NID 8000-108
NPR 8000.4A

Effective Date: October 24, 2016
Expiration Date: October 24, 2017
Expiration date extension: March 24, 2018

Subject: Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

a. This National Aeronautics and Space Administration (NASA) Interim Directive (NID) provides the requirements for risk management for the Agency, its institutions, and its programs and projects as required by NASA Policy Directive (NPD) 1000.0, Governance and Strategic Management Handbook; NPD 7120.4, Program/Project Management; and NPD 8700.1, NASA Policy for Safety and Mission Success. Risk management includes two complementary processes: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM).

b. This NID establishes requirements applicable to all levels of the Agency's organizational hierarchy. It provides a framework that integrates the RIDM and CRM processes at all levels. It requires formal processes for risk acceptance and accountability that are clear, transparent, and definitive. This NID also establishes the roles, responsibilities, and authority to execute the defined requirements Agency wide. It builds on the principle that program and project requirements should be directly coupled to Agency strategic goals and applies this principle to risk management processes within all Agency organizations at a level of rigor that is commensurate with the stakes and complexity of the decision situation that is being addressed.

c. The implementation of these requirements leads to a risk management approach that is coherent across the Agency and achieves appropriate coverage of risks (including cross-cutting risks) within NASA. "Coherent" means that (a) Agency strategic goals explicitly drive RIDM and, therefore, CRM, at all levels, (b) all risk types are considered collectively during decision making, and (c) risk management activities are coordinated horizontally and vertically, across and within programs, projects, and institutions.

d. This NID contains requirements for risk management. Detailed explanations and descriptions are provided in associated procedural handbooks.

P.2 APPLICABILITY

a. This NID applies to all Agency activities, including:

(1) NASA Headquarters and NASA Centers, including Component Facilities and Institutional/Mission Support Offices, and to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, and other contractors to the extent specified in their respective contracts.

(2) New and existing programs and projects that provide aeronautics and space products or capabilities; i.e., flight and ground systems, technologies, and operations for aeronautics and space.

b. In this NID, 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 or is" denote descriptive material.

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

P.3 AUTHORITY

a. The National Aeronautics and Space Act, as amended, 51 U.S.C. § 20113(a).

b. NPD 1000.0, Governance and Strategic Management Handbook.

c. NPD 1000.5, Policy for NASA Acquisition.

d. NPD 1200.1, NASA Internal Control.

e. NPD 7120.4, NASA Engineering and Program/Project Management Policy.

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

P.4 APPLICABLE DOCUMENTS AND FORMS

a. NPD 1000.3, The NASA Organization.

b. NPD 1440.6, NASA Records Management.

c. NPR 1441.1, NASA Records Retention Schedules.

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

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

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

g. NPR 7123.1, NASA Systems Engineering Processes and Requirements.

P.5 MEASUREMENT/VERIFICATION

Compliance with the requirements contained in this NID will be verified through the application of the integrated assessment model required by paragraph 2.2.d.

P.6 CANCELLATION

None.

CHAPTER 1. Introduction

1.1 Background

1.1.1 General

a. Generically, risk management is a set of activities aimed at understanding, controlling, and, as appropriate, accepting risk to the achievement of objectives. Risk management operates continuously in an activity, proactively risk-informing the selection of decision alternatives and then managing the implementation risks associated with the selected alternative. In this NID, risk management is defined in terms of RIDM and CRM. This NID addresses the application of these processes to the safety, technical, cost, and schedule mission execution domains throughout the life cycle of programs and projects, including acquisition. This NID also adds requirements for a formal process of risk acceptance that assigns accountability for each risk acceptance decision to a single responsible, authoritative individual (e.g., organizational unit manager) rather than to a committee or group of individuals. In addition, institutional risks and the coordination of risk management activities across organizational units are addressed.

b. The purpose of integrating RIDM and CRM into a coherent framework is to foster proactive risk management: to better inform decision making through better use of risk information, and then to more effectively manage implementation risks using the CRM process, which is focused on the baseline performance requirements informed by the RIDM process. Within a RIDM process informed by Analysis of Alternatives (AoA), decisions are made taking into account applicable risks and uncertainties; then, as the decisions are carried out, CRM is applied to manage the associated risks in order to achieve the performance levels that drove the selection of a particular alternative. Proactive risk management applies to programs, projects, and institutional or mission support offices. Correspondingly, the requirements within this NID are broadly applicable to these areas. Figure 1 shows where the specific processes from the discipline-oriented NASA Procedural Requirements (NPR) 7123.1, NASA Systems Engineering Processes and Requirements, and NID 8000.4, Agency Risk Management Procedural Requirements, intersect with product-oriented NPRs, such as NPR 7120.5, NASA Space Flight Program and Project Management Requirements; NPR 7120.8, NASA Research and Technology Program and Project Management Requirements; and NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Requirements. In much the same way that NPR 7123.1 is intended to define specific systems engineering processes that work within program and project contexts, this NID is intended to define a risk management process in a manner that can be applied within the various contexts.

c. This NID supports NASA's internal control activities as specified in NPD 1200.1, NASA Internal Control, which implements Office of Management and Budget (OMB) Circular A-123 (Management's Responsibility for Enterprise Risk Management (ERM) and Internal Control) and the related Government Accountability Office Standards for Internal Control in the Federal Government including GAO-14-704G, Standards for Internal Control in the Federal Government (the GAO Green Book). The framework in this NID for conducting risk management across strategic, programmatic, financial, and institutional activities is compatible with the ERM integrated framework provided by the Committee of Sponsoring Organizations of the Treadway Commission Framework (COSO, 2004) and the guidance provided in OMB Circulars A-11 and A-123. This risk management framework and associated activities provide a basis for establishing internal controls to ensure that identified risks are maintained within

tolerable levels. The effectiveness of the internal controls is assessed and reported in accordance with the requirements contained in NPD 1200.1.

d. This NID is not intended to dictate organizational structure, but rather to be applied and implemented within existing organizations.

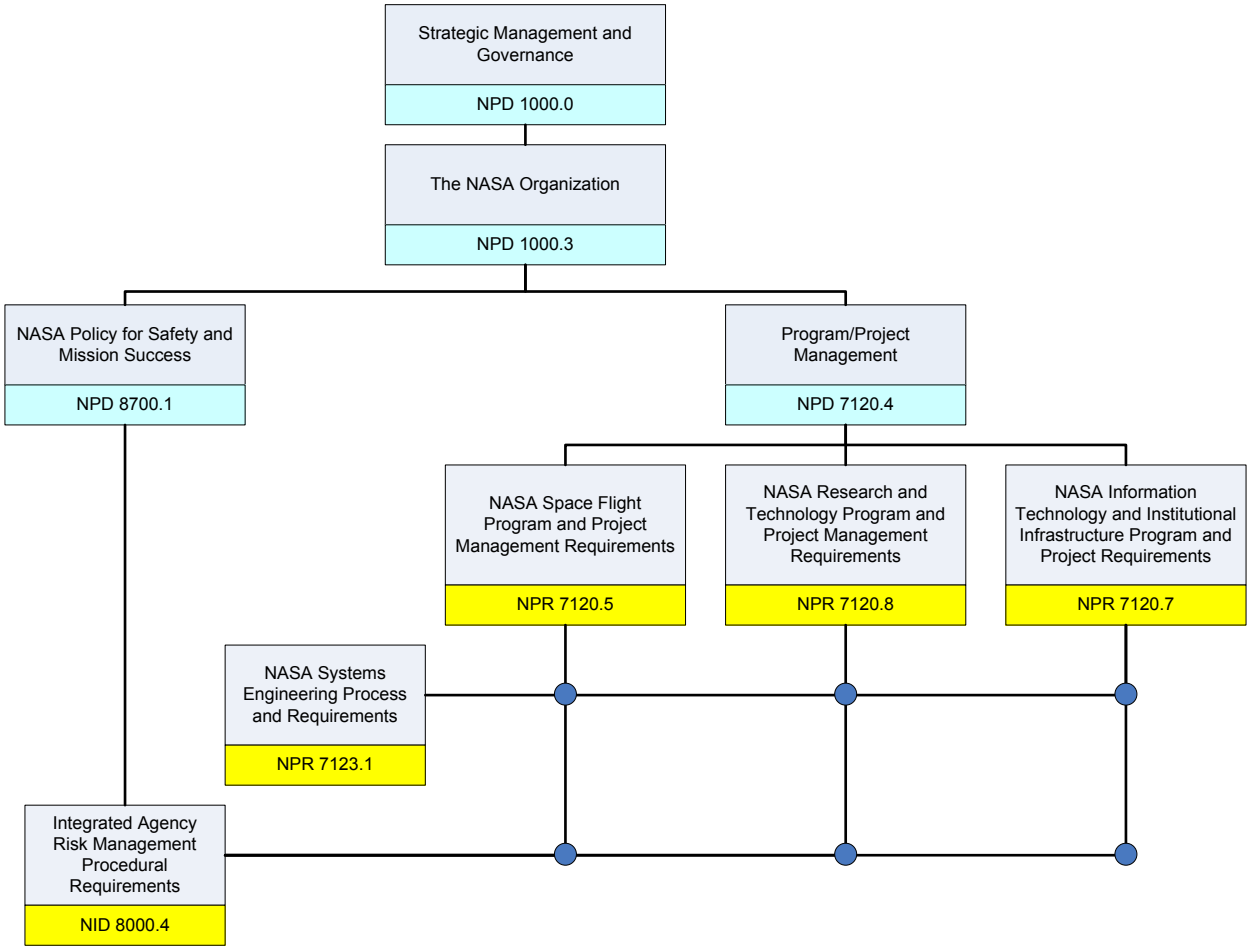

Figure 1. Intersection of Discipline-Oriented and Product-Oriented NPRs

1.1.2 Precedence

The order of precedence in cases of conflict among requirements is: The National Aeronautics and Space Act, as amended 51 U.S.C. § 20113(a); NPD 1000.0, Governance and Strategic Management Handbook; and NPD 1000.3, The NASA Organization.

1.1.3 Requirement Verbs

In this NID, a requirement is identified by "shall," a good practice by "should," permission by "may" or "can," expected outcome or action by "will," and descriptive material by "is" or "are" (or another form of the verb "to be").

1.1.4 Figures

The figures within this NID are intended to be illustrative, not prescriptive.

1.2 Risk Management Within the NASA Hierarchy

1.2.1 Key Concepts

a. In the context of mission execution, risk is the potential for performance shortfalls 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:

(1) Safety

(2) Technical

(3) Cost

(4) Schedule

b. In this NID, the term "Performance Measure" is defined generically as a metric to measure the extent to which a system, process, or activity fulfills its intended objectives. Performance Measures for mission execution may relate to safety performance (e.g., avoidance of injury, fatality, or destruction of key assets), technical performance (e.g., thrust or output, amount of observational data acquired), cost performance (e.g., execution within allocated cost), or schedule performance (e.g., meeting milestones). Similar performance measures can be defined for institutional support.

c. NASA's decisions for managing risk involve characterization of the three basic components of risk:

(1) The *scenario(s)* leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage);

(2) The *likelihood(s)* (qualitative or quantitative) of those scenario(s); and

(3) The *consequence(s)* (qualitative or quantitative severity of the performance degradation) that would result if the scenario(s) was (were) to occur.

> *Note 1: "Likelihood" is a measure of the possibility that a scenario will occur, which accounts for the frequency of the scenario and the timeframe in which the scenario can occur. For some purposes, it can be assessed qualitatively. For other purposes, it is quantified in terms of frequency or probability.*
>
> *Note 2: A complete characterization of the scenarios, likelihoods, and consequences also calls for characterization of their uncertainty.*

d. Each “Acquirer” is accountable *for* overseeing the risk management processes of its “Providers” at the next lower level, as well as for managing risks identified at its own level. The term “Acquirer” is

used to denote a NASA organization that tasks one or more "Provider" organizations, either within NASA or external to NASA, to produce a system or deliver a service (see Glossary in Appendix A). In most cases, an Acquirer at a given level within NASA negotiates with each Provider a set of objectives, deliverables, performance measures, baseline performance requirements, resources, and schedules that defines the tasks to be performed by the Provider. Once this is established, the Provider is accountable *to* the Acquirer for managing its own risks against these specifications.

> *Note: The definition of the relationship between an "acquirer" and a "provider" in this NID is not intended to supersede or alter any provisions of previously approved Agency directives or any other official NASA document (e.g., Program Plan, Memorandum of Understanding, etc.)*

As appropriate, the Provider reports risks and elevates decisions for managing risks to the Acquirer, based on predetermined risk thresholds (illustrated below) that have been negotiated between the Provider and Acquirer. Figure 2 depicts this concept. Risk management decisions are elevated by a Provider when those risks can no longer be managed by the Provider. This may be the case if, for example, resources are not available, or the Provider lacks the decision authority needed in order to manage those risks. In many cases, elevation needs to occur in a timely fashion, in order to allow upper management to respond effectively. The approach is performance-based in the sense that each unit determines the best way to achieve its objectives and performance requirements, rather than being told in detail how these are to be achieved. Risk management decisions may be elevated beyond the next higher level, but it is assumed that a risk management decision is elevated through a stepwise progression. This discussion applies to the risk management process, not to other Agency processes that govern the handling of dissenting opinions or safety concerns.

> *Note: The relationships between a performance requirement, risks, and associated thresholds can be illustrated using the following example. Suppose that for development of a particular science module, a "mass" performance measure has a baseline performance requirement of 50 kg. Lower mass is preferred; mass significantly greater than 50kg has not been allowed for. The risk associated with this technical performance requirement is characterized in terms of one or more scenarios leading to higher mass, their associated likelihoods, and the severity of the associated mass exceedance in each case. A threshold for elevation might be established probabilistically; e.g., as a specified probability (P) of exceeding the baseline mass requirement (50 kg in this case).*

e. Mission Directorates are responsible for management of programmatic risks within their domains and are responsible for elevating risks to the Management Councils (Program Management Council, Operations Management Council, and Strategic Management Council) at the Agency level as appropriate. Center Directors are responsible for management of institutional risks at their respective Centers. Headquarters Mission Support Offices are responsible for management of Agency-wide institutional risks. Program and project managers are responsible for program and project risks within their respective programs and projects. Refer to Chapter 2 for a full description of roles and responsibilities.

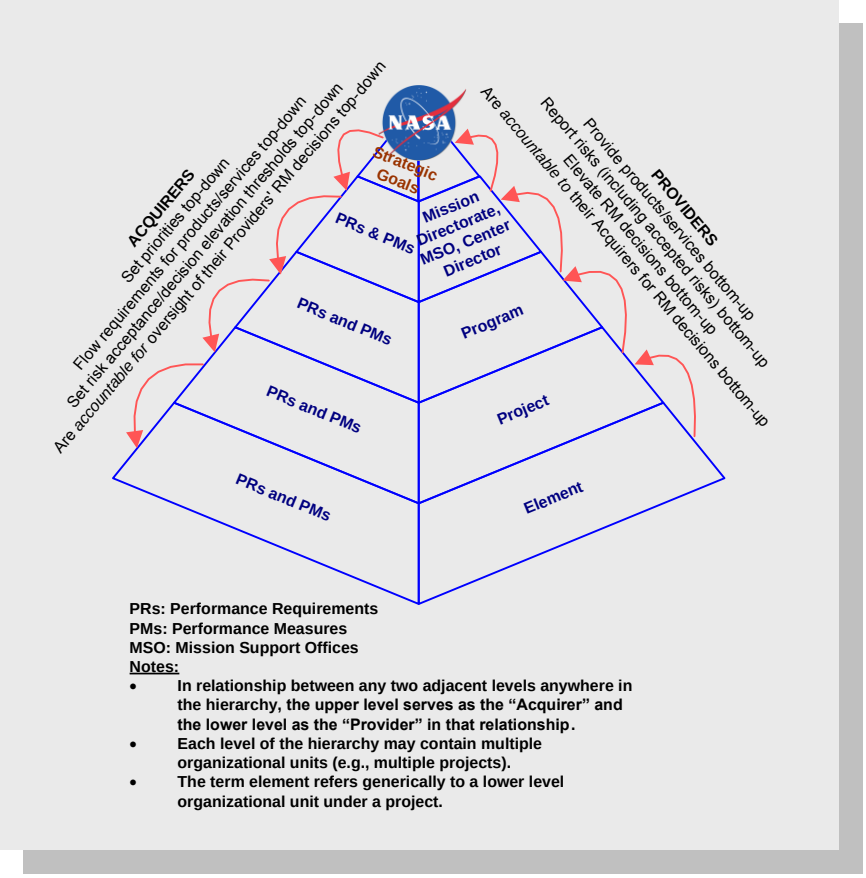

Figure 2. Risk Management in NASA's Organizational Hierarchy

f. Risk management at the Agency level addresses risks identified at the Agency level, as well as risk decisions elevated from Mission Directorates and Mission Support Offices. These may have been elevated for any of several reasons, including:

(1) A need for the Agency to allocate additional resources for effective mitigation.

(2) Agency-level coordination/integration is needed with other organizations/stakeholders.

(3) A finding that a risk identified within a directorate is, in fact, an Agency-level concern.

g. Risk management at the Agency level integrates the full spectrum of risks.

(1) Dealing with risk as a strategic issue, from a high Agency-level/corporate perspective.

(2) Engaging all functions and line management levels in the process.

(3) Bridging the gaps between the mission execution domains of risk management (i.e., safety, technical, cost, and schedule).

h. At the Agency level, emphasis is placed on optimizing and improving the Agency's mission objectives and goals versus individual project or program goals/objectives. Per NPD 1000.0, this is carried out by the Agency's Management Councils.

1.2.2 RIDM

a. As shown in Figure 3, RIDM within each organizational unit involves:

(1) **Identification of Alternatives**: Formulate Objectives and a diverse set of Performance Measures (to support decision making); Formulate Decision Alternatives, Recognizing both Risks and Opportunities.

(2) **Analysis of Alternatives**: Conduct Integrated Analysis of Risk of Each Alternative; Develop the Technical Basis for Deliberation.

(3) **Risk-Informed Alternative Selection**: Deliberate; Select an Alternative and Accept the Associated Risk Informed by Risk Analysis Results, and Document the Decision and its Rationale.

b. RIDM is conducted in many different venues based on the management processes of the implementing organizational unit. These include boards and panels, Authority to Proceed milestones, Safety Review Boards, Risk Reviews, Engineering Design and Operations Planning decision forums, Configuration Management processes, and commit-to-flight reviews, among others.

c. As part of a risk-informed process, the complete set of performance measure values (and corresponding assessed risks) is used, along with other considerations, within a deliberative process to improve the basis for decision making. Deliberation helps the organization to make the best possible use of its experience and tacit knowledge. For example, in order to inform decisions that affect safety, safety performance measures (such as crew safety) and related risks (such as contributions to the probability of loss of crew due to micrometeoroid impact) can be considered in light of aspects of performance history that are not captured in the risk models, or aspects of risk that do not relate immediately to existing performance measures. Moreover, deliberation may identify opportunities not only for improvements that are within the purview of the organizational unit, but also for improvements that could be realized by the acquiring organization or by the program as a whole. Communication of such opportunities to the organizational units best situated to seize them can result in modifications to previously selected alternatives and a rebaselining of the requirements (safety, technical, cost, schedule) that are flowed down to Provider organizations.

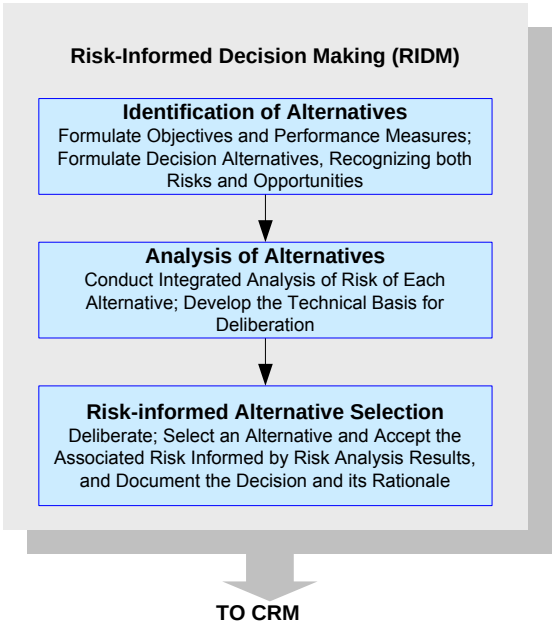

Figure 3. RIDM Process

d. Once a decision alternative has been selected for implementation, the performance measure values that informed its selection define the baseline performance requirements for CRM. As discussed in paragraph 1.2.4.e, situations may arise in which it is necessary to revisit the decision and rebaseline the performance requirements.

e. In order to focus effort and accountability during implementation of the selected alternative, CRM may focus on a set of individual risk contributors (i.e., specific "risks"). However, for some purposes, decision making needs to be supported by evaluation of the "aggregate risk" associated with a given performance measure; i.e., aggregation of all contributions to the risk associated with that performance measure. For example, it may not be sufficient to consider only a list of "risks" to the crew of a human-crewed space vehicle; in order to support some decisions, it is necessary to evaluate the total probability of loss of crew, considering all contributions, as an aggregated risk. Similarly, cost risk is usually treated in the aggregate. For some performance measures, it may not be practical to quantify the aggregate risk; the feasibility of quantifying aggregate risk is determined for each performance measure and then documented in the Risk Management Plan (see paragraph 3.1.1.i) for each organizational unit.

1.2.3 CRM

a. NASA uses a specific process for the management of risks associated with implementation of designs, plans, and processes. This process, which is represented by the graphic in Figure 4 below, is referred to as CRM.

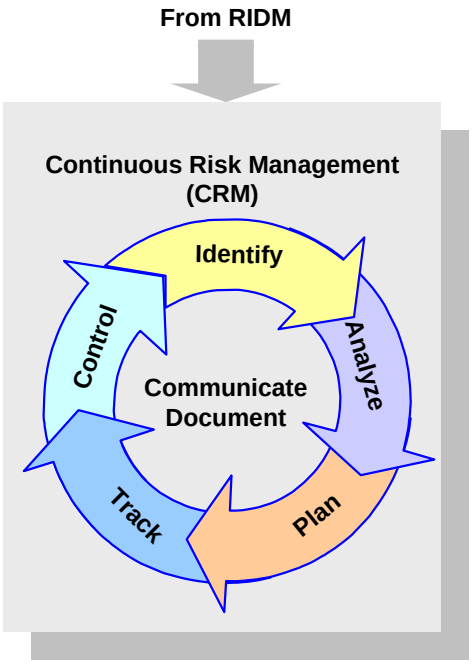

Figure 4: CRM Process

b. Steps in the CRM process include:

(1) **Identify**: Identify contributors to risk (shortfalls in performance relative to the baseline performance requirements).

> *Note: 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.*

(2) **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.

(3) **Plan**: Decide on risk disposition and handling, develop and execute mitigation *plans*, and decide what will be tracked.

> *Note: Risk acceptance is among the possible dispositions. The requirements of paragraph 3.4 apply to acceptance of risks to safety or mission success.*

(4) **Track**: *Track* observables relating to performance measures (e.g., technical performance data, schedule variances), as well as the cumulative effects of risk disposition (handling) decisions.

(5) **Control**: *Control* risk by evaluating tracking data to verify effectiveness of mitigation plans, making adjustment to the plans as necessary, and executing control measures.

(6) **Communicate and document**: *Communicate and document* the above activities throughout the process.

1.2.4 Coordination of RIDM and CRM Within and Across Organizational Units

a. The right-hand portion of Figure 5 shows RIDM (previously shown in Figure 3) and CRM (previously shown in Figure 4) as complementary processes that operate within every organizational unit. Each unit applies the RIDM process to decide how to fulfill its performance requirements and applies the CRM process to manage risks associated with implementation.

b. The left portion of Figure 5 (previously shown in Figure 2) shows the hierarchy of organizations tasked with carrying out a mission. At any given level below the Agency level, there may be multiple organizational units conducting RIDM and CRM. Associated coordination activities include flowdown of performance requirements, risk reporting, and elevation of decisions. Coordination of risk management is suggested by Figure 5. This coordination enables the optimum flow of risk information at all levels of the Agency.

Note: Tools of Knowledge Management (KM) are expected to be particularly valuable in this regard.

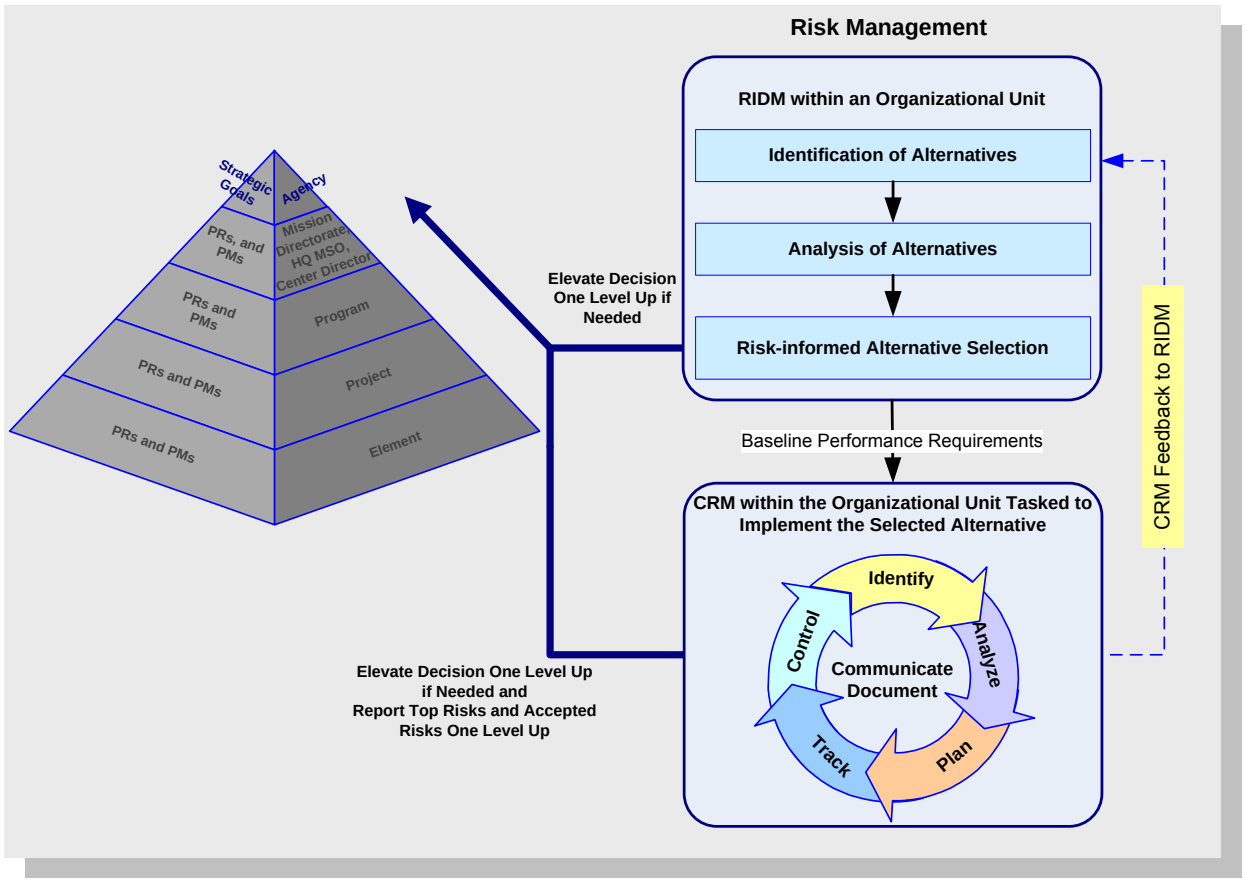

Figure 5. Coordination of RIDM and CRM Within the NASA Hierarchy (Illustrative)

c. Each organizational unit reports on its risk management activities to the sponsoring organization at the next higher level and may elevate individual risk management decisions to that level, if it is determined that those risks cannot be addressed by the originating unit. Refer to paragraph 1.2.1.

d. Within each organizational unit, disposition of risks includes the use of defined thresholds whose exceedance should initiate a risk control response by the unit, including the possible elevation of risk management decisions to the Acquirer at the next higher level (as discussed in paragraph 1.2.1.d). The Risk Management Plan articulates decision rules for dispositioning individual and aggregate risks, including the consideration of uncertainties in the decision process.

e. It is the responsibility of the Acquirer to assure that the performance requirements assigned to the Provider reflect appropriate tradeoffs between/among competing objectives and risks. It is the responsibility of the Provider to establish the feasibility of managing the risks of the job it is accepting, including risks to fulfillment of derived requirements, and identification of mission support requirements. The performance requirements can be changed, if necessary, but redefining and rebaselining them need to be negotiated with higher levels, documented, and subject to configuration control. Performance requirements work together, so redefinition and rebaselining one performance requirement may force redefinition and rebaselining of another, if the overall program/project objectives are to be satisfied. Redefinition and rebaselining, therefore, imply a tradeoff that is the responsibility of the Acquirer.

f. Both CRM and RIDM are applied within a graded approach (refer to the Glossary in Appendix A).

g. At each Center, management of institutional risks affecting multiple programs/projects is carried out within Center organizational units. These units are distinct from the program/project units. Analogously to lower-level program/project organizational units, support organizations receive requirements from, and report risks to, the organizational units that they support. However, management of institutional risks is done within the Center support hierarchy and coordinated with the program/project organizational units as needed. Since the program/project organizational units are affected by institutional risks without being in a position to manage them proactively, in the event that institutional risks threaten accomplishment of program/project organizational unit performance requirements, the program/project organizational units need either to manage those risks with their own resources or elevate them to the next level within the program/project hierarchy.

h. Agency-wide institutional risks are addressed by NASA Headquarters Mission Support Offices and the Operations Management Council.

Note: NASA/SP-2011-3422, NASA Risk Management Handbook, provides technical guidance for the implementation of the requirements of this NID.

CHAPTER 2. Roles and Responsibilities

2.1 General

2.1.1 The implementation of the requirements of this NID is the responsibility of Mission Directorates, Headquarters Mission Support Offices, Center Directors, and program/project managers. They are responsible for determining which organizational units within their domains are subject to the risk management requirements in this NID, including the staffing and execution of the risk management function.

2.1.2 Some requirements in this NID are identified as applying only to organizational units of a particular type, such as Center support units or program/project units. Where the type of unit is not specified, requirements should be understood to apply to all types of organizational units.

2.1.3 Risks of all kinds are addressed in this NID, but management of institutional risks is the focus of mission support and Center support units, while management of mission execution risks is the focus of program/project organizational units.

2.1.4 Organizational unit managers are accountable for risk management decisions in their units.

2.1.5 Technical Authorities are accountable for:

a. Concurrences in the soundness of the technical (safety, engineering, health and medical) cases relied upon by the organizational unit managers in acceptance of risk to safety or mission success;

b. Concurrences that risk acceptance decisions are within the authority of the organizational unit managers;

c. Concurrences that the risk is acceptable (per NPD 1000.0);

> *Note: The Technical Authority (TA's) concurrence that the risk is acceptable includes agreement that the decision appropriately balances Agency priorities in the consideration of safety, mission success, cost, and schedule.*

d. Nonconcurrences regarding (a), (b), or (c), above, and elevation of the decision to the next higher level of management in accordance with the dissenting opinion process (NPD 1000.0).

2.1.6 When there is risk to humans, the actual Risk Takers (or official spokesperson[s] and official supervisory chain) are accountable for consenting to assume the risk.

> *Note: The Administrator is the official Agency spokesperson to consent to any exposure to human safety or property risk on behalf of the general public.*

2.1.7 Per NPD 1000.0, risk management at the Agency level is the responsibility of the Chairs of the Agency's Management Councils.

2.1.8 The Safety and Mission Assurance organizations at the NASA Centers are responsible for providing risk management consultation, facilitation, and training to program/project organizations.

2.2 Requirements

a. Mission Directorate Associate Administrators shall specify organizational units within their Directorates responsible for the implementation of the requirements of this NID.

b. Program/project managers shall specify the organizational units and the hierarchy within their respective domains to which the requirements of this NID apply.

c. Headquarters Mission Support Office heads and Center Directors shall specify the organizational units and the hierarchy within their respective domains to which the requirements of this NID apply.

d. The Chief, Safety and Mission Assurance shall:

(1) Verify that this NID is appropriately implemented across the Agency.

(2) Prepare an integrated assessment model to be used to establish compliance determinations across Mission Directorates, programs and projects, Centers, and Headquarters Mission Support Offices.

(3) Provide handbooks and training opportunities to facilitate implementation of this NID.

CHAPTER 3. Requirements for Risk Management

As discussed in Chapter 2, Roles and Responsibilities, the applicability of these requirements to individual organizational units is determined by the management of the organizational hierarchy within which those organizational units function.

Four categories of requirements are presented in this chapter: General Risk Management Requirements, Requirements for the RIDM Process, Requirements for the CRM Process, and Special Requirements for Acceptance of Risks to Safety or Mission Success. Acceptance of risks to safety or mission success needs to be justified in part by a finding that all that can be done practically to eliminate or mitigate risks to safety has been done.

If during development, it becomes evident that it is not practical to satisfy one or more performance requirements, it may be necessary to obtain a waiver to those requirements, rebaseline those requirements, or rebaseline the requirements overall. Insofar as such actions affect risk to safety or mission success, they constitute risk acceptance decisions and are treated with special formality (see paragraph 3.4). This is the case even if administratively the risk is not dispositioned as "accepted" under the CRM Plan requirements of paragraph 3.3.2.3.b.(1)).

In the subsections below, requirements are levied on "the manager." This term is used in this NID to refer to the manager of the organizational unit. It is understood that the manager cannot be personally involved in all details of every decision or every step in the CRM process; the manager is strongly encouraged to delegate the execution of certain processes to other sub-element managers within the organizational unit as specified in the Risk Management Plan. However, the wording is meant to convey that the manager is *accountable for* fulfilling the process requirements and for the decisions that are made, specifically including risk acceptance decisions as defined in the Risk Management Plan.

3.1 General Risk Management Requirements

Some of the following requirements apply specifically to either Acquirers or Providers. Those requirements are labeled either "Acquirer organizations" or "Provider organizations," as appropriate.

3.1.1 The manager of each organizational unit (hereafter "the manager") shall:

a. Ensure that the RIDM and CRM processes are implemented within the unit, and that key decisions of the organizational unit are risk-informed.

> *Note: Examples of key decisions include: Architecture and design decisions, make-buy decisions, source selection in major procurements, budget reallocation (allocation of reserves), and acceptance of risks to safety or mission success.*

b. Allocate performance requirements to Provider organizations that are consistent with the unit's own performance requirements, and coordinated with each other. (Acquirer organizations)

c. Ensure, during procurement activities, that risks are identified and analyzed in relation to the performance requirements for each offeror to the unit, and that risk analysis results are used to inform the source selection. (Acquirer organizations)

Note: Appendix C contains good practices for procurement/contract risk management.

d. Establish elevation thresholds to be applied by Provider organizations reporting to the unit. (Acquirer organizations)

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

Note 1: In general, the cross-cutting character of a given risk is best determined by an organizational unit at a level above the level at which that risk is first identified.

Note 2: Tools of KM are expected to be particularly valuable in this regard.

f. Coordinate the management of cross-cutting risks being managed within the unit with other involved organizational units; e.g., Centers, Mission Support Offices, programs, projects.

g. Ensure that dissenting opinions arising during risk management decision making are handled through the dissenting opinion process as defined in NPD 1000.0.

h. Ensure that risk management activities of the organizational unit support, and are consistent with, ongoing internal control activities defined in NPD 1200.1.

i. Ensure the development of a Risk Management Plan that:

(1) Explicitly addresses safety, technical, cost, and schedule risks.

(2) Delineates the unit's approach for applying RIDM and CRM within a graded approach (see Glossary in Appendix A).

(3) Incorporates, or cites, a complete set of requirements to be met by the organization, including the top-level Safety and Mission Success requirements, derived requirements, process requirements, and commitments (e.g., testing) (applicable to Provider organizations).

Note 1: This plan serves to clarify what detailed requirements (commitments, ...) the Provider expects to address in the ensuing development of the system. Satisfaction of these requirements is intended to provide evidence of satisfaction of the top-level requirements; correspondingly, risks to fulfillment of the commitments or satisfaction of the requirements are a key focus of Risk Management. The Acquirer's review of this portion of the plan provides an early opportunity to ensure that the Provider is adequately addressing the safety performance requirements and is implementing a risk-informed process in development of the system.

Note 2: For each performance requirement, this portion of the plan will designate whether the associated risks (including the aggregate risk) are to be assessed quantitatively or qualitatively.

Note 3: NPR 7123.1 describes processes for systematically treating top-level performance requirements and derived requirements implied by them. Accordingly, the present requirement allows for citation, rather than replication, of those requirements in the Risk Management Plan. However, in addition to such requirements on performance of the system or service being

developed, the Risk Management Plan also contains Provider commitments (e.g. to perform tests) that are deemed to provide evidence (Assurance) to the Acquirer of satisfaction of the performance requirements.

Note 4: Within this formulation, cancellation of commitments to perform tests or demonstrations amounts to either a rebaselining or a waiver proposal, and is correspondingly subject to requirements on Risk Acceptance in paragraph 3.4.

(4) Is coordinated with other management plans, as appropriate, such as the Systems Engineering Management Plan (SEMP), when applicable per NPR7123.1.

(5) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories.

(6) Identifies stakeholders, such as Risk Review Boards, to participate in deliberations regarding the disposition of risks.

(7) Documents risk acceptability criteria/thresholds, and elevation protocols (the specific conditions under which a risk management decision must be elevated through management to the next higher level). (Agreement between Acquirer and Provider organizations)

Note: A "risk acceptability criterion" is a rule for determining whether a given organizational unit has the authority to decide to accept a risk.

(8) Establishes risk communication protocols between management levels, including the frequency and content of reporting, as well as identification of entities that will receive risk tracking data from the unit's risk management activity.

Note 1: This communication may be accomplished using standard reporting templates, including risk matrices, whose formulation and interpretation are agreed between the affected units, recognizing that risk communication inputs to any given level (e.g., the program level) from different units (e.g., projects) should be defined consistently, in order to support decision-making at that level.

Note 2: In general, elevation protocols and communication protocols are specific to levels and units. A risk decision that requires elevation from one level to the next may well be manageable at the higher level, since the unit at that level has more flexibility and authority. The overall effectiveness of the risk management effort depends on the proper assignment of risk acceptability criteria and thresholds.

Note 3: For Center support units, protocols are needed for reporting risks to affected program/project units.

(9) Establishes a form for documentation of the manager’s decisions to accept risks to safety or mission success, the technical basis supporting those decisions, the concurrence of the cognizant Technical Authorities, and consent of the risk takers (if applicable) (refer to paragraph 3.4.2 for application of this form).

(10) Delineates the processes for coordination of risk management activities and sharing of risk information with other affected organizational units.

(11) Documents the concurrence of the Acquirer to which the manager of the organizational unit reports, including its risk reporting requirements. (Provider organizations)

j. Ensure that decisions to rebaseline performance requirements, grant waivers, or modify Providers' Risk Management Plans that affect risk to safety or mission success are risk-informed consistent with the RIDM process described in Chapter 1, and that they are processed as risk acceptance decisions (refer to requirements in paragraph 3.4.).

> *Note: Per requirements in paragraph 3.1.1.i., the Risk Management Plan contains not only performance requirements, but also commitments (e.g., to testing or demonstration activities). A reduction in certain commitments could entail acceptance of some risk to safety or mission success.*

3.2 Requirements for the RIDM Process

3.2.1 The manager shall ensure that key decisions are informed by Analysis of Alternatives carried out with a level of rigor appropriate to the significance and the complexity of the decisions, by following the steps of the RIDM process described in Chapter 1.

> *Note: The requirements of paragraph 3.4 also apply to decisions that have implications for risks to safety or mission success.*

For the course of action selected, the manager shall:

a. Ensure that the bases for performance requirement baselines (or rebaselines) are captured, and that these baselines are applied to scope the unit's CRM implementation.

b. Negotiate institutional support performance requirements with Center support units when required to meet program/project requirements for program/project units.

3.3 Requirements for the CRM Process

3.3.1 General Requirements

The manager shall:

a. Implement the CRM process (as defined in this NID in paragraph 3.3.2) (see also Figure 4 and associated discussion).

b. Coordinate the unit's CRM process with the CRM processes of organizational units at levels above and below, including contractors if applicable.

c. Ensure that risk documentation is maintained in accordance with NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules, 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 Plan.

3.3.2 Specific Requirements

Note: Because the "Document and Communicate" function of CRM is integral to all of the steps in the CRM process (Figure 5), requirements for documentation and communication are integrated into the following steps rather than treated as a separate step.

3.3.2.1 Identify

a. The manager shall ensure that the execution of the risk identification step is thorough and consistent with the baseline performance requirements of that unit.

b. The manager shall ensure that risk analyses performed to support RIDM are used as input to the "Identify" activity of CRM (see paragraphs 3.2.a and 3.2.b).

c. The manager shall ensure that the results of risk identification are documented to provide input to the "Analyze" step and to characterize the risks for purposes of tracking.

Note: Depending on the type of risk, this documentation will take the form of a "risk statement" or "risk scenario." Each risk statement or scenario is accompanied by a descriptive narrative, which captures the context of the risk by describing the circumstances, contributing factors, uncertainty, range of possible consequences, and related issues (such as what, where, when, how, and why).

3.3.2.2 Analyze

a. The manager shall determine the protocols for estimation of the likelihood and magnitude of the consequence components of risks, including the timeframe, uncertainty characterization, and quantification when appropriate, and document these protocols in the Risk Management Plan.

Note: The requirement to consider uncertainty is to be implemented in a graded fashion. If uncertainty can be shown to be small based on a simplified (e.g., bounding) analysis, and point estimates of performance measures clearly imply a decision that new information would not change, then detailed uncertainty analysis is unnecessary. Otherwise, some uncertainty analysis is needed to determine whether the expected benefit of the decision is affected significantly by uncertainty. In some cases, it may be beneficial to obtain new evidence to reduce uncertainty, depending on the stakes associated with the decision, the resources needed to reduce uncertainty, and programmatic constraints on uncertainty reduction activities (such as schedule constraints).

(1) When a risk management decision is elevated from a lower-level organizational unit, the manager shall recalibrate the associated risk with respect to the requirements, thresholds, and priorities that have been established at the higher level, and enter the recalibrated risks into "Plan," "Track," and "Control" activities (paragraphs 3.3.2.3 through 3.3.2.5) at the higher level.

(2) Wherever determined to be feasible (as documented in the Risk Management Plan), the manager shall ensure the characterization of aggregate risk through analysis (including uncertainty evaluation), as an input to the decision-making process.

(3) The manager shall ensure that analyzed risks are prioritized and used as input to the "Plan," Track," and "Control" activities.

(4) The manager shall ensure that the results of the "analyze" step are documented and communicated to unit management.

3.3.2.3 Plan

a. Each manager shall ensure that decisions made on the disposition of risks (including decisions regarding implementation of control measures) are informed by the risk analysis results and are consistent with the defined thresholds established in paragraph 3.1.1.i(8).

b. The manager shall ensure that only one of the following possible risk dispositions is applied to any given risk and that, depending on the risk disposition, the appropriate requirement, below, is applied.

(1) When a decision is made to *accept* a risk, the manager shall ensure that each acceptance is clearly documented in their organizational unit's risk database (list), including the rationale for acceptance, the assumptions and conditions (including programmatic constraints) on which the acceptance is based, and the applicable risk acceptance criteria. Additionally, for acceptance of risks to safety or mission success, the requirements in paragraph 3.4 apply.

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

(3) When a decision is made to *close* a risk, the manager shall ensure that the closure rationale is developed, and that both rationale and management approval are documented in the risk database.

(4) When a decision is made to *watch* a risk, the manager shall ensure that tracking requirements are developed and documented in the risk database (list).

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

(6) When dispositions (1), (2), (3), (4), or (5) above cannot be applied, the manager shall elevate the decision to the organizational unit management at the next higher level (typically the Acquirer) and document the action taken in the risk database (list).

Note: Center support units elevate risks within the Center hierarchy.

c. For "mitigate," "watch," and "research," the manager shall designate an appropriate entity to implement the disposition.

Note: The entity designated to implement the disposition is typically referred to as the "risk owner."

d. The manager shall ensure that all risks categorized as "watch" have decision points, dates, milestones, necessary achievements, or goals identified.

3.3.2.4 Track

a. The manager shall ensure the development and implementation of a process for acquiring and compiling observable data to track the progress of the implementation of risk management decisions.

b. The manager shall ensure tracking of the cumulative effects of risk management decisions and risk acceptance decisions (i.e., the net effect of the decisions that have been made).

c. The manager shall ensure the dissemination of tracking data to entities identified in the Risk Management Plan as recipients of these data.

3.3.2.5 Control

a. The manager shall ensure the evaluation of tracking data in order to advise its organizational unit management on the status and effectiveness of decisions implemented in paragraph 3.3.2.3.b.

b. The manager shall provide feedback to affected organizational units, including its Acquirer at the next higher level, on any changes in the status of tracked risks such as, but not limited to, acceptance of a risk or changing a mitigation plan.

c. Based on the tracking data, in order to control a given risk, the risk owner shall recommend actions to the manager and oversee implementation of risk control actions with which the manager has concurred.

3.4 Special Requirements for Acceptance of Risks to Safety or Mission Success

3.4.1 All decisions that have implications for risks to safety or mission success, not only decisions that arise in the “Plan” step of CRM as “risk acceptance” decisions, are subject to the following requirements on creation of the basis for the decision, TA concurrence, and risk taker consent (if applicable). This includes decisions made at Key Decision Points, significant milestones, when performance requirements are being rebaselined, when waivers are being considered, or when an Acquirer is taking delivery of a system.

Note: Although these decisions are not necessarily couched as “risk acceptance” decisions, they nevertheless have implications for safety or mission success. KDPs and reviews at significant milestones entail consideration of decisions to proceed despite existing risks; rebaselining to relax safety requirements tacitly accepts safety risk, even though it is not necessarily described as a “risk acceptance” decision in the CRM sense; waivers of safety requirements may increase risk; Acquirer acceptance of a delivered system or capability entails Acquirer assumption of responsibility for managing the associated risks, including risks previously accepted by the Provider.

3.4.2 Each manager shall ensure that each decision accepting risk to safety or mission success (e.g.,

requirements definition/compliance/waiver, change requests, formal board directives and decisions, dissenting opinion dispositions, etc.) is clearly documented in the organizational unit's risk database (list), in the formal configuration management system where the associated decision was approved, or in a formal safety process system, on a program-defined form including:

a. The manager's signature, documenting or referencing:

(1) The case (technical and programmatic) relied upon to justify the decision;

(2) The assumptions, programmatic constraints, evaluation of aggregate risk, and the acceptance criteria on which the decision is based;

(3) The rationale for acceptance, including satisfaction of the organization's risk acceptance criteria.

> *Note: The form and content of the "case (technical and programmatic) relied upon" depends on the circumstances. For example: 1) for acceptance of individual risks, the case may include Analysis of Alternatives considering the balance between safety, cost, schedule, and technical performance considerations. 2) At a KDP, a comprehensive, integrated case will have been developed to support a decision to progress to the next phase of the life cycle.*

b. The TAs' signatures with their concurrence positions, documenting or referencing their evaluations of the technical merits of the case, the manager's authority to accept the risk, and the acceptability of the risk.

> *Note 1: Refer to Note 1 under paragraph 2.1.5.(c).*
>
> *Note 2: The purpose of the requirements in this subsection is not to compel execution of the processes for acceptance of every minor risk individually, but rather to foster management of the outstanding risks as a group: to promote understanding of the aggregate risk being accepted based on a considered and technically sound integrated analysis, and to fix accountability for risk acceptance with the programmatic decision-makers.*

c. When there is risk to humans, the signature of actual risk-taker(s) (or official spokesperson[s] and applicable supervisory chain) documenting their consent to assume the risk.

3.4.3 In the event of TA or risk taker (if applicable) nonconcurrence in a manager's risk acceptance decision, the TA(s) or risk taker(s) shall elevate the risk acceptance decision one level up in the organizational hierarchy in accordance with the dissenting opinion process (NPD 1000.0).

3.4.4 In the event of TA and risk taker (if applicable) concurrence in a manager's risk acceptance decision, the manager shall report each decision accepting risks to safety or mission success one level up in the organizational hierarchy, regardless of whether the risk acceptance decision comports with the organization's risk acceptance criteria.

> *Note: Risks are reported up one level because it is important to track and manage the aggregate risk at the Acquirer's level.*

3.4.5 When an Acquirer takes delivery of the system or service, management of the outstanding risks

of the system or service, including risks previously accepted by the Provider, becomes the Acquirer's current responsibility. The Acquirer shall integrate the outstanding risks into the Acquirer's risk management process, assuming that the Acquirer decides to accept the risks, based on:

a. The TA findings accompanying the Provider's technical basis,

b. Independent evaluation of the technical basis.

> *Note 1: Risks that were previously accepted by the Provider may now be reducible, given the additional resources and flexibility available to the Acquirer.*
>
> *Note 2: A decision by the Acquirer not to accept responsibility for managing (or accepting) the risk is tantamount to refusing delivery of the system. This situation is intended to be precluded by processes described above.*

APPENDIX A. Definitions

Acquirer: An Acquirer is a NASA organization that tasks another organization (either within NASA or external to NASA) to produce a system or deliver a service.

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.

Continuous Risk Management (CRM): As discussed in paragraph 1.2.3, 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 NID, 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.

Dispositions (Risk)

a. Accept: The formal process of justifying and documenting a decision not to mitigate a given risk. (See also Risk Acceptability Criterion).

> *Note: A decision to "accept" a risk is a decision to proceed without further mitigation of that risk (i.e., despite exposure to that risk).*

b. 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.

c. 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.

> *Note: Some organizational units within NASA use the term "escalate" to mean "elevate."*

d. 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.

> *Note: Mitigation does not automatically imply acceptance of any risk that may remain after the modification has been implemented.*

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

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

Graded Approach: A "graded approach" applies risk management processes at a level of detail and rigor that adds value without unnecessary expenditure of unit resources. The resources and depth of analysis are commensurate with the stakes and the complexity of the decision situations being addressed.

> *Note: 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, how complex and diverse the hazards are, and how large the uncertainties are compared to operating margin, among other things. Both RIDM and CRM are formulated to allow for this.*

Institutional 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 institutional flexibility to respond to changing mission needs and compliance with external requirements (e.g., Environmental Protection Agency or Occupational Safety and Health Administration regulations).

Knowledge Management: Knowledge management is getting the right information to the right people at the right time and helping people create knowledge and share and act upon information in ways that will measurably improve the performance of NASA and its partners.

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.

Organizational Unit: An organization, such as a program, project, Center, Mission Directorate, or Mission Support Office 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.

> *Note: Performance measures should in general relate to observable quantities. For example, engine performance parameters, cost metrics, and schedule are observable quantities. Although safety performance measures can be observed in principle, many of them have to be modeled. Partly because of this, in ranking decision alternatives, one may use a risk metric (e.g., probability of loss of crew) as a surrogate for a performance measure.*

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.

Provider: A Provider is a NASA or contractor organization that is tasked by an accountable organization (i.e., the Acquirer) to produce a product or service.

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, 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.

Note: This does not mean that all risks satisfying the criterion are accepted, or that a combination of such individual risks is automatically acceptable in the aggregate, but rather that, subject to aggregate risk considerations, the given unit has the authority to decide to accept individual risks satisfying the criterion.

Risk-Informed Decision Making (RIDM): A risk-informed decision-making process 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.

Note: A decision-making process relying primarily on a narrow set of model-based risk metrics would be considered "risk-based."

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 informed by the RIDM process.

Risk Owner: The "risk owner" is 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.

Note: This NID uses the term "safety" broadly to include human safety (public and workforce), environmental safety, and asset safety.

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

Threshold: A level for a performance measure or a risk metric whose exceedance "triggers" management processes to rectify performance shortfalls.

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.

APPENDIX B. Acronyms

AoA	Analysis of Alternatives
CRM	Continuous Risk Management
FAR	Federal Acquisition Regulation
KM	Knowledge Management
MSO	Mission Support Offices
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
PR	Performance Requirement
QASP	Quality Assurance Surveillance Plan
RIDM	Risk-Informed Decision Making
SEMP	Systems Engineering Management Plan
TA	Technical Authority

APPENDIX C. Procurement/Contract Risk Management

Procurement risks should be considered during acquisition formulation and implementation activities that include strategy development, development of requirements and solicitation instructions, evaluation of proposals, source selections, surveillance planning, and post-award contract monitoring. The various members of the acquisition team ensure that acquisition-related risks are identified and reassessed during each stage of the acquisition life cycle.

The Federal Acquisition Regulation (FAR) Parts 7 and 15 and NASA FAR Supplement Parts 1807 and 1815 provide requirements for acquisition/contract risk management. The good practices provided below complement these requirements.

C.1 Acquisition Strategy Development

a. For each acquisition, the organizational unit manager should ensure that risks are identified and analyzed in relation to the performance requirements of the acquisition, as part of the acquisition planning process.

b. For each acquisition, the organizational unit manager should ensure that the project technical team is supported by personnel that have demonstrated expertise in the identification and analysis of various risk types.

> *Note: The risk types should include those associated with safety, technical, cost, schedule, institutional/mission support, information technology, export control, security, and other applicable areas.*

c. For each acquisition, the Acquirer's manager should ensure that the project technical team provides a thorough discussion of the identified and analyzed risks for inclusion in written acquisition plans and/or Procurement Strategy Meeting documents.

d. For each acquisition, contracting officers should ensure that the identified and analyzed risks are documented in written acquisition plans and/or Procurement Strategy Meeting documents.

C.2 Requirements Development

a. The Acquirer's manager should ensure that the project technical team addresses the risks identified in paragraph C.1.a, above, in the solicitation requirements.

b. The Acquirer's manager should ensure that the project technical team prepares a preliminary surveillance plan (referred to as a Quality Assurance Surveillance Plan (QASP)) for tracking risks.

> *Note: The preliminary QASP, which the project office prepares in conjunction with the statement of work, reflects the Government's surveillance approach relative to the perceived risks. The preliminary QASP is written at a general rather than specific level because the risks will not be completely identified at that time.*

C.3 Solicitation

a. The Acquirer’s manager should ensure that the project technical team develops, and provides to the Contracting Officer, solicitation instructions for offerors to identify and describe risks and submit plans to address those risks and risks identified by the Government.

b. The Acquirer’s manager should ensure that solicitation instructions require the offeror to describe the interface between their risk management process and the organizational unit's risk management process.

c. The proposal evaluation team should develop, and include in the solicitation, criteria to evaluate the effectiveness of the offeror's risk management process (see NASA FAR Supplement 1815.305) based on the acquisition plan and solicitation.

C.4 Source Selection

a. As part of the evaluation of proposals, and consistent with the solicitation evaluation criteria, the proposal evaluation team should evaluate risk information associated with the proposal and present the evaluation results to the Source Selection official(s) to risk-inform the source selection decision.

C.5 Post-Selection Surveillance and Contract Monitoring

a. The Acquirer’s managers should develop a risk-informed surveillance plan to monitor the contractor’s performance in key areas related to risk and periodically review it to ensure currency.

b. The Acquirer’s managers should ensure that acquisition-related risks are continuously managed using the CRM process.

APPENDIX D. References

D.1 48 CFR Federal Acquisition Regulation parts 7 and 15.

D.2 48 CFR NASA Federal Acquisition Regulation Supplements parts 1807 and 1815.

D.3 NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

D.4 NASA/SP-2011-3422, NASA Risk Management Handbook.