NASA Procedural Requirements

NPR 8000.4B
Effective Date: December 06, 2017
Expiration Date: December 06, 2022

COMPLIANCE IS MANDATORY

Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

P.1 Purpose

a. This NASA Procedural Requirements (NPR) provides the requirements for risk management for the Agency, its institutions, and its programs and projects as required by NPD 1000.0; NPD 7120.4; NPD 8700.1, and other Agency directives. 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's organizational hierarchy. It provides a framework that integrates the RIDM and CRM processes across levels. It requires formal processes for risk acceptance and accountability that are clear, transparent, and definitive. This directive also establishes the roles, responsibilities, and authority to execute the defined requirements Agency-wide. It builds on the principle that program, project, and institutional 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 in that (a) it applies to all Agency strategic goals and the objectives and requirements that derive from them, (b) it addresses all sources of risk, both internal and external to NASA, (c) all risks are considered collectively during decision-making, and (d) risk management activities are coordinated horizontally and vertically, across and within programs, projects, and institutions, to ensure timely identification of cross-cutting risks and balanced management of risks Agency wide.

d. This directive contains requirements for risk management. Detailed explanations, descriptions, and technical guidance are provided in associated handbooks, including NASA/SP-2011-3422, NASA Risk Management Handbook (Reference D.7).

P.2 Applicability

a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This directive applies to Jet Propulsion Laboratory (JPL) (a Federally-Funded Research and Development Center), other contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.

b. This directive applies to all Agency activities, including 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.

c. In this directive, 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" and "is" denotes descriptive material.

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

P.3 Authority

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

b. NPD 1000.0, Governance and Strategic Management Handbook.

P.4 Applicable Documents and Forms

a. NPD 1200.1, NASA Internal Control.

b. NPD 1440.6, NASA Records Management.

c. NPD 2810.1, NASA Information Security Policy.

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

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

f. NPD 8900.5, NASA Health and Medical Policy for Human Space Exploration.

g. NPR 1441.1, NASA Records Management Program Requirements.

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

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

j. NPR 8705.4, Risk Classification for NASA Payloads.

P.5 Measurement/Verification

Compliance with the requirements contained in this directive will be verified through the application of the assessment process required by paragraph 2.2.5.b.

P.6 Cancellation

a. NPR 8000.4A, Risk Management Procedural Requirements, dated December 16, 2008.

b. NASA Interim Directive (NID) Agency Risk Management Procedural Requirements, dated October 24, 2016.

Chapter 1. Introduction

1.1 Background

1.1.1 Generically, risk management is a set of activities aimed at understanding, communicating, and managing 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 risks associated with implementation of the selected alternative. In this NPR, risk management is defined in terms of RIDM and CRM. This NPR addresses the application of these processes to all Agency activities directed toward the accomplishment of Agency strategic goals, including: strategic planning and assessment; program and project concept development, formulation, and implementation; institutional management of infrastructure, including physical, human, and information technology resources; and acquisition. This NPR 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.

1.1.2 The purpose of integrating RIDM and CRM into a coherent framework is to foster proactive risk management: to inform better decision making through better use of risk information, and then to manage more effectively 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. NPD 1000.0 cites this NPR with regard to the topics of "Clear Roles, Responsibilities, and Decision Making" and "Authority roles regarding risk." Figure 1 shows that this NPR intersects with program/project management (e.g., NPD 7120.4), safety and mission success (e.g., NPD 8700.1), health and medical (e.g., NPD 8900.5), and other domain-specific directives (e.g., NPD 2810.1) and associated requirements.

1.1.3 This NPR supports NASA's internal control activities as specified in NPD 1200.1, which implements Office of Management and Budget (OMB) Circular A-123 and the related Government Accountability Office Standards for Internal Control in the Federal Government, including GAO-14-704G). The framework in this NPR for conducting risk management across strategic, programmatic, financial, and institutional activities is compatible with the Enterprise Risk Management (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 acceptable levels. The effectiveness of the internal controls is assessed and reported in accordance with the requirements contained in NPD 1200.1.

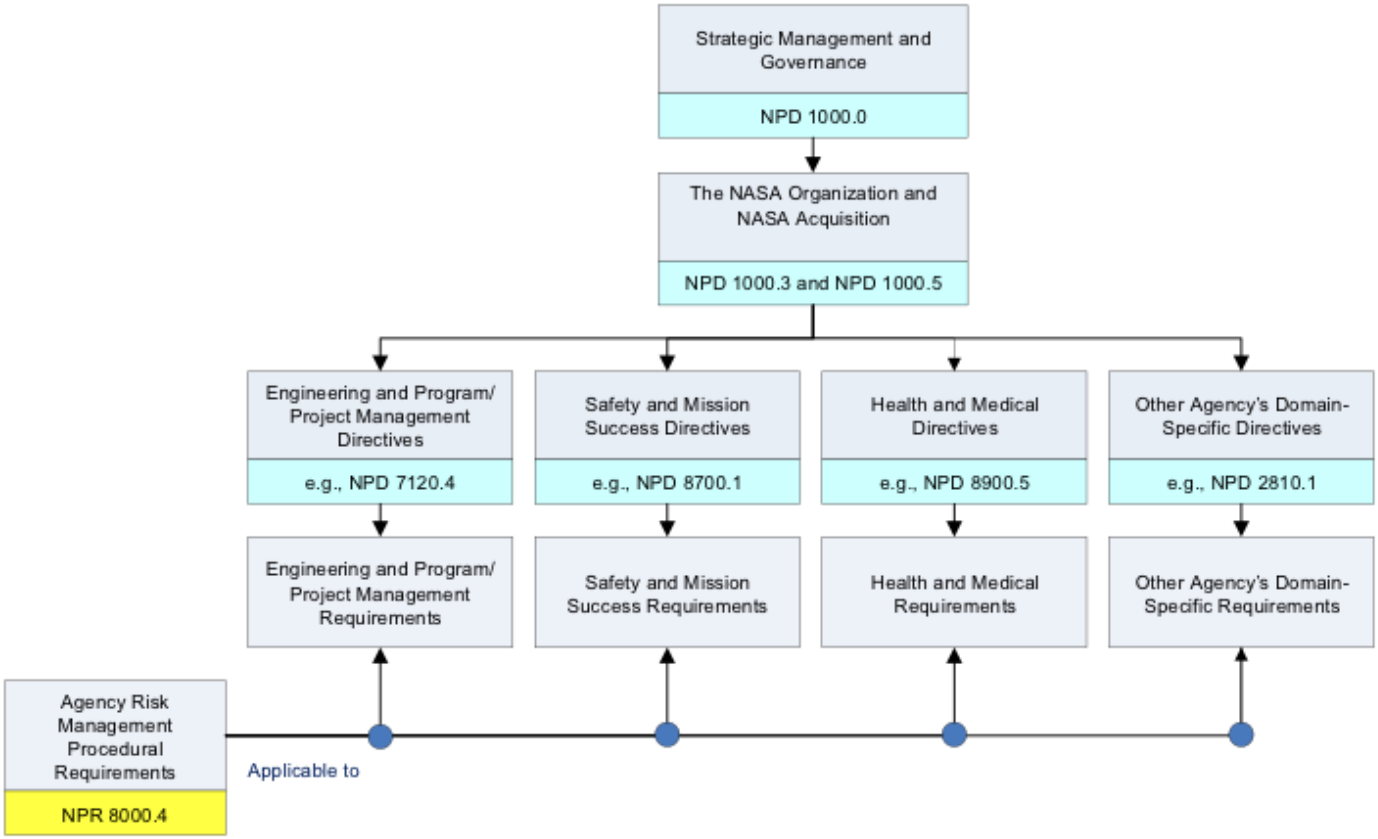

Figure 1. Intersection of NPR 8000.4 with Program/Project and Domain-Specific Directives and Requirements

1.1.4 This NPR supports NASA's information security activities as specified in NPD 2810.1, which implements security policy best practices and guidance outlined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series and Federal Information Processing Standards. The framework in this NPR for managing risks associated with cybersecurity threats is compatible with the Framework for Improving Critical Infrastructure Cybersecurity provided by NIST. The NIST framework, which presents a risk-based approach to managing cybersecurity risk that complements NASA's existing risk management processes and cybersecurity programs, supports the implementation of and compliance with the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283) and is mandated for use by NASA per Presidential Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

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

1.2 Risk Management within the NASA Hierarchy

1.2.1 Key Concepts

1.2.1.1 In general, risk is concerned with uncertainty about future outcomes. For the purposes of this NPR, risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives. As applied to programs and projects, these objectives are translated into performance requirements, which may be related to institutional support for mission execution or related to any one or more of the following domains:

a. Safety

b. Mission Success (Technical)

c. Cost

d. Schedule

1.2.1.2 In this NPR, 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), mission success (technical) performance (e.g., thrust or output, amount of observational data acquired), cost performance (e.g., execution within allocated budget), or schedule performance (e.g., meeting milestones). Similar performance measures can be defined for institutional support.

1.2.1.3 Conceptually, the risk to an objective consists of the following set of triplets:

a. 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);

b. The likelihood(s) (qualitative or quantitative) of those scenario(s); and

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

> *Note: "Likelihood" is the probability that a scenario will occur. Its assessment 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. A complete assessment of likelihood also calls for characterization of its uncertainty.*

1.2.1.4 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 define 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 NPR 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.).*

1.2.1.5 The Provider reports risks and/or 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.

> *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 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).

1.2.1.6 Mission Directorates are responsible for management of technical and programmatic risks within their domains and are responsible for elevating risks to the Program Management Council at the Agency level. Center Directors are responsible for management of institutional risks at their respective Centers. Headquarters Administrator Support Offices and Mission Support Offices are responsible for Agency-wide risk management in their domains in accordance with NPD 1000.3. Center Directors and Mission Support Offices are responsible for elevating risks to the Mission Support Council. 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.

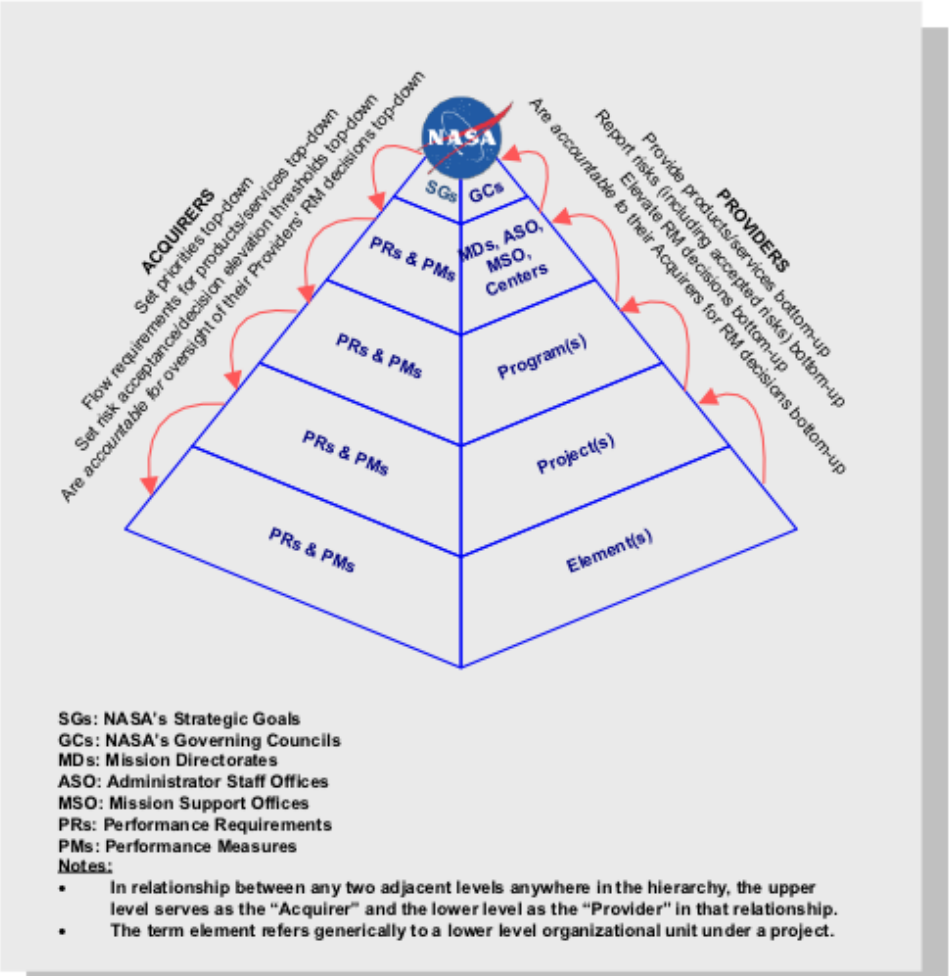

Figure 2. Risk Management in NASA's Organizational Hierarchy

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

a. A need for the Agency to allocate additional resources for effective mitigation.

b. Agency-level coordination/integration is needed with other organizations/stakeholders.

c. A finding that a risk identified within a Center or Mission Directorate is, in fact, an Agency-level risk.

1.2.1.8 Risk management at the Agency level integrates the full spectrum of risks by:

a. Dealing with risk strategically from an Agency-level perspective. At the Agency level, emphasis is placed on achievement of 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.

b. Engaging all functions and line management levels.

c. Risk-informing program, mission support, and capability portfolio development and management.

d. Supporting institutional management of infrastructure, e.g., cybersecurity risk management.

1.2.2 RIDM

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

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

b. Analysis of Alternatives: Conduct Integrated Analysis of Risk of Each Alternative; Develop the Technical Basis for Deliberation.

c. 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.

1.2.2.2 Rather than an isolated activity, RIDM is a key element of the risk management approach used by institutional and programmatic organizations. It informs all aspects of strategic, program and mission, and mission-enabling decision making and is, therefore, conducted in many different venues based on the organization and management processes of the implementing organizational unit. These include council, board, and panel meetings, Authority to Proceed milestone reviews, Safety Review Board meetings, Risk Reviews, Engineering Design and Operations Planning decision forums, and commit-to-flight reviews, among others.

1.2.2.3 Within the RIDM process, the complete set of performance measures (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, mission success, cost, schedule) that are flowed down to Provider organizations.

1.2.2.4 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 1.2.4.5, situations may arise in which it is necessary to revisit the decision and rebaseline the performance requirements.

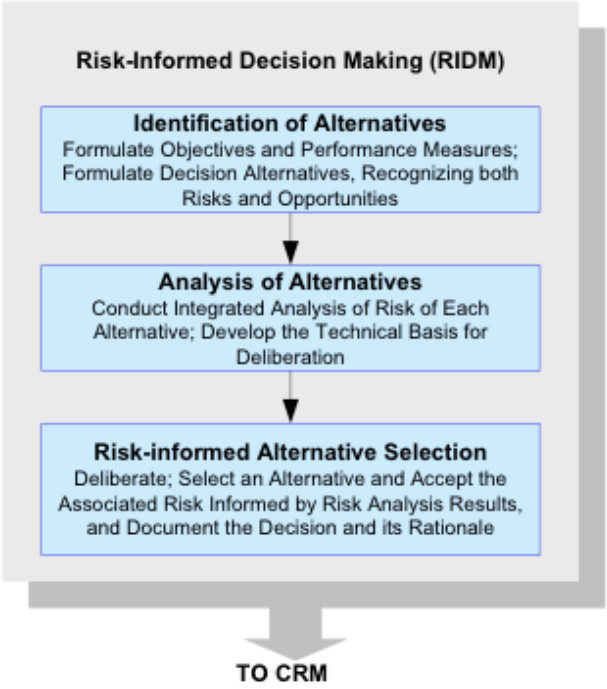

Figure 3. RIDM Process

1.2.2.5 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 and schedule risk are analyzed probabilistically in an integrated fashion using a Joint Confidence Limit (JCL) analysis per NPR 7120.5. 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 3.2.2.i) for each organizational unit.

1.2.3 CRM

1.2.3.1 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, is referred to as CRM.

Figure 4. CRM Process

1.2.3.2 Steps in the CRM process include: a. IDENTIFY: Identify contributors to risk (shortfalls in performance relative to the baseline performance requirements).

> *Note: Performance measures determine the scope of CRM. Sometimes, the relationship between an identified risk and performance measures is indirect, but risks within the proper scope of CRM are addressed because they may affect one or more performance measures.*

b. ANALYZE: Estimate the probability and consequence components of the risk through analysis, including uncertainty in the probabilities and consequences and, if feasible, estimate aggregate risks.

c. PLAN: Decide on risk disposition and handling, develop and execute mitigation plans, develop contingency plans, and decide what will be tracked.

> *Note: Risk acceptance is among the possible dispositions (see paragraph 3.4.2.i.(1)). The requirements of paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks) apply to risk acceptance decisions.*

d. 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.

e. CONTROL: Evaluate tracking data to verify effectiveness of mitigation plans, making adjustment to the plans as necessary and executing control measures.

f. 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

1.2.4.1 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.

1.2.4.2 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.

1.2.4.3 Each organizational unit reports on its risk management activities to the Acquirer 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 1.2.1.5.

1.2.4.4 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 1.2.1.5).

1.2.4.5 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 needs to be negotiated with higher level organizations, 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 needs to be approved by the Acquirer.

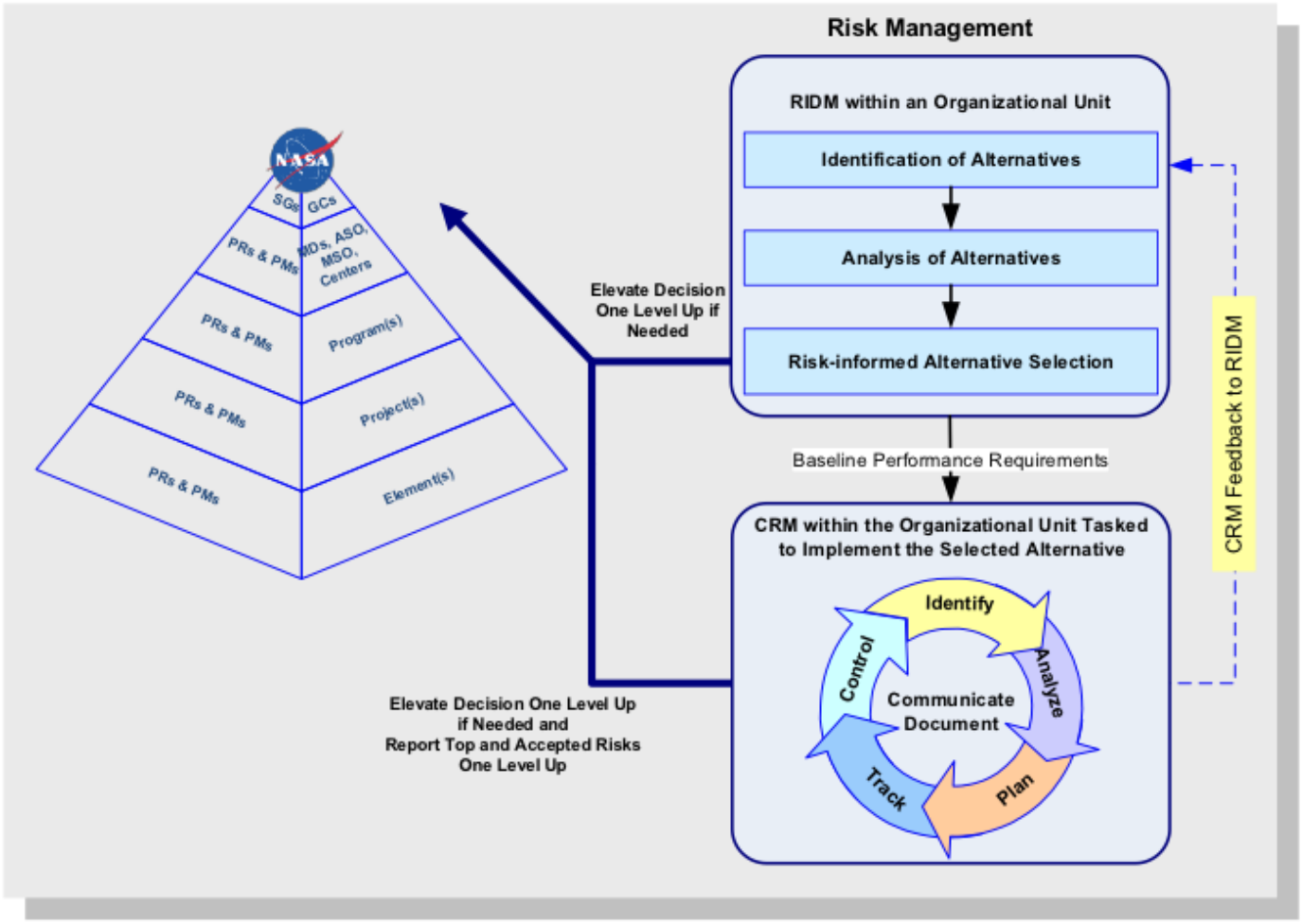

Figure 5. Coordination of RIDM and CRM within the NASA Hierarchy (Illustrative)

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

1.2.4.7 At each Center, management of institutional risks affecting programs/projects at the Center is done within the Center institutional hierarchy and coordinated with the program/project units as needed. Since the program/project units are affected by institutional risks without being in a position to control them, in the event that institutional risks threaten accomplishment of program/project unit performance requirements, the program/project units may need to elevate them to the next level within the program/project or Center hierarchies.

1.2.4.8 Agency-wide institutional risks are addressed by NASA Headquarters Administrator Support Offices, Mission Support Offices, and the Mission Support 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 Headquarters and Center mission support and institutional organizations, while management of mission execution risks is the focus of program/project organizational units.

2.2 Organizational Roles and Responsibilities

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

2.2.2 Mission Directorate Associate Administrators specify organizational units within their Directorates responsible for the implementation of the requirements of this NPR.

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

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

2.2.5 The Chief, Safety and Mission Assurance:

a. Verifies that this NPR is appropriately implemented across the Agency.

b. Prepares an assessment process to be used to establish compliance determinations across Mission Directorates, programs and projects, Centers, and Headquarters Mission Support Offices.

c. Collaborates with other key stakeholders to ensure that handbooks and training opportunities are available to facilitate implementation of this NPR.

2.2.6 The Chief Information Officer develops and implements the Agency's Information Technology (IT) Risk Management framework, compatible with both the NIST risk management framework and the risk management framework in this NPR, for managing risks to NASA's IT infrastructure.

2.2.7 Capability portfolio managers (e.g., the Manager for Rocket Propulsion Testing (RPT) Program), in collaboration with the stakeholders identified in NPD 1000.3, risk-inform the development and implementation of their respective asset and capability portfolios for the Agency.

2.3 Individual Accountabilities for Risk Acceptance

2.3.1 Programmatic authorities, e.g., program/project managers are accountable for risk acceptance decisions for their programs or projects, commensurate with their delegated authority.

2.3.2 Center Directors are accountable for risk acceptance decisions for institutional activities at their Centers.

2.3.3 Formally delegated 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).

Note: The TA role also includes framing safety and mission success issues of concern (potentially underappreciated risks) in terms of candidate risks for formal adjudication and disposition by the organizational unit managers.

2.3.4 When there is risk to humans, the actual Risk Takers (e.g., astronauts, pilots) (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.

Chapter 3. Requirements for Risk Management

3.1 General

3.1.1 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.

3.1.2 Four categories of requirements are presented in this chapter: General Risk Management Requirements, Requirements for the RIDM Process, Requirements for the CRM Process, and Requirements for Risk Acceptance. Acceptance of risks to safety 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.

3.1.3 If it becomes evident that it is not practical to satisfy one or more 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 paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks)). This is the case even if, administratively, the risk is not dispositioned as "accepted" under the CRM Plan requirements of paragraph 3.4.2.i.(1).

3.1.4 In the subsections below, requirements are levied on "the manager." This term is used in this NPR to refer to the manager of the organizational unit. The manager can delegate the execution of certain processes as specified in the Risk Management Plan. However, the wording is meant to convey that the manager is accountable for fulfilling the requirements of this NPR and for the decisions that are made, specifically including risk acceptance decisions as defined in the Risk Management Plan.

3.2 General Risk Management Requirements

3.2.1 Some of the following requirements apply specifically to either Acquirers or Providers. Those requirements are labeled either "Acquirer organizations" or "Provider organizations," according to their context.

3.2.2 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. (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 criteria 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 scopes all the risk types within the purview of the organizational unit, e.g., for programs/projects, these would be safety, mission success, 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) Cites the documents that capture the complete set of requirements (within the scope established in (1), above) to be met by the organization, including the top-level Safety and Mission Success requirements levied on the organization, derived requirements, process requirements, and commitments (e.g., testing) (Provider organizations).

Note 1: This plan serves to clarify what detailed requirements (and 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 and, in particular, the specification of risk acceptability criteria (see item (7) below). The Acquirer's review of this portion of the plan provides an early opportunity to ensure that the Provider is adequately addressing the safety and mission success requirements and is implementing a risk-informed process in development of the system.

Note 2: For each 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 paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks).

Note 5: Per NPR 7120.5, cost and schedule commitments are derived from JCL analysis.

(4) Is coordinated with other management plans, such as higher level risk management plans and the Systems Engineering Management Plan (SEMP), when applicable per NPR 7123.1.

(5) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories. Determines and documents the protocols for estimation of the likelihood and severity of the consequence components of risks, including uncertainty characterization and quantification.

Note: The characterization of 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).

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

Note 1: A "risk acceptability criterion" is a rule for determining whether a given organizational unit has the authority to decide to accept a risk.

Note 2: The Risk Management Plan required in 3.2.2.i. delineates (refer to subparagraph (3)) a body of performance requirements to be met by the Provider. Risk acceptability criteria are formulated to allow the Provider engineering discretion, while still assuring satisfaction of those performance requirements. As long as the performance requirements are being satisfied, the Provider has discretion to act; if satisfaction of the requirements would be placed in doubt by acceptance of a risk, then either the risk is elevated, or the requirements are rebaselined.

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

(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 mission support and institutional organizations, protocols are needed for reporting risks to affected program/project units and vice versa.

(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 3.5.3 for application of this form).

(10) Establishes an interval for the periodic review of the assumptions on which risk acceptance decisions are based.

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

(12) Documents the manager's signature and the concurrence of the Acquirer to which the manager reports, which includes concurrence that the Risk Management plan meets the Acquirer's requirements. (Provider organizations)

j. Ensure that decisions to rebaseline performance requirements, grant waivers, or modify Risk Management Plans that affect safety, mission success, or institutional risk 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 paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks)). Note: Per requirements in paragraph 3.2.2.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.

k. Ensure that risk documentation for both RIDM and CRM 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.

3.2.3 Within a graded approach, managers responsible for lower-cost, lower-priority missions that may have lower likelihood of success (e.g., Cubesat, Risk Class D missions (see NPR 8705.4)) fulfill the above requirements by committing to satisfy levied technical requirements and reporting at milestone reviews on the status of satisfying the requirements, including concurrence(s) from the concurring authority for the assets put at risk by the project.

Note: Satisfaction of properly defined technical requirements means that the project will "do no harm" to assets potentially put at risk by the project. For example, a secondary payload does not pose risk to the launch vehicle, primary payload(s), host platform (e.g., International Space Station), or operational environment (e.g., orbital debris environment, etc.).

3.3 Requirements for the RIDM Process

3.3.1 The manager shall ensure that key decisions, including risk acceptance decisions, are informed by Analysis of Alternatives carried out by applying the RIDM process (refer to Figure 3) with a level of rigor that is commensurate with the significance and the complexity of the decisions.

3.3.2 The manager shall ensure that:

a. The rationale for the selected decision alternative is developed and documented to include contending decision alternatives considered, a summary of risk analysis results for each alternative, and the pros and cons of each alternative.

b. The bases for performance requirement baselines (or rebaselines) informed by the RIDM process are captured and documented and that these baselines (including associated institutional requirements) are applied to scope the unit's CRM implementation.

3.4 Requirements for the CRM Process

3.4.1 The manager shall coordinate the unit's CRM process (refer to Figure 4) with the CRM processes of organizational units at levels above and below, including contractors.

3.4.2 The manager shall ensure that:

a. Risk identification is comprehensive and consistent with the baseline performance requirements of that unit. (related to IDENTIFY step)

b. Risk analyses performed to support RIDM (see paragraph 3.3.) are used as input to the "IDENTIFY" step of CRM. (related to IDENTIFY step)

c. The results of risk identification are documented to provide input to the "ANALYZE" step and to characterize the risks for purposes of tracking. (related to IDENTIFY step)

> *Note: When this documentation takes the form of a "risk statement" or "risk scenario," NASA/SP-2011-3422 uses the following format: "Given that [CONDITION], there is a possibility of [DEPARTURE] from the baseline adversely impacting [ASSET], thereby leading to [CONSEQUENCE]." (Refer to NASA/SP-2011-3422 for more information on risk statements.) 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).*

d. When a risk management decision is elevated from a lower-level organizational unit, the associated risk is recalibrated with respect to the requirements, thresholds, and priorities that have been established at the higher level, and the recalibrated risks are entered into the "PLAN," "TRACK," and "CONTROL" steps (paragraphs h. through q.) at the higher level. (related to ANALYZE step)

e. Wherever determined to be feasible (as documented in the Risk Management Plan), aggregate risk is characterized through analysis (including uncertainty evaluation), as an input to the decision-making process. (related to ANALYZE step)

f. Analyzed risks are prioritized and used as input to the "PLAN," TRACK," and "CONTROL" steps. (related to ANALYZE step)

g. The results of the "ANALYZE" step are documented. (related to ANALYZE step)

h. 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 3.2.2.i.(6). (related to PLAN step)

i. Only one of the following possible risk dispositions is applied to any given risk. (related to PLAN

step)

(1) When a decision is made to ACCEPT a risk, each acceptance is clearly documented in the organizational unit's risk database, including the rationale for acceptance, the assumptions (including the conditions (e.g., programmatic constraints)) on which the acceptance is based, the applicable risk acceptance criteria, and the interval (as required by the Risk Management Plan) after which the assumptions will be periodically reviewed for any changes that might affect the continued acceptability of the risk. Additionally, for risk acceptance decisions, the requirements in paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks) apply.

(2) When a decision is made to MITIGATE a risk, a risk mitigation plan (including contingency planning) is developed and documented in the risk database (including the parameters that will be tracked to determine the effectiveness of the mitigation).

(3) When a decision is made to CLOSE a risk, the closure rationale is developed, and both rationale and management approval are documented in the risk database.

(4) When a decision is made to WATCH a risk, tracking requirements are developed and documented in the risk database. All risks categorized as "WATCH" have triggering events, decision points, dates, milestones, necessary achievements, or goals identified.

(5) When additional information is needed to make a decision, efforts to RESEARCH a risk (obtain additional information) are documented and tracked in the risk database.

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

j. For "MITIGATE," "WATCH," and "RESEARCH," an entity is designated to implement the disposition. (related to PLAN step)

k. A process for acquiring and compiling observable data to track the progress of the implementation of risk management decisions is developed and implemented. (related to TRACK step)

l. The cumulative effects of risk management decisions and risk acceptance decisions (i.e., the aggregate effect of accumulated, accepted risks, to ensure the aggregate risk remains tolerable) are tracked. (related to TRACK step)

m. The assumptions on which risk acceptance decisions are based (see 3.4.2.i.(1)) are periodically tracked. (related to TRACK step)

n. Tracking data are disseminated to entities identified in the Risk Management Plan as recipients of these data. (related to TRACK step)

o. Tracking data are evaluated in order to assess the effectiveness of decisions implemented in paragraph 3.4.2.i. (related to CONTROL step)

p. Feedback is provided to affected organizational units, including the 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. (related to CONTROL step)

q. If warranted by the tracking data, necessary control action(s) is(are) implemented. (related to CONTROL step)

Note: Because the "Document and Communicate" function of CRM is integral to all of the steps in the CRM process (Figure 4), requirements for documentation and communication are

integrated into the preceding steps rather than treated as a separate step.

3.5 Requirements for Decisions to Accept Risks to Safety or Mission Success

3.5.1 All key program/project decisions that threaten: 1) fulfillment of the Acquirer's top-level safety and mission success (S&MS) requirements levied on the Provider; 2) fulfillment of derived S&MS requirements developed by the Provider and accepted by the Acquirer as sufficing to demonstrate compliance with top-level requirements; or 3) satisfaction of other Provider commitments (e.g., commitments to conduct flight testing), are subject to the requirements of this section on creation of the basis for the decision, TA concurrence, and risk taker consent (if applicable). This includes decisions made at Key Decision Points (KDP); significant milestones (e.g., Flight Readiness Reviews), which entail consideration of decisions to proceed despite existing risks; when performance requirements are being rebaselined, e.g., rebaselining to relax safety requirements, which tacitly accepts safety risk; when waivers are being considered, e.g., waivers of safety requirements, which may increase risk; and when an Acquirer is taking delivery of a system or capability, which entails assumption of responsibility for managing the associated risks, including risks previously accepted by the Provider.

3.5.2 Although the above decisions are not necessarily couched as "risk acceptance" decisions, they nevertheless have implications for safety or mission success. Each KDP functions as an integrated system-level roll-up of the many decisions at different levels in the organization through which risk has been implicitly or explicitly accepted up to that point, and a decision to proceed represents both formal acceptance of this risk and accountability for this risk going forward.

3.5.3 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, 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 1: 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, mission success, cost, and schedule 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.

Note 2: The purpose of this requirement is not to compel execution of the formal processes for acceptance of every minor risk or decision individually but rather to foster the identification and management of credible risks, both individually and as a group, based on a technically sound analysis, in order to promote understanding of the aggregate risk being accepted, and to assign accountability for risk acceptance with the programmatic decision makers.

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: Refer to Note under paragraph 2.3.3.c.

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.

3.5.4 In the event of TA or risk taker 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).

3.5.5 In the event of TA concurrence and risk taker consent (if applicable) 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.

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

3.5.6 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, based on:

a. The TA (at the Provider's level) findings accompanying the Provider's technical basis.

b. Independent evaluation of the technical basis by the TA at the Acquier's level.

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.

3.5.7 For lower-cost, lower-priority missions that may have lower likelihood of success (e.g., Cubesat, Risk Class D missions (see NPR 8705.4)), responsible project managers may limit formal risk acceptance decisions (excluding those related to personnel or public safety) to milestone and flight readiness reviews (see paragraph 3.2.3).

Note: Refer to paragraph 3.2.3 for "graded approach" considerations.

3.6 Requirements for Decisions to Accept Institutional Risks at Centers

For "institutional risks" (as defined in Appendix A), the Center Director shall develop, document in the institutional risk management plan, and implement a process for institutional risk acceptance that meets the intent of the requirements of paragraph 3.5. Depending upon the nature of the risk, the process should specify who the individual risk acceptor is and who serves as the concurring authority (analogous to the TA role in paragraph 3.5), with the understanding that the Center Director remains accountable for institutional risk acceptance decisions at the Center.

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 goal, objective, or 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.

Candidate Risk: A potential risk that has been identified and is pending adjudication by the affected programmatic or institutional authority.

Consequence: The key, possible negative outcome(s) of the current key circumstances, situations, etc., causing concern, doubt, anxiety, or uncertainty.

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.

Cybersecurity Risk: Threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism. (From National Cybersecurity Protection Act of 2014.)

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.

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 no longer exists (e.g., the underlying condition no longer exists), has become a problem and is now tracked as such, because the associated scenario likelihoods are low (e.g., the likelihood has been reduced below a defined threshold), or the associated consequences are low (e.g., the consequence has been reduced below a defined threshold).

> *Note: Closing a risk due to low likelihood is still a risk acceptance decision. From a risk acceptance perspective, it is still necessary to account for the cumulative effects of risks closed due to low likelihood (see section l.).*

(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: After mitigation, there will still be a need to accept any remaining risk and account for its contribution to the aggregate risk.

(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, operations, occupational safety and health, environmental management, security, or programmatic constraints that affect capabilities and resources necessary for mission success, including institutional flexibility to respond to changing mission needs and compliance with internal (e.g., NASA) and 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: Probability of occurrence.

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: Risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives. As applied to programs and projects, these objectives are translated into performance requirements, which may be related to mission execution domains (safety, mission success, cost, and schedule) or institutional support for mission execution. Risk is operationally characterized 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 identification of scenarios.

Note: A risk is an uncertain future event that could threaten the achievement of performance objectives or requirements. A "problem," on the other hand, describes an issue that exists now, or an event that has occurred with 100 percent certainty, and is threatening the achievement of the objective or requirement.

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 inform better decision making through better use of risk information, and then to manage more effectively implementation risks by focusing the CRM process on the baseline performance requirements informed by the RIDM process.

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 NPR 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
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
GAO	Government Accountability Office
IT	Information Technology
KDP	Key Decision Point
KM	Knowledge Management
MSO	Mission Support Offices
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OMB	Office of Management and Budget
QASP	Quality Assurance Surveillance Plan
RIDM	Risk-Informed Decision Making
TA	Technical Authority

Appendix C. Procurement/Contract Risk Management

C.1 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.

C.2 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.3 Acquisition Strategy Development

C.3.1 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.

C.3.2 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, mission success, cost, schedule, institutional/mission support, information technology, export control, security, and other applicable areas.

C.3.3 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.

C.3.4 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.4 Requirements Development

C.4.1 The Acquirer's manager should ensure that the project technical team addresses the risks identified in paragraph C.3.1, above, in the solicitation requirements.

C.4.2 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.5 Solicitation

C.5.1 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.

C.5.2 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.5.3 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.6 Source Selection

C.6.1 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.7 Post-Selection Surveillance and Contract Monitoring

C.7.1 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.

C.7.2 The Acquirer's managers should ensure that acquisition-related risks are continuously managed using the CRM process.

Appendix D. References

D.1 Federal Acquisition Regulation, 48 CFR, ch. 1, pts. 7 and 15.

D.2 NASA Federal Acquisition Regulation Supplement, 48 CFR, ch. 18, pts. 1807 and 1815.

D.3 GAO-14-704G, Standards for Internal Control in the Federal Government (the GAO Green Book).

D.4 OMB Circular A-11, Preparing, Submitting, and Executing the Budget (08/01/2017).

D.5 1OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (07/15/2016).

D.6 NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

D.7 NASA/SP-2011-3422, NASA Risk Management Handbook.

D.8 Committee of Sponsoring Organizations of the Treadway Commission Framework (COSO, 2004).

D.9 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, E. O. 13800, May 11, 2017.

D.10 Federal Information Security Modernization Act of 2014, Pub. L. 113-283, (2014).