NASA Procedural Requirements

NPR 8000.4A
Effective Date: December 16, 2008
Expiration Date: December 16, 2013

COMPLIANCE IS MANDATORY

Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Appendix B. Acronyms

Appendix C. Procurement/Contract Risk Management

Preface

P.1 Purpose

a. This NASA Procedural Requirements (NPR) document 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 NPR establishes requirements applicable to all levels of the Agency. It provides a framework that integrates the RIDM and CRM processes at all levels. This NPR 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 NPR contains requirements for risk management. Detailed explanations and descriptions will be provided in associated procedural handbooks.

P.2 Applicability

This NPR applies to all Agency activities, including:

a. NASA Headquarters and NASA Centers, including Component Facilities and Institutional/ Mission Support Offices, and to the Jet Propulsion Laboratory and other contractors to the extent specified in their respective contracts.

b. 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.

P.3 Authority

a. National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. § 2473 (c) (l).

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 8700.1, NASA Policy for Safety and Mission Success.

P.4 Applicable Documents

a. NPD 1000.3, The NASA Organization.

b. NPD 1440.6, NASA Records Management.

c. NPR 1441.1, NASA Records Retention Schedules.

d. NPR 7120.5D, 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.

h. NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

i. Federal Acquisition Regulation parts 7 and 15.

j. NASA Federal Acquisition Regulation Supplements parts 1807 and 1815.

P.5 Measurement/Verification

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

P.6 Cancellation

NPR 8000.4, Risk Management Procedural Requirements, dated April 25, 2002.

/S/
Bryan O'Connor
Chief, Safety and Mission Assurance

Chapter 1. Introduction

1.1 Background

1.1.1 General

a. Generically, risk management is a set of activities aimed at achieving success by proactively risk-informing the selection of decision alternatives and then managing the implementation risks associated with the selected alternative. In this document, risk management is defined in terms of RIDM and CRM. The document 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. 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 emerging from the RIDM process. Within an RIDM process, decisions are made with regard to outcomes of the decision alternatives, taking into account applicable risks and uncertainties; then, as part of the implementation process, CRM is used to manage those risks in order to achieve the performance levels that drove the selection of a particular alternative. Proactive risk management applies to programs, projects, and institutional or mission support offices. Correspondingly, the requirements within this NPR are broadly applicable to these areas. Figure 1 shows where the specific processes from the discipline-oriented NPR 7123.1 and NPR 8000.4 intersect with product-oriented NPRs, such as NPR 7120.5D, NPR 7120.8, and NPR 7120.7. 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 NPR is intended to define a risk management process in a manner that can be applied within the various contexts.

c. This NPR supports NASA's internal control activities as specified in NPD 1200.1, which implements Office of Management and Budget Circular A-123 (Management's Responsibility for Internal Control) and the related Government Accountability Office Standards for Internal Control in the Federal Government. This NPR establishes the framework for conducting risk management across programmatic, financial, and institutional activities. These risk management activities provide a basis for establishing internal controls to mitigate the identified risks. The effectiveness of the internal controls is assessed and reported in accordance with the requirements contained in NPD 1200.1.

d. This NPR is intended to be applied and implemented within the organizational structure of the activity being performed. It is not intended to dictate that organizational structure.

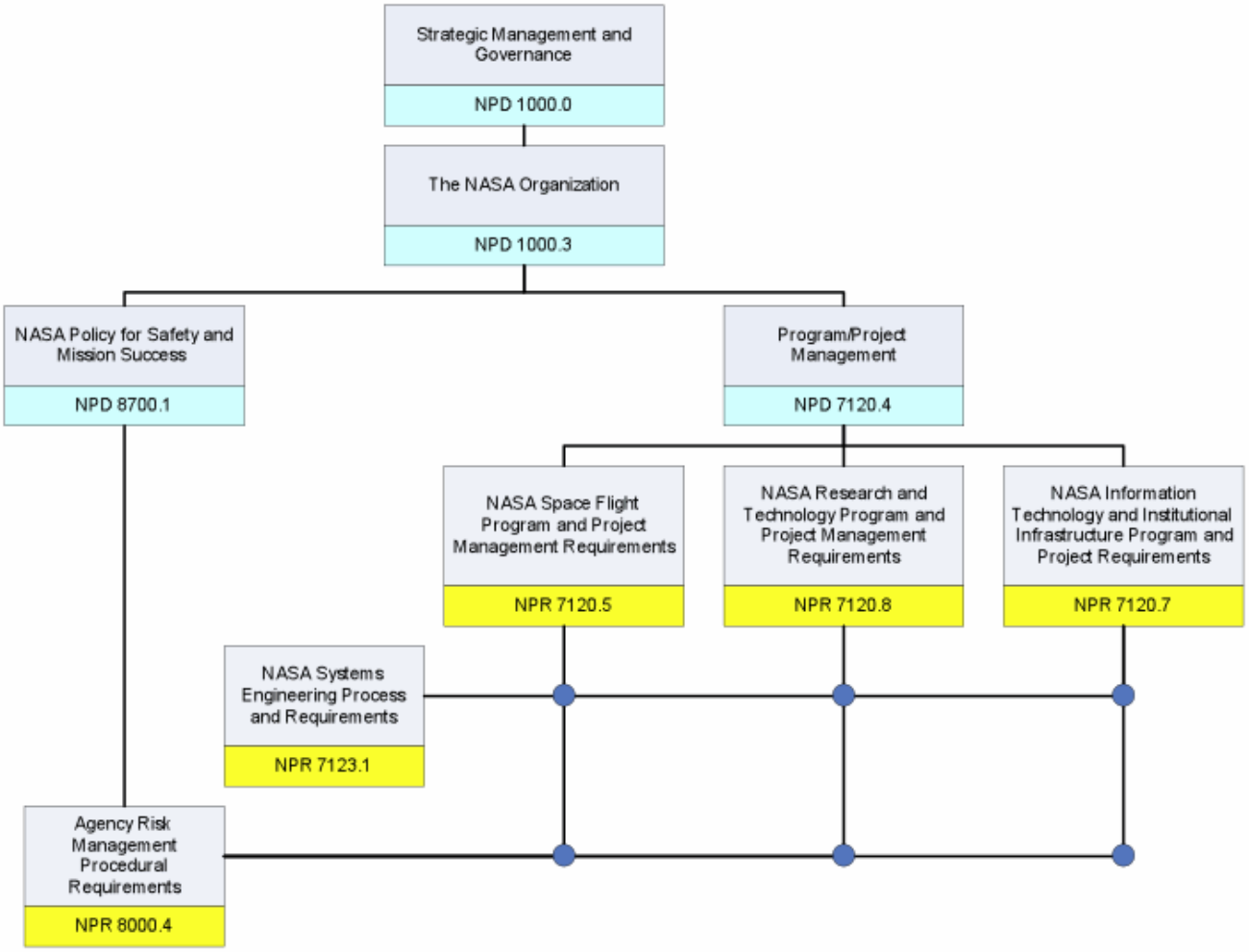

Figure 1. Intersection of Discipline-Oriented and Product-Oriented NPRs

1.1.2 Precedence

The order of precedence in cases of conflict among requirements is 42 U.S.C. 2473(1), Section 203(1), National Aeronautics and Space Act of 1958, as amended; NPD 1000.0, Governance and Strategic Management Handbook; and NPD 1000.3, The NASA Organization.

1.1.3 Requirement Verbs

In this NPR, 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 NPR 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, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements. The performance shortfalls may be related to institutional support for mission execution or related to any one or more of the following mission execution domains:

(1) Safety

(2) Technical

(3) Cost

(4) Schedule

b. In this document, 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 organizational unit will oversee the risk management processes of those unit(s) at the next lower level, as well as manage risks identified at its own level. In most cases, an organizational unit, at a given level, within NASA negotiates with the unit(s) at the next lower level in the organizational hierarchy a set of objectives, deliverables, performance measures, baseline performance requirements, resources, and schedules that defines the tasks to be performed by the unit(s). Once established, the lower level organizational unit manages its own risks against these specifications, and, as appropriate, reports risks and elevates decisions for managing risks to the next higher level based on predetermined risk thresholds (illustrated below) that have been negotiated between the two units. Figure 2 depicts this concept. Risk management decisions are elevated by an organizational unit when those risks can no longer be managed by that unit. This may be the case if, for example, resources are not available, or the organizational unit 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 measure 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.

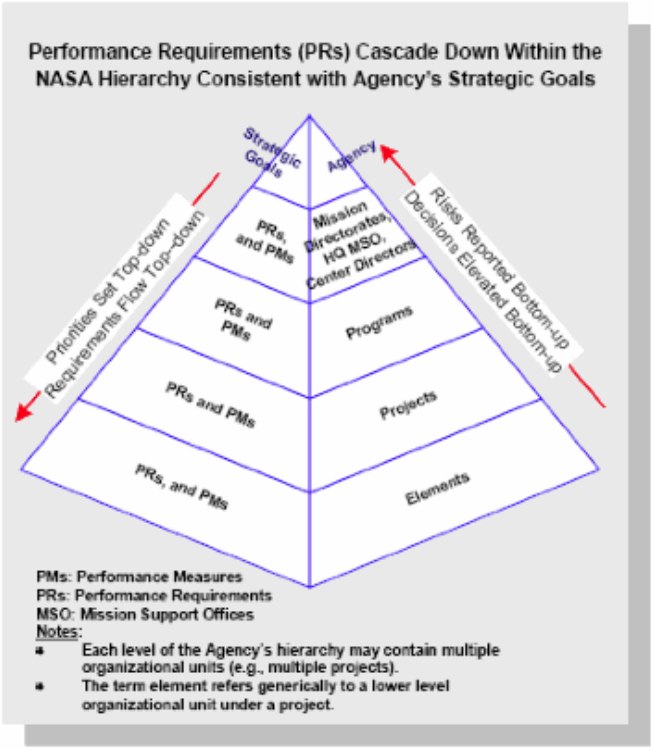

Figure 2. Flowdown of Performance Requirements (Illustrative)

f. Risk management at the Agency level addresses risks identified at the Agency level, as well as risks elevated from Mission Directorates and Mission Support Offices. These risks 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 domains of risk management (e.g., safety, technical, financial/cost, institutional).
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 decision alternatives, recognizing opportunities where they arise, and considering a sufficient number and diversity of performance measures to constitute a comprehensive set for decision-making purposes.

(2) Risk analysis of decision alternatives to support ranking.

(3) Selection of a decision alternative *informed by* (not solely based on) risk analysis results.

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.

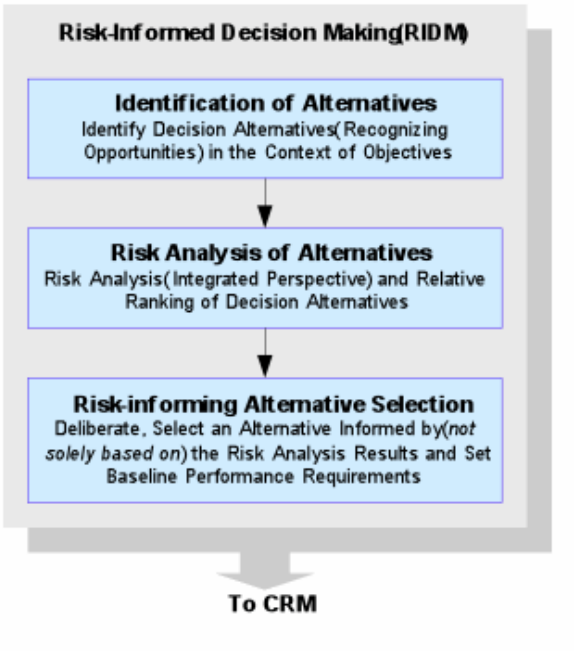

Figure 3. RIDM Process

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.

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.f, 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 quantification 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 quantify 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 3.1.2) 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.

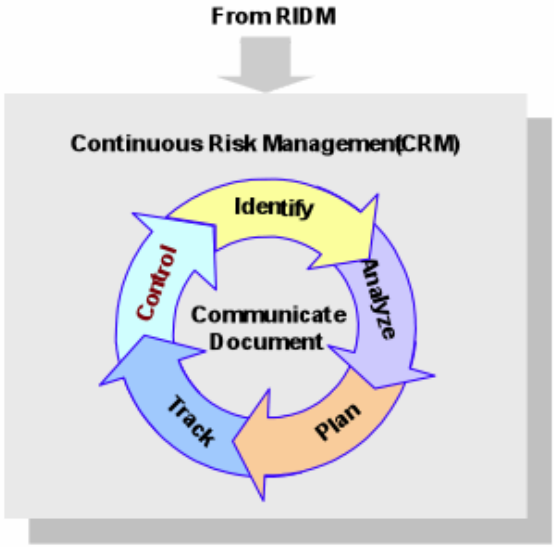

Figure 4: CRM Process

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.

(4) Track: *Track* observables relating to performance measures (e.g., technical performance data, schedule variances).

(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.

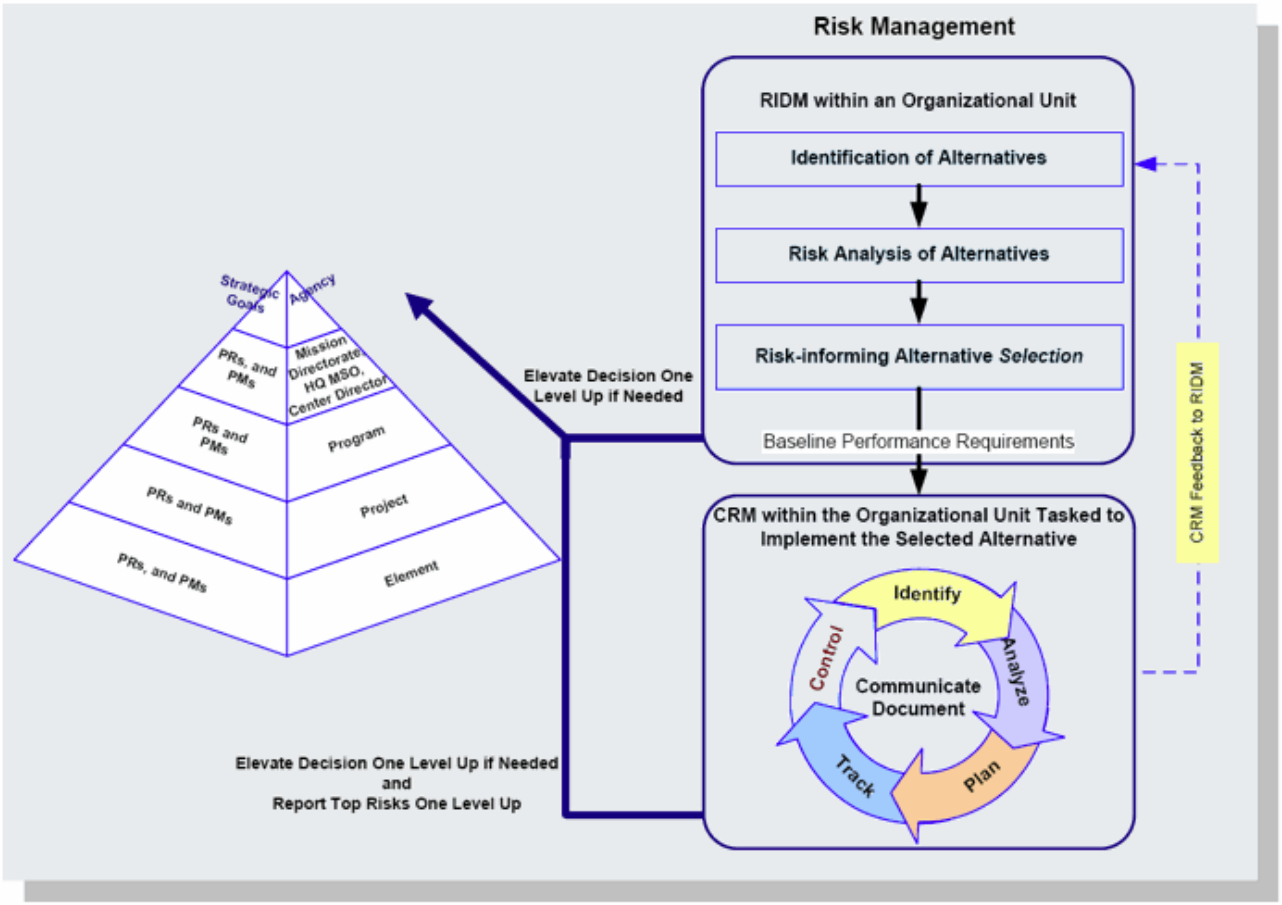

Figure 5. Coordination of RIDM and CRM Within the NASA Hierarchy (Illustrative)

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 sponsoring organization at the next higher level (as discussed in paragraph 1.2.1d). The Risk Management Plan articulates decision rules for dispositioning individual and aggregate risks, including the consideration of uncertainties in the decision process.

e. Satisfaction of performance requirements needs to be demonstrated by the lower level organizational unit to the upper level through periodic reporting of the status of risks associated with each performance measure. A basis for the evaluation of the performance measures and their associated risks should be agreed upon and documented in advance (or indicated by reference) in the Risk Management Plan (see paragraph 3.1.2.c).

f. It is the responsibility of the organizational unit at the higher level to assure that the performance requirements assigned to the organizational unit at the lower level reflect appropriate tradeoffs between/among competing objectives and risks. It is the responsibility of the organizational unit at the lower level to establish the feasibility of managing the risks of the job it is accepting, including 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 higher level.

g. Both CRM and RIDM are applied within a graded approach. The resources and depth of analysis need to be commensurate with the stakes and the complexity of the decision situations 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, 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.

h. 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.

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

Chapter 2. Roles and Responsibilities

2.1 General

2.1.1 The implementation of the requirements of this NPR 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 NPR, including the staffing and execution of the risk management function.

2.1.2 Some requirements in this NPR 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 NPR, 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 Per NPD 1000.0, risk management at the Agency level is the responsibility of the Agency's Management Councils.

2.1.5 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 NPR (Requirement 59242).

b. Program/project managers shall specify the organizational units and the hierarchy within their respective domains to which the requirements of this NPR apply (Requirement 59243).

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 NPR apply (Requirement 59244).

d. The Chief, Safety and Mission Assurance shall:

(1) Verify that this NPR is appropriately implemented across the Agency (Requirement 59246).

(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 (Req (Requirement 59247).

(3) Provide handbooks and training opportunities to facilitate implementation of this NPR (Requireme (Requirement 59248).

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.

3.1. General Risk Management Requirements

3.1.1 The manager of each organizational unit shall:

a. Ensure that the RIDM and CRM processes are implemented within the unit (Requirement 59253.

b. Designate the risk manager(s) for that unit (Requirement 59254).

Note: The role of risk manager may not need to be a full-time position. The amount of time devoted to performing the risk manager function is commensurate with the size of the organizational unit and the scope of risk that applies to the organizational unit. In addition, rather than assigning individual risk managers to subordinate organizational units, organizational unit managers may choose to incorporate all or some of the subordinate organizational units under the control of a single risk manager provided that the single risk manager has access to each of the subordinate activities for the purpose of performing the risk management function. The intent of the requirement is to assure that the function is performed, not to constrain how the organizational unit manager assigns responsibilities.

c. Ensure that the designated risk manager has experience in risk and decision analysis and in the CRM process (Requirement 59256).

d. Ensure that key decisions of the organizational unit are risk-informed (Requirement 59257).

Note: Examples of key decisions include: Architecture and design decisions, make-buy decisions, source selection in major procurements, budget reallocation (allocation of reserves).

e. Ensure that risks are identified and analyzed in relation to the performance requirements for each acquisition of the organizational unit and risk analysis results are used to inform the source selection (Requirement 59259)

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

f. Ensure, and concur in, the definition of elevation thresholds to be applied by lower-level organizational units reporting to the unit(Requirement 59261).

g. Ensure that cross-cutting risks and interdependencies between risks are properly identified as cross-cutting and either managed within the unit or elevated (Requirement 59262).

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

h. 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 (Requirement 59265).

i. Ensure that dissenting opinions arising during risk management decision making are handled through the dissenting opinion process as defined in NPR 7120.5D (Requirement 59266).

j. Ensure that risk management activities of the organizational unit support, and are consistent with, ongoing internal control activities defined in NPD 1200.1 (Requirement 59267).

3.1.2 The risk manager of each organizational unit shall:

a. Facilitate the implementation of RIDM and CRM (Requirement 59269).

b. Ensure that appropriate training is provided to organizational unit staff on risk management policies, tools, and processes, and ensure that the training material is consistent with the requirements of this NPR (Requirement 59270).

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

(1) Is integrated into the Systems Engineering Management Plan (SEMP), when applicable per NPR 7123.1 (Requirement 59293)

for program/project units).

Note: In the case of organizational units that do not have a SEMP, the Risk Management Plan is a stand-alone document or a part of program/project plans.

(2) Explicitly addresses safety, technical, cost, and schedule risks (Requirement 59295).

(3) Delineates the organizational unit's approach for applying RIDM and CRM within a graded approach (Requirement 59296).

Note: A "graded approach" applies risk management processes at a level of detail and rigor that adds value without unnecessary expenditure of unit resources.

(4) For each performance requirement, documents, or indicates by reference, whether its associated risks (including the aggregate risk) are to be assessed quantitatively or qualitatively and provides a rationale for cases where it is only feasible to assess the risk qualitatively (Requirement 59298).

(5) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories (Requirement 59299).

(6) Identifies stakeholders, such as Risk Review Boards, to participate in deliberations regarding the disposition of risks (Requirement 59300).

(7) Establishes 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)(Requirement 59301).

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(Requirement 59303)

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 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) Delineates the processes for coordination of risk management activities and sharing of risk information with other affected organizational units (Requirement 59307).

(10) Documents the concurrence of the organizational unit management to which the risk manager's organizational unit reports, including its risk reporting requirements (Requirement 59308).

d. Periodically review the risk management plan to ensure its currency (Requirement 59309).

3.2 Requirements for the RIDM Process

The manager of each organizational unit shall:

a. Ensure that performance measures defined for the organizational unit are used for risk analysis of decision alternatives to assist in RIDM (Requirement 59312).

b. Ensure that the bases for performance requirement baselines (or rebaselines) are captured (Requirement 59313).

c. Negotiate institutional support performance requirements with Center support units when required to meet program/project requirements (Requirement 59314)

for program/project units).

d. Ensure that performance measures defined for the organizational unit are used to scope the unit's CRM process (Requirement 59315).

3.3 Requirements for the CRM Process

3.3.1 General Requirements

The risk manager shall:

a. Implement the CRM process (as defined in this NPR in paragraph 3.3.2) (see also Figure 4 and associated discussion) (Requirement 59319).

b. Coordinate the unit's CRM process with the CRM processes of organizational units at levels above and below, including contractors if applicable (Requirement 59320).

c. Ensure that risk documentation is maintained in accordance with NPD 1440.6 and NPR 1441.1, and under formal configuration control, with a capability to identify and readily retrieve the current and all archived versions of risk information and the Risk Management Plan (Requirement 59321).

3.3.2 Specific Requirements

3.3.2.1 Identify

a. The risk manager of any given unit shall ensure that the execution of the risk identification step is thorough and consistent with the baseline performance requirements of that unit (Requirement 59324).

b. The risk 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) (Requirement 59325).

c. The risk 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 (Requirement 59326).

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 risk 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 (Requirement 59329).

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).

b. When a risk management decision is elevated from a lower-level organizational unit, the risk 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 at the higher level (Requirement 59331).

c. Wherever determined to be feasible (as documented in the Risk Management Plan), the risk manager shall ensure the characterization of aggregate risk through analysis (including uncertainty evaluation), as an input to the decision-making process (Requirement 59332).

d. The risk manager shall ensure that analyzed risks are prioritized and used as input to the "Plan," "Track," and "Control" activities (paragraphs 3.3.2.3 through 3.3.2.5) (Requirement 59333).

e. The risk manager shall ensure that the results of the "analyze" step are documented and communicated to unit management (Requirement 59334).

3.3.2.3 Plan

a. Each organizational unit manager, supported by the risk 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 3.1.2.c.(7) (Requirement 59336).

b. The organizational unit 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 (Requirement 59337).

(1) When a decision is made to *accept* a risk, the risk manager shall ensure that each acceptance is clearly documented in their organizational unit's risk database (list), including the assumptions and conditions (risk acceptability criterion) on which the acceptance is based (Requirement 59338).

(2) When a decision is made to *mitigate* a risk, the risk manager shall ensure that a risk mitigation plan is developed and documented in the risk database (list) (including the appropriate parameters that will be tracked to determine the effectiveness of the mitigation) (Requirement 59339).

(3) When a decision is made to *close* a risk, the risk manager shall ensure that the closure rationale is developed, approval of closure is obtained from the unit manager, and that both rationale and management approval are documented in the risk database (Requirement 59340).

(4) When a decision is made to *watch* a risk, the risk manager shall ensure that tracking requirements are developed and documented in the risk database (list). (Requirement 59341).

(5) When additional information is needed to make a decision, the risk manager shall ensure that efforts to *research* a risk (obtain additional information) are documented and tracked in the risk database (list) (Requirement 59342).

(6) When dispositions (1), (2), (3), (4), or (5) above cannot be applied, the organizational unit

manager shall *elevate* the decision to the organizational unit management at the next higher level and document the action taken in the risk database (list) (Requirement 59343).

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

c. For "mitigate," "watch," and "research," the organizational unit manager, supported by the risk manager, shall designate an appropriate entity to implement the disposition (Requirement 59345).

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

d. The risk manager shall ensure that all risks categorized as "watch" have decision points, dates, milestones, necessary achievements, or goals identified (Requirement 59347).

3.3.2.4 Track

a. The risk 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 (Requirement 59350).

b. The risk manager shall ensure the dissemination of tracking data to entities identified in the Risk Management Plan as recipients of these data (Requirement 59351).

3.3.2.5 Control

a. The risk 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.c (Requirement 59353).

b. The organizational unit manager shall provide feedback to affected organizational units, including the sponsoring unit 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 (Requirement 59354).

c. Based on the tracking data, in order to control a given risk, the risk owner shall recommend actions to the organizational unit manager and oversee implementation of risk control actions with which the organizational unit manager has concurred (Requirement 59355).

Appendix A. Definitions

A.1 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.

A.2 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.

A.3 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.

A.4 Deliberation. In the context of this NPR, 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.

A.5 Dispositions (Risk)

A.5.1 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.

A.5.2 Research. The investigation of a risk in order to acquire sufficient information to support another disposition; i.e., close, watch, mitigate, accept, or elevate.

A.5.3 Watch. The monitoring of a risk for early warning of a significant change in its probability, consequences, uncertainty, or timeframe.

A.5.4 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.

A.5.5 Accept. The formal process of justifying and documenting a decision not to mitigate a given risk associated with achieving given objectives or given performance requirements. (See also A.13, Risk Acceptability Criterion).

A.5.6 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."

A.6 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).

A.7 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.

A.8 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.

A.9 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.

A.10 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.

A.11 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.

A.12 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.

A.13 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.

A.14 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."

A.15 Risk Management. Risk management includes RIDM and CRM in an integrated framework. This is done in order to foster proactive risk management, to better inform decision making through better use of risk information, and then to more effectively manage implementation risks by focusing the CRM process on the baseline performance requirements emerging from the RIDM process.

A.16 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.

A.17 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.

A.18 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 NPR uses the term "safety" broadly to include human safety (public and workforce), environmental safety, and asset safety.

A.19 Scenario. A sequence of events, such as an account or synopsis of a projected course of action or events.

A.20 Threshold. A level for a performance measure or a risk metric whose exceedance "triggers" management processes to rectify performance shortfalls.

A.21 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

CRM	Continuous Risk Management
FAR	Federal Acquisition Regulation
KM	Knowledge Management
NASA	National Aeronautics and Space Administration
MSO	Mission Support Offices
NFS	NASA FAR Supplement
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
QASP	Quality Assurance Surveillance Plan
RIDM	Risk-Informed Decision Making
PR	Performance Requirement
SEMP	Systems Engineering Management Plan

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 postaward 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 organizational unit 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 organizational unit manager should ensure that the project technical team addresses the risks identified in paragraph C.1.a, above, in the solicitation requirements.

b. The organizational unit 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 organizational unit 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 organizational unit 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. Organizational unit managers should periodically review the surveillance plan to ensure currency related to risks.

Note: This final QASP should not be included in the contract but should be periodically reviewed to ensure its currency.

b. Organizational unit managers should ensure that acquisition-related risks are continuously managed using the CRM process.