

APPENDIX I

FOA Amendment 00002

RISK REGISTER AND RISK MANAGEMENT PLAN APPLICATION PREPARATION INSTRUCTIONS *(applicable to Demos, Risk Reduction and ARC-20)*

1. **BACKGROUND.** The core of the risk management is the structured cyclical process of identifying, analyzing, and responding to the potentials that have opportunities or undesirable consequences to achieving an organizational objective. These potentials (risks) occur at every level of activities within a project. Risk Management should be considered in a layered approach. Contextual awareness of objectives and requirements are critically important to developing risk and the associated assessments at various levels in the project.

A framework needs to be tailored to the specific needs of the project, documented, and formalized across the project activities. The structure and process outlined will be evaluated, along with the corresponding risk registers and profiles, which should be traceable from project impacts to activities and vice versa, and identify those risks that are internal and external. The benefit of the granularity is that it allows the risk assessment to cross-cut the project and identify commonalities.

The risk management process can be an important tool to current year tactical and out year strategic planning. Identified risk can be areas for investment, changes in resources, areas that require negotiation in order to accomplish the projects strategic objectives, and emerging risk due to environmental changes. It is vital that risks be specific and actionable, that mitigations strategies can be monitored, and that re-evaluation of the risk is ongoing to allow for adjustments to the mitigation strategy or control functions as needed. Risk should be continually identified and assessed in response to achieving a project's objectives. Linking risks with objectives within the project ensures that the risk identification process focuses on those risks that are critical to mission performance, rather than being vague and/or diverting by generalized concerns.

2. **DEFINITIONS.**
 - a. **Acceptance:** Risk response where no action is taken to respond to the risk based on the insignificance of the risk; or the risk is knowingly assumed to seize an opportunity.
 - b. **Aggregate Risk:** The total or cumulative amount of exposure associated with a specified risk. Aggregate risk is comprised of two components: significance and likelihood, and does not include the effect of risk strategies, controls, or other measures in place designed to mitigate the effect or reduce exposure to the specified risk.
 - c. **Avoidance:** Risk response where action is taken to stop the operational process, or the part of the operational process causing the risk.
 - d. **Control Activities:** The policies and procedures that help ensure management directives are effectively carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at

all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

- e. Cyber Information Security Risk: Risk that could expose the Project to exploitation of vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by its information systems.
- f. Impact: The effect of an event on strategic goals and objectives. Impact can be positive or negative, related to the organization's objectives.
- g. Internal Control: A process, affected by an organization's management or other personnel, designed to provide reasonable assurance regarding the achievement of objectives.
- h. Legislative Risk: Risk that legislation could significantly alter the mission (funding, customer base, level of resources, services, and products) of the Project.
- i. Likelihood: The probability that a given event will occur.
- j. Monitoring: Monitoring of the control system is essential in helping internal control remain aligned with changing objectives, environment, laws, resources, and risks. Internal control monitoring assesses the quality of performance over time. Corrective actions are a necessary complement to control activities in order to achieve objectives.
- k. Objective Setting: One of the eight components of ERM. Objective setting involves establishing desired objectives (goals) to complete within a specified period of time. Objective setting occurs at all levels of an organization. Objectives, set at the strategic level, help establish a basis for operations, reporting, and compliance. Objective setting is a precondition to other ERM components, including event identification, risk assessment, and risk response.
- l. Operational Risk: The risk of direct or indirect loss arising from inadequate or failed internal processes, people, systems, or external events. It can cause financial loss, reputational loss, loss of competitive position, or regulatory sanctions.
- m. Opportunity: A favorable or positive event. In context of risk management, it refers to the possibility that an event will occur and positively affect the achievement of objectives.
- n. Probability: A quantitative measure indicating the possibility that a given event will occur. Probability is usually indicated in terms of a percentage, frequency of occurrence, or another numerical metric.
- o. Reduction Risk response where action is taken to reduce the likelihood or impact of the risk.
- p. Regulatory Risk: The risk of problems arising from new or existing regulations. Such problems may include: changes in laws or regulations having significant impact on the organization, an inability for an organization to establish the right policies and procedures to be in compliance with regulations, or an increase in the cost and complexity to ensure compliance with new and existing regulations.

- q. Residual Risk: The amount of risk left over after action has been taken to manage it, (such as establishing internal controls).
 - r. Review (Verification and Validation): The process by which assessment of risks is evaluated by senior management.
 - s. Risk: The effect of uncertainty on achievement of objectives. An effect is a deviation from the desired outcome – which may present positive or negative results.
 - t. Risk Assessment: The identification and analysis of risks to the achievement of business objectives. It forms a basis for determining how risks should be managed. Risk assessment involves evaluating the significance and likelihood of a risk, as well as any controls or other measures that mitigate or eliminate that risk.
 - u. Risk Impact: A measurement of the effect that could result from the occurrence of a particular identified risk.
 - v. Risk Management: A coordinated activity to direct and control challenges or threats to achieving an organization's goals and objectives.
 - w. Risk Mitigation: Strategy for managing risk that seeks to lower or reduce the significance and/or likelihood of a given risk.
 - x. Risk Profile: A prioritized inventory of an organization's most significant risks.
 - y. Risk Response: Management's strategy for managing (or responding to) a given risk. Risk response strategies include avoidance, sharing, reduction, transfer, and acceptance.
 - z. Risk Tolerance: The acceptable level of variance in performance relative to the achievement of objectives.
 - aa. Sharing Risk: Response where action is taken to transfer or share risks across the organization or with external parties, such as insuring against losses.
 - bb. Significance: Magnitude or potential impact of a specified risk.
 - cc. Strategic Risk: Risk that would prevent an area from accomplishing its objectives (meeting the mission).
 - dd. Uncertainty: The inability to know in advance the exact likelihood or impact of future events.
3. Risk Management includes two complementary processes: Risk-Informed Based Decision Making (RBDM) and Integrated Risk Management (IRM). It requires formal processes for risk acceptance and accountability that are clear, transparent, and definitive
 4. Risk Management at the Project level addresses risks that have been identified/elevated for any of several reasons, including:

- a. The need for the Project to allocate additional resources for mitigation/control activities.
- b. Project-level coordination/integration is needed with other organizations/stakeholders.
- c. A finding that a risk identified externally is, in fact, a Project-level risk.

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

- a. Dealing with risk strategically from a project-level perspective, emphasis is on achievement of the project's mission objectives and goals versus individual goals/objectives, this is carried out by the Project's sub-elements.
- b. Engaging all functions and line management levels.
- c. Supporting project management.

Steps in the IRM process include:

- a. IDENTIFY: Identify contributors to risk (shortfalls in performance, relative to the baseline performance requirements).
- 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.
 - 1) Note: Risk acceptance is among the possible dispositions.
- 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.
- d. COMMUNICATE: Communicate and document the above activities throughout the process.

Within each project, disposition of risks includes the use of defined thresholds whose exceedance should initiate a risk control response, including the possible elevation of risk management decisions to the next higher level. Each internal unit reports on its risk management activities to 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.

It is the responsibility of the project to assure that the performance requirements assigned reflect appropriate tradeoffs between/among competing objectives and risks. The performance requirements can be changed, if necessary, but redefining them needs to be negotiated,

documented, and subject to configuration control. Performance requirements work together, so redefinition of one performance requirement may force redefinition of another.

5. IMPLEMENTATION

The project must:

- a. Ensure that the RBDM and IRM processes are implemented and key decisions of the project are risk-informed. Note: Examples of key decisions include architecture and design decisions, make-buy decisions, source selection in major procurements, resource reallocation, and acceptance of risks to safety or mission success.
- b. Establish internal performance requirements.
- c. Ensure that cross-cutting risks and interdependencies between risks are properly identified as cross-cutting and managed or elevated.
 - (1) Note 1: In general, the cross-cutting character of a given risk is best determined at a level above the level at which that risk is first identified.
- d. Ensure the development and Identification of:
 - (1) Categories for likelihood and consequence severity, when risk characterization requires specifying risks in terms of such categories. Determines and documents the protocols for estimation of the likelihood and severity of the consequence components of risks, including uncertainty characterization and quantification.
 - (2) Risk acceptability criteria/thresholds and elevation protocols (the specific conditions under which a risk management decision is elevated through management to the next higher level).
 - (3) 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.
 - (a) Note 1: This communication should be accomplished using standard reporting templates, including risk matrices.
 - (b) Note 2: In general, elevation protocols and communication protocols are specific to levels. A risk decision that requires elevation from one level to the next may well be manageable at the higher level, since that level has more flexibility, and authority effectiveness of the risk management effort depends on the proper assignment of risk acceptability criteria and thresholds.
 - (4) Intervals for the periodic review of the assumptions on which risk acceptance decisions are based.
 - (5) The processes for coordination of risk management activities and sharing of risk information with others affected.

- (6) Decisions to redefine performance requirements that affect safety, mission success, or institutional risk, are risk-informed consistent with the RBDM process described and that they are processed as risk acceptance decisions
 - (7) Risk information is maintained in the Project Risk Register, with a capability to identify and readily retrieve the current and all archived versions of risk information. For the Risk Register, it is to be included as a summary describing major risks, and is to be part of the Risk Management Plan; a full Risk Register is not required to be submitted.
 - (8) Key decisions, including risk acceptance decisions, are informed by Analysis carried out by applying the RBDM process with a level of rigor that is commensurate with the significance and the complexity of the decisions.
 - (9) 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 IRM at the higher level.
- e. Only one of the following possible risk dispositions is applied to any given risk. (related to PLAN step)
- (1) When a decision is made to ACCEPT a risk, each acceptance is clearly documented in the organizational unit's risk database, including the rationale for acceptance, the assumptions (including the conditions (e.g., programmatic constraints)) on which the acceptance is based, the applicable risk acceptance criteria, and the interval (as required by the Risk Management Plan) after which the assumptions will be periodically reviewed for any changes that might affect the continued acceptability of the risk. Additionally, for risk acceptance decisions, the requirements in paragraphs 3.5 (for program/project risks) or 3.6 (for institutional risks) apply.
 - (2) When a decision is made to CONTROL a risk, a risk mitigation plan (including contingency planning) is developed and documented in the risk database (including the parameters that will be tracked to determine the effectiveness of the mitigation).
 - (3) When a decision is made to ARCHIVE a risk, the closure rationale is developed, and both rationale and management approval are documented in the risk database.
 - (4) 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.
 - (5) When dispositions (1), (2), (3), or (4) 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.