted, or closed.

**Risk**. The potential for shortfalls to achieving explicitly established objectives; considering the probability of the undesired event and the consequences, impact, or severity if it occurred.

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

> *Note: This does not mean that a combination of individual risks is automatically acceptable in the aggregate; it is subject to aggregate risk considerations that the given unit has the authority to accept individual risks using this criterion.*

**Risk Acceptance.** 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 except periodic review (every six months) to ensure assumptions or circumstances have not changed. Accepting a risk requires approval by the governing decision authority.

> *Note: This process assigns accountability for each risk acceptance decision to a single responsible authoritative individual, rather than to a committee or group of individuals.*

**Risk Assessment Index (RAI).** Measure of relative risk determined by which region of the risk scorecard (high, moderate, or low) a risk falls, based on pairing of likelihood of occurrence with the highest consequence.

**Risk Analysis**. An evaluation of all identified risks to estimate the likelihood of occurrence, consequence of occurrence, timeframe when mitigation actions are needed, classification into sets of related risks, and priority ranking.

**Risk Control**. An activity that utilizes the status and tracking information to decide about a risk or risk mitigation effort, including resource allocation. Risk control is comprised of four decisions; continue as planned, replan, invoke a contingency plan, or close the risk.

**Risk Escalation.** The process of raising risk visibility by reporting the risk to a higher level in the organization, per the defined Center, directorate, or programmatic criteria. This action is to raise risk awareness, call attention to adverse changes, or request resources that are not available to handle the risk at the lower level. The risk would be escalated to one or more levels above the level at which it is owned and mitigated. Risk Ownership resides at the original level.

**Risk Identification.** A continuous effort to capture, acknowledge and document risks as found.

**Risk Informed Decision Making (RIDM)**. A process that uses a diverse set of performance measures (some of which are quantitative or model-based risk metrics) along with other considerations within a deliberative process to inform decision-making to establish baseline performance requirements for organizations, programs, and projects.

**Risk Management (RM)**. Coordinated flow of activities to identify, evaluate, and address risk with appropriate actions that combines RIDM and CRM in an integrated framework. This is done to foster proactive management of risk items, better inform decision-making through use of risk information, and then effectively manage implementation of risk-related activities and actions by focusing the CRM process on baseline performance requirements informed by the RIDM process.

**Risk Management Plan (RMP)**. A document that formally defines and establishes an organization's approach and strategy for risk management including organizational structure, relationships, and responsibilities for managing risk; process guidelines/policies, metrics, and tools for executing and communicating an integrated RM methodology; and the RM resource investments required.

**Risk Owner**. The individual who implements and tracks the risk mitigation approach and actions (the focal point for integrating all the risk information and ensuring adequate management and closure). The risk owner has oversight of the resources (budget and workforce) required to mitigate the risk, either by delegation or routine operations.

**Risk Planning (Handling Strategy)**. Establishes the proper course of action for dealing with a particular risk. The resulting actions are to research, watch, accept, or mitigate.

**Risk Review Boards/Panels**. Formally established groups of people assigned specifically to review risk information. The output is twofold: 1) Improve the management of risk and 2) Serve as an input to decision-making bodies in need of the risk information.

**Risk Tracking**. An activity to capture, compile, and report risk attributes and metrics to determine whether risks are being mitigated effectively and whether risk mitigation plans are being implemented correctly.

**Success Criteria**. The minimum set of measures that establish the accomplishment of predefined goals and objectives for risks mitigation activities.

**Technical Authorities (TA)**. Are formally delegated to ensure engineering, safety/mission assurance, and health communities have an independent, influential role in providing alternate perspectives during the decision-making process. TAs ensure technical thoroughness and rigor are applied, and formal dissents are fully considered.

**Threat.** Circumstance or event with potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of assets or information, and/or denial of service *[adapted from NIST-SP 800-30, Rev. 1, Guide for Conducting Risk Assessments].*

**Transfer.** The act of allocating authority, responsibility, and accountability for a risk to another person or organization with the consent of the intended recipient.

**Validate Risk**. The process of examining a candidate risk to verify that it has been written in such a way as to allow further analysis and that mitigation actions (if they exist) are within the scope of the organization, program, project, or task in question.

**Watch**. The monitoring of an identified risk and its attributes for early warning of critical changes in consequences, likelihood, timeframe, or other indications that might reveal a risk event is imminent.

**Watch List.** A list containing risks with a watch approach, where the reassessment of each risk should occur every 6 months. A metric is created for each risk to monitor the risk level or specific trigger indicating when conditions or attributes have changed. When exceeded, metric thresholds are set to trigger specific mitigation plans or a reevaluation of the risk.

# Appendix B: Acronyms

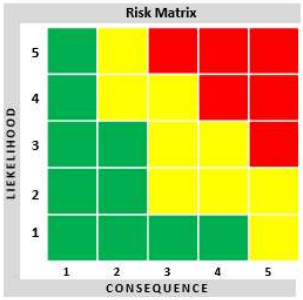
| | |
|---|---|
| BPR | Baseline Performance Review |
| CMC | Center Management Council |
| CRM | Continuous Risk Management |
| CRMWG | Center Risk Management Working Group |
| FAR | Federal Acquisition Regulation |
| GLC | Glenn Charter |
| GLP | Glenn Plan |
| GLPR | Glenn Procedural Requirements |
| GRC | Glenn Research Center |
| HSE | Health, Safety, Environmental |
| L x C | Likelihood versus Consequence |
| MLC | Most Likely Cost |
| MSC | Mission Support Council |
| MSEO | Mission Support Enterprise Organizations |
| NASA | National Aeronautics and Space Administration |
| NPD | NASA Policy Directive |
| NFS | NASA Federal Acquisition Regulation Supplement |
| NPR | NASA Procedural Requirements |
| OCFO | Office of Chief Financial Officer |
| OSMA | Office of Safety and Mission Assurance |
| RIDM | Risk-Informed Decision Making |
| RM | Risk Management |
| RMIT | Risk Management Implementation Tool |
| RMP | Risk Management Plan |
| SAC | Strategic Advisory Council |
| SMAD | Safety and Mission Assurance Directorate |
| SMB | Safety and Mission Assurance Management Board |
| TA | Technical Authorities |

# Appendix C: NASA Glenn Research Center Risk Scorecard

## GRC Risk Scorecard

| Likelihood Rating* | | | |
|---|---|---|---|
| 5x5 Rating | Rating | Qualitative | Quantitative |
| 5 | Very Likely | Expected to happen. Controls have minimal to no effect. | Greater than 90% |
| 4 | Likely | Likely to happen. Controls have significant limitations or uncertainties. | 60% to 90% |
| 3 | Possible | Could happen. Controls exist, with some limitations or uncertainties. | 40% to 59% |
| 2 | Unlikely | Not expected to happen. Controls have minor limitations or uncertainties. | 10% to 39% |
| 1 | Highly Unlikely | Extremely remote possibility that it will happen. Strong controls in place. | Less than 10% |

** Use Qualitative OR Quantitative analysis to determine the likelihood the situation or circumstance will occur.*




| Time Frame | |
|---|---|
| Near-Term | 6 Months to 1 Year |
| Mid-Term | 1 to 2 Years |
| Long-Term | > than 2 Years |

| Risk Assessment Index (Possible Mitigation Strategies) | |
|---|---|
| | High (Mitigate) |
| | Moderate (Watch, Mitigate, Accept) |
| | Low (Watch, Mitigate, Accept) |

| Consequences | Subcategories | Very Low | Low | Moderate | High | Very High |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Health Safety Environment (HSE) | *Personnel Safety* | Minor Injury | Short-Term injury or Illness | Injury or Illness Resulting in Days Away from Work OR Hospitalization | Injury or Illness Resulting in Permanent Partial Disability OR Hospitalization of 2+ people | Injury or Illness Resulting in a Fatality OR Permanent Total Disability |
| | *Property Damage* | <$20K | $20K to $50K | >$50K to $500K | $500K to <$2M | ≥$2M |
| | *Compliance, Environment* | Negligible Impact to Compliance; or Minor or Non-Reportable Hazard or Incident | Minimal Impact to Compliance; or Administrative OSHA Violation | Moderate Hazard or Reportable Violation; or Minor OSHA Violation | Significant Threat to Regulatory Requirement; Event Requires Immediate Remediation | Cannot Comply with Regulatory Requirements; or Catastrophic Hazard |
| Technical Performance | *Infrastructure and Asset* | Insignificant Impact to Mission Support Infrastructure and/or Asset | Minor Impact to Mission Support Infrastructure and/or Asset | Significant Impact to Mission Support Infrastructure and/or Asset | Major Impact to Mission Support Infrastructure and/or Asset | Severe Impact or Loss of Mission-Critical or Agency-Unique Infrastructure and/or Asset |
| | *Organizational Objectives* | Negligible Impact to Objectives | Minimal Impacts | Moderate Impacts, workaround(s) available | Significant Threats, no feasible workaround(s) | Failure to Meet Critical Objectives |
| Agency Capabilities | *Service Delivery* | Incidental Disruption of Institutional Services or Operational Support | Short-Term Disruption of Institutional Services or Operational Support | Significant Disruption of Institutional Services or Operational Support | Major Disruption of Key Institutional Services or Operational Support | Work Stoppage of Key Institutional Services or Operational Support |
| | *Workforce* | Insignificant Impact, Reduced Efficiency of Mission Support Resources | Minor Impact, Reduced Efficiency of Mission Support | Significant Impact, Reduced Efficiency of Operational Support | Major Impact to Effectiveness of Mission Operations Support | Severe Impact, Loss of Critical Skills or Capabilities |
| Cost | *Organizational Budget Impacts* | $0 to <$500K OR <2% Increase over allocated and neglible impact on reserve | $500K to <$1M OR 2% to 5% Increase over allocated and can handle with reserve | $1M to <$2.5M OR 5% to 10% Increase over allocated and cannot handle with reserve | $2.5M to <$5M OR 10% to 15% Increase over allocated and exceeds reserves | >$5M OR >15% Increase over allocated and exceeds reserves |
| Schedule | *Project Timelines* | Neglible Impact | Minimal Impact, Slip is Within Schedule Dwell Time, No Impact to Milestones | Moderate Impact, Project Milestone Slip, No Impact to Budget | Significant Impact, Project Milestone Slip Impacts Budget by <3 months | Major Impact, Project Milestone Slip Impacts Budget by >3 months |

# GRC Risk Scorecard

## RISK DEFINITIONS

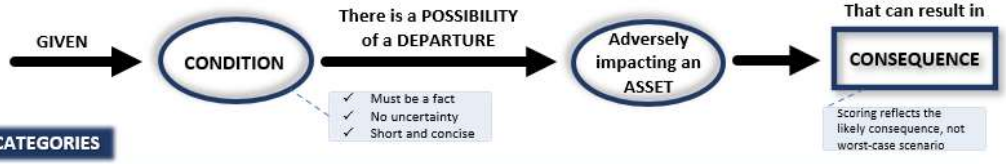
**Risk Management:** An organized, systematic process to effectively identify and analyze performance shortfall risks, develop mitigation options, and implement approved mitigation strategies to reduce or eliminate risk likelihood and/or consequence. RIDM and CRM are key components integrated into this process (see below).

**Risk:** A potential threat with negative consequence to HSE, Center-controlled cost/schedule, or mission objectives for which a resolution is unlikely without focused management attention; or potential inability to fully implement agreements with NASA stakeholders or partners (commercial, governmental, international).

**Concern:** A candidate risk with insufficient or immature info to analyze or define mitigation options. Can be managed internally with existing resources/processes.

- **Top/Center Risk:** Requires Center management resources or direction to resolve; could have cross-cutting impacts that affect two or more GRC organizations.
- **Top Directorate Risk:** Requires directorate management direction and/or resources to resolve; affects one or more divisions within the Directorate.
- **Top Organizational Risk:** Requires division management direction and/or resources to resolve; affects one or more sub-organizations.

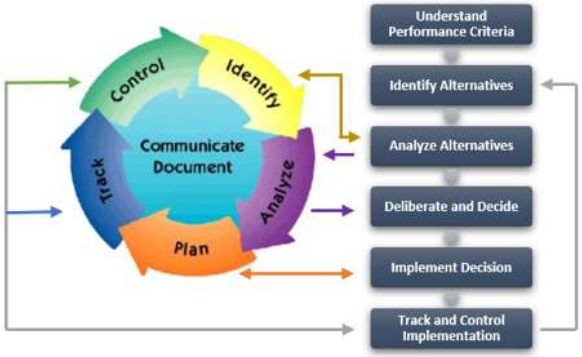
## Writing a Risk Statement




## RM PROCESS

**Risk-Informed Decision Making (RIDM):** To inform GRC decision making through use of quantitative and qualitative risk information to establish baseline performance requirements for mission support organizations, programs, and projects.

**Continuous Risk Management (CRM):** To manage risk associated with the implementation of baseline performance requirements.




## CONSEQUENCE CATEGORIES

**HSE: Health, Safety and Environment – Avoiding risk to:**

**Injury:** Injury or illness per NASA mishap classification levels and OSHA regulations as well as harm to the general public safety caused by NASA activities.

**Property Damage:** Hazards/Mishaps causing damage to federal, public, or private property caused by NASA or NASA-funded activities OR resulting in NASA mission failure before completion of the planned mission.

**Environment:** Protecting the environment from adverse effects (e.g., leaks), per Federal (EPA/OSHA), State, and local regulations; and NASA assets from the effects of the natural environment.

**Technical: Performance to baseline requirements.**

Risk of noncompliance with applicable laws and regulations; and risk of failing to detect/report activities that are noncompliant with statutory, regulatory, or organizational requirements or objectives.

**Agency Capabilities: Infrastructure / resources required to support the CESO or Enterprise Functional Office, and programs and projects:**

**Infrastructure:** Failures affecting facilities/systems serving the Center or Agency, and associated services.

**Workforce:** Ability to attract, retain and effectively utilize the requisite knowledge base/critical skills.

**Cost: Mitigation strategy exceeds budget:** Defined as % of budget or range of dollar amount of EFO/CESO funding needed

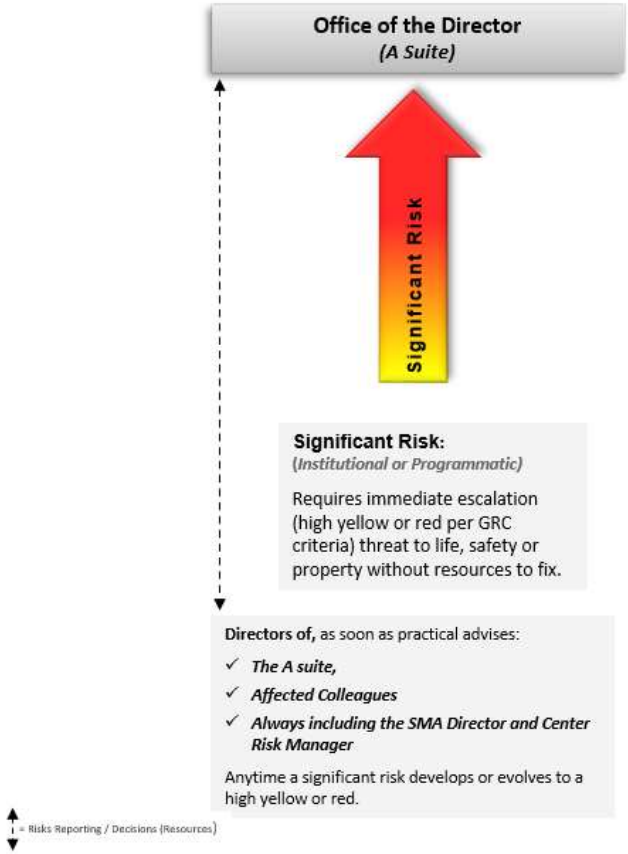
**Schedule: Ability to complete requirements by designated milestones**

As related to critical path activity, dependencies or interrelationships with other activities, and schedule margin for recovery.

2 of 2

# Appendix D: GRC Urgent Risk Reporting Process

## GRC Urgent Risk Reporting Process

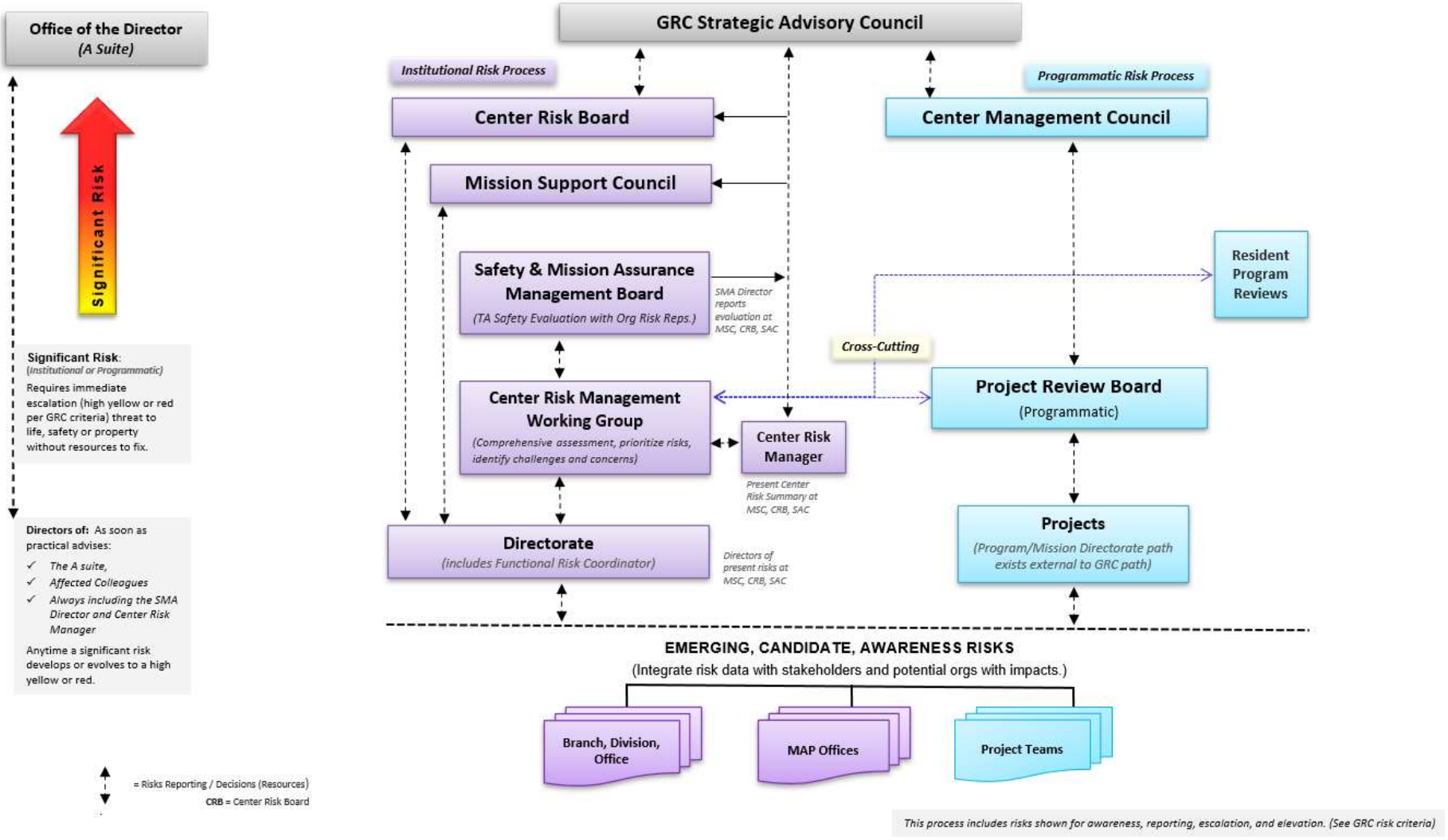



- **Criteria:** A risk in this context is a significant (high Yellow or Red) threat to life, safety, or property without the resources to fix it. When those resources are applied, the risk becomes an issue until it's resolved.
- **Reporting:** A Director Of has the obligation to advise the A Suite and affected colleagues as soon as practical (always including the Director of Safety & Mission Assurance and the Center Risk Manager) anytime a risk develops or evolves to a high Yellow or Red level.
- E-mail is the preferred method of delivery with a synopsis of:
  - ✓ the situation,
  - ✓ the risk itself,
  - ✓ the proposed way forward (e.g., monitoring, mitigation, impacts, etc.)
- A text or a phone call to those affected is also an option. (the A-Suite's pocket contact card for senior staff is a useful tool).

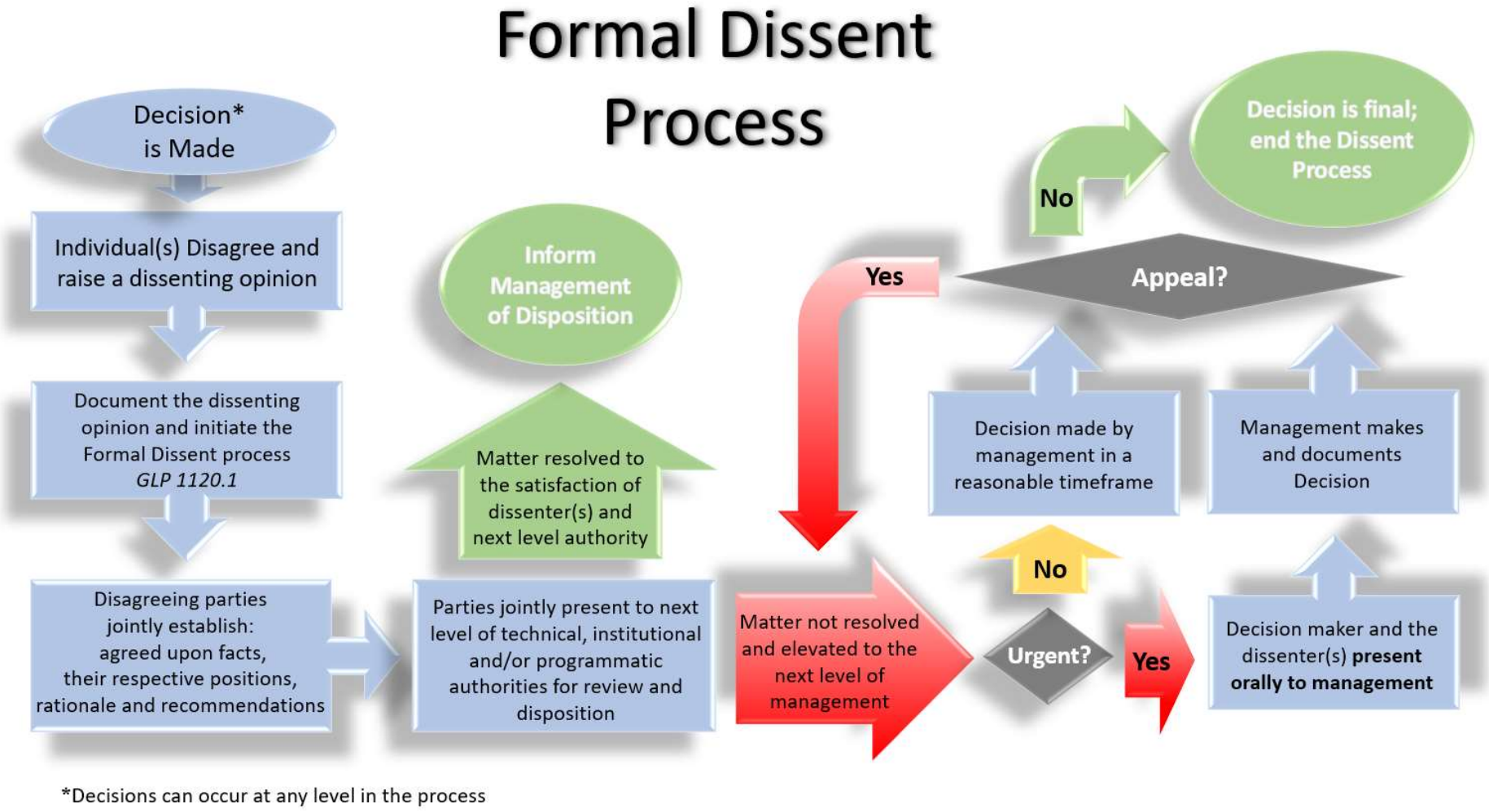
** It's better to over-inform than under-inform. If there is any doubt, there is no doubt: tell it. **

# Appendix E: GRC Risk Reporting/Escalation

## GRC Risk Reporting/Escalation: Simplified View



# Appendix F: Formal Dissent Process



# Appendix G: Institutional Risk Escalation Criteria

## Escalation to Center Risk Board

Requires center management resources or direction to resolve; could have cross-cutting impacts that affect two or more GRC organizations.

Emerging risks have the potential of affecting multi-directorates or have Center-level impact.

A decision, general awareness, or visibility to the next higher management level is needed due to the potential severity or consequence of the risk

Potential transfer of the risk to another organization;

Coordination and integration is needed with other organizations/stakeholders both inside and outside the organization due to cross-cutting significance

New risk (Defined threshold within zone structure)
Score change
Color change

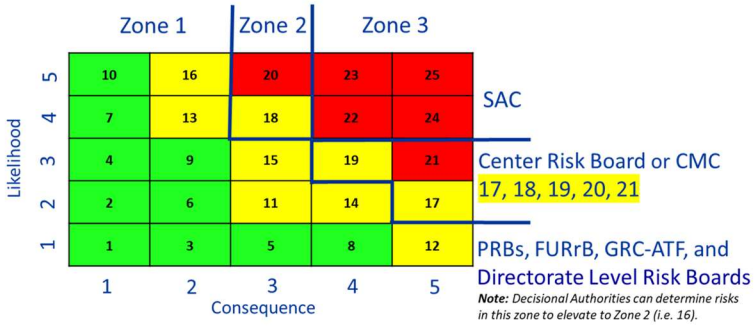
## Escalation to SAC

Risks with High Safety Consequences requiring OSMA Attention

HQ MSD/MAP risks for awareness and/or requiring advocacy for mitigation

Risks requiring Center CMO resources

Risks requiring Center Director acceptance




## Advocacy (Funding, Policy, Headcount)

Requires Agency Solution

MAP Center Impacts:

- Policy/resource decisions: Potential for significant impact on Center risk mitigation strategies
- Varying risk tolerance levels: Policy/resource decisions by varying functional leaders may affect Center strategies for inter-related Multi-Directorate risks.
- Associated risks for non-MAP functions (i.e. IT contract costs, Center will need flexibility to adjust FTEs as needed to meet workload)
- Center Director Control
- Construction of Facilities

## Awareness

Risks submitted to HQ

Enterprise cross-cutting

MAP related:

- Authority to operate processes
- Residual risks
- Risks submitted to HQ for awareness

## Emerging

Risks having the potential of affecting multiple Directorates or may have Center-level impact (include Top Directorate/Organizational risks)

- This can include agreements and commitments (internal & external stakeholders), outreach and knowledge capture.

**Note:** Emerging risks are the risks an org knows exist but are not well understood.

# Appendix H: Programmatic Risk Escalation Criteria

## Center Risk Board vs CMC
## Institutional Risk Reporting Criteria

| Center Risk Board (CMC/MSC) | CMC |
|---|---|
| Infrastructure | Resources necessary for mission success |
| Information Technology | Programmatic constraints that affect capabilities and resources necessary for mission success |
| Resources/Personnel | Facility de-conflicts |
| Assets | Skill mix / staffing gaps impacting missions |
| Security | |
| Processes/Operations | |
| Occupational Health and Safety | |
| Environmental Management | |
| Institutional flexibility to respond to changing mission needs and compliance with NASA and external requirements (i.e. EPA or OSHA) | |

## Programmatic Risk Escalation Criteria

| Escalation to CMC | Escalation to SAC |
|---|---|
| Requires Directorate or Office of Center Director resources or direction to resolve; could have cross-cutting impacts that affect two or more GRC organizations. | Programmatic Risks requiring institution attention and additional resources |
| Emerging risks have the potential of affecting multi-directorates or have Center-level impact. | High likelihood x consequence risks with significant mission success impact |
| A decision, general awareness, or visibility to the next higher management level is needed due to the potential severity or consequence of the risk. | Risks requiring Center Director acceptance |
| Potential transfer of the risk to another organization; | Top Program Risk List for awareness |
| Coordination and integration is needed with other organizations/stakeholders both inside and outside the organization due to cross-cutting significance | |
| **Risks escalating from PRB to CMC for *decision:*** | |
| Any Risk determined by the PRB whereby the Center *can affect the outcome* by enabling mitigation action, such as:<br>• request the Center for additional funding and/or workforce and/or facility utilization to enable corresponding mitigation steps, AND/OR<br>• request the Center to establish Center priorities to deconflict and enable mitigation steps to proceed | |
| **Risks raised from PRB to CMC for *awareness:*** | |
| Any Risk determined by Directorate management to be discussed in senior management interactions, and primarily through the monthly Directorate CMC Stoplight Package reporting. These awareness risks *may be used* to:<br>• assist in variance explanations for Cost, Schedule, Technical, or Management of a particular CMC reportable area, OR<br>• identify potential GRC-centric areas of a strategic programmatic nature, a capability pursuit, or a compilation of project risks that identifies an overarching GRC risk | |

# Appendix I: Center Risk Management Working Group (CRMWG) Membership and Training Criteria

**Risk Management Experience:**

- Possess an understanding of the Center Risk Management process, and the established risk management process and interfaces within their Directorate or Enterprise office.
- Knowledgeable about Directorate or Enterprise risks and methods of managing them.
- Well-informed about Directorate or Enterprise activities and processes. Is able to engage appropriate Subject Matter Experts within their organization to ensure organizational risks mitigation plans are well researched, written and represented.
- Possess adequate risk management skills and experience to equip the CRMWG to perform its function.
- Include members of management or the leadership team that is responsible for various areas of risk management or oversight.
    - CRMWG should possess enough collective knowledge and experience to promote a broad perspective, open dialogue, and useful insights regarding risk.
    - Awareness of Center-wide functions and operations to understand how risks inter-relate to other organizations/enterprises and be able to integrate risks from across the Center/Enterprise.

**Demonstrated Management and Leadership Skills:**

- Participates in leadership roles that interfaces with Directorate management.
- Demonstrate ability and willingness to work effectively and collaboratively in a group.
- Ability to lead and influence others to engage in activities to accomplish goals.
- Able to establish and understand clear metrics aimed at achieving strategic goals.
- Exhibits open communication
- Effectively resolves conflict

**Commitment:**

- Understands the size and scope of risk management within their Directorate or Enterprise; and the time required to serve as active contributors to achieve goals.
- Have sufficient availability to perform the CRMWG charter duties. Includes engaging in activities to contribute to monthly Center Risk Board meetings.

**Training:**

1) Complete the 2-hour GRC Continuous Risk Management course instructed by a certified Risk Facilitator.
2) Participate in the follow on 1.5-hour risk identification workshop led by the instructor.
3) Complete CRMWG charter, roles, and responsibilities training instructed by Center Risk Manager or designee.

# GLPR 8000.4B
# Change History

| Change | Date | Description/Comments |
|---|---|---|
| Basic | 9/11/2007 | Document converted from CLP (GRC-P2.9) to GLPR 8000.1. |
| A | 3/1/2016 | This document has been revised to clarify the requirements for performing, supporting, and evaluating the risk management provisions in accordance with NPD 7120.4, NPR 7120.5, NPR 8000.4, NPR 7120.7, NPR 7120.8, and NPR 8820.2. Changed the document's serial number from 8000.1 to 8000.4 to better align with the NASA directives numbering scheme. It was also updated to conform to current directive content and format requirements per NPR 1400.1 |
| Change 1 | 3/2/2016 | Replaced the word "cost" with "institutional" in section 2.4e and added "Collaborating with the Center Management and Operations Project Manager to insure institutional risks are captured" in section 2.5e. In the footer, changed GLPR 8000.4 to GLPR 8000.4A to reflect the current revision throughout. |
| Change 2 | 3/8/2016 | Expiration date corrected – from 2020 to 2021. |
| Change 3 | 12/01/2020 | Administrative Change: Extend expiration date from 03/01/2021 to 03/01/2022 to complete substantial changes per GLPR 1410.1 |
| B | 07/14/2022 | Rewritten to meet current requirements from the Senior Management LSS project for Center risk management; the new process was approved by the Center Director. Some of the prior document content was consolidated.<br><br>Key risk management process changes include:<br><br>- Detailed process for org tiers, boards, councils, etc.<br>- Risk Reporting and Escalation process<br>- New GRC Risk Scorecard<br>- New escalation criteria<br>- Addressing staffing related risks<br>- MAP orgs inclusion<br>- Dissenting Opinions Process<br>- Directorate Risk Coordinator membership and training criteria<br>- Center Risk Board presentation templates<br>- Annual Directorate risk report and templates<br><br>Name changes:<br>- Functional Risk Coordinator Working Group to Center Risk Management Working Group<br>- Functional Risk Coordinator to Directorate Risk Coordinator<br><br>Updated to meet requirements of GLPR 1410.1 |
| Change 1 | 10/01/2024 | Administrative Changes:<br>- Appendix F flowchart now references local directive GLP 1120.1 for the formal dissent process, instead of NPD 1000.0C. The formal dissent process remains consistent across both documents.<br>- Moved NPR 8715.1 to P.3 as an authority document. |