S3001: Guidelines for Risk Management

Version: G

Effective Date: October 16, 2017

Note: The official version of this document is maintained in IV&V's internal IV&V Management System Website (https://confluence.ivv.nasa.gov:8445/display/IMS). This document is uncontrolled when printed.

Purpose

The purpose of this document is to provide guidelines that allow for the creation of a consistent and documented method of performing risk management within the NASA IV&V Program.

Scope

The guidelines in this document apply to risk management performed by the NASA IV&V Program on any IV&V Program-managed project.

Definitions and Acronyms

Note that the definitions provided here correspond with those provided in NPR 8000.4, *Agency Risk Management Procedural Requirements*, and NASA/SP-2011-3422, *NASA Risk Management Handbook*. If a conflict exists between this document and a definition in the NPR, the NPR should take precedence. If a conflict exists between this document and a definition in the Handbook, this document will take precedence.

- **Candidate Risk**
  - A candidate risk is an identified concern that is pending adjudication/ validation by the

governing Risk Review Board (RRB).

- **Consequence**
  - A consequence is the quantitatively or qualitatively expressed outcome of a risk that may lead to degraded performance with respect to one or more performance measures, such as an injury, fatality, destruction of key assets, cost overruns, schedule slippages or other events that may prevent a desired outcome from occurring or may result in a windfall.
- **Consequence Category**
  - A consequence category describes a functional area in which a risk can impact a project. Consequence categories used in this document are safety, performance, cost, and schedule.
- **Consequence Statement**
  - A consequence statement is a single phrase or sentence that describes the key outcome associated with a given risk.
- **Impact Horizon**
  - Impact horizon allows for the categorization of impact time frames in relation to the current date. It represents an abstract time frame in which the risk may occur. Impact horizon values can be near, mid, or long term.
- **Impact Time Frame**
  - Impact time frame represents the time when the risk may occur. Impact time frame consists of two pieces of data: a sunrise date that indicates the earliest time the risk could become realized, and a sunset date that indicates the latest time the risk could become realized.
- **Likelihood**
  - Likelihood is a measure of the possibility that a consequence is realized. This probability accounts for the frequency of the consequence and the timeframe in which the consequence can be realized. For some purposes, it can be assessed qualitatively. For other purposes, it is quantified in terms of frequency of probability.
- **Priority Score**
  - The Priority Score is numerically represented by a cross-reference of the likelihood and consequence scores of a risk plotted on a Risk Matrix.
- **Project Team Member**
  - Project Team Members are personnel assigned to work on a defined Project or activity. Project Team Members can be NASA civil servants or contract employees. Project Team Members are responsible for bringing potential risks to the attention of their Project Managers (PMs) and may also be requested to assist or perform risk analysis to determine the consequence and likelihood associated with a risk. The Project Team Members also may collect data to assist in the monitoring and tracking of a risk. A Project Team Member may be an owner of a risk or simply a subject matter expert that can supply critical information to support analysis of the risk.
- **Realized Risk**
  - A realized risk is an adverse situation that currently exists. There is no opportunity to avoid this as it is already occurring. A realized risk may also be known as a problem. It is an undesirable event that has occurred and its occurrence cannot be stopped or directly controlled. Reactive management is necessary to deal with this, because realized risks can lead the project into new risks. Realized risks can have contingency plans that may minimize the impact of the consequence. The contingency plans may have risks associated with them.
- **Risk**
  - A risk is the potential for performance shortfalls which may be realized in the future with

respect to achieving explicitly established and stated performance requirements. The performance shortfalls may be related to institutional support for project execution or related to any one of more of the following project execution domains:

1. Safety
2. Technical
3. Cost
4. Schedule

- **Risk Acceptance**
  - Risk acceptance is the formal process of justifying and documenting a decision not to mitigate a given risk associated with achieving given objectives or given performance requirements. Risk acceptance can take place when the consequences are tolerable should the risk occur, or when the risk cannot be reasonably mitigated with further action.
- **Risk Analysis**
  - Risk analysis examines risks in detail to determine the extent of the risks and the relationships among them. Risk analysis also classifies risks into sets of related risks and ranks them according to importance. Risk analysis evaluates all identified risks to estimate the likelihood of occurrence, consequence of occurrence, and timeframe for necessary mitigation actions.
- **Risk Approval**
  - Risk approval is the decision to validate a candidate risk. Risk approval can be performed by the governing RRB at any level within the NASA IV&V Program. An approval simply means that the risk is well stated and meaningful within the domain of the governing RRB.
- **Risk Assessment**
  - Risk assessment is the qualitative and/or quantitative evaluation of the likelihood and consequence of a risk occurring.
- **Risk Attribute**
  - Risk attributes are characteristics of likelihood and consequence that describe or define standard ways of assessing the consequence or success of a Risk Mitigation Plan. Risk attributes are chosen during risk planning and provide meaningful information that can enable more informed control decisions.
- **Risk Closure**
  - Risk closure is the determination that a risk no longer exists or is no longer cost-effective to track, because (for example) the associated consequence likelihoods are low (e.g., the underlying condition no longer exists).
- **Risk Elevation**
  - Risk elevation is 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.
- **Risk Identification**
  - Risk identification examines each element of a project to identify risks that may impact the NASA IV&V Program/Project, and then documents the risks found. Risk identification occurs at all organizational levels and begins as early as possible in a successful project continuing throughout the lifetime of that project.
- **Risk Management**
  - Risk management is an overarching process that encompasses identification, analysis, mitigation planning, and tracking of root causes and their consequences.

- **Risk Management Planning**
  - Risk management planning develops and documents an organized, comprehensive, and interactive strategy for identifying and tracking root causes, developing Risk mitigation Plans, performing continuous risk assessments, and assigning adequate resources.
- **Risk Management Team**
  - The Risk Management Team owns the risk management process and provides training on the implementation of that process. The Risk Management Team uses a metrics-based approach to understand how well the risk management process is working and to improve process when needed.
- **RiskManager Tool**
  - The RiskManager Tool (RMT) is a web-based automated tool that can be accessed by the IV &V Program Portal. The RMT is a controlling function of the process to document, communicate, track, and manage risks.
- **Risk Matrix**
  - A Risk Matrix is a graphical representation of the likelihood and consequence scores of a risk. It is sometimes called a "5x5 Matrix" because it contains five rows and five columns. The rows of a Risk Matrix show likelihood scores, while the columns show the consequence scores. Each cell in a Risk Matrix can be represented by a Priority Score.
- **Risk Mitigation**
  - Risk mitigation is action taken to reduce the severity of a risk by reducing the likelihood of its occurrence, and/or minimizing the consequences of occurrence.
- **Risk Mitigation Plan**
  - A Risk Mitigation Plan is a document that captures the actions to be taken to reduce the likelihood of risk occurrence. This document is the output of risk mitigation planning.
- **Risk Mitigation Planning**
  - Risk Mitigation Planning is the process of analyzing a risk to determine actions that may be taken to reduce the likelihood of risk occurrence.
- **Risk Owner**
  - The "risk owner" is the entity, usually a named individual, designated as the lead for overseeing the implementation of the agreed disposition of that risk.
- **Risk Research**
  - Risk research is the investigation of an identified risk. Risk research continues until there is enough information to determine if risk ownership is still properly assigned and to determine the risk mitigation strategies (i.e., accept, watch, or mitigate the risk).
- **Risk Review Board (RRB)**
  - Risk Review Boards (RRBs) are 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. This generally takes the form of understanding and approving candidate risks as well as evaluating proposed mitigation plans and approving them. The RRBs are held primarily at the functional organization level (Office level) and at the Office of the Director Level (Program Level providing information to the functional organization leader and Program Management).
- **Risk Stakeholder**
  - A risk stakeholder is a person, group, or organization that is affected by a risk or a risk mitigation strategy.
- **Risk Statement**

    - A risk statement is a single descriptive statement that defines the risk's current or possible condition and undesired consequence. The risk statement is generally written in a format *of* " Given that [CONDITION], there is a possibility of [DEPARTURE] adversely impacting [ASSET], thereby leading to [CONSEQUENCE]."
    - A CONDITION is a single phrase that describes the current key fact-based situation or environment that is causing concern, doubt, anxiety, or uneasiness.
    - A DEPARTURE describes a possible change from the (program, project, or activity) baseline project plan. It is an undesired event that is made credible or more likely as a result of the condition.
    - The ASSET is an element of the functional organization portfolio (analogous to a WBS). It represents the primary resource that is affected by the individual risk.
    - The CONSEQUENCE is a single phrase that describes the foreseeable, credible negative impact(s) on the organizational unit's ability to meet its performance requirements.
    - The Risk Statement is not equivalent to the solution. The Risk Statement is written in matter-of-fact, straightforward language, avoiding the excessive use of technical terms or jargon.
- **Risk Tracking**
    - Risk tracking is the capturing, compiling, and reporting of risk attributes and metrics that determine whether or not risks are being mitigated effectively, and whether Risk Mitigation Plans are implemented correctly.
- **Sensitive Risks**
    - Sensitive risks are risks that contain information requiring restricted or limited access, such as supervisory, legislative, or procurement sensitive information.

Acronyms

ECD	Estimated Completion Date
ECM	Enterprise Content Management
FY	Fiscal Year
IMS	NASA IV&V Management System
IVVO	IV&V Office
NODIS	NASA Online Directives Information System
NPR	NASA Procedural Requirements
OSHA	Occupational Safety and Health Administration
PDR	Preliminary Design Review
PFM	Program Financial Management

PL	Project Lead
PM	Project Manager
QM	Quality Manual
RMS	Risk Management System
RMT	RiskManager Tool
RRB	Risk Review Board
SP	Special Publication
SRR	System Requirements Review
SSO	SMA Support Office
WBS	Work Breakdown Schedule

Procedure

This section provides additional guidance on how to create and process IV&V Program risks, from developing a strategy to documenting and communicating those risks.

All risks and associated information resulting from the execution of this risk process shall be captured in the RMT and/or Enterprise Content Management (ECM) System. In this document, references made to a "risk database" indicate these repositories.

Develop Strategy

The first step in any risk management effort is to define the approach for risk management. The designated program/project/activity manager/lead (hereafter referred to as the PM) for any effort shall determine the approach needed to manage risk on projects assigned to him.

The approaches may vary depending upon the size of the project. Large, complex projects may need a documented plan detailing the approach to performing risk management as well as defined interactions with the project's governing RRB. Smaller projects may only need a simple process by which they identify any risks, document them, and take them before the governing RRB.

For IV&V projects, there is also a need to define a strategy for dealing with external risks discovered through the course of performing IV&V analysis. So, all IV&V projects may have both an internal and external risk strategy defined.

The basic risk management strategy is intended to identify both technical and non-technical critical

areas and risk events, and take necessary actions to handle them before they can become problems and cause serious safety, cost, schedule, or performance consequences. PMs can extensively use typical risk sources/risk drivers to handle new risks populated throughout the project's lifecycle.

The PM needs to ensure that he has defined performance goals or measures for his project in order to adequately plan the risk strategy. The performance measure should be created with input from the functional organization under which the project falls.

The basic strategy that is developed should include the identification, analysis, planning, tracking, and control of risk associated with that project.

Risk information will be a part of all program/project/activity reviews. The PM will conduct additional reviews periodically to update current risk status and to ascertain if new risks exist. The goal is to continuously look for future risks in areas that may -impact individual project/activities as well as the NASA IV&V Program.

Everyone has some responsibility for risk management. However, there is an overall structure to the responsibility that starts with the IV&V Program Director and flows down to the functional organizations and the projects.

Identify Risks

The first step in the risk management process is the identification of risks. Risks can be identified using a number of processes. This document does not define how any specific risk identification process is to be performed, as different types of projects may require different approaches; however, some of the more common approaches are listed in the following table:

Formal	Informal
System safety assessments – fault tree analysis, hazard analysis, failure modes and effects analysis	Brainstorming
Quantitative risk assessments	Test and verification
System and software engineering	Pause and learn sessions
Program planning and control – cost and schedule risk analysis	Experience – previous analysis, lessons learned, historical data
Models and simulations	

Table 4-1 - Risk Identification Methods

Risk identification depends heavily on both open communication and a forward-looking perspective. This encourages all personnel to communicate new risks and to plan beyond their immediate problems. Although individual contributions play a role in risk management, teamwork improves the chances of identifying new risks by allowing all personnel to combine their knowledge and understanding of the project.

Risk identification shall begin as early as possible and continue throughout the project lifecycle, including ad hoc risk identification, as well as identification approaches captured in the Project's risk management strategy (see *Develop Strategy*).

Risk Documentation

The PM (or designee) shall document each risk identified to include a title, risk statement, context statement (descriptive narrative which captures the context of the risk by describing the circumstances, contributing factors, uncertainty, range of possible consequences and related issues), and closure criteria. This is performed for both internal and external risks(1).

The RMT is a web-based automated tool to facilitate documenting risk status of the IV&V Program. The RMT is the controlling function of the risk management process to document, communicate, track, and manage risks that can be accessed by the IV&V Program Portal.

Title

The title should be written to gain attention and focus on the appropriate audience. It should answer the question "So what?"

Risk Statement

The risk statement should be written in a condition/consequence format. The following is the expected format for a risk statement:

"Given that [CONDITION], there is a possibility of [DEPARTURE] adversely impacting [ASSET], thereby leading to [CONSEQUENCE]."(2)

It is the job of the risk identifier, working as needed with risk management personnel, to develop the verbiage for the CONDITION, DEPARTURE, ASSET, and CONSEQUENCE components of the risk statement.

- **CONDITION –** The CONDITION is a single phrase that describes the current key fact-based situation or environment that is causing concern, doubt, anxiety, or uneasiness. The fact-based aspect of the CONDITION helps to ground the individual risk in reality, in order to prevent the risk database from becoming a repository for purely speculative concerns. The CONDITION represents evidence in support of the concern that can be independently evaluated by risk management personnel and which may be of value in determining an appropriate risk management response during the *Plan* step.
- **DEPARTURE –** The DEPARTURE describes a possible change from the baseline project plan. It is an undesired event that is made credible or more likely as a result of the CONDITION. Unlike the CONDITION, the DEPARTURE is a statement about what might occur at a future time. It is the uncertainty in the occurrence or non-occurrence of the DEPARTURE that is the initially identified source of risk.
- **ASSET –** The ASSET is an element of the organizational office (this is usually a specific project or a specific portion of a project and may be seen as similar to a portion of a WBS). It represents the primary resource that is affected by the individual risk.

- **CONSEQUENCE –** The CONSEQUENCE is a single phrase that describes the foreseeable, credible negative impact(s) on the functional organization's ability to meet its performance requirements. It should describe the impact(s) in terms of failure to meet requirements that can be measured, described, and characterized.

It is important to keep in mind that risk statements need to be crafted without regard to potential mitigations or other risk responses that may suggest themselves to the risk identifier. The risk statement should not be equivalent to the solution and should not be written to provide a solution. The risk statement should not presume anything that is not in the current baseline project plan other than the CONDITION, which has its basis in fact.

An example of an incorrect risk statement is, "If we do not get more funding, then the project will not be able to complete the analysis." This risk statement incorrectly implies that the only possible resolution is extra funding. The risk statement should be written in matter-of-fact, straightforward language. Excessive use of technical terms or jargon should be avoided.

(1) External risks are risks generated as a result of IV&V analysis performed on development projects. They are risks that affect the developer of the project and not risks that affect the ability of the IV&V project to meet its performance requirements.

(2) The format provided here is specified in the NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0 (Nov 2011) and is intended to provide consistency in the risk statements; clarify which functional organization is responsible for the risk; as well as, provide a better understanding of the event that must occur for the CONSEQUENCE to result. The CONSEQUENCE is the inability to meet a performance requirement. Other formats for risk statements may be accepted, but they need to clearly establish the functional organization responsible for the risks as well as the event that will cause the CONSEQUENCE.

Context Statement

The risk statement provides a concise description of the risk; however, this is usually not sufficient to capture all the information that the risk identifier has to convey, nor carry enough information for others to understand and respond to the risk effectively. The context statement provides the background information so that the risk can stand on its own and be understood by someone not otherwise familiar with the risk. The context statement is format-free and can include:

- Key circumstances surrounding the risk
- Contributing factors
- Uncertainties
- The range of possible consequences

- Related information such as what, where, when, how and why

The context statement should include only facts, not assumptions. Ensure that no new risks are introduced here. The author should cite related requirements and objectives that may be affected if the risk is realized. A well-written context statement serves as the starting point for the development of a Risk Mitigation Plan. In fact, the risk identifier can suggest or recommend potential mitigations or other risk responses that he feels is most appropriate.

The risk identifier is usually someone with significant subject matter expertise in the affected asset and it is important to capture that expertise not only concerning the nature of the possible consequence but also its remedy. When a risk response is recommended, the risk identifier should also record the rationale for the recommendation, preferably including an assessment of the expected risk shifting (for example, from a safety risk to a cost risk) that would result.

There may be times when a development project risk generates an IV&V Project risk. In these instances, it is beneficial to note the development project's risk in the context statement.

Closure Criteria

The closure criteria should document how the risk can be eliminated, or how the likelihood of the risk can be reduced to an acceptable level. The closure criteria should be specific and measurable, and should state how the risk can be closed or eliminated. Risk closure is the goal of risk mitigation, and is the last step in the Risk Mitigation Plan.

Analyze Risk

It is important to the success of the risk management program that every individual risk receives the appropriate level of analysis needed to incorporate it into the overall risk perspective for the program, project, or activity.

The PM and/or risk owner shall analyze and prioritize identified risks. This is accomplished by comparing the likelihood of occurrence, consequence, impact time frame (sunrise and sunset dates), and impact horizon (impact time frame in relation to the current date (Near, Mid, and Long term)).

The likelihood can be determined in a quantitative or qualitative manner. In either case, the results of the analysis are used in conjunction with Table 4-2 *Risk Likelihood Criteria*, to assign a likelihood score from 1 to 5.

Likelihood		
Score	**Likelihood of Occurrence (p)**	
5	Near certainty	p > 80%
4	Highly Likely	60% < p 80%

3	Likely	40% < p 60%
2	Low likelihood	20% < p 40%
1	Not likely	p 20%

Table 4-2 - Risk Likelihood Criteria

The consequence score is determined by assessing the consequence of the risk and assigning a consequence score from 1 to 5 based on the criteria in Table 4-3, *Risk Consequence Criteria*. Risks must be analyzed and scored on each separate consequence category.

CONSEQUENCE					
	1	**2**	**3**	**4**	**5**
Performance	Minimal consequence to objectives/goals	Minor consequence to objectives/goals	Unable to achieve a particular objective/ goal, but remaining objective goals represent better than minimum success or outcome	Unable to achieve multiple objectives/ goals but minimum success can still be achieved or claimed	Unable to achieve objectives/goals such that minimum success cannot be achieved or claimed
Safety **Human**	Discomfort or nuisance	First aid event per OSHA criteria	No lost time injury or illness per OSHA criteria	Lost time injury or illness per OSHA criteria	Loss of life
Asset	Minimal consequence: asset has no sign of physical damage	Minor consequence: asset has cosmetic damage and is repairable	Minor consequence: asset is damaged but repairable	Major consequence asset is substantially damaged but repairable	Destroyed: asset is compromised, and un-repairable: a total loss
Schedule	Minimal consequence	Critical path is not slipped; total slack of slipped tasks will not impact critical path in less than 10 days	Critical path is not slipped; total slack of slipped tasks is within 10 days of impacting the critical path	Critical path slips	Critical path slips and one or more critical milestones or events cannot be met
Cost	Minimal consequence	Minor cost consequence. Cost variance ≤ 5% of total approved FY baseline	Cost consequence. Cost variance >5% but ≤ 10% of total approved FY baseline	Cost consequence. Cost variance >10% but ≤15% of total approved FY baseline	Major cost consequence. Cost variance >15% of total approved FY baseline

Table 4-3 - Risk Consequence Criteria

S3001 Table 4-3 -- 04-03-2017.docx

The highest score from these four consequence categories is then used as the final consequence score. For instance, a risk with a likelihood score of 3 that has safety consequence score of 2, a performance consequence score of 3, a schedule consequence score of 4, and a cost consequence score of 3 would be considered a “3x4” risk (the likelihood score is 3, and the schedule consequence score is 4, which is the highest consequence score). If one of the consequence categories is not applicable, that consequence score is 0 (i.e., if a risk has no consequence for safety, the safety consequence score should be 0).

In addition to likelihood and consequence scores, the impact time frame and impact horizon are determined. The impact time frame consists of two dates: a sunrise date that indicates the earliest time the risk could become realized, and a sunset date that indicates the latest time the risk could become realized. These two values can be used to prioritize the risks in addition to the consequence and likelihood. The impact horizon is then determined from the dates in the impact time frame using Table 4-4, *Impact Horizon Definition*. The impact horizon is used to help further prioritize risks according to the time frame in which they will occur. The impact horizon can be one of three values based simply on the sunrise time:

Impact Horizon	Sunrise	Sunset
Near	<2 months	> Sunrise
Mid	2-6 months	> Sunrise
Long	>6 months	> Sunrise

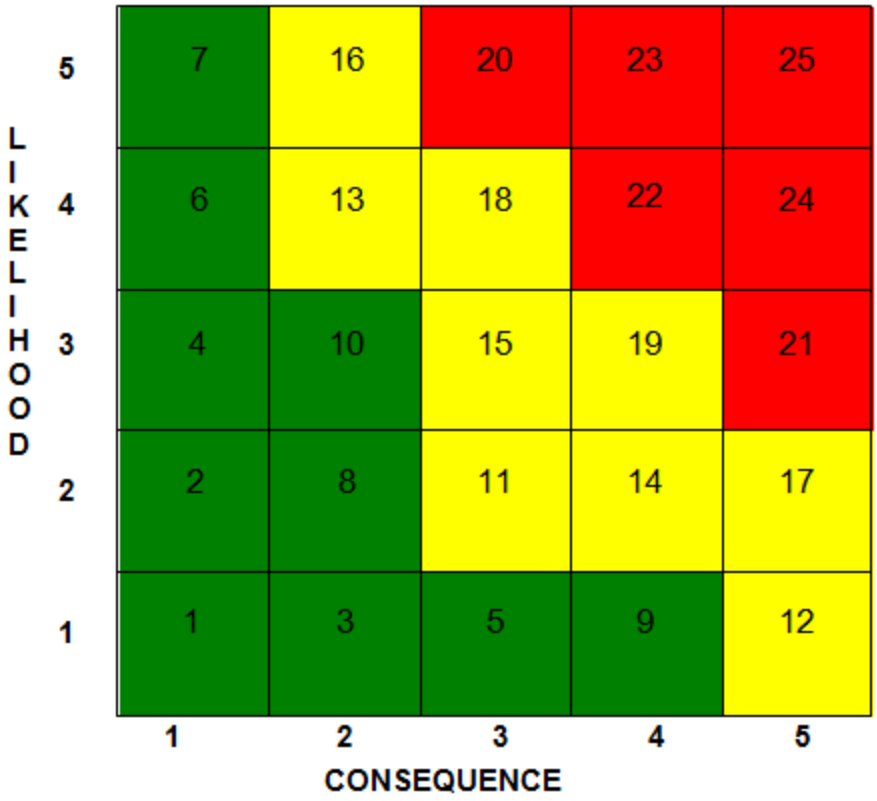
Table 4-4 - Impact Horizon Definition

Risk scoring is performed to facilitate risk review, integration, roll-up, prioritization, and summarization. Risks should be evaluated at a level of analysis that is sufficient to determine the relative importance for planning cost-effective mitigation strategies and for tracking. For example, high-likelihood, high-severity risks require a more detailed level of analysis to plan effective mitigation strategies.

External risks are analyzed in the same manner described for internal risks to determine likelihood of occurrence, consequence, impact time frame, and impact horizon. However, the likelihood and consequence criteria from the development project are used in place of the criteria depicted in this document. Typically the concepts of sunrise, sunset, and impact horizon are not used for external risks.

Prioritizing risks

Once the likelihood score, consequence score, impact time frame, and impact horizon have been determined, a risk can be prioritized by determining its Priority Score. The Priority Score is the score assigned via the Risk Matrix cell into which the risk falls. The Risk Matrix cell into which the risk falls is based on the risk's likelihood and consequence scores (see Figure 4-5, *Risk Matrix*). For example, a risk with a likelihood score of 3 and a consequence score of 4 would yield a Priority Score of 19.



S3001 Figure 4-5 --04-03-2017.docx

Figure 4-5 - Risk Matrix

Development projects may or may not have prioritization processes or criteria. If the development project has such processes, then follow those processes to prioritize external risks. If the development project does not have a prioritization process, then for purposes of this process, use the Priority Score described above to determine the level of review required for the risk.

Risk prioritization is a part of risk analysis and provides a basis for allocating mitigation and contingency resources, developing mitigation plans, and preparing individual mitigation tasks. Funding and schedule constraints generally do not allow all project risks to be mitigated. Risk prioritization is vital in determining which critical risks get mitigated and when, and which risks need to be escalated to the NASA IV&V Program level for determination and resolution. A key objective in prioritizing risks is to determine which risks will be fully accepted, actively controlled, closely tracked, or only watched. The risk prioritization process is closely related to the elevation process (see *Communicate* section).

Risk Review

Once analysis of the risks is complete, the risks are presented at the governing RRB for acceptance using the RMT. The goal of the RRB is two-fold: (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. This generally takes the form of understanding and approving candidate risks as well as evaluating proposed mitigation plans and approving them. The RRBs are held primarily at the functional organizations level (Office level) and the Office of the Director Level (Program Level), providing information to the functional organizations leader, Program Management, and other personnel.

The governing RRB should consider the following questions to validate a risk:

i. Does the risk (i.e., risk statement and context statement) adequately communicate the possible sequence of events leading from the CONDITION through the DEPARTURE to the ASSET and the CONSEQUENCE?
ii. Is the risk based on relevant documentation or individual/group knowledge?
iii. Does the risk involve a change from the program/project/activity baseline plan for which an adequate contingency plan does not exist? (Note: If it involves an existing contingency plan that is believed to be inadequate, the failure of that contingency plan should be addressed in the DEPARTURE portion of the risk statement.)
iv. Is the CONDITION factually true and supported by objective evidence?
v. Is the DEPARTURE credible (possible)?
vi. Does the risk impact at least one agency/program/project/ activity requirement that can be objectively measured, described, and characterized?
vii. Is the CONSEQUENCE written without regard to potential mitigations?
viii. Is the risk actionable (i.e., can something be done to prevent or reduce the likelihood of the DEPARTURE and/or severity of the CONSEQUENCE)? (Note: Determination of whether a risk is actionable is based on current assumptions about funding and other programmatic constraints.)

If the risk is valid, the process diverges into two distinct processes. If the risk is internal, the process continues with the *Planning* section. If the risk is external, the process continues with the *Communicate, Control, and Track Risks* section. No Risk Mitigation Plan is required for an external risk.

The risk review process is performed at various points throughout a risk's lifecycle via presenting the risk at the governing RRB.

In all risk reviews, a rejected risk is returned to its previous state for the PM or Risk Owner to provide corrective action.

Planning

Planning addresses what, if any, action should be taken to address an activity's performance risk. In this process, decisions and mitigation strategies are developed based on current knowledge of project risks.

The planning process is only applicable to internal risks. If the risk is external, proceed to the *Co mmunicate, Control, and Track Risks* section.

Develop Mitigation and Contingency Plans

Once the initial risk review is complete, the risk then enters a planning phase. During this phase, the risk shall be further analyzed to ensure that the consequence and likelihood scores are correct, and that the risk has the correct owner. There are four basic tasks that take place during this phase. These tasks are:

1) Generate a set of candidate risk response alternatives;

2) Conduct a risk analysis of each alternative;

3) Deliberate and select an alternative for implementation; and

4) Implement the selected alternative.

Developing a mitigation plan includes defining the leading risk driver(s). These drivers are the uncertain elements in a risk with the most potential to contribute to a performance shortfall. A risk driver can be a single performance parameter, a single event, a set of performance parameters collectively, or a set of events collectively that, when varied over their range of uncertainty, causes the performance risk to change from tolerable to intolerable (or perhaps marginal). The intent of a risk driver is to focus risk management attention on those potentially controllable situations that present the greatest opportunity for risk reduction.

The type of risk response options to be considered for a given risk depends on the nature of the uncertainty that makes it a driver. When the uncertainty is primarily caused by variability in the system or the environment, risk reduction is typically accomplished via mitigation. If the uncertainty is primarily due to a lack of knowledge, then the response often begins with research to better understand the facts of the matter and proceeds to mitigation if, after the research is complete, the risk is still intolerable.

The Risk Score also serves as criteria for determining response options. When the Risk Score is less than or equal to 7, there is no specific requirement to generate a mitigation plan. The only requirement is to identify and track the risk drivers to ensure the risk remains tolerable.

When the Risk Score is at 8 or higher, the risk drivers are identified and, depending on the nature of the uncertainty, as noted above, a mitigation plan may be developed or further research may be performed.

These criteria are captured in Table 4-6, *Risk Planning*.

	Risk Score ≤ 7	Risk Score ≥ 8
Research	Identify the risk drivers.	Determine risk drivers for tracking. If uncertainty comes from lack of knowledge, perform research to increase understanding and to determine mitigation approaches
Plan	Track the risk drivers	If uncertainty is due to variability in the project/environment, document mitigation approach along with risk drivers that will be used for trending

Table 4-6 - Risk Planning

S3001 Table 4-6 -- 04-03-2017.docx

The research phase concludes with either risk ownership affirmation or risk reassignment, and the development of a plan that recommends the risk approach strategy as either "watch" or "mitigate".

Watch

Risks can be watched if one of the following conditions exists:

- The risk is low priority (priority less than 8).
- Sufficient mitigation resources are not available.
- Mitigation cost is comparable to recovery costs if the risk was to occur.
- The likelihood of mitigation success is uncertain.

Watched risks can be placed on a watch list where each risk is periodically (at least quarterly) reassessed. For watched risks, the risk attributes are continually monitored for early warning of critical changes in likelihood, consequence, time frame, or other aspects.

Placing the risk on the watch list does not remove the requirement for monthly risk attribute tracking.

To watch a risk, the PM or Risk Owner shall create decision points, dates, milestones, necessary achievements, or goals that shall move the likelihood of the risk lower or higher. When the defined metrics exceed the trigger points, specific risk mitigation actions should be taken.

Mitigate

Risk mitigation reduces the likelihood of risk occurrence, or shifts the time frame in which the risk will occur through the execution of a predetermined set of action steps (e.g., Risk Mitigation Plan). A layout of a Risk Mitigation Plan is shown in Figure 4-7, *Ri sk Mitigation Plan*, which is also part of the RMT. The execution of a Risk Mitigation

Plan may require additional resources; however, the selected approach may result in an acceptable risk level.

Risk Mitigation Plans may be generated simply by denoting each mitigation task along with a goal (exit or success criteria) that provides measurable and objective evidence of task completion. Risk reduction only occurs when the resulting likelihood score is reduced as a result of task completion. The goal of risk mitigation is to reduce the likelihood of the risk to the closure level before the sunrise date, if possible.

Risk Mitigation Plans that require additional funding because they include non-baseline/non-funded work must be worked through the appropriate NASA IV&V Program process. The Risk Mitigation Plan will include the estimated cost for implementing a risk mitigation step. Approval of the Risk Mitigation Plan approves the estimated cost, but does not provide for the allocation of the costs. The allocation must be accomplished through the appropriate NASA IV&V Program process (e.g., Baseline revision request).

It is the goal of the NASA IV&V Program to minimize risks to the lowest practical level within the allocated resources. When choosing to mitigate a risk, the following questions should be considered:

a. Cost
    i. Is the Risk Mitigation Plan within the current funded budget and scope?
    ii. How much does each mitigating option cost, and how likely are they to succeed?
    iii. Is the mitigation going to cost more than the actual cost of the risk consequence?
    iv. What are the costs of mitigation versus the benefits and uncertainties of risk reduction?
b. Schedule
    i. Are each of the mitigation tasks part of the in-scope work? Should they be?
    ii. What tasks are new work that should be addressed through the IV&V budget processes?
    iii. Who is responsible for each of the mitigation tasks?
    iv. What is the consequence for the project schedule for each mitigation option?
    v. Does the risk impact a critical or significant milestone? Are there clear references to these consequences?
c. Are all stakeholders identified and included in the mitigation planning?
d. What is the confidence level for successful completion of each mitigation option?
e. What is the amount of risk reduction at the completion of the Risk Mitigation Plan?

All Risk Mitigation Plans are reviewed and concurred upon at the governing RRB to determine which risk mitigation activities will be actively pursued (see the *Communicate , Control, and Track Risks* section). Ownership of the Risk Mitigation Plans is assigned to the appropriate level for execution. If the choice is to mitigate the risk, the Risk Owner develops a detailed Risk Mitigation Plan. Each plan may have several action

steps that need to be performed for effective mitigation (individual action steps should be assigned to the most appropriate Project Team Members, even though the overall plan is managed by the Risk Owner). The Risk Owner implements the Risk Mitigation Plan and oversees that all the mitigation actions are completed until the risk reaches an acceptable limit or is eliminated. At that time, the Risk Owner recommends to management that the risk is accepted (residual risk remaining) or closed (risk eliminated). Based on the amount of residual risk remaining, the risk can either remain open or move into the "watch" state.

Accepted mitigation activities are integrated into the project schedule to ensure that the schedule accounts for all task dependencies, and to monitor progress on all Risk Mitigation Plans. In some instances, a mitigation task may represent new work that requires a baseline revision (or other approval) to be processed to execute the mitigation task.

Risk Mitigation Plans are approved and controlled by the governing RRB and/or NASA IV&V Program/ Project management in the RMT. After Risk Mitigation Plan tasks have been approved by the governing RRB and/or NASA IV&V Program/Project management and incorporated into the project master schedule, changes to the tasks or completion dates are controlled through the Baseline revision process (see IVV 07, *Financial Data Control*, section *Baseline*, PFM System tool, and IVV 09-4, *Project Management*, for additional information). Budget requirements for risk mitigation are included in the fiscal planning process.

Key Mitigation Action Planned	Goal (note Risk reduction)	Additional Cost	Planned Start Date	Actual Completion Date	Results of Action
#1: [Mitigation Action Title] *{The first Mitigation Action Title correlates to the first Planned Priority Score of "25" in the example above, and its date (MMM-YY) is consistent with the Sunrise/Sunset Dates; this Mitigation Action Title describes the first measurable, proactive action to reduce Risk to acceptable level (residual Risk), or to eliminate it (closed Risk), prior to Sunset Date; Causal factors should be addressed by Mitigation Actions.}*	[Goal of Mitigation Action # 1] *{Used with Results of Action to track Planned/Actual Risk Reduction/Escalation}*	[Cost] *{The cost outside of budget necessary to perform Mitigation Action # 1.}*	[MM/DD/YY] *{Planned Start Date of Mitigation Action # 1.}*	[MM/DD/YY] *{Actual Completion Date of Mitigation Action # 1.}*	[Results of Mitigation Action #1] *{Used with Goal to track Planned/Actual Risk Reduction/Escalation}*
#2: [Mitigation Action Title] *{The second Mitigation Action Title correlates to the second Planned Priority Score of "22" in the example above . . .*					
#[N]: Risk Closure *{The last Mitigation Action Title is Risk Closure.}*	Risk Closure	N/A	N/A	[MM/DD/YY] *{Actual Date of Risk Closure.}*	Risk Closed: [Closure Rationale]

Figure 4-7 - Risk Mitigation Plan

Risk Mitigation Plan Review

For any internal risk with a Priority Score greater than 7, the PM will discuss the Risk Mitigation Plan with the Functional Lead. This step will ensure quality assurance and concurrence on the Risk Mitigation Plan. The review is not an approval of the Risk

Mitigation Plan; it is an assessment of the completeness and consistency of the Risk Mitigation Plan.

Communicating the Risk Mitigation Plan to the Risk Management Team is valuable in determining if there may be other potential risk stakeholders, ensuring that requests for risk transfers are acted upon, and raising significant concerns with the PM.

Any conflicting opinions will be discussed with the appropriate Office Lead.

There is no requirement to generate a Risk Mitigation Plan for external risks. The NASA IV&V Program is not responsible for the mitigation of external risks. The development project is responsible for mitigating its own risks.

Internal risks with Priority Scores of less than 8 do not require a Risk Mitigation Plan. However, all other risks require a Risk Mitigation Plan. Risk mitigation plans are presented at the governing RRB when they are first generated for approval/ concurrence and whenever a mitigation task has been or is scheduled for completion or if the plan is updated.

Approval occurs during RRBs. Approval occurs at the lowest level that has authority to implement the risk mitigation plan. Some plans may need to be elevated if higher authority is needed to implement the plan. The highest approval level within the IV&V Program is at the IV&V Program RRB.

Office RRB meetings and IV&V Program RRB meetings are generally led by the Office Lead and the NASA IV&V Director, respectively, with support from the risk manager. The governing RRBs shall approve Risk Mitigation Plans. These plans may also include requirements for the creation of contingency reserves necessary for effective risk mitigation. The Office Lead or NASA IV&V Director shall authorize the creation of contingency reserves in accordance with other applicable NASA IV&V Program procedures.

If the plans do not gain concurrence from the governing RRB, they are returned to the Risk Owner for corrective action.

Communicate, Control, and Track Risks

Communicate Risks

Risk communication takes place among stakeholders within the IV&V Program and externally including the Office of Safety and Mission Assurance (OSMA), Mission Directorates, Missions, and Projects. Communication can take place in a variety of forms and forums ranging from informal meetings and e-mails to tech discussions. The formal communication method within the IV&V Program is the RRB It is through the Office level and Program level RRB that the formal communication of risks is made. Communication starts at the project level and works its way up to the OSMA level as shown in Figure 4-8, *Ri sk Communication and Escalation*. Risks that ultimately are reported to the OSMA, on a quarterly basis, are formally communicated through the Program level RRB as depicted in the escalation process. External Risks approved by the Office Level RRB and

communicated to the Program Level RRB are submitted to the IV&V projects by the PM for disposition. External risk disposition status is documented and updated in the RMT by the PM.

The goal of the communication effort is to assure that:

- Every functional organization is aware of the individual risks that affect its performance risk.
- Individual risks are integrated into the risk analyses of the affected functional organizations in a consistent fashion (i.e., using consistent modeling assumptions).
- Every functional organization's risk driver list is available to other units and is updated according to an established schedule.
- Every functional organization that is affected by a risk driver, or by the proposed responses to a risk driver, is adequately engaged in planning a response to it, including deliberation and selection of a response for implementation.
- Every functional organization is aware of the risk responses that affect its performance risk and/or its risk analysis.
- Elevation of risk management decisions is timely and unambiguous.

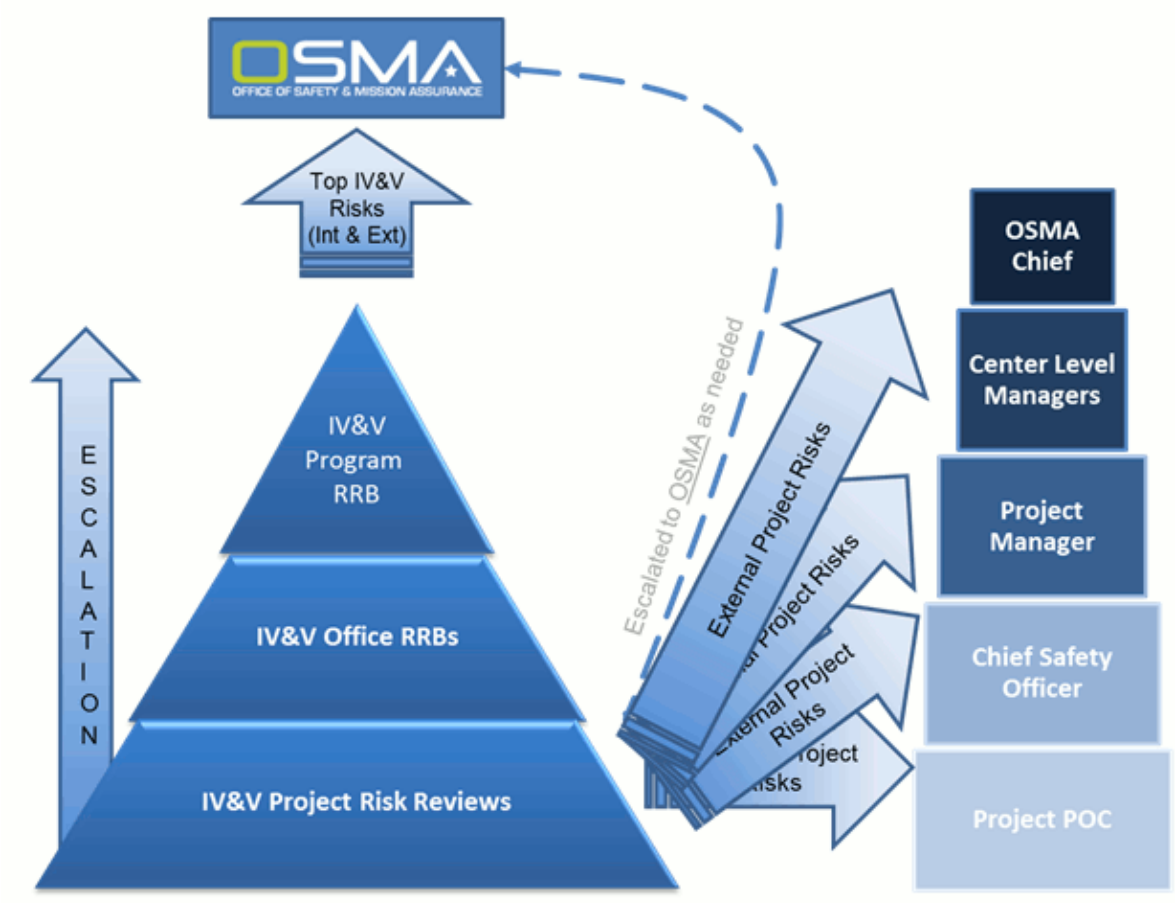


Figure 4-8 - Risk Communication and Escalation

This tiered approach of managing risks at the lowest appropriate level is the foundation of the NASA IV&V Program risk management process.

The PM shall communicate risks both horizontally (within the project) and vertically to ensure that significant risks are understood and influence key NASA IV&V Program/Project activities. Each Project has a defined risk approach that includes internal communication of risks as well as the presentation of risks to the governing RRB. The PM controls, integrates, reassigns, and provides resources or guidance as necessary to ensure successful risk mitigation within the context of the project.

The risk communication process as facilitated by the RMT establishes a real-time top risk list for an office by communicating risk information and status to the next organizational level. This communication mainly results in risk prioritization, as well as proper risk integration and transfer.

Any risk has the potential to be elevated to the next level. There are several reasons for elevating a risk, but elevation of a risk should only be made in response to an inability of the functional organization to effectively manage the risk at its level in the organizational hierarchy. As such, elevation should not be proposed as an initial option. Instead, it should be reserved for a situation in which the available risk response options have been analyzed and shown to be inadequate. Only then should Elevation be proposed.

Elevated risks are discussed at the next-level RRB. Risk elevation is either initiated by a lower-level RRB pushing its top risks up to the next-level RRB, or by a higher-level RRB pulling subordinate risks up from a lower-level RRB.

Note that risk elevation and risk ownership are two different constructs. Risk elevation does not necessarily change ownership of a given risk, only the specific attention and focus on the risk at a given level. The Risk Owner is the individual ultimately responsible for coordination and resolution/mitigation of the risk.

In addition, any individual risk can be elevated to multiple levels simultaneously. Thus, the same risk may be elevated to the Office and NASA IV&V Program levels simultaneously.

RiskManager Tool

The primary form of communication/elevation of internal and external risks is through the RRBs. All risks, including risks that contain Sensitive But Unclassified (SBU) information, presented at an RRB meeting shall be entered in the RMT with the exception of risks that are sensitive or classified/CNSI risks. Sensitive risks (e.g. procurement, supervisory, or legislative risks) shall be documented using the template T2006, *Risk Review Template*, and the RMT. The T2006 template will document the risk details and shall be stored by an appropriate civil service employee in a manner that properly restricts access. The RMT will be used for tracking sensitive risks (Risk Number, Title, Score, etc.) but consists of limited information. Classified/CNSI risks are to be handled according to IVV 22-1: *CNSI Risk Management* and S3007: *IV&V Guidelines for Handling CNSI*.

Risk States

The Risk States utilized in the RMT are defined as follows:

a. **Draft** - Candidate risks that have not yet been submitted to the RRB. (Internal and External)
b. **Ready for RRB Review** – Risks submitted for review and/or approval by the RRB. (Internal and External)
c. **Approved for Mitigation Planning** – Risk approved by the RRB for formulation of plans and actions to mitigate the risk AND plans and actions to take if risk becomes realized. (Internal)
d. **Mitigating** - a) Approved risk on which we are taking action (based on an approved plan) to reduce probability, consequence severity, or uncertainty, or shift timeframe. (Internal)
   b) Approved risk that has been recognized by the mission project/program and is being actioned at the mission project/program level. (External)
e. **Watching** – Approved risk which is being monitored for potential change (i.e., no action is being taken to mitigate the risk), and one or more of the following conditions exist: a) Sufficient mitigation resources are not available; b) Mitigation cost is comparable to recovery costs if the risk was to occur; c) The likelihood of mitigation success is uncertain or deemed too low to warrant action. (Internal and External)
f. **Accepted** – Approved risk for which a formal decision (including justification and documentation) has been made to proceed without further mitigation (despite exposure to that risk). (Internal and External)
g. **Closed** – Approved risk that no longer exists or is no longer cost-effective to track, because, for example, the associated scenario likelihoods are low (e.g., the underlying condition no longer exists), or the associated consequences are low. The risk may be closed by one of the IV&V RRBs or mission project RRBs (PM will coordinate with the Office Lead/IV&V Program Risk Manager to close external risks in the RMT). (Internal and External)
h. **Withdrawn** – a) Risk that never passed board review. (Internal)
   b) Approved risk submitted to the mission project, but later dispositioned by the mission project and IV&V to be invalid. (External)
i. **Ext To Submit** – Approved risk that has not yet been communicated to the program/project. (External)
j. **Ext Submitted** – Approved risk that has been communicated to the program/project but has yet to be dispositioned. (External)
k. **Ext In Dispute** – Approved risk which IV&V and the program/project disagree on either the validity of the risk or a proposed or implemented resolution to the risk. (External)

External Risks

External risks are primarily development project related risks applicable to the IV&V and SSO Office analysis projects. External risk communication within the IV&V Program is facilitated by the RMT. The RMT documents, tracks, and captures the

development of external risks through the various maturation states.

Note: External risks approved to be submitted to the project will be informally managed in the RMT by the PM/PL. Thus no additional RRB action is required but periodic informal coordination with the Office Lead/ IV&V Program Risk Manager is required.

External risks are communicated and escalated as previously defined in the previous section but are unique in that they are ultimately communicated formally to the external project. The PM gains approval for all external risks in the "Ext To Submit" state with the Office Lead via the Office Level RRB prior to sending them to the customer project. Once approved the risk can be submitted to the project and is informally managed and transitioned to the various states at the PM level in the RMT. The various risk states as defined previously, and as facilitated by the RMT, provide automated status and awareness to the various stakeholders associated with the IV&V Program. The goal is to ensure that the NASA IV&V Program is aware of the external risks that are being written prior to sending them to the development project. In addition, this facilitates communicating the status and escalation of any ongoing risks.

Internal Risks

Once they are identified and analyzed, all internal risks are communicated to the Office Lead via the RRB prior to the execution of any planning as noted in the *Planning* sectio n above. The goal of this communication is to make the Office Lead aware of any new risks that have been documented prior to the planning stage.

Once risk planning is complete (see Table 4-6, *Risk Planning*, for the types of risk planning), the plan is approved by the governing RRB. This only applies to risks with a Priority Score greater than 7 (see the *Planning* section above). The goal of this communication is to make the Office Lead aware of the planned approach for dealing with risks, and to provide concurrence on the Risk Mitigation Plan. This communication path also provides the status of any ongoing risks on that office's top risk list.

Some internal risks are also communicated at the IV&V Program RRB. Only risks that have a priority greater than 16 are required to be reported at IV&V Program RRB meetings. However, any risk that has significance to an Office Lead (i.e., has been on his/her top risk list) can be communicated at the IV&V Program RRB meetings (generally, communication of these risks are for information only, and no concurrence is needed from the NASA IV&V Director).

IV&V Program RRB meetings

The core objectives of the IV&V Program RRB meeting is to make the NASA IV&V Director and Senior Leadership aware of the Program's risk status, posture, and trends, including overviews of existing risks, mitigation approaches, and state transitions dealing with priority score/level risks. Additionally, the IV&V Program RRB reviews and approves risks generated at the program level, and risks proposed to be reported quarterly to OSMA.

Control

The purpose of the Control step is to evaluate the tracking data to determine whether or not risk responses are being implemented as planned, and if so, whether or not they are affecting the anticipated changes in the targeted risk drivers and in the performance risk generally. As long as the mitigation plan risk responses remain on track the responses are kept within the control function. However, if the objective of the risk response cannot be obtained within the current plan, the Plan step is reinitiated and a new or modified risk response alternative is selected for implementation.

Risk control is primarily the responsibility of the risk owner. The risk owner evaluates the status of the risk drivers to determine changes to the uncertainty associated with those drivers. This information is documented and communicated to the governing RRB periodically. Changes in risk drivers may occur due to changes in the environment or due to the completion of planned mitigation steps.

When changes to a risk driver prevent the risk owner or owning functional organization to effectively mitigate the risk, elevation of the risk to a higher-level RRB can occur.

The following strategies can be selected during risk control:

- Continue as planned
- Re-plan (develop a new or updated Risk Mitigation Plan)
- Close or accept the risk
- Elevate the risk to a higher-level RRB
- Determine that the risk is now realized (execute contingency plans, if applicable)

All decisions and directions regarding risks and Risk Mitigation Plans shall be captured in the risk database.

Risk Closure

If the risk drivers for a risk no longer exist or are no longer cost-effective to watch, the risk may be closed. Generally, if a risk has a risk score of less than 5 (see Figure 4-5, *Risk Matrix*), then the risk is a candidate for closure.

The risk owner must present closure rationale to the governing RRB and the RRB must concur with the criteria. The rationale should document that the probability of occurrence or the consequence potential has been reduced below a defined level of insignificance. Alternately, if the continued cost of watching or mitigating the risk drivers is no longer practical, the risk owner may present rationale for closing the risk.

A risk may also be closed if the sunset date has passed.

Closing a risk indicates not only that it is currently not a significant contributor to performance risks, but that there is no expectation that it will be a significant contributor to performance risk in the future.

Risk Acceptance

A risk response of Accept indicates that no risk management actions need to be taken, given the current analyzed performance risk. This is done typically when the performance risks associated with the performance requirements are all within tolerable levels, reflecting an activity that is on track to accomplish its objectives within

established risk tolerances. This means that none of the identified risk drivers are of sufficient magnitude to create intolerable performance risk.

Accepting a risk does not mean that no risk management action with respect to the risk drivers will be needed in the future. As the program/project/ activity proceeds, additional conditions and departures may be identified that compound the effects of existing drivers in a manner that produces intolerable performance risk.

A risk response of Accept must be documented by the risk owner including the assumptions and conditions on which it is based. Accepted risks must be reviewed periodically (at least quarterly) to ensure the assumptions and conditions have not changed such that the risk is no longer tolerable. It is important that the rationale is clear because these are important factors considered during the periodic reviews.

This response must also be concurred with by the governing RRB as well as the highest level RRB to which the risk has been elevated; in most instances this would be the IV&V Program RRB.

All decisions that have implications for risks to safety or mission success are subject to the requirements outlined in NID 8000-108, *Agency Risk Management Procedural Requirements*, section 3.4, Special Requirements for Acceptance of Risks to Safety or Mission Success.

Risks That Are Realized

A risk can transition to a realized risk during the Impact Time Frame, between the risk sunrise and sunset dates. A realized risk is an adverse situation that currently exists. Prior to becoming realized, hopefully it was identified as a risk and mitigated to reduce impact and/or consequence.

At the point that a risk has been realized, an undesirable event has occurred. Reactive management is necessary to deal with the realized risk, because it can lead the project into new risks.

Risks that are realized are documented in the RMT as such and continue to be managed as a risk. Note that these realized risks can have contingency plans that may minimize the impact but can incur additional risks.

Track

The PM will track the progress of the implementation of the selected risk response. The goal is to not only monitor the implementation status of risk response options, but also their effectiveness once implemented. Tracking applies only to the *Mitigate* and *Watch* risk response types.

Mitigation – A mitigation plan produces changes to the baseline project plan that reflects that implementation of selected mitigation options. The progress of the mitigation effort should monitor the status of these mitigation options as well as document their effectiveness in reducing the risk relative to the forecasted risk reduction.

Watch – The decision to watch a risk driver entails the scheduled monitoring of observables related to that risk driver that can be used to assess the current performance risk and the

contribution of the risk driver to that risk. Tracking these parameters serves as an early warning so that further action can be taken. In contrast to the *Mitigate* risk response type, the *Watch* response does not involve changes to the baseline project plan, and consequently does not involve the monitoring of implementation.

Each risk should already have an attribute/indicator system designed to provide early warning of changes in status. This allows management (PMs, Functional Leads, and Program Management) to respond proactively before the risk becomes a problem.

Risk tracking is not a problem-solving technique; rather, it is a technique to provide a basis for developing additional risk mitigation options and/or approaches, updating existing risk mitigation strategies, and/or re-analyzing known risks. In some cases, tracking results may also be used to identify new risks and revise some aspects of risk planning.

Also, risks can change over time. Every action taken, or not taken, changes the basic facts from which each risk is derived. Continually monitoring risks and reassessing their potential consequence (i.e., repeating the risk identification, assessment, and mitigation steps at periodic intervals) is essential for appropriately managing risks.

Lessons Learned and Success Stories

When a risk is closed, the PM and the Risk Management Team shall assess the risk for inclusion in the Lessons Learned and/or Success Stories database. These processes are documented in IVV 23, *Lessons Learned,* and IVV 24, *Success Stories*.

Metrics/Tool

Several potential metrics, as listed below, may be used to periodically evaluate the effectiveness of the IV&V risk management process. Metrics evaluated to assess the effectiveness of risk management extend beyond the data derived from the risk management process, and include various IV&V Program/Project health metrics that ascertain whether there are areas where potential risks were not identified (i.e., whether problems are arising that were not identified as potential risks). This allows continuous re-evaluation of the risk management process, which increases the effectiveness and provides insight into where structured risk identification or mitigation reviews should be conducted.

The Risk Management Team tracks and reports metrics as requested to Program Management.

Below are some potential metrics for consideration. They may not need to be reported to Program Management, but can be used to assess the performance of the risk management process:

1) Number of risks – Tracking the number of risks by functional organization (categorized by criticality and graphically represented by a cumulative bar) provides indication of the health and responsiveness of the IV&V risk management process and the progression of risk mitigation strategies.

2) Risk Mitigation Plan stability – Tracking the stability of Risk Mitigation Plans provides an indication of responsiveness to critical project schedules and commitments, and is different than

mitigation tardiness, which just identifies tasks that are late. Tracking Risk Mitigation Plan stability provides insight into the number of plans that are underperforming the proposed mitigations (e.g., behind schedule, over budget). Data for tracking Risk Mitigation Plan stability should be collected in conjunction with IV&V Program/Project planning to establish late completion of a major or critical mitigation step. A critical step is considered to be one tied to a step-down in Priority Score. Stability of a Risk Mitigation Plan is determined by the movement of the estimated completion date (ECD) for the critical mitigation steps (a re-plan). A critical step completed within seven days of the ECD is not considered late or a consequence for the metric. Thus, this metric only contains slips of critical steps greater than seven days. The percentage of non-moving critical tasks should be charted against the percentage of critical tasks that did move.

3) New/Open/Closed risks – Tracking new/open/closed risks on a monthly basis provides insight into the amount of risk activity occurring each month related to risk identification and mitigation efforts. Tracking new/open/ closed risks indicates the length of time risks have been in the RMS (e.g., less than 30 days, 31 to 60 days, 61 to 90 days). This tracking will also include data to show the amount of time it takes to move a risk through each concurrence activity. For example, once a risk is made available to the Risk Management Team, how long does it take for the Risk Management Team to provide concurrence on the risk? This would also include information to show how many times risks are not concurred with, and how long it takes to rework them and reach concurrence. It is expected that as the RMS matures, the trend should show more risks accepted or closed than opened.

4) Mitigation Tardiness – Tracking mitigation tardiness (the number of steps re-planned or completed late) provides early indication of potential schedule risk. It also provides insight into the frequency of change requests for Risk Mitigation Plans. The thresholds for reporting tardiness are determined in the ranges of 5 to 30 days (green), 31 to 60 days (yellow), and more than 60 days (red).

5) Number of escapements – Identified issues/problems that could have been mitigated if identified early as risks.

6) Number of duplicate candidate or risk entries – How well risks are documented and communicated by an integrated team (ensure that risks are not being worked in parallel).

7) Trends in number of processes/people/production – The maturity of the project relative to the types of risks identified (may expect to see different types of risks for different milestones, System Requirements Review [SRR], Preliminary Design Review [PDR], etc.).

8) Number of candidates – How many candidate risks are being identified each month to provide an indication of risk focus by project personnel.

9) Length of time from risk identification to risk determination – The length of time it takes before a candidate risk is evaluated and either approved or rejected.

10) Length of time from risk to mitigation strategy – How long it takes for the risk mitigation strategy to be identified and approved once a candidate risk is approved as a risk (i.e., will it be mitigated, watched, accepted, or researched?).

11) Action items issued by the RRB to Risk Owner – How well a Risk Owner is doing her/his homework prior to the RRB (was the Risk Owner able to anticipate questions from the RRB?).

12) Number of times RRB meetings occurred as planned – Trends in RRB meeting postponements indicate if risk management may be taking a back seat to other issues.

13) Length of time it takes to distribute minutes from the RRB meeting – The length of time that it takes for the release of the minutes from the RRB meeting (this provides an indication of workload).

14) Unfunded mitigations – Unfunded mitigation activity cost threats indicate how much risk has been accepted by not funding mitigation activities (it also may indicate the effectiveness of escalating risks to the appropriate levels for additional resources).

15) Cost threats/liens – Cost threats/liens (as a compilation of financial consequences for management reserve in the eventuality that a risk is realized [not mitigated]), aids in determining financial exposure and when to apply funds for risk mitigation, as opposed to accepting the risk. The cost threat/lien is calculated using the estimated cost consequence of the risk consequence, factored by the likelihood (percentage) of the risk occurring. The sum of all risk cost liens gives an expected consequence value to the NASA IV&V Program from risks occurring. In addition, as a risk is mitigated, the likelihood is reduced and the cost/lien to the NASA IV&V Program is reduced.

References

REFERENCES	
Document ID/Link	**Title**
IVV QM	NASA IV&V Quality Manual
IVV 07	Financial Data Control
IVV 09-4	Project Management
IVV 22	Risk Management
IVV 22-1	CNSI Risk Management
IVV 23	Lessons Learned and Organizational Learning
IVV 24	Success Stories
NASA/SP-2011-3422	NASA Risk Management Handbook
NID 8000-108	Agency Risk Management Procedural Requirements
T2006	Risk Review Template

If any procedure, method, or step in this document conflicts with any document in the NASA Online Directives Information System (NODIS), this document shall be superseded by the NODIS document. Any external reference shall be monitored by the Document Owner for current versioning.

Version History

VERSION HISTORY				
Version	**Description of Change**	**Rationale for Change**	**Author**	**Effective Date**
Basic	Initial Release		Kenneth Costello	1/24/2008
A	Update IV&V Program Risk Review Process, Risk Closure Section		Kenneth Costello	6/16/2008
B	Changed “IV&V Facility” to “IV&V Program”		Stephanie Ferguson	3/25/2009
C	Updated to reflect organizational changes		Stephanie Ferguson	10/8/2010
D	Updated to streamline and clarify processes		Kenneth Costello	9/27/2012
E	Add RiskManager Tool (RMT) verbiage. Use T2006, Risk Review Template, for sensitive risks only. Other cleanups for accuracy and clarity.	PAR 2013-P-390. Integration of the new RiskManager Tool (RMT) into the IV&V Program Risk Management System.	Scott Kinney	1/22/2014
F	Updates as a result of expanding the external risk states, clarifications of risk communication, escalation and approval. Changed “organizational units” to “functional organizations”, and other editorial changes.	Process improvement and recommended updates as a result of an internal audit	Scott Kinney	12/17/2014

G	Simplify the risk states (also in the RMT). Clarified use of CNSI risks: Add references to IVV 22-1, CNSI Risk Management, and S3007, IV&V Guidelines for Handling CNSI. Removed definition, Risk Classification, to avoid any confusion with CNSI.	Improve management and communication of realized risks (a.k.a. issues). Clarify handling of risks with SBU or CNSI (new docs for handling CNSI risks now exist).	Scott Benton	10/16/2017