



National Aeronautics and
Space Administration

KSC-PLN-8000.4

BASIC

RELEASE DATE: 10/11/2012

JOHN F. KENNEDY SPACE CENTER INSTITUTIONAL RISK MANAGEMENT PLAN

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 2 of 22
Title: KSC Institutional Risk Management Plan	

THIS PAGE INTENTIONALLY LEFT BLANK.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 3 of 22
Title: KSC Institutional Risk Management Plan	

John F. Kennedy Space Center Institutional Risk Management Plan

Approved by:

Kelvin Manning
Associate Director

Concurrence:

Russell R. Romanella
Director, Safety and Mission Assurance

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 4 of 22
Title: KSC Institutional Risk Management Plan	

REVISION AND HISTORY PAGE

Status	Revision No.	Change No.	Description	Release Date
Draft	Basic	-	Draft KSC Institutional Risk Management Plan for KAITS review	10/11/2012

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 5 of 22
Title: KSC Institutional Risk Management Plan	

TABLE OF CONTENTS

1	INTRODUCTION	6
1.1	PURPOSE	6
1.2	SCOPE	6
1.3	AUTHORITY	6
1.4	RESPONSIBILITY/CHANGE AUTHORITY	6
1.5	REFERENCE DOCUMENTS	6
2	KSC RISK MANAGEMENT	8
2.1	OVERVIEW.....	8
2.2	RISK-INFORMED DECISION MAKING (RIDM).....	9
2.2.1	PART 1 – IDENTIFICATION OF ALTERNATIVES.....	9
2.2.2	PART 2 – RISK ANALYSIS OF ALTERNATIVES	9
2.2.3	PART 3 – RISK-INFORMED ALTERNATIVE SELECTION	9
2.3	CONTINUOUS RISK MANAGEMENT (CRM).....	10
3	ROLES AND RESPONSIBILITIES.....	12
3.1	KSC DIRECTORATE ORGANIZATIONS.....	12
3.2	KSC CENTER RISK MANAGER	13
4	PROCEDURE	14
4.1	RISK IDENTIFICATION.....	14
4.2	RISK ANALYSIS	15
4.3	RISK PLANNING (HANDLING STRATEGY)	15
4.3.1	OPTIONS FOR HANDLING STRATEGY	16
4.3.2	RISK ESCALATION	16
4.4	RISK TRACKING	17
4.5	RISK CONTROL	17
4.6	RISK DOCUMENTATION.....	18
	APPENDIX A: KSC RISK MANAGEMENT SCORECARD	20
	APPENDIX B: ACRONYMS AND ABBREVIATIONS	22

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 6 of 22
Title: KSC Institutional Risk Management Plan	

1 INTRODUCTION

1.1 PURPOSE

This John F. Kennedy Space Center (KSC) Institutional Risk Management Plan (RMP) defines a common framework for identifying, analyzing, planning, tracking, controlling, documenting, and communicating KSC institutional risks, including the interface between KSC and resident programs as well as commercial users. The purpose of this plan is to foster effective management of Center institutional risks to increase the potential of achieving current and future KSC goals and objectives, and to minimize potential future liabilities for the Center.

1.2 SCOPE

The KSC Institutional RMP is applicable to all KSC organizational elements and programs/projects assigned to KSC. KSC organizational elements may establish their own risk management implementation mechanisms (e.g., Directorate RMPs, processes, risk management working groups) provided they comply with this plan. For programs/projects assigned to KSC, this KSC Institutional RMP neither supersedes nor negates specific, established program/project RMP responsibilities, requirements, and processes for the identification and management of programmatic risks (e.g., safety, performance, cost, schedule).

1.3 AUTHORITY

The KSC RMP is authorized by NPR 8000.4, Agency Risk Management Procedural Requirements and KNPd 8000.4, KSC Center Risk Management System, and complies with the requirements delineated in NPR 8000.4. Risk management activities are consistent with internal control activities defined in NPD 1200.1, NASA Internal Control.

1.4 RESPONSIBILITY/CHANGE AUTHORITY

The KSC Office of Primary Responsibility for this document is the Safety and Mission Assurance (S&MA) Directorate. The KSC Center Risk Manager, who resides within the S&MA Directorate, facilitates the Center risk management process. This plan will be reviewed and updated, as required, to reflect changes and improvements to the Center's institutional risk management system, including risk management processes, tools, and techniques. Proposed changes to the document should be submitted to the KSC Center Risk Manager for consideration and disposition.

1.5 REFERENCE DOCUMENTS

C-0003	Charter, Center Risk Management Working Group
KDP-KSC-P-3616	Center Risk Management System

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 7 of 22
Title: KSC Institutional Risk Management Plan	

IT76-SRS-03 System Requirements Specification for the Calysto Risk
Management Tool

NASA/SP-2011-3422 NASA Risk Management Handbook

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 8 of 22
Title: KSC Institutional Risk Management Plan	

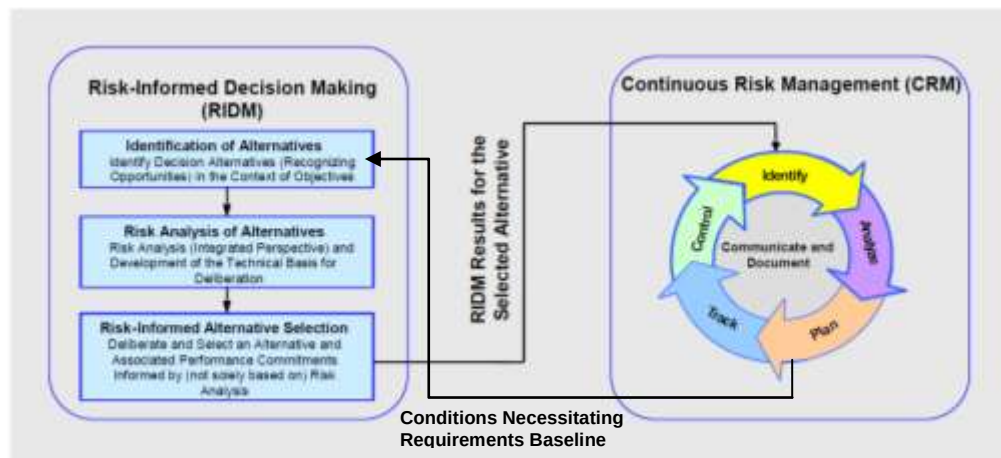
2 KSC RISK MANAGEMENT

2.1 OVERVIEW

KSC Institutional Risk Management is a deliberative, systematic process to analyze and communicate the risk of performance shortfalls as they relate to the institution. Institutional risks include those that affect the strength and mix of the workforce; the viability and maintenance of facilities; the ability to meet safety or quality assurance standards; the effectiveness and accessibility of Center support to program, project, commercial companies; and the usefulness and maintainability of information systems that support day-to-day operations. The risk management process involves the development of risk handling and mitigation options and the implementation of approved strategies to reduce or eliminate the likelihood of occurrence and/or severity of the consequence of identified risks. Institutional risks document a potential threat to the ability to meet performance objectives with adverse consequences to safety, Center capabilities, technical performance, budgets, or schedules. KSC Institutional Risk Management integrates risks from various sources to: 1) inform decisions; 2) efficiently allocate resources; 3) enable KSC to meet Center goals and objectives; 4) align the Center institution with resident programs/projects; and position the Center for future business.

The approach used by KSC for Institutional Risk Management is an integration of Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM) (see [Figure 1: NASA RIDM-CRM Risk Management Paradigm](#)). Integrating RIDM and CRM into a coherent framework fosters proactive risk management in order to better inform decision-making through the use of risk information. In the RIDM process, decisions are made regarding the outcomes of the decision alternatives, taking into account applicable risks and uncertainties. Then, as part of the implementation process, CRM is used to effectively manage those risks in order to achieve the performance levels (and associated performance requirements) that drove the selection of a particular alternative. This approach is consistent with the Agency risk management procedures and will provide insight to address technical, management, and business challenges and opportunities at the Center.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 9 of 22
Title: KSC Institutional Risk Management Plan	



Risk Management = RIDM + CRM

FIGURE 1: NASA RIDM-CRM RISK MANAGEMENT PARADIGM

2.2 RISK-INFORMED DECISION MAKING (RIDM)

A Risk-Informed Decision Making process is a structured manner of effectively and comprehensively using risk information to improve the quality and consistency of decision-making. KSC uses the three-part RIDM process which is required by NPR 8000.4, Risk Management Procedural Requirements and thoroughly discussed in NASA SP/2011-3422, NASA Risk Management Handbook. The three-part RIDM process is outlined below and has been expanded to include supporting steps in the process from an institutional risk management perspective.

2.2.1 PART 1 – IDENTIFICATION OF ALTERNATIVES

- Identify and understand the baseline performance criteria (and the potential threat or performance shortfall associated with Center Goals and Objectives, Directorate Business Objectives and Agreements, and associated Performance Measures).
- Propose and identify decision alternatives.

2.2.2 PART 2 – RISK ANALYSIS OF ALTERNATIVES

Perform risk analysis in accordance with [Section 4.2](#) of this RMP, and rank the decision alternatives.

2.2.3 PART 3 – RISK-INFORMED ALTERNATIVE SELECTION

- Deliberate and choose a decision alternative.
- Document the decision rationale.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 10 of 22
Title: KSC Institutional Risk Management Plan	

c. Implement and track the selected decision using the CRM process.

These steps support improved decision-making by focusing initially on objectives and associated performance criteria, then developing decision alternatives with those objectives clearly in mind, and finally on developing decision alternatives that have been developed under other systems engineering processes. The risk analysis of decision alternatives ([Section 2.2.2](#)) not only guides selection of a preferred alternative, but it also relies on the Identify and Analyze steps of the CRM process. Selection of a preferred alternative is based in part on an understanding of the risks associated with that alternative. Alternative selection is followed immediately by a planning activity in which key implementation aspects are addressed, namely, how the risks are to be handled (e.g., mitigated). Risk handling plans are executed as the decision alternative is implemented. New risks may also be identified during the planning and implementation of the selected decision alternative.

2.3 CONTINUOUS RISK MANAGEMENT (CRM)

CRM is a widely used risk management technique within NASA. CRM is initiated at the beginning of (and continues throughout) the life cycle of Center and program/project activities to identify, analyze, plan, track, control, and document/communicate risk. It is an iterative and adaptive process that promotes the successful handling of risk. Each step of the paradigm builds on the previous step through the feedback of generated information, leading to improved performance regarding Center goals and objectives.

a. The CRM steps are:

(1) Identify: State the risk in terms of an existing condition that may result in an undesired consequence (e.g., degraded performance of a Center goal or objective) and capture the context of the risk (e.g., what, when, where, how and why), including key risk drivers.

(2) Analyze: Perform qualitative/quantitative assessments to determine risk likelihood (probability) and severity of consequence (impact of degraded performance); consider the mitigation timeframe (time to initiate action to mitigate the risk); group similar or related risks; and prioritize risks.

(3) Plan: Assign a risk owner; determine a risk planning approach (i.e., research, accept, mitigate, or watch); if the risk will be mitigated, define the mitigation plan (e.g., action list or more detailed task plan) and goal; and execute the mitigation plan.

(4) Track: Acquire/update, compile, analyze, and organize risk data; report tracking results; and verify and validate mitigation actions over time.

(5) Control: Analyze tracking results; decide how to proceed (e.g., re-plan, close the risk, invoke contingency plans, continue tracking); and execute the risk control

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 11 of 22
Title: KSC Institutional Risk Management Plan	

decisions. Report risk status and request direction or concurrence at the appropriate management decision level.

(6) Communicate and Document: Document supporting information for each key element in a system organized to track details, plans, progress, and risk decisions.

In addition to Center risks being identified by assessing potential performance shortfalls associated with Center Goals and Objectives, Center risks may be identified during the analysis of alternatives or during the planning and implementation of the chosen alternatives. Hence, the risk management process is continuous, proactively seeking out and managing risks to foster successful accomplishment of Center Goals and Objectives.

b. Application of RIDM and CRM involves a graded approach, and the level of risk mitigation and prioritization should be commensurate with the complexity of the risk or severity of consequence if a Center risk is realized. These factors dictate the rigor applied to make a risk-informed decision.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 12 of 22
Title: KSC Institutional Risk Management Plan	

3 ROLES AND RESPONSIBILITIES

The KSC Center Director is responsible for the Center's institutional risk management effort (per KNPd 8000.4, KSC Center Risk Management System), including establishing and implementing risk processes, tools, and reporting mechanisms involving Center management and Directorate organizations. The process owner for the day-to-day management of Center institutional risk management is the S&MA Directorate, and specifically the Center Risk Manager, who resides in the S&MA Directorate. The Center Risk Manager coordinates all institutional risk activities, including the Center Risk Management Working Group (CRMWG).

All KSC personnel should continuously and systematically review their respective areas using appropriate methods to identify any event that could adversely affect the achievement of planned center performance. Personnel should identify, evaluate, and manage risks in accordance with this document. Specific Center institutional risk management roles and responsibilities for KSC Directorate Organizations and the KSC Center Risk Manager are outlined further in this section.

3.1 KSC DIRECTORATE ORGANIZATIONS

- a. Identify, assess, evaluate, manage, and report risks associated with meeting Center goals and objectives and Directorate business objectives and agreements.
- b. Manage and report risks affecting Center goals using a standard risk management process (KDP-KSC-P-3616, Center Risk Management System) and associated risk management tools.
- c. Evaluate Top Directorate Risks for potential evaluation as Top Center Risks and forward candidate Top Center Risks to the CRMWG for disposition.
- d. Coordinate the management of cross-cutting risks being managed at the Center level with other involved organizations.
- e. Report resident Program/Project risks that affect the Center institution through the CRMWG.
- f. Present new and updated Top Center Risks to the Kennedy Institutional Management Council (KIMC).
- g. Provide a representative to the CRMWG.
- h. Ensure that RIDM and CRM processes are implemented and that performance measures defined for the organization are for risk analysis of decision alternatives.
- i. Ensure that key decisions of the organization are risk-informed.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 13 of 22
Title: KSC Institutional Risk Management Plan	

j. Ensure that risks are identified and analyzed in relation to the performance requirements for major acquisitions of the organization and risk analysis results are used to inform the source selection.

3.2 KSC CENTER RISK MANAGER

- a. Perform day-to-day management of Center institutional risk management activities.
- b. Establish and chair the CRMWG (see C-0003, Charter, Center Risk Management Working Group).
- c. Implement a risk database for tracking Center institutional risks.
- d. Coordinate periodic Center Risk Review briefings at Senior Management Councils (e.g., KIMC).
- e. Provide risk management consultation, facilitation, and training to KSC Directorates.
- f. Serve as the KSC member to the Agency Institutional Risk Management Network.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 14 of 22
Title: KSC Institutional Risk Management Plan	

4 PROCEDURE

This section expands on the Center institutional risk management procedure delineated in KDP-KSC-P-3616, Center Risk Management System.

4.1 RISK IDENTIFICATION

Institutional risk management begins with the identification of perceived shortfalls against a performance objective, including key drivers and impacts. Potential risks are identified based on a condition, event, or review of requirements, products, and services needed to execute a Directorate business objective and agreement, a KSC goal and objective, a planned mission, or to comply with a NASA HQ or Federal mandate. Emphasis is on early identification of potential risks related to: Health, Safety, and Environmental; Technical Performance; Center Capabilities (infrastructure, personnel); and Cost or Schedule threats. Risks also may be identified when implementing corrective or preventive actions.

a. Examples of key considerations for institutional risks include:

- (1) Funding requirements and priority: Likelihood of budget shortfall and rationale; impact if not funded (e.g., reduced scope, impact to internal/external stakeholders); and risk buy-down that would be achieved with full or incremental funding.
- (2) Cross-cutting risks: A risk-owning organization has primary risk impact, but based on potential risk handling/disposition and mitigation timeframe, consequences also may impact one or more NASA organizations or external stakeholders.
- (3) Center capabilities: Infrastructure and resources as required for achievement of institutional objectives and program/project support requirements.
- (4) Transition planning: Requirements for changing Agency or Center conditions or objectives.

b. An identified risk is documented in a risk statement in the following scenario-based format: "Given the [condition]; there is a possibility that [consequence] will occur." The condition must be a fact-based; the consequence must describe the adverse outcome if the risk were to occur. A well-formed risk statement should be concise.

c. A candidate risk, where information is insufficient or too immature to analyze or define mitigation options, may be captured as a Concern. Concerns may be managed internally within existing resources and processes. Once the risk is vetted and more information is available, the Concern may be elevated to a formal risk.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 15 of 22
Title: KSC Institutional Risk Management Plan	

4.2 RISK ANALYSIS

Institutional risks will be analyzed to determine the likelihood of occurrence and impacts to the associated performance objective. In accordance with RIDM-CRM principles (NPR 8000.4), the risk analysis steps are as follows:

- a. Evaluate risk data. Identify and understand the impact from each risk contributor, including the uncertainty inherent in each.
- b. Perform qualitative and/or quantitative analysis. Assess the likelihood of occurrence and the consequences (e.g., degraded performance, loss of function, key milestone slip, personal injury, cost escalation).

(1) Qualitative analyses assess risk based on the best judgment of the assigned risk owner, team, or organization initiating the risk. The risk attribute definitions used as guidelines in determining consequence and likelihood are in the KSC Risk Scorecard (refer to Appendix A). In the consequence criteria, the risk level selected (1-5) is the rating which is the highest within the sub-criteria for Safety, Health, and Environmental; Technical Performance; Center Capabilities; Cost; and Schedule. When there is insufficient knowledge to reasonably assess the Likelihood x Consequence (L x C) risk score, the estimate should be conservative (i.e., trending toward the worst case). In addition, the mitigation timeframe (i.e., the time period when action must be taken to mitigate the risk) will be assigned.

(2) Quantitative risk analyses should be applied to the maximum extent practical. Use of quantified analysis is based on scope of the decision to be made and similarities among suitable alternatives (graded approach).

4.3 RISK PLANNING (HANDLING STRATEGY)

The risk owning organization will determine a plan of action for each risk (referred to as the handling strategy). Pairing likelihood of occurrence with the highest impact rating yields a relative characterization of the risk, a key consideration when selecting a handling strategy.

- a. High Risk – Expected to occur with severe impacts if realized; denoted in the upper right-hand (red) region of the KSC Risk Management Scorecard.
- b. Moderate Risk – May occur and impacts would be significant but not catastrophic; denoted in the middle (yellow) region of the Risk Management Scorecard.
- c. Low Risk – Not likely to occur or potential impacts are not expected to be significant; denoted in the lower left-hand (green) region of the Risk Management Scorecard.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 16 of 22
Title: KSC Institutional Risk Management Plan	

4.3.1 OPTIONS FOR HANDLING STRATEGY

The intent of a handling strategy is to minimize the L x C risk score over time, thereby minimizing the total risk. The preferred strategy and supporting data are approved at the appropriate management level. Options include:

- a. Research – Consider and review all pertinent information sources to understand the risk.
- b. Mitigate – Develop a mitigation strategy to measurably reduce the L x C risk score. Specify the mitigation Estimated Completion Date (ECD), resulting L x C score, rationale, and success criteria.
- c. Watch – For risks where circumstances do not warrant immediate mitigation steps, define triggers that indicate the need for action. Include a timeframe for re-evaluation and active mitigation or alternate handling strategies.
- d. Accept – If no further resources will be expended to mitigate residual risk, a risk owner may recommend ceasing active mitigation, to include key assumptions and conditions on which the decision to accept will be based. Periodically assess for changing conditions.

4.3.2 RISK ESCALATION

a. Risk owners will perform due diligence to understand the risk scoring rationale, ranking, and escalation. The owning organization determines if a risk requires escalation to the next level. Directorates escalating risks to the Center level will submit the risk through the CRMWG for review and concurrence before presenting the risk to the KIMC. Reasons for escalation may include:

- (1) Additional resources are needed to mitigate the risk.
- (2) Direction is needed from the next level of management.
- (3) External integration is required (e.g., with other programs/projects/centers).
- (4) The risk has cross-cutting significance.

b. Each Directorate will review its risks on a periodic basis. The following levels are defined to support the Center's risk escalation process:

- (1) Top Center Risk (TCR) – Requires Center management resources or direction to resolve; could have cross-cutting impacts that affect two or more KSC organizations.
- (2) Top Directorate Risk (TDR) – Directorate Management direction and/or resources are sufficient for resolution.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 17 of 22
Title: KSC Institutional Risk Management Plan	

c. Resident programs/projects will review their program/project risks to determine which risks are candidate TCRs. Program/project risks which affect the Center institution shall be submitted to the CRMWG for evaluation as candidate TCRs. If it is determined that a program/project risk is a candidate TCR, the risk will be input into the Calysto Risk Management Tool (see [Section 4.6](#) for more details).

4.4 RISK TRACKING

a. The risk owner will track the risk attributes (i.e., consequence, likelihood, mitigation timeframe) over the risk life-cycle to determine if:

- (1) Mitigation steps are performed in a timely manner.
- (2) Steps taken are effectively managing the risk. The owner tracks observable data related to performance measures such as cost/schedule variance or changing conditions.

b. The risk owning organization's track and update risks on a recurring basis to reflect current status and progress, and to use the results to communicate risk status and information (quantitative or qualitative) as required for effective control and management decisions.

4.5 RISK CONTROL

The risk control function assesses and verifies that the mitigation plan effectively reduces the L x C threat.

a. Based on analysis of tracking data, types of control decisions may include:

- (1) Continue as Planned – Progress is satisfactory (as expected).
- (2) Re-plan – Mitigation is not achieving the desired outcome or conditions have changed.
- (3) Invoke a Contingency Plan – If the current plan proves inadequate, an alternative is developed, approved, and implemented.
- (4) Close – To close a risk, rationale must be approved at the appropriate management level to demonstrate that the risk has been eliminated, residual risk is negligible such that further steps are unnecessary, or the threat has been subsumed by a new risk. Center risks proposed for closure must obtain concurrence by the CRMWG prior to presentation for closure at the KIMC.
- (5) Transfer – Transfers generally occur if a risk was identified outside of the primary affected organization or due to a change in either organizational responsibilities or control of resources. Transfers must be mutually agreed upon by the affected parties.

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 18 of 22
Title: KSC Institutional Risk Management Plan	

(6) Accept – Risk may be accepted when rationale is developed and approved by the owning organization and key stakeholders. Further mitigation is not cost-effective. Residual risk is non-negligible but at an acceptable level due to a significant change in the current situation. The risk owning organization must review accepted risks periodically to determine that acceptance rationale remains applicable.

b. Collaboration with KSC organizations is essential for incorporating risk management into the Center Management decision-making process. Risks are a key input to the process and reflect specific challenges to meeting commitments. Recommendations for resource allocation take into consideration the trade-offs between finite resources and prioritized risks.

c. New and updated Center risks will be reviewed at the CRMWG on a monthly (or as required) basis and on a quarterly basis at the KIMC. The Center Risk Manager will prepare the Center Risk Review Briefing, with individual Center risk owners presenting the new/updated Center risks.

4.6 RISK DOCUMENTATION

As institutional risks are identified and mitigation strategies developed, the owning organization must document and maintain current the risk. The [Calysto Risk Management Tool](#) (RMT) is the preferred method for documenting center level risks. The Calysto RMT is a SharePoint application that is aligned with the KSC organizational hierarchy and allows the user to “roll-up” a risk from the directorate level to the CRMWG where the risk can be considered for escalation to the Center level. Each KSC Directorate has the option of obtaining an independently managed Calysto project which can be customized to reflect the Directorate’s organizational structure. If a Directorate chooses to use Calysto they will work directly with the Information Technology (IT) Directorate as Calysto is owned and maintained by IT.

The following risk information, as a minimum, will be input into the Calysto RMT:

- a. Risk Title
- b. Risk Statement
- c. Risk Context
- d. Likelihood of Occurrence
- e. Consequences (Safety, Health, and Environmental; Technical Performance; Center Capabilities; Cost; and Schedule)
- f. Mitigation Timeframe for action to be taken
- g. Cost of Consequence (if known)

Revision: Basic	Document No: KSC-PLN-8000.4
Release Date: 10/11/2012	Page: 19 of 22
Title: KSC Institutional Risk Management Plan	

- h. Mitigation Plan
- i. Risk Owner and Organization
- j. Risk Planning Approach
- k. Status Report
- l. Estimated Completion Date
- m. Closure Rationale (when submitting for closure)

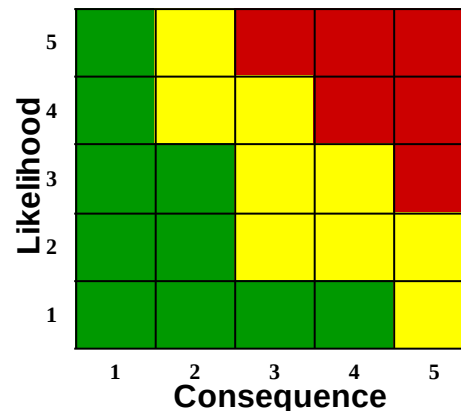
After the risk is created in Calysto, individual Mitigation Tasks must be assigned to implement the risk Mitigation Plan. An actionee is assigned and an estimated Completion Date and resulting Likelihood, Consequence, and Mitigation Timeframe are documented on the Mitigation Task. The actionee will be notified via email that they have been assigned a Mitigation Task. The risk owner is responsible for implementing the Mitigation Plan and ensuring that all the assigned Mitigation Tasks are completed until the risk reaches an acceptable limit or is mitigated. At that time, the owner will recommend "acceptance" or "closure" of the risk to the appropriate level. The risk will remain open, be accepted, or closed based on the amount of residual risk remaining.

For additional information about the Calysto application, please refer to [IT54-UG-33, User Guide for the KSC Institutional SharePoint \(IT54\) Calysto Version 12.0.0.](#)

Revision: Basic (Draft)	Document No: KSC-PLN-8000.4
Release Date: MM/DD/YYYY	Page: 20 of 22
Title: KSC Institutional Risk Management Plan	

APPENDIX A: KSC RISK MANAGEMENT SCORECARD

Likelihood Risk Attribute Definitions				
Level	Probability	Qualitative Criteria	Quantitative Criteria	
			Safety	Other Impacts
5	Very High	Highly likely. Existing controls have little or no effect and cannot prevent this risk scenario; no alternative controls are available.	$P > 10^{-1}$	$P > 90\%$
4	High	Likely. Existing controls have significant limitations and/or uncertainties and will likely not prevent this risk scenario; additional actions will be required.	$10^{-2} < P \leq 10^{-1}$	$67\% < P \leq 90\%$
3	Moderate	Could happen. Existing controls have some limitations and/or uncertainties and may prevent this risk scenario; additional actions may be required.	$10^{-3} < P \leq 10^{-2}$	$33\% < P \leq 67\%$
2	Low	Unlikely. Existing controls have minor limitations and/or uncertainties and usually are sufficient to prevent this risk scenario; some additional actions may be required.	$10^{-6} < P \leq 10^{-3}$	$10\% < P \leq 33\%$
1	Very Low	Highly unlikely. Existing controls are strong and are expected to prevent this risk scenario.	$P \leq 10^{-6}$	$P \leq 10\%$



Mitigation Timeframe Definitions	
Near-Term	0-3 Months
Mid-Term	3-9 Months
Far-Term	>9 Months

Consequence Risk Attribute Definitions						
Level		1	2	3	4	5
Consequence Categories		Very Low	Low	Moderate	High	Very High
Safety, Health, and Environmental	Personnel Safety	A condition that could cause the need for minor first aid	A condition that may cause short-term, minor injury, impairment, or incapacitation	A condition that may cause long-term, severe injury, impairment, or incapacitation	A condition that may cause permanent, severe injury, impairment, or incapacitation	A condition that may cause loss of life
	Facilities/Equipment	A condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear	A condition that may cause minor property damage to facilities, systems, equipment, or flight hardware	A condition that may cause moderate property damage to facilities, systems, equipment, or flight hardware	A condition that may cause major property damage to facilities, systems, equipment, or flight hardware	A condition that may cause destruction of critical facilities on the ground, major systems, or vehicle during ground operations
	Environmental	Insignificant release to the environment; negligible or non-reportable EPA violation	Minor release to the environment; warning letter or self-reportable EPA violation without penalty	Significant release to the environment; possible formal EPA enforcement action with possible penalty	Major release to the environment; formal EPA violation with minor penalty	Catastrophic release to the environment; formal EPA enforcement action with major penalty and/or criminal investigation
Technical	Meeting performance requirements or goals and objectives	Negligible impact to program/project/institutional services performance requirements and/or goals and objectives	Minor impact to program/project/institutional services performance requirements and/or goals and objectives	Moderate impact to program/project/institutional services performance requirements and/or goals and objectives	Major impact to program/project/institutional services performance requirements and/or goals and objectives	Failure to meet program/project/institutional services performance requirements and/or goals and objectives
Center Capabilities	Workforce	Negligible impact to workforce	Minor impact to workforce	Moderate impact to workforce (reduced capability in one or more skill sets)	Major impact to workforce (loss of skill set)	Loss or a workforce core competency
	Infrastructure/Facilities	Negligible impact to infrastructure/facilities	Minor impact to infrastructure/facilities (reduced effectiveness)	Moderate impact to infrastructure/facilities (reduced operational support)	Major impact to infrastructure/facilities (delays in Center operations)	Extended loss of an infrastructure/facility critical capability
Cost	Program/Project or Organizational impacts	Negligible cost impact < 2% budget impact or <\$1M CMO threat	Minor cost impact 2-5% budget impact or \$1M-\$5M CMO threat	Moderate cost impact 5-10% budget impact or \$5M-\$10M CMO threat	Major cost impact 10-15% budget impact or \$10M-\$35M CMO threat	Catastrophic cost impact > 15% budget impact (potential cancellation) or >\$35M CMO threat
Schedule	Ability to support activity milestones	Negligible schedule impact	Minor overall schedule impact (Accommodate with reserve, no impact to critical path)	< 1 month impact to critical path/milestones	1-6 month impact to critical path/milestones	> 6 month impact to critical path/milestones or possible program/activity cancellation

Revision: Basic (Draft)	Document No: KSC-PLN-8000.4
Release Date: MM/DD/YYYY	Page: 21 of 22
Title: KSC Institutional Risk Management Plan	

Risk Management Definitions and Terms	
Risk Management (RM)	An organized, systematic decision making process that efficiently identifies, analyzes, tracks, controls, communicates, and documents risks that increase the potential for achieving goals and objectives associated with an activity. The RM process includes two key components: Risk-Informed Decision Making and Continuous Risk Management.
Risk	A potential threat to safety, Center-controlled cost or schedule, or organizational/mission objectives for which a resolution is unlikely without focused management attention; or potential inability to fully implement agreements with NASA stakeholders or partners. Risks are future events characterized by the combination of the probability (qualitative or quantitative) that an activity will experience an undesired event (e.g., safety mishap, cost overrun, schedule slippage, inability to achieve a goal or objective) and the consequence, impact, or severity of the undesired event, were it to occur. All risks must be actionable.
Risk-Informed Decision Making (RIDM)	A process for informing KSC decision makers through the use of qualitative and/or quantitative risk information to establish baseline performance requirements for institutional organizations in support of programs and projects.
Continuous Risk Management (CRM)	A structured, formalized practice with processes, methods, and tools for managing risks associated with implementation of baseline performance requirements for an activity.



Using the KSC Risk Management Scorecard (In Conjunction with CRM)		
1	Identify (Locate risks before they become problems)	- Start with a concern. Is this a risk? Gather/utilize information listed below - Early identification and management methods include, but are not limited to: Budget Reviews, Expert Interviews, Trend Analyses, Program/Project Reviews, Engineering Analyses, Trade Studies, Brainstorming - Key areas to assess include: Budget, Requirements, Technology, Management, Supportability, Operations, Safety, Programmatic - Information Sources: Organizational Objectives, Performance Data, Metrics, Historical Data, Resources, Plans, Proposed Changes, Test Results <u>Generate a Well-Formed Risk Statement</u> - FORMAT: Given the condition (A); there is a possibility that (B) will occur. (A): Single phrase briefly describing current key circumstances or situations that are causing concern, doubt, anxiety, or uncertainty (B): Consequence of the current condition that could be realized if (A) occurs - Condition must be a FACT or perceived to be a FACT; must be REALITY BASED (Avoid IF-THEN approaches) - Risk Statement represents a concise scenario that must be ACTIONABLE
2	Analyze (Score risk attributes and determine relative risk priorities)	- Perform analysis to gain a better understanding of the risk by establishing risk attribute values for Consequence, Likelihood, and Mitigation Timeframe - Consequence is the loss or effect on an activity if the risk occurs - Likelihood is the likelihood that the risk scenario will occur; Likelihood reflects the controls currently in-place - Result of Consequence/Likelihood scoring is a mapping on the risk matrix - Mitigation Timeframe is the period when you must take action to mitigate the risk (<u>NOT</u> when the risk will occur); this risk attribute is independent of the Consequence/Likelihood risk attributes
3	Plan (Determine planning approach and develop mitigation actions)	- Determine what to do with the risk. Is it my risk, or another organization's? - Assign a Risk Owner/Point of Contact (organization responsible for ensuring risk and associated mitigation efforts are addressed/implemented) - Determine risk planning approach (Research, Accept, Watch, Mitigate) - Define balanced mitigation strategy to reduce severity of the consequence and/or reduce the likelihood of occurrence; assign mitigation actionees - Develop contingency plans in case primary mitigation strategy is not working - When risk cannot be efficiently mitigated further, consider closing or accepting the risk; closure/acceptance rationale must be documented
4	Track (Monitor risk mitigations)	- Evaluate risk mitigation strategies to determine whether the strategy is working, and on schedule - Evaluate each risk attribute to determine mitigation strategy effectiveness - Update risk information as needed to reflect changes in the risk attributes
5	Control (Make risk decisions)	- Report status to appropriate forum (e.g., KSC Councils, CRMWG) to give management the complete risk picture so an informed decision can be made - Provide recommendations regarding how to disposition the risk (e.g., close the risk, continue tracking, accept the risk, invoke contingency plans) - Typical products include Center Risk List, Risk Information Sheets
6	Communicate and Document (Provide risk feedback)	- Integral to all the other CRM steps - Ensures understanding and visibility of risk information - Establishes an effective, ongoing dialog between management and organization stakeholders

Revision: Basic (Draft)	Document No: KSC-PLN-8000.4
Release Date: MM/DD/YYYY	Page: 22 of 22
Title: KSC Institutional Risk Management Plan	

APPENDIX B: ACRONYMS AND ABBREVIATIONS

CRM	Continuous Risk Management
CRMWG	Center Risk Management Working Group
ECD	Estimated Completion Date
KIMC	Kennedy Institutional Management Council
L x C	Likelihood x Consequence
RIDM	Risk-Informed Decision Making
RMP	Risk Management Plan
RMT	Risk Management Tool
S&MA	Safety and Mission Assurance
TCR	Top Center Risk
TDR	Top Directorate Risk