**NASA Procedural Requirements**

**NPR 8000.4C**
Effective Date: April 19, 2022
Expiration Date: April 19, 2027

**COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES**

# Agency Risk Management Procedural Requirements

## Responsible Office: Office of Safety and Mission Assurance

# Table of Contents

## Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

## Chapter 1. Introduction

1.1 Background
1.2 Risk Management within the NASA Hierarchy

## Chapter 2. Roles and Responsibilities

2.1 General 2.2 Organizational Roles and Responsibilities
2.3 Individual Accountabilities for Risk Acceptance

## Chapter 3. Requirements for Risk Management

3.1 General
3.2 General Risk Management Requirements
3.3 Requirements for the RIDM Process
3.4 Requirements for the CRM Process
3.5 Requirements for Programmatic Decisions to Accept Risks to Safety, Mission Success, Physical Security, or Cybersecurity

3.6 Requirements for Decisions to Accept Institutional Risks to Safety or Mission Success
3.7 Requirements for Decisions to Accept Risks to Safety and Mission Success Affecting Both Programmatic and Institutional Organizational Units

**Appendix A. Definitions**
**Appendix B. Acronyms**
**Appendix C. Technical Notes on Physical Security and Cybersecurity Risk Management**
**Appendix D. Procurement/Contract Risk Management**
**Appendix E. References**

# Preface

## P.1 Purpose

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

b. This directive 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 are 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, whether of a random or an intentional and adversarial nature, that originate internally or externally 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, the NASA Risk Management Handbook (Reference D.1).

## 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 (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" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but

not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. Where conflicts exist between provisions of this directive and Federal statutes or regulations, or higher-level NASA directives, those statutes, regulations, and higher-level NASA directives take precedence.

e. In this directive, all document citations are assumed to be the latest version unless otherwise noted. Use of more recent versions of cited documents may be authorized by the responsible Institutional and Technical Authorities.

f. In this directive, documents categorized as authority, applicable, or reference documents may be cited as a different categorization, which characterizes its function in relation to the specific context.

# 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.

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

# P.4 Applicable Documents and Forms

None

# 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 2.2.6.

# P.6 Cancellation

NPR 8000.4B, Risk Management Procedural Requirements, dated December 06, 2017.

# 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 the interfacing and reciprocally complementing RIDM and CRM processes. 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 evaluated at activity-start by application of RIDM, and then to manage more effectively implementation risks using the CRM process, which is focused on managing, in the execution of an activity, the risk to the baseline performance requirements informed by the RIDM process, and is supplemented where appropriate by RIDM-enabled risk-control selection processes. Within a RIDM process informed by Analysis of Alternatives (AoA) at the start of an activity or project, decisions are made taking into account applicable risks and uncertainties; then, as the decisions are carried out, CRM is applied during activity execution to manage the associated risks in order to achieve the performance levels that drove the selection of a particular alternative. RIDM AoA steps are also included and integrated within the CRM process as part of the risk mitigation planning steps, whenever this appears to be necessary or useful for the identification and selection of risk control options optimized on a risk-reduction versus cost-of-implementation basis. For additional information, see NPD 1000.0 with regard to the topic of "Authority roles regarding risk." Figure 1 shows that this NPR identifies risk management objectives that are applicable to all NASA activities, but that are especially relevant in certain key domains, such as program and project management, safety and mission success, health and medical, physical security and cybersecurity, which are also governed by their own domain-specific directives and associated requirements. For additional information, see NPD 7120.4, NPD 8700.1, NPD 8900.1, NASA Health and Medical Policy for Human Space Exploration, and NPD 2810.1, NASA Information Security Policy.

1.1.3 This NPR supports NASA internal control activities as specified. For additional information, see NPD 1200.1, NASA Internal Control, Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, and the related Government Accountability Office Standards for Internal Control in the Federal Government GAO-14-704G, Standards for Internal Control in the Federal Government (the GAO Green Book). 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 developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). For additional information, see OMB Circular A-11, Preparing, Submitting, and Executing the Budget, and OMB Circular 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. For additional information, see NPD 1200.1.

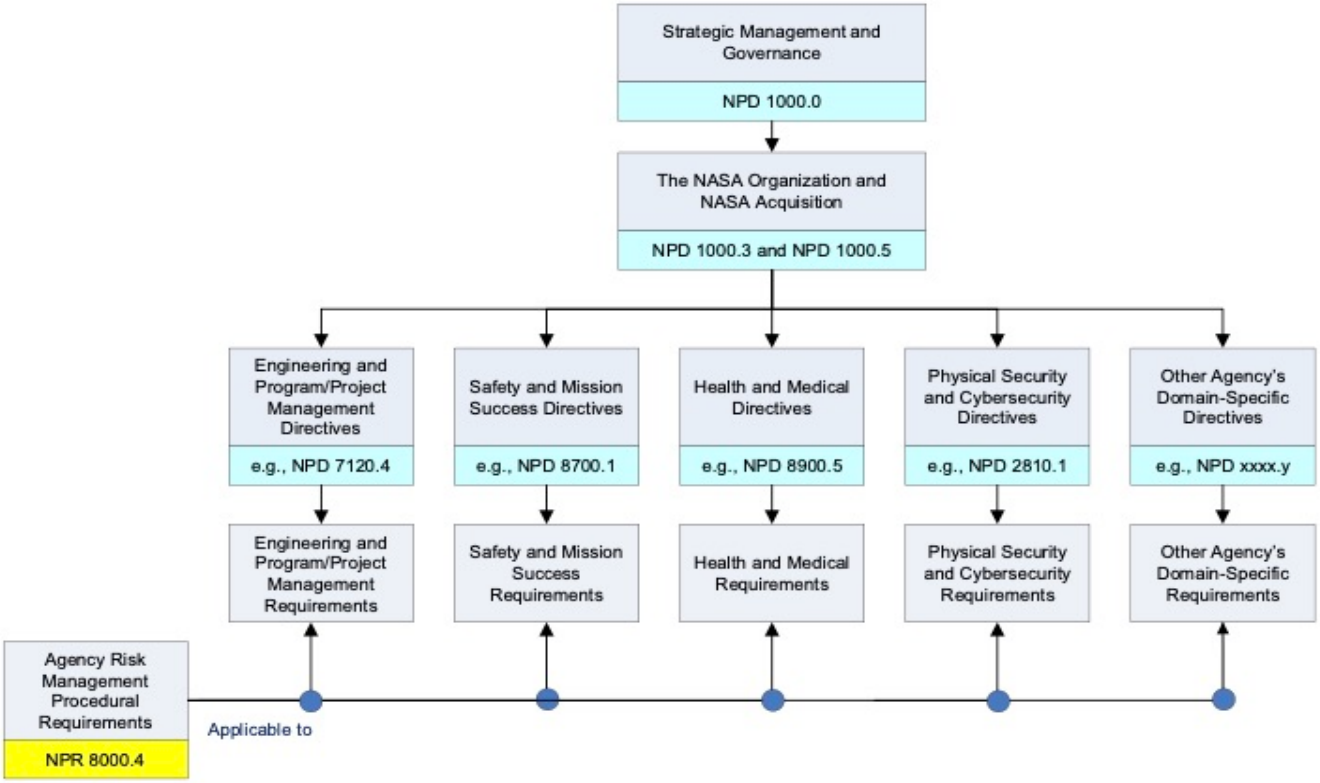


**Figure 1. Intersection of NPR 8000.4 with Program and Project and Domain-Specific Directives and Requirements**

1.1.4 This NPR supports NASA's security objectives at project, program, and institutional infrastructure level, including both physical security and cybersecurity activities. For additional information on such objectives, see NPD 1600.2E, NASA Security Policy, NPR 1620.3B, Physical Security Requirements for NASA Facilities and Property, NPD 2810.1, NASA Information Security Policy, and 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 physical security and cybersecurity threats is driven by the mission success and protection objectives of specific projects, maintaining at the same time full alignment and consistency with the broadly applicable national directives intended to ensure the protection or the institutional resources and infrastructure of all U.S. Government agencies, such as, in the cybersecurity domain, the Framework for Improving Critical Infrastructure Cybersecurity provided by NIST.

*Note: The above cited NIST Framework presents a risk-based approach to managing cybersecurity risk, complementing NASA's existing risk management processes and cybersecurity programs, and supporting the implementation of and compliance with the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, (2014). Application of the Framework is mandated by Strengthening the Cybersecurity of Federal Networks and Critical*

*Infrastructure), E.O. 13800 (2017).*

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, or any other objective-driven activity and mission, these objectives are translated into performance requirements, which may be related to institutional support for mission execution or related to one or more of the domains that are relevant to NASA activities carried out at any level (enterprise, program, or project), such as:

a. Safety.

b. Mission Success.

c. Physical Security and Cybersecurity.

d. Cost.

e. Schedule.

*Note 1: The above identification of key domains of interest to NASA in relation to performance and risk management objectives is given for the purpose of making clear that risk items affecting such domains are relevant in any NASA activity and cannot be overlooked. This does not imply that the five listed risk domains are the only ones within which relevant risk issues can be identified, nor that any given risk must always be characterized as belonging to one of the five listed categories.*

*Note 2: The term "mission success" may in a general context be interpreted as referring to success of a mission or project in all relevant domains of performance, e.g., including technical, safety, security, cost, schedule, and any other performance objectives that may be of concern. However, in the context of this NPR and for consistency with NPD 8700.1, "mission success" takes on the more limited meaning of "success with respect to the technical performance objectives of an activity or mission."*

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), schedule performance (e.g., meeting milestones), or cybersecurity (e.g., avoidance of data disclosure if a hacking attack occurs, avoidance of mission control interference if an adversary seeks to take control). Similar performance measures can be defined for institutional support (e.g., staffing levels, facility availability, supply chain metrics).

*Note: Performance measures and associated risk metrics can be expressed in full quantitative terms if the performance dimension of concern is intrinsically quantitative (e.g., the mass to*

*orbit capability of a launch system). For dimensions of performance that are more qualitative in nature (e.g., the degree of compliance of a design process with an applicable technical standard), constructed scales of discrete values associated with corresponding "binning" criteria and definitions may also be used. When possible, quantitative characterizations of performance and corresponding risk levels are preferable, as they more directly enable risk vs. benefit "analysis of alternative" (AoA) evaluations that constitute the foundation of the RIDM support to decision making.*

1.2.1.3 Managing risk requires the coordination of risk identification, assessment, decision and communication activities. All levels of NASA executives and managers, at all levels of the organizational hierarchy, are responsible to enable such a coordination. Risk coordination starts at the agency executive level with the formulation and communication of risk leadership principles, to increase decision velocity and pursue mission and science development opportunities within the risk posture deemed appropriate, with input from the affected stakeholders, for major activities, programs, or projects of concern. The definition and common sharing of a risk posture, in turn, enables the definition of risk tolerances applicable in risk management and risk-informed decision-making processes applicable to a specific activity or project.

1.2.1.4 Risk proceeds from sources that may be internal or external to a mission or activity; either type may take the form of a randomly-occurring event or of an intentional action. Main resulting broad-class combinations include:

a. Internal Random Event (e.g,, the random failure of a mission-critical hardware component).

b. Internal Intentional Action (e.g., equipment sabotage by a mission insider, or intentional neglect by a responsible party to carry out a required safety procedure).

c. External Random Event (e.g,, a lightning strike).

d. External Intentional Action (e.g., hackers' attack to an information system, or to a mission control network, or to a software-controlled physical system).

*Note: The identification of the above categories of risk sources is provided to clearly indicate that risk sources may exist inside or outside the perceived boundaries of an activity and its attending organization(s), and also that risk scenarios may be originated by willful human actions as well as by randomly occurring events. This clarification is not to be interpreted as a requirement to mandatorily "bin" all risks into one of the four broad classes identified above.*

1.2.1.5 Conceptually, and regardless of the type of source or mission-objective domain to which it relates, the risk to an objective can be represented via a set of triplets, each constituted by the following composing elements:

a. The scenario(s) leading from a source of risk to a 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; scenario leading to information system compromise),

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 1: In the representation of risk resulting from random events, "Likelihood" is the*

*probability that a full scenario sequence, from source to consequences, 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. Given that quantification must often be carried out without the benefit of large amounts of statistical evidence, a complete assessment of likelihood also calls for characterization of the uncertainty that may be present in its estimation.*

*Note 2: In the representation of risk resulting from intentional actions (e.g., a type of intentional cybersecurity-attack threat posed by a specific type of adversary), a quantification or even a qualitative classification (e.g., "high," "low," etc.) of the frequency or probability of such actions may be difficult to produce with sufficient degree of confidence. In such cases, a "Conditional Likelihood" evaluation is generally more meaningful, and as such recommended (see full discussion in Appendix C).*

1.2.1.6 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 deliver a product (e.g., a system) or 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.).*

1.2.1.7 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.

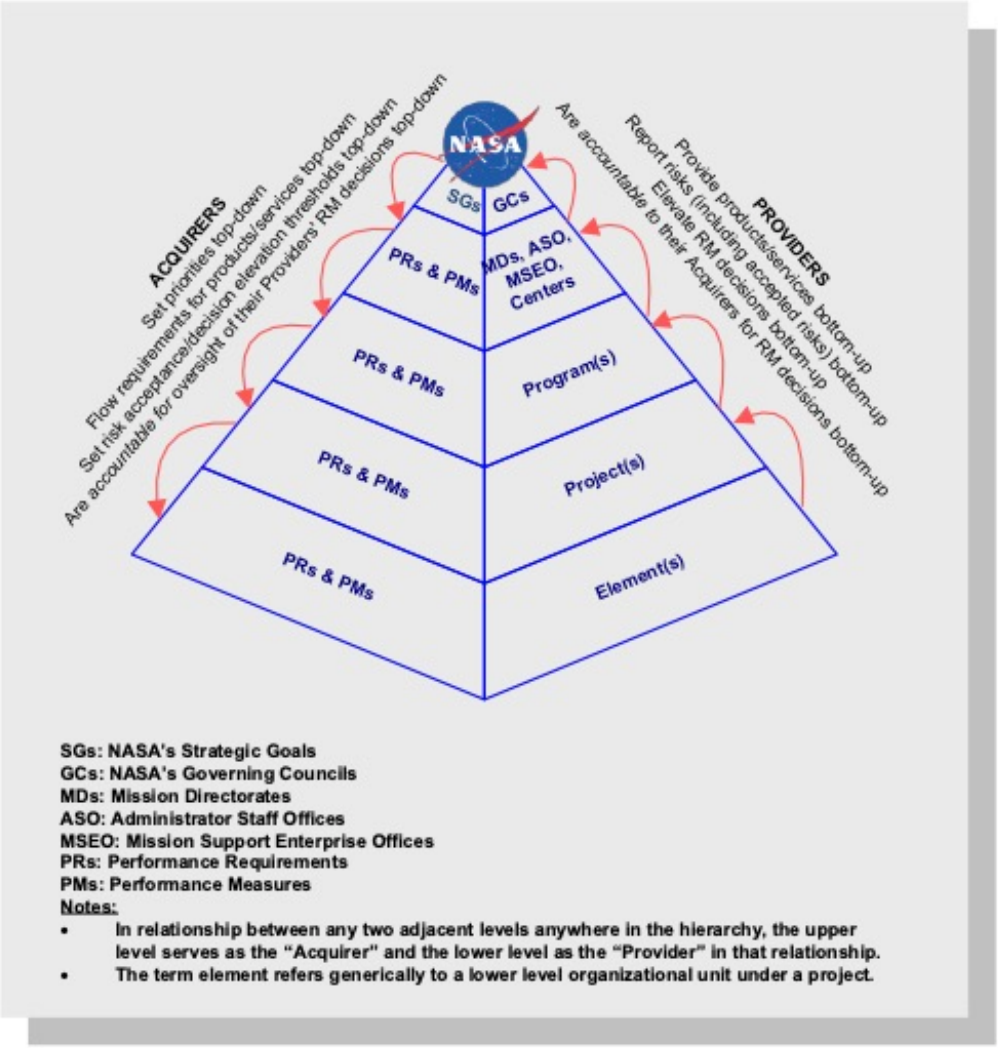


**Figure 2. Risk Management in NASA's Organizational Hierarchy**

*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).*

1.2.1.8 Mission Directorates are responsible for management of technical and programmatic risks within their domains and are responsible for elevating risks to the appropriate Management Council at the Agency level. Center Directors are responsible for management of institutional risks at their respective Centers and for coordinating institutional risk management activities with other Agency offices that are stakeholders for institutional risks. Headquarters Administrator Staff Offices and Mission Support Enterprise Offices are responsible for Agency-wide risk management in their domains. For additional information, see NPD 1000.3. Center Directors and Mission Support Enterprise 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, and are responsible for coordination in management of cross-cutting risks. Refer to Chapter 2 for a full description of roles and responsibilities.

1.2.1.9 Risk management at the Agency level addresses risks identified at the Agency level, as well as risk decisions elevated from Administrator Staff Offices, Mission Directorates, and Mission Support Enterprise 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.

d. A risk cuts across programmatic and institutional organizations, and needs to be addressed at the Agency level.

1.2.1.10 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., addressing cross-agency aspects of cyber-risk management above individual project or mission levels.

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; 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 institutional 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 RIDM interfaces with CRM in two main modes of risk management integration:

a. At the start or re-start of a project or activity, once a decision alternative has been selected for implementation, the performance measure values that informed its selection define the baseline performance requirements for CRM. An activity “re-start” may occur when, as discussed in paragraph 1.2.4.5, situations arise in which it is necessary to revisit the decision and rebaseline the performance requirements.

b. Within the execution of an activity or project, if alternative options appear possible for the mitigation and/or control of an identified risk, each with its risk-reduction value and its implementation resource costs, CRM should utilize the AoA capability of the RIDM processes to assist the identification and selection of an optimal solution that balances implementation cost versus risk reduction worth.

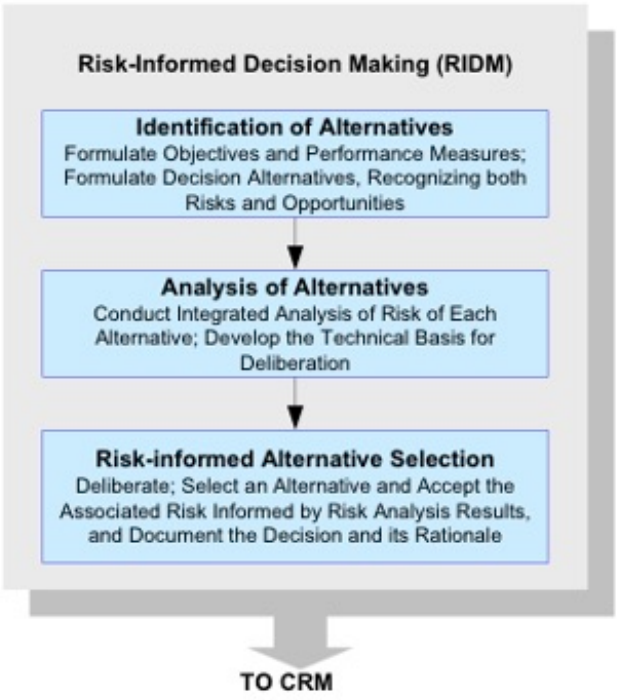


**Figure 3. RIDM Process**

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 3.4.2i(1)). The requirements of paragraphs 3.5 (for program and 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.

1.2.3.3 In order to focus effort and accountability during implementation of a 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. For additional information, see NPR 7120.5, NASA Space Flight Program and Project Management Requirements. 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 3.2.2i) for each organizational unit.

> *Note: When considering risk produced by intentional threat sources, such as cybersecurity risk, aggregate risk representation will not be feasible in traditional form if the corresponding scenarios are only partially quantifiable (e.g., via "Conditional Likelihood" or "(Conditional) Potential Vulnerability," as suggested in 1.2.1.5c Note 2). Surrogate aggregate risk indices can still be formulated for such kinds of scenarios, when this is still considered useful for specific purposes, by substituting threat weights (e.g., reflecting expert judgment supported by relevant and timely sources of information, such as intelligence input) to initiating threat frequency or probability measures.*

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 paragraphs 1.2.1.6 and 1.2.1.7.

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 paragraphs 1.2.1.6 and 1.2.1.7).

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 or project objectives are to be satisfied. Redefinition and rebaselining, therefore, imply a tradeoff that needs to be approved by the Acquirer.

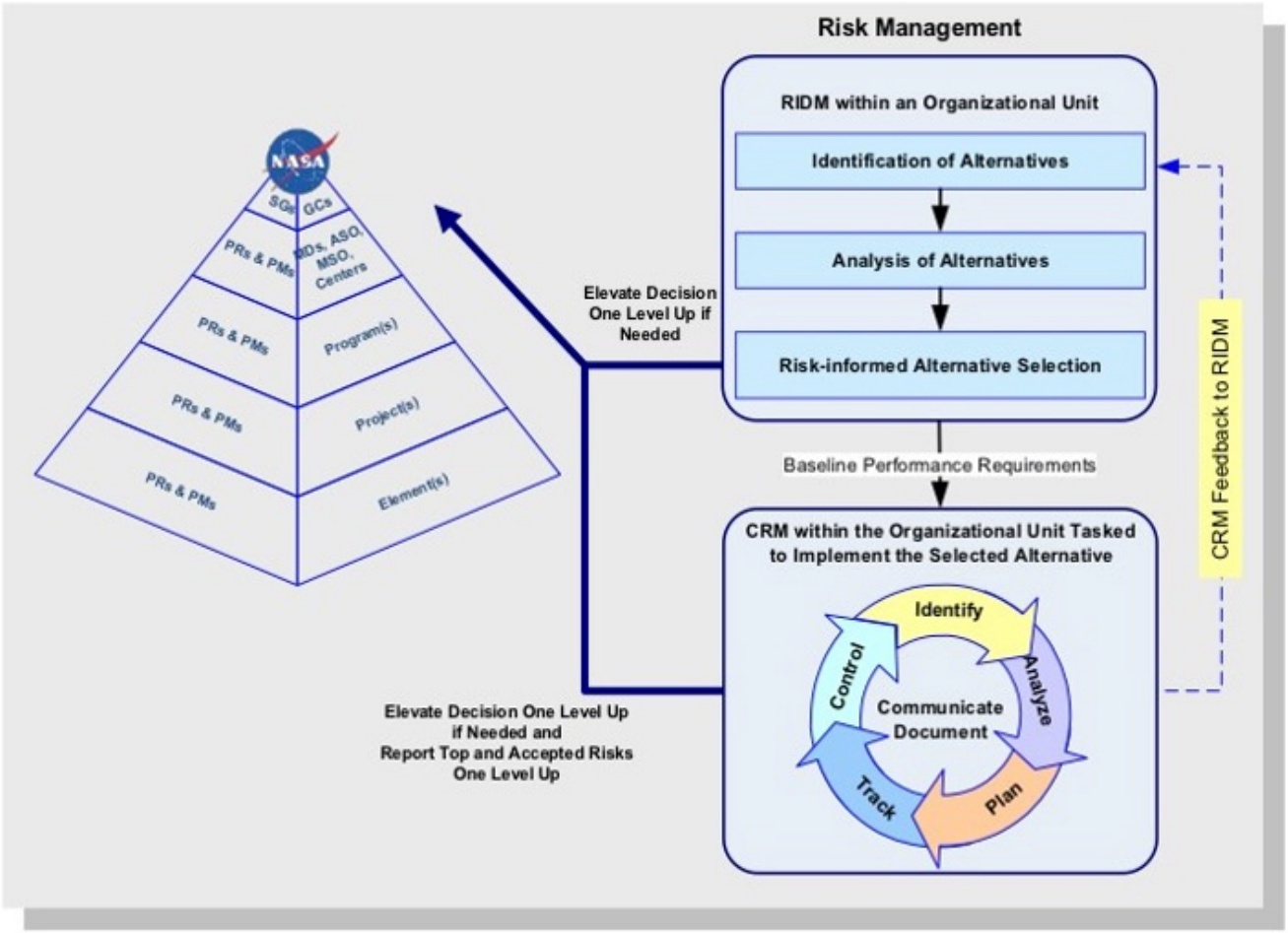


**Figure 5. Coordination of RIDM and CRM within the NASA Hierarchy (Illustrative)**

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

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

1.2.4.8 Agency-wide institutional risks are addressed by NASA Headquarters Administrator Support Offices, Mission Support Enterprise Offices, and the Mission Support Council.

# Chapter 2. 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 Enterprise Offices, Center Directors, and program or 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 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 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 Establishment of the risk posture associated with human space flight is done by the Administrator. Establishment of the risk posture for science missions is done by the Associate Administrator for SMD. The risk posture affects risk-acceptance decision-making at all levels of the Agency.

2.2.3 Mission Directorate Associate Administrators:

a. specify organizational units within their Directorates responsible for the implementation of the requirements of this NPR;

b. designate organizational units that are authorized to acquire turnkey launch services based on fulfillment of requirements in 3.5.3, 3.5.4, and 3.5.5 of this NPR, accepting the risks as having been managed by the Provider, without assumption by the Acquirer of active management of the risks of launch services.

2.2.4 Project managers specify the organizational units and the hierarchy within their respective domains to which the requirements of this NPR apply.

2.2.5 Organizational unit managers coordinate the management of cross-cutting risks being managed within their units with other involved organizational units. More specifically, the MSD Associate Administrator and the Mission Support Enterprise Office heads:

a. Define institutional risk processes to ensure coordination across the Agency of institutional risk management activities efficiency and consistency;

b. In coordination with Center Directors, specify the organizational units and the hierarchy within their respective domains to which the requirements of this NPR apply.

*Note: Refer to 3.7 for the detailed requirements concerning these areas of potentially shared responsibility*.

2.2.6 The Technical and other Institutional Authorities (e.g., Institutional Safety Authorities) assure that risk management processes addressing their areas of responsibility are implemented in accordance with this NPR.

2.2.7 Per NPR 2810.1 the Chief Information Officer:

a. Develops and implements the Agency's cybersecurity policy and information system risk management framework for authorizing and operating information systems in accordance with Federal standards.

b. Evaluates and approves the appointment of all NASA information system Authorizing Officials, who are the primary authorities for acceptance of risk affecting, or resulting from, the operation of information systems.

2.2.8 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., project managers, have risk leadership responsibility and are accountable for risk acceptance decisions for their programs or projects, to be produced in timely fashion, and commensurate with their delegated authority and with the risk posture established for such activities or projects.

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

*Note 1: Center Directors should proactively coordinate with MSD and its MSEO offices to make sure their risk related decision processes are carried out consistently with the cross-agency infrastructure optimization strategies promoted by MSD,*

*Note 2: Center Directors should also proactively coordinate with other stakeholders across the Agency when they determine that their risk acceptance decisions may impact or affect such stakeholders and their institutional roles and responsibilities.*

2.3.3 The Associate Administrator for the Mission Support Directorate (MSD) is separately accountable for risk acceptance decisions for those institutional activities across the Agency that are managed by his/her Office.

*Note 1: The Associate Administrator for MSD should proactively coordinate with Center Directors across the Agency when he/she determines that MSD's risk acceptance decisions may impact or affect institutional activities at a Center.*

*Note 2: In the event of disagreement between the Center Directors and the Associated*

*Administrator for the MSD regarding a risk acceptance decision, the non-accepting party invokes the formal dissent process.*

2.3.4 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 reflects the Agency's risk posture: that it 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 formal dissent 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.*

2.3.5 When there is risk to humans, the actual Risk Taker[s]' (e.g., astronauts', pilots') official spokesperson[s] and applicable supervisory chain must formally consent to assume the risk on behalf of the Risk Takers.

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

2.3.6 When risk is produced by, or affecting, a specific information system, the Authorizing Official (AO) for that system is accountable for risk acceptance. If such a risk also affects a specific program, project, or activity, risk acceptance requires coordination between the responsible manager and the information system AO.

# 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 project risks), 3.6 (for institutional risks), or 3.7 (for cross-cutting 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.j.

3.1.4 In the following sections, 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, even in such cases the manager remains 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: 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 D 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 Enterprise Offices, programs, projects, and other designated responsible authorities, e.g., the information system Authorizing Official with regard to cybersecurity.

*Note: Note: Refer to Section 3.7 for special requirements on management of cross-cutting risks affecting both institutional and programmatic organizations.*

g. Ensure that formal dissent arising during risk management decision making are handled through the formal dissent 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. For additional information, see NPD 1200.1.

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

(1) Reflects the risk leadership principles the organizational unit is directed to apply by the next higher level in the pursuit of its objectives, and defines a corresponding risk posture via the definition of risk tolerances and explicit risk acceptance criteria to be applied in the execution of the unit’s activities and projects.

(2) Explicitly scopes all the risk types within the purview of the organizational unit, e.g., for projects: safety, mission success, physical security and cybersecurity, cost, and schedule risks.

(3) Addresses all the principal possible sources of risk, e.g., for projects or defined activities: both internal and external random events, both internal and external intentional actions.

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

(5) 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 acceptance criteria (see item (8)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: 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 RMP. However, in addition to such requirements on performance of the system or service being developed, the RMP 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. For additional information, see NPR 7123.1, NASA Systems Engineering Processes and 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 project risks), 3.6 (for institutional risks), or 3.7 (for cross-cutting risks).*

*Note 5: Cost and schedule commitments are derived from JCL analysis in major programs and projects, or from simpler processes of estimations judged adequate for the purpose, in other programs or projects. For additional information, see NPR 7120.*

(6) Is coordinated with other management plans, such as higher-level risk management plans and the Systems Engineering Management Plan (SEMP) when applicable. For additional information, see NPR 7123.1.

(7) Defines categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories, and determines and documents the protocols for estimation of the likelihood and severity of the consequence components of risks, including uncertainty characterization and quantification. For risks resulting from intentional-action sources, where the likelihood dimension of risk may be characterized in conditional terms, i.e., assuming that an intentional source is present, provides and documents corresponding definitions and determinations for categories or metrics that it selects to characterize the conditional likelihood characterization of such risks.

*Note 1: As part of the definition of likelihood / probability categories, the RMP can also establish criteria that can be used to apply practical distinction between conditions to be treated as risks and those that can be considered existing issues. Generally, a risk event can be considered to be an "issue" when its undesired consequences have already occurred, or are going to occur with very high likelihood if no remedial action is taken.*

*Note 2: 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).*

(8) Reflects the overall programmatic risk posture by documenting risk acceptance 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 acceptance criterion" is a rule for determining whether a given organizational unit has the authority to decide to accept a risk.*

*Note 2: The RMP required in 3.2.2i. delineates (refer to subparagraph (3)) a body of performance requirements to be met by the Provider. Risk acceptance criteria are formulated to allow the Provider 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.*

(9) Identifies stakeholders, such as Risk Review Boards and the information system Authorizing Official (for cybersecurity risk), to participate in coordinated deliberations regarding the disposition of risks.

(10) 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. Also establishes guidance to make sure that communication between management levels and across the organization reflects any criteria established to distinguish “risks” from “issues,” especially when this is associated with different types of handling and assignment of order of priority.

*Note 1: This communication may be accomplished using standard reporting templates defined in the RMP, including risk matrices (and conditional risk matrices for intentional-action risks; see Note 2 below), whose formulation and interpretation are agreed between the affected units, recognizing that communication of risk from one level to another level (e.g., from project to program level) must be executed consistently with the risk classification criteria of the receiving organization, in order to support decision-making at that level.*

*Note 2: In case of intentional-action risk scenarios, such as cybersecurity risk, conditional-risk matrices may be used, to communicate the risk level corresponding to a given type of intentional threat, if the latter is assumed to be present. This type of communication may be adopted when it is judged that a probability or frequency-based representation of the potential types of threat is not possible or meaningful.*

*Note 3: 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 be manageable at the higher level, since the organizational unit at that level has more flexibility and authority.*

*Note 4: For Center mission support and institutional organizations, protocols are particularly important for reporting risks to affected project units and vice versa.*

(11) 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, if applicable, the agreement of the Risk Takers' responsible managers to assume the risk (refer to paragraph 3.5.3 for application of this form).

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

(13) Delineates the processes for coordination of risk management activities and sharing of risk information with other affected organizational units and responsible authorities (e.g., the information system Authorizing Official for cybersecurity risk). This includes management of cross-cutting risks (risks affecting multiple organizational units), including risks affecting both programmatic and institutional organizations.

(14) Documents the manager's signature, as well as:

(a) 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), and

(b) the concurrence of the cognizant Technical Authorities or other Institutional Authorities (e.g., Institutional Safety Authorities) that the Risk Management Plan meets the requirements of this NPR.

j. Ensure that decisions to rebaseline performance requirements, grant waivers, or modify RMPs 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 project risks), 3.6 (for institutional risks), or 3.7 (for cross-cutting risks)).

> *Note: Note: Per requirements in paragraph 3.2.2i., the RMP 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, NASA Records Management, and NPR 1441.1, NASA Records Management Program Requirements, and under formal configuration control, with a capability to identify and readily retrieve the current and all archived versions of risk information and the RMP.

3.2.3 Managers responsible for lower-cost, lower-risk-classification missions that have to satisfy less stringent success criteria (e.g., Cubesat, Risk Class D missions) may fulfill the above requirements according to the graded approach directives for risk management established by NPR 8705.4, Risk Classification for NASA Payloads.

# 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 RMP), 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 3.2.2i(8). (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 RMP) 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 project risks), 3.6 (for institutional risks), or 3.7 (for cross-cutting 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. The parameters that will be tracked to determine the effectiveness of the mitigation are identified in the mitigation plan.

(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.j(1)) are periodically tracked. (related to TRACK step)

n. Tracking data are disseminated to entities identified in the RMP 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.j. (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 Programmatic Decisions to Accept Risks to Safety, Mission Success, Physical Security, or Cybersecurity

3.5.1 Many decisions that are not necessarily couched as "risk acceptance" decisions nevertheless have implications for safety, mission success, or physical security and cybersecurity. For example, 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. Such implicit risk-acceptance decisions need to be justified in the same way as decisions that are explicitly framed as risk-acceptance decisions.

3.5.2 All key project decisions that accept risks to safety or mission success - either implicitly or explicitly - are subject to the requirements of 3.5.3 on creation of the basis for the decision, TA or other cognizant authority (see Note below) concurrence, and, if human Risk Taker[s] are involved, the consent of their managers to the Risk Takers' assumption of the risk. 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 or security 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.

Examples of such decisions include:

a. Decisions and associated concurrence or consent acts that concern the procurement by an Acquirer of a system or of a specific set of services from a Provider on a turnkey basis;

b. Provider decisions that effectively rebaseline the Acquirer's top-level safety and mission success requirements levied on the Provider;

c. Provider decisions to rebaseline derived requirements developed by the Provider and accepted by the Acquirer as sufficing to demonstrate compliance with top-level requirements;

d. Reduction in other Provider commitments (e.g., commitments to conduct flight testing), or

e. Relaxation of physical security and cybersecurity requirements.

> *Note: In the case of a program or project risk involving the configuration or operation of an information system, the risk disposition decision requires coordination with the information system Authorizing Official (AO).*

3.5.3 Each manager shall ensure that:

a. Each decision for accepting risk to safety, mission success, or physical security and cybersecurity (e.g., requirements definition/compliance/waiver, change requests, formal board directives and decisions, formal dissent dispositions, etc.) can be traced to the risk posture established for the affected mission or project, and

b. All such decisions and their rationales are 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 or security process system, on a program-defined form including:

(1) The manager's signature, documenting or referencing:

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

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

(c) 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, physical security and cybersecurity, 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; for the decision to utilize a "turn-key" mission or flight service, the technical case may be based on the Acquirer's development and communication to the turn-key system or service Provider of performance-based risk-control goals and objectives, and the correspondingly compatible, convincingly established safety and performance record of the turn-key system or service being accepted for use, evaluated within the context of the Agency's current risk posture for those specific missions.*

*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.*

(2) 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 2.3.4.c.*

3.5.4 In the event of TA nonconcurrence in a manager's risk acceptance decision, the TA shall elevate the risk acceptance decision one level up in the organizational hierarchy in accordance with the formal dissent process (NPD 1000.0).

3.5.5 In the event of TA concurrence in a manager's risk acceptance decision, the manager shall report each decision accepting risks to safety, mission success, or physical security and cybersecurity 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 a Provider's system or service, acceptance and/or 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 and/or acceptance 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 Acquirer'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 the 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) 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). For additional information, see NPR 8705.4.

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

3.5.8 Besides all of the above, whenever specific Federal Government regulations apply to the acceptance of risk issues (e.g., as in the case of cybersecurity policies and regulations), they shall be complied with by the NASA authority accountable for risk acceptance, or by any contractor / provider to whom NASA has delegated that authority.

# 3.6 Requirements for Decisions to Accept Institutional Risks to Safety or Mission Success

3.6.1 For "institutional risks" (as defined in Appendix A) to safety or mission success, the Center Director shall develop, document in an institutional risk management plan, and implement a formal process for institutional risk acceptance that meets the intent of key requirements of paragraphs 3.5.3, 3.5.4, and 3.5.5.

*Note: Per 3.2.2i, all organizations, including Centers, are managed to satisfy explicit performance criteria, including criteria for safety and mission success. Institutional risks to safety or mission success are either risks to the satisfaction of these criteria, or relaxations of the criteria themselves.*

3.6.2 Depending upon the nature of the risk, the process should specify whether risk acceptance responsibility is formally delegated by the Center Director to the manager of a specific Center office, and who serves as the concurring authority (analogous to the TA role in paragraph 3.5). The Center Director remains ultimately accountable for institutional risk acceptance decisions at his/her Center, even when he/she has delegated the risk acceptance decision authority for certain risks to a manager who reports to the Director within the Center organizational structure.

*Note: Center Directors should identify in the respective institutional risk management plans the circumstances and criteria under which they should communicate and coordinate institutional risk acceptance with other potentially affected stakeholders within the Agency.*

# 3.7 Requirements for Decisions to Accept Risks to Safety and Mission Success Affecting Both Programmatic and Institutional

# Organizational Units

3.7.1 Some risks affect both programmatic and institutional organizations. Organizational units shall proactively communicate the status of that risk to affected organizations.

3.7.1.1 Risks created by institutional facilities are managed by institutional organizations, who should satisfy the requirements of 3.6 for risk acceptance and proactively communicate risk dispositions to affected programmatic organizations. Affected programmatic organizations can accept risks created by institutional organizations only if:

a. Those risks satisfy their risk acceptance criteria,

b. The requirements of 3.5 are followed, and

c. The affected programmatic organization's Acquirer (the organization that concurred in the organization's risk acceptance criteria) concurs in the acceptance of risks created by institutional organizations.

> *Note: In a case such as this, the affected programmatic organization's acceptance and elevation protocols will not, in general, have been drafted with cross-cutting risks in mind. It is therefore necessary to keep the higher levels informed of such decisions. If human risk-takers are involved, their spokespersons' concurrence will have been required at a high organizational level.*

3.7.1.2 Risks created by programmatic organizations are managed by those organizations, who should satisfy the requirements of 3.5 for risk acceptance and proactively communicate risk dispositions to affected institutional organizations. Affected institutional organizations can accept risks created by programmatic organizations only if:

a. Those risks satisfy their risk acceptance criteria,

b. The requirements of 3.6 are followed, and

c. The affected institutional organization's Acquirer (the organization that concurred in the institutional organization's risk acceptance criteria) concurs in the acceptance.

> *Note: See preceding note. Risk acceptance and elevation protocols will not, in general, have been formulated with cross-cutting risks in mind.*

3.7.2 Managers in all organizations potentially affected by a given risk should have access to current status information relating to that risk, and WATCH that risk. In the event that any of the affected organizations deems the risk to warrant proactive measures not being taken by the managing organization, that affected organization should take the following steps, iterating the process until managing and affected organizations agree on the appropriate approach to management of that risk.

a. Propose a different management approach to the managing organization.

b. If the managing organization does not take actions deemed adequate by the affected organization, the affected organization will elevate the risk to the next level in its hierarchy, which should either provide the originating affected organization with resources sufficient to address the risk in a different way, raise the issue with its counterpart in the managing organization's hierarchy, or elevate the risk to the next higher level of its own hierarchy.

c. This process should be iterated until either the risk has been addressed by the managing hierarchy, addressed using an alternative risk control strategy by the affected hierarchy, accepted by the affected hierarchy, or elevated to the appropriate Management Council.

# Appendix A. Definitions

**Acquirer.** A NASA organization that tasks another organization (either within NASA or external to NASA) to deliver a product (e.g., a system) or 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.

**Conditional Likelihood.** A synonym of Conditional Probability (see definition thereof), more commonly used when qualitative ratings (such as “high likelihood,” or “low likelihood”) are provided instead of a numerical probability quantification.

**Conditional Probability.** The probability that some event or condition occurs, if (and only if) other specific events or conditions have already occurred **1**.

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

**Continuous Risk Management.** 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.** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation [source: Office of Management and Budget Memorandum Circular A-130, Managing Information as a Strategic Resource, July 2016] **2**.

**Cybersecurity Risk.** Threats to and vulnerabilities of cyber-assets – i.e., data, information, control systems, and information systems stored and/or implemented in digital form – and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of cyber-assets, including such related consequences caused by an act of terrorism [adapted and extended from National Cybersecurity Protection Act of 2014, to explicitly include threats to digital control systems].

**Deliberation.** In the context of this NPR, the formal or informal process for communication and collective consideration, by stakeholders designated in the RMP, of all pertinent information, especially risk information, in order to support the decision maker.

**Dispositions (of Risk):**

a. **Accept**. The formal process of justifying and documenting a decision not to mitigate a given risk

beyond some assessed or projected level. (See Section 3.5 and definitions of Risk Acceptance Criterion and Risk Acceptance).

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).

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.

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.

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.** The application of 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 **3**.

**Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [from 44 U.S.C., Sec. 3502].

**Institutional Risks.** Risks to infrastructure, information technology, resources, personnel, assets, processes, operations, occupational safety and health, environmental management, security (physical security and cybersecurity), 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).

**Intentional Threat.** A threat originated, directly or indirectly (i.e., via the use of automated machinery or digital equipment) by human agents. See also Threat.

**Knowledge Management.** 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, expressed in either qualitative (e.g., “Low,” “High,” etc.) or quantitative terms.

**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 **4**.

**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.

**Physical Security.** The objective and function of securing an organizational infrastructure, program, project, mission, or activity, and protecting their material, functional, control, information, and human assets from interferences of a physical and material nature that are capable of causing damage, or of resulting in unauthorized possession or control of such assets **5**.

**Potential Vulnerability.** The characteristic of a system, system security procedures, internal controls, or implementation that may represent a weakness in relation to the capabilities of a particular threat source and could be exploited by that threat source. (See also Vulnerability).

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

**Risk.** 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 (mission success, safety, physical and cybersecurity, cost, and schedule) or institutional support for mission execution **6**. Risk is operationally characterized as a 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 or compromise 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; unconditional or conditional) of those scenarios.

c. ***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.

**Risk Acceptance Criterion.** A rule for determining whether a given organizational unit has the authority to decide to accept a risk **7**.

**Risk Acceptance.** A decision to accept the level of risk that remains after implementation of available net-beneficial mitigations of a given risk. Risk acceptance can be deliberate or not, depending on whether the risk implications of the decision are recognized, acknowledged, and taken into account by the decision-maker(s); or whether they remain for any reason undesirably hidden or overlooked **8**.

**Risk-Informed Decision Making.** As discussed in paragraph 1.2.2, a risk-informed decision-making process that uses a diverse set of performance measures (some of which are model-based risk metrics) along with other considerations within a deliberative process to inform decision making **9**.

**Risk Leadership.** One of the “NASA Senior Leadership Focus Areas” referred to in NPD 1000.0C, it is there described as the application by NASA of a risk culture that has the goal of “increasing ‘decision velocity’ within a proper risk posture.” It is implemented from the higher levels of management by communicating to the work force a clear and balanced understanding of risk and benefits, by defining and indicating appropriate technical standards, and by ensuring the workforce has the proper experience and commitment to collaboration [adapted from NASA NPD 1000.0C].

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

**Risk Posture.** An expression of the agreed upon limits of risk an organization's leadership team is willing to accept in order to achieve one or more of its objectives. It is defined up front and in tandem with the development of objectives, consistently with Risk Leadership principles, and serves as the attitudinal framework for seeking a balance between the likelihood and benefit of achieving the objective(s), vs. the likelihood and severity of risks that may be introduced by the pursuit of achievement. Risk posture may change with time, in reflection of the evolution of leadership team attitudes or because of changes in priorities, but at any particular time, risk posture provides the de-facto basis for risk-informed decision making and continuous risk management **10**.

**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.

**Risk Tolerance.** An expression of the limit of acceptable probability of a shortfall with respect to the achievement of an explicitly established and stated objective, which is defined consistently with the overall agreed upon Risk Posture and risk vs. benefit balance pursued by an organization, according to its established and communicated Risk Leadership principles **11**.

**Safety.** In a risk-informed context, 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 **12**.

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

**Threat.** A circumstance or event with the potential to adversely impact organizational operations and missions, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of assets or information, and/or failure or denial of service [adapted from NIST-SP 800-30, Rev. 1, Guide for Conducting Risk Assessments]. A "threat" may exist in a given context as an intrinsic characteristic of the related activities and events, or be introduced by intentional adverse actions, including organized adversarial actions by an enemy entity, organization, or nation **13**. See also Intentional Threat.

**Threat Source.** An intent and method targeted at the intentional exploitation of a system characteristic, which may become a system weakness in relation to such an intent or method; or a situation and method that may accidentally trigger a vulnerability or system weakness **14** [adapted from NIST-FIPS 200, Minimum Security Requirements for Federal Information and Information Systems].

**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.

**Vulnerability.** A known weakness in the characteristics of a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a known threat source [adapted from NIST-SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations].

---

**1** In a risk scenario described as a sequence of events, it is standard practice to quantify an event by means of its conditional probability, i.e., the probability that it will occur, if all the events that precede it in the scenario sequence have in fact occurred. As discussed in paragraph 1.2.1.5, in the case of a risk driven by an intentional source, the conditional probability or conditional likelihood of a resulting system or mission compromise is a useful metric to assess the system potential vulnerability to the type of threat that acts as the risk source, even if it may be difficult to estimate the likelihood or probability of the threat itself.

**2** Achieving overall security at any level (institutional, program, project, or mission) may require consideration of interactive aspects of physical security and cybersecurity, as well as aspects of either type of security that may not be explicitly recognized in traditional definitions, such as the security of control systems that are implemented via a combination of networks, computers, and other electronic and/or mechanical components. As such, overall security requires the application of both physical security and cybersecurity provisions and protections

**3** 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.

**4** 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.

**5** Achieving overall security at any level (institutional, program, project, or mission) may require consideration of interactive aspects of physical security and cybersecurity, as well as aspects of either type of security that may not be explicitly recognized in traditional definitions, such as the security of control systems that are implemented via a combination of networks, computers, and other electronic and/or mechanical components. As such, overall security requires the application of both physical security and cybersecurity provisions and protections.

**6** A risk is an uncertain future event, or combination of events, that could threaten the achievement of performance objectives or requirements. A "problem," on the other hand, describes an issue that is certain or near certain to exist now, or an event that has been determined with certainty or near certainty to have occurred and is threatening the achievement of an objective or requirement. It is generally at the discretion of the decision authority to define at what level of certainty (i.e., likelihood) an event may be classified and addressed as a "problem" rather than as a "risk." A risk may actually be conditional upon a problem, i.e., an existing issue may or may not develop into performance-objective consequences, or the extent to which it may is at the present time uncertain.

**7** Not all risks satisfying a defined risk acceptance criterion are automatically accepted, nor a combination of such individual risks is always automatically acceptable in the aggregate; rather, subject to aggregate risk considerations, a given organizational unit has the authority to decide to accept individual risks satisfying the criterion.

**8** A non deliberate risk acceptance condition may be the result of a decision not to investigate a potential risk beyond some initial qualitative level.

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

**10** Risk Posture is an indication provided by the executive managers / leaders of an activity or project as to their disposition towards risk concerning the key performance measures for that activity or project, in relation to, and balance with, the opportunities and benefits of achieving gains in some of those performance dimensions, or in some additional areas judged to be important to the project and to the organization. For example, the baseline risk posture for development of a new launch vehicle may be expressed in terms of the following performance requirements, and associated risk tolerance levels:

Baseline Performance:
minimum mass-to-orbit > 90 metric tons at 99% confidence;
reliability > 99% at 90% confidence

A more complete expression of risk posture by project leadership and stakeholders for this situation might also be provided by indicating, in addition to the above, that a lower level of confidence in achieving the reliability target may be acceptable if certain gains, above and beyond the minimum requirements, could be pursued and achieved. The following declarations of acceptable "deltas" in risk tolerance limits would then provide, together with the initial baseline indications, a definition of the project risk posture that reflects, in its balancing of pursued objectives vs. associated risk tolerances, more flexibility than would be expressed by the baseline performance measures and risk tolerances alone:

Delta Case A:
acceptable reliability performance > 98% at 90% confidence
IF mass-to-orbit > 100 metric tons at 95% confidence
Delta Case B:
acceptable reliability performance > 99% at 50% confidence
IF eco-friendly propulsion is employed in new launch vehicle

**11** A Risk Tolerance threshold defines the level of risk declared to be acceptable with respect to the achievement of a performance measure requirement. This is usually expressed by what probability of not meeting a performance target can be tolerated and accepted, and is the "other side of the coin" of stating the "confidence level" by which a performance requirement is to be met. In the note and example discussion of Risk Posture provided above, Risk Tolerances are expressed or implied as follows:

Baseline Case:
Risk Tolerance for mass-to-orbit:
probability of not meeting 90 ton requirement < 1%
Risk Tolerance for reliability:
probability of not meeting 99% reliability requirement < 10%
Acceptable Delta Case A:
Risk Tolerance for mass-to-orbit:

probability of not meeting 100 ton requirement < 5%
Risk Tolerance for reliability:
probability of not meeting 98% reliability requirement < 10%
Acceptable Delta Case B:
Risk Tolerance for mass-to-orbit:
probability of not meeting 90 ton requirement < 1%
Risk Tolerance for reliability:
probability of not meeting 99% reliability requirement < 50%

**12** This NPR uses the term "safety" broadly to include human safety (public and workforce), environmental safety, and asset safety.

**13** In the context of this NPR, "threat" is a broad term that refers to a possible condition or combination of conditions, relative to a risk scenario, which can have a relevant role in the origination or realization of the risk. The means by which the threat may materialize may be physical, or non-physical (e.g., software-based), or even weapon-grade in case of an open aggression by an enemy entity

Example 1: the existence of a disgruntled employee with access privileges to a protected network constitutes a "threat" to the security objectives for that network.

Example 2: the existence of defective components in a space vehicle represents a "threat" to the success of the mission that such a vehicle is designed to execute.

Example 3: the jamming capabilities of an ill-intentioned enemy represent a threat to NASA satellite GPS and communication functions.

**14** With reference Example 1 in the Note for the definition of "Threat," the "threat source" is that the disgruntled employee can use his/her access privileges to compromise network systems or information. In Example 2, the "threat source" is that defective components can prematurely fail and cause a mission failure.

# Appendix B. Acronyms

| | |
|---|---|
| AO | Authorizing Official |
| 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 |
| MSEO | Mission Support Enterprise 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 |
| RMP | Risk Management Plan |
| SEMP | Systems Engineering Management Plan |
| S&MS | Safety and Mission Success |
| TA | Technical Authority |

# Appendix C. Technical Notes on Physical Security and Cybersecurity Risk Management

## C.1 General Considerations

As implied by their definitions (see Appendix A) risk in the domains of Physical Security and Cybersecurity (PS&C) has the unique characteristic of being often associated with intentional acts of aggression carried out by an "hostile agent" - i.e., an ill-intentioned individual, entity, or even foreign government - against the assets or activities of the affected organization. This may occur in the context of a covert operations, such as the infiltration of a computer system by hackers who intend to take control of its stored information, or of more overt attacks, such as the attempt by a terrorist group to inflict damage to the physical facilities of an organization.

## C.2 PS&C Risk Modeling

Despite the above specific characteristic of being often associated with the acts of an hostile human agent (or multiple coordinated agents), PS&C risk scenarios do not differ from any other risk scenarios, in the fact that their progression is still determined by sequences of concatenated events. Accordingly, they can still be represented and described by means of the same types of logic models that are used for other types of risk scenario; however, as further explained below, the "intentional act" characteristics of PS&C risks suggests for their qualitative or quantitative assessment an approach that differs from that customarily applied for most other risks.

In general, detailed representation of complex risk scenario situations may require the use of combinations of different models (e.g., a combination of event trees and fault trees, such as often done in PRA (Probabilistic Risk Assessment). However, for the purposes of the discussion in this Appendix, it is sufficient to refer to a simple conceptual model that corresponds to the "risk statement" descriptions of risk recommended by the NASA RM Handbook [E20].

Per [E20], a risk statement takes the form shown in the below indented paragraph:

> *GENERIC RISK STATEMENT:*
> *"Given that [CONDITION], there is a possibility of [DEPARTURE] from the baseline adversely impacting [ASSET], thereby leading to [CONSEQUENCE]."*

In logic model terms, the above risk statement can be translated into a simple Event Sequence Diagram (ESD) format, as illustrated by Figure C1 below. While a real scenario can be complex and typically include multiple relevant events and/or conditions, at the conceptual level such events can always be grouped into the basic blocks identified in the above generic form of a risk statement, and in the corresponding ESD shown in Fig. C1.

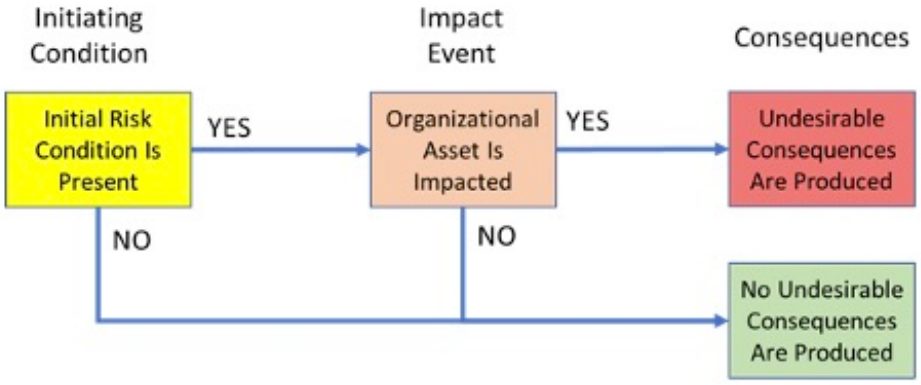


**Figure C1 – ESD rendition of a "standard" generic risk statement**

For the case of a PS&C risk involving a human hostile agent, the risk statement and corresponding ESD model would take the more specific forms shown, respectively, by the following indented paragraph and by Figure C2:

> *RISK STATEMENT FOR PS&C RISK INVOLVING HOSTILE:*
> *"Given that [HOSTILE AGENT IS PRESENT], there is a possibility of [BREACH OF SECURITY] from the baseline adversely impacting [ASSET], thereby leading to [CONSEQUENCE]."*

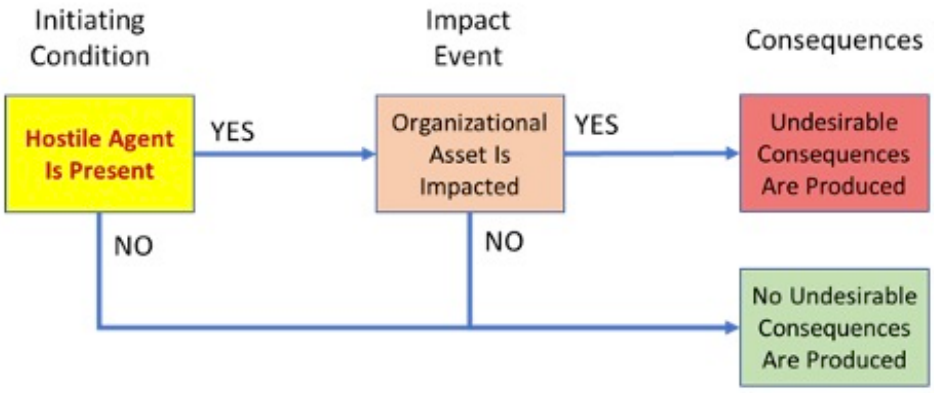


**Figure C2 - ESD rendition of a risk statement for PS&C risk involving an hostile agent**

The above considerations provide the basis for introducing the concepts of "conditional likelihood" and "conditional risk," as metrics relevant to the evaluation of PS&C domain risk. These concepts directly follow from the general formula that can be used to calculate the likelihood metric as a standard component in the classic risk-metric-duo, i.e., likelihood and consequence severity. When referred to a risk scenario defined in one of the above formats, such a formula is as shown below:

$$\text{Likelihood} = P(IC) \times P(IE \mid IC), \qquad \text{(Eqn.C1)};$$

where:

IC = Initiating Condition
IE = Impact Event
P(IC) = probability of Initiating Event

P(IE | IC) = conditional probability of Impact Event, given the Initiating Condition is present

In the representation of risk resulting from random events, "Likelihood" is the probability that a full scenario sequence, from source to consequences, 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.

In the representation of risk resulting from intentional actions by an hostile agent (e.g., a type of intentional cybersecurity threat posed by a specific type of adversary), a quantification or even a qualitative classification (e.g., "high," "low," etc.) of the frequency or probability of such actions may be difficult to produce with sufficient degree of confidence. In such cases, the "Conditional Likelihood" of the portion of the scenario that follows the scenario Initiating Condition "Hostile Agent Is Present" (shown in Fig. C2) corresponds to the component P(IE ??IC) of Eqn.C1. This component is referred to as a "Conditional Likelihood," rather than "Conditional Probability," to indicate that it may be estimated and expressed in qualitative, rather than fully quantitative terms, if this is appropriate and sufficient for risk evaluation purposes. The term "Conditional Probability" may be interchangeably used for such a metric, when it is expressed in fully quantitative terms.

It follows from the above that the Conditional Likelihood (or Conditional Probability) metric, P(IE ??IC) in Eqn.C1, represents the likelihood that, if an intentional threat identified as the risk scenario Initiating Condition (i.e., "Hostile Agent" in the Fig. C2 example) is assumed to be present, such a threat will be successful in producing the scenario consequences. It should be further noted that assuming the Initiating Condition as being present is equivalent, in quantitative terms, to assuming that its probability, P(IC) in Eqn.C1, is equal to 1.

C.2.1 PS&C Risk Modeling for Realistic Multi-Event Scenarios

When a realistic risk representation includes multiple concatenated events, as may be necessary for more complex scenarios, the Conditional Likelihood evaluation still requires considering the scenario as being composed of two conditionally linked primary blocks of events, which will be referred here as Event Block A (EB-A) and Event Block B (EB-B).

In this type of overall scenario sequence, EB-A will represent the risk Initiating Condition constituted by the event, or group of events, willfully caused to occur by an intentional cybersecurity threat, or other type of intentional hostile action against a system.

EB-B, the block of events conditionally following EB-A and only possible if all events in the latter have actually occurred, will instead represent the possible failure of the specifically engineered, or otherwise naturally present defenses that may protect the system of concern from the effects of EB-A.

The considerations made above for the simplified scenario representations and formulations given by Figs. C1 and C2, and by Eqn.C1 remain valid when the individual scenario components IC and IE are replaced by the corresponding "event blocks," EB-A and EB-B.

C.3 PS&C Risk Evaluation

Per the discussion presented above in C.2, for PS&C risks affecting a given system and involving as their Initiating Condition a specific type of assumed intentional threat to that system, the risk

evaluation can be based on a modified risk-metric-duo that will include, besides the customary Consequence Severity metric, a Conditional Likelihood metric as a replacement of the (unconditional) Likelihood metric used for all the other non-intentionally-initiated risk scenarios.

The modified duo constituted by the Conditional Likelihood and Consequence Severity metrics therefore expresses a "Conditional Risk" level for a system of concern, given an intentional threat / "Hostile Agent" which is assumed present. For a given system, a set of Conditional Risks will usually be assumed if the corresponding intentional / Hostile Agent threats are deemed possible and credible.

While in theory Initiating Conditions involving intentional threats can be evaluated / assessed via probability / likelihood estimation, the variability of the underlying driving factors (e.g., political conditions, conflict conditions, etc.) can make such assessments difficult to execute with confidence and unreliable over time. The Conditional Risk evaluation approach sidesteps these difficulties. The possible EB-A Initiating Condition types can be prioritized within the PS&C risk approach framework by qualitative relevance ratings - e. g., as per inputs from intelligence agencies, updated at regular time intervals to reflect the evolving driving factors, while the correspondingly identified EB-B events and factors can be evaluated using standard logic-probabilistic models and estimations, to assess the probability that the affected system or mission may be compromised by each type of intentional threat in the prioritized PS&C threat list, if such a threat is assumed to be present and active against the system.

### C.3.1 Potential Vulnerability and Control Effectiveness in PS&C Risk Scenarios

The conditional likelihood of system compromise (the Impact Event, or EB-B in the above discussions), given a certain specified type of threat being present and active (Initiating Condition or EB-A in those same discussions), is a measure of the system "Potential Vulnerability" to that type of threat.

The attribute "potential" is used in the term Potential Vulnerability to differentiate it from the deterministic, definitions of "vulnerability" that can be found in cybersecurity lexicons, whereby, by stating that a vulnerability to a certain type of threat exists in a given system, it is meant that such a system is completely unprotected from that type of threat and certain to be compromised if the threat materializes. Potential Vulnerability, as used in this NPR document, indicates instead a degree of vulnerability to an assumed type of threat, which can be expressed in Conditional Likelihood or Conditional Probability terms.

As an illustration of the concept, consider a network which is assessed as having a 50% conditional probability (or, qualitatively speaking, a "high" conditional likelihood) of unauthorized access to sensitive data, if an attacker sends phishing emails to its authorized user. It would then be reasonable to characterize such a network as having "high potential vulnerability" to phishing attacks.

In certain PS&C risk situations, the Conditional Risk evaluation may assess that a given system has significant degree of Potential Vulnerability to credible threats. In such situations, the development of realistic logic-probabilistic models of the factors that determine the conditional probability of the "EB-B" portions of the associated risk scenarios provides the means for identifying the risk control provisions that can be implemented to reduce the system potential vulnerabilities and cybersecurity risks. The reduction in system Potential Vulnerability produced by the application of a risk control, or set of controls, is a measure of the Control Effectiveness of that control or control-set.

### C.3.2 Assessment of PS&C Aggregate Risk

When considering risk produced by intentional threat sources, such as cyber-risk, the representation and assessment of aggregate risk, i.e., the ensemble of credible individual risks of the PS&C intentional-threat kind, will not be feasible in traditional form, since the corresponding scenarios are only partially quantifiable (e.g., via "Conditional Likelihood" or "(Conditional) Potential Vulnerability" metrics as suggested above).

For such cases and associated scenarios, surrogate aggregate risk indices can still be formulated, if this is still considered useful for specific purposes, by substituting threat weights (e.g., reflecting expert judgment supported by relevant and timely sources of information, such as intelligence input) in place of the initiating threat frequency or probability measures that would be used for all other more traditional and common types of risks and scenarios.

# Appendix D. Procurement/Contract Risk Management

D.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.

D.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.

## D.3 Acquisition Strategy Development

D.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.

D.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 (including both physical security and cybersecurity), and other applicable areas.*

D.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.

D.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.

## D.4 Requirements Development

D.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.

D.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.*

# D.5 Solicitation

D.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.

D.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.

D.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.

# D.6 Source Selection

D.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.

# D.7 Post-Selection Surveillance and Contract Monitoring

D.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.

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

# Appendix E. References

E.1 Federal Information Security Modernization Act of 2014, Pub. L. 113-283, (2014).

E.2 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), E.O. 13800 (2017).

E.3 Acquisition Planning, 48 CFR pt.7.

E.4 Contracting by Negotiation, 48 CFR pt.15.

E.5 Acquisition Planning, 48 CFR pt.1807.

E.6 Contracting by Negotiation, 48 CFR pt. 1815.

E.7 OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (07/15/2016).

E.8 OMB Circular A-11, Preparing, Submitting, and Executing the Budget (08/01/2017).

E.9 NPD 1000.0, Governance and Strategic Management Handbook.

E.10 NPD 1000.3, The NASA Organization.

E.11 NPD 1200.1, NASA Internal Control.

E.12 NPD 1440.6, NASA Records Management.

E.13 NPD 2810.1, NASA Information Security Policy.

E.14 NPD 7120.4, NASA Engineering and Program/Project Management Policy.

E.15 NPD 8700.1, NASA Policy for Safety and Mission Success

E.16 NPD 8900.5, NASA Health and Medical Policy for Human Space Exploration.

E.17 NPR 1441.1, NASA Records Management Program Requirements.

E.18 NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

E.19 NPR 7123.1, NASA Systems Engineering Processes and Requirements.

E.20 NPR 8705.4, Risk Classification for NASA Payloads.

E.21 NPR 8715.002B, NASA Emergency Management Program Procedural Requirements.

E.22 NASA/SP-2011-3422, NASA Risk Management Handbook.

E.23 Committee of Sponsoring Organizations of the Treadway Commission (COSO), Enterprise Risk Management - Integrated Framework (2004).

E.24 GAO-14-704G, Standards for Internal Control in the Federal Government (the GAO Green Book).

E.25 NIST-FIPS 200, Minimum Security Requirements for Federal Information and Information

Systems, dated March 2006.

E.26 NIST-SP 800-30, Rev. 1, Guide for Conducting Risk Assessments, dated September 18, 2012.

E.27 NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A system Life Cycle Approach for Security and Privacy. NIST-SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, dated September 2020.