



Procedures and Guidelines (PG)

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

APPROVED BY Signature: Adrian Gardner
NAME: Adrian R. Gardner
TITLE: Chief Information Officer

COMPLIANCE IS MANDATORY

Responsible Office: Code 740 / Program Integration & Management Division (PIMD)

Title: Risk Management Procedures and Guidelines (RM PG)

PREFACE

P.1 PURPOSE

This procedures and guidelines (PG) establishes the standard practices for risk management (RM) within Information Technology & Communication Directorate (ITCD) and establishes the requirements for the organization, programs, and projects to establish and execute efforts using a Risk Management Plan (RMP).

An RMP has several purposes:

- Specifies the RM requirements an organization, program, or project shall follow;
- Identifies the roles and responsibilities of those involved in the RM process;
- Outlines how the RM activities will be performed, recorded, and monitored;
- Documents how and when risks are communicated and escalated;
- Details the schedule and budget for the RM activities; and,
- Identifies the tools and techniques that will be used by the organization, program, or project and team members.

This document, and the RM practices contained within, shall be adopted using one of the following approaches:

- Report the adoption of this PG as the RMP in its entirety via a reference within the documented Project Plan (PP) for the effort; or,
- Create an organization-, program-, or project-specific RMP using the Project Management Office (PMO) approved template to document how the organization, program, or project is adopting this RM PG in its entirety, stating any effort-specific data.

This PG can be adopted for use by other organizations following the process identified in Goddard Procedural Requirement (GPR) 1410.1G, Directives Management.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

Organizations, programs and projects may seek tailoring approval or waiver requests from specific RM practices contained within this PG, based on specific documented constraints or requirements. These requests will be considered on a case-by-case basis by the PMO.

The PMO is a dynamic organization within ITCD, sponsored and managed by the Program Integration and Management Division (PIMD). PIMD is engaged in transforming into an IT Project Management center of excellence that will deliver results that enable mission success. PIMD is tasked with improving the delivery of IT services and solutions to ITCD customers, better enabling executive decision-making, instituting a professional development framework, and improving organization alignment and coordination.

P.2 APPLICABILITY

This procedural guidance shall apply to all organizations, services, activities, programs and/or projects within ITCD.

Given this PG was developed using best practices for risk management, any Goddard IT project required to follow NPR 7120.7 and/or 7150.2A can opt to use these risk management processes to manage IT projects.

P.3 AUTHORITY

- a. NPR 8000.4A, Agency Risk Management Procedural Requirements
- b. GPR 7120.4D, Risk Management

P.4 REFERENCES

NASA resources used in the development of this PG include, but are not limited to:

NASA Document	Title
NPR 7120.7 (NID 7120.99)	IT & Institutional Infrastructure Program and Project Management Requirements
NPR 7123.1A	Systems Engineering Processes and Requirements
NPR 7150.2A	Software Engineering Requirements
NPR 8705.5A	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
NPR 8715.3C	NASA General Safety Program Requirements
NHBK SP-2011-3422	Risk Management Handbook
NHBK SP-2010-576	Risk Informed Decision Making Handbook
NHBK SP-610S	Systems Engineering Handbook

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

Industry resources also used in the development of this PG include:

- a. Project Management Institute (PMI) Project Management Book of Knowledge (PMBOK, 4th edition): Project Risk Management
- b. Carnegie Mellon’s Software Engineering Institute (SEI) Capability Maturity Model Integration – Service (CMMI-Svc), Version 1.3: Risk Management

Other referenced items include:

- a. Project Plan
- b. Project Status Reports, Directorate Status Reports, and Monthly Status Reports (PSR, DSR, and MSR)
- c. Risk Management Plan (and related template)
- d. Risk List (and related template)
- e. Goddard’s 5x5 Risk Matrix
- f. “Top 10” Issue Reporting
- g. Risk Scorecard and Risk Ranking

P.5 CANCELLATION

None.

P.6 SAFETY

None.

P.7 TRAINING

Training on the contents of this PG is provided by PIMD.

There are many RM training courses currently available via the System for Administration, Training and Educational Resources for NASA (SATERN), including but not limited to:

- APPEL-Continuous Risk Management
- APPEL-Risk Management I
- APPEL-Risk Management II
- Applying The Risk Management Framework To Federal Information Systems
- Center Risk Management Workshop
- Risk Management Overview
- Information Risk Management: Analysis, Mitigation, and Monitoring
- Information Risk Management: Program Framework and Risk Assessment
- Risk Management

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- Risk Management Planning
- Risk Management: Assessing Risk
- Risk Management: Dealing with Risk
- Risk Management: Identifying Risk

P.8 RECORDS

The following records are produced by the RM efforts, and shall be retained by ITCD in accordance with NASA records retention policies:

Record Title	Record Custodian	Retention
Risk Management Plan (RMP)	Performing Organization	*NRRS 8/107: for program/project records having operational value to the Agency throughout the program/project life. Temporary. Destroy/delete between 5 and 30 years after program/project termination.
Completed Risk Lists		
Risk Status Reports		

* *NRRS – NASA Records Retention Schedule* ([NPR 1441.1](#))

Official records for ITCD risk management shall be filed on the ITCD SharePoint portal.

Copies of those RM records and work products (i.e., artifacts) designated below shall be provided to the PMO:

- RMP (when an effort has opted to establish a standalone RMP that contains effort-specific data)
- Completed Risk Lists, provided monthly
- Risk Status Reports, provided monthly
- Other Risk Management artifacts/work products that provide evidence of RM planning execution, provided as appropriate

P.9 MEASUREMENT/VERIFICATION

ITCD organizations, programs and projects shall keep the following risk metrics: the total number of risks identified, the current number of open and closed risks, the total number of accepted risks, and the total number of risks that were realized (achieved a 100% likelihood of occurrence).

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

ITCD organizations, programs and projects will be able to express the age of a risk item and average age of risks i.e., how long before a risk is closed or realized.

ITCD organizations, programs and projects shall provide copies of risk management records to the PMO for verification, measurement, and analysis of the risk landscape across ITCD.

P.10 DOCUMENT STANDARDS

In this document, a requirement is identified by “shall,” a good practice by “should,” permission by “may” or “can,” expectation by “will,” and descriptive material by “is.”

Additionally, the first use of any RM-specific term or acronym has been identified using the convention of bold and italicized font-face text (i.e., “*Risk Management*”). The definitions for these terms can be found in [Appendix A: Terms, Definitions & Acronym Lists](#).

In this document the term “*effort*” is used synonymously to reflect ITCD’s services, activities, programs and/or projects (the terms “services, activities, and projects” are defined in GPR 2800.2), and the terms “*Organization, Program or Project Manager, or Assigned Lead*” are used to describe the appropriate party that is responsible for the overall success and execution of the ITCD effort.

PROCEDURES

1 RISK MANAGEMENT OVERVIEW

1.1 GOAL OF RISK MANAGEMENT

Risk Management is an organized, systematic decision-making process that efficiently identifies, analyzes, plans, tracks and controls, communicates, and documents risk to increase the likelihood of success.

A successful RM approach requires commitment, participation, empowerment, and accountability from all members of the team.

Team members, within their respective areas of expertise, shall proactively report and assess risks when assigned risk ownership.

Risk owners shall subsequently formulate and execute mitigation actions to control the **Likelihood** (synonymous with “probability of occurrence”) and **Consequences** (synonymous with “severity” and “impact of occurrence”) of risks and take maximum advantage of opportunities.

1.2 RISK MANAGEMENT CONCEPTS

1.2.1 Definition of Risk

Risk is the combination of the likelihood (also referred to throughout this document as **probability**) that an organization, program, or project will experience an undesired event (e.g., failure to achieve success criteria, cost overrun, schedule slippage, etc.) and the consequences (also referred to throughout this document as **severity** and **impact**) of the undesired event, were it to occur.

1.2.2 Differences between Risks, Issues, and Assumptions

It is important for the risk owners to understand, capture, and manage all of the risks, issues, and assumptions. A risk is an uncertain event or condition that, if it occurs, has a typically negative effect on an effort’s objectives. Simply put, a risk is something that may impact the successful delivery of an effort. A risk may be avoided or reduced with careful planning and directed action.

An **Issue** is a risk that has actually occurred (was not avoided or reduced) and that has impacted the effort in some way. ITCD issues shall be communicated, escalated, and managed to closure using the “Top 10” process.

An **Assumption** is a statement accepted or supposed true without proof or demonstration. If proven false, an assumption may become a risk to the effort. Assumptions will be documented for all ITCD efforts.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

One example of an assumption could be: “The effort assumes that no additional funding or further flexibility in the schedule will be provided to the effort for risk mitigation activities. It is assumed that such mitigations must be funded and scheduled through the use of resources already allocated to the effort.”

Assumptions are sometimes made when there are elements that reach beyond the scope of the effort and are not within the owner’s control. These should not be classified using the definitions of risk and/or issue. The risk owner must assume that these concerns will be addressed so that the effort can proceed successfully.

1.2.3 Risk Management Lifecycle

RM is performed at all times, beginning with the planning efforts.

The RM lifecycle is an iterative process requiring continuous identification, monitoring, and controlling of RM activities throughout the lifecycle. It includes five elements:

1. **Risk Management Planning** – Deciding how to approach and conduct the RM activities, including: scheduling recurring activities, tool selection and set up, roles and responsibilities assignment, etc.
2. **Risk Identification** – An initial and continuous effort to identify, quantify, document, and assign ownership of risks
3. **Risk Analysis** – Evaluating risks to determine their likelihood, consequences, anticipated impact(s), criticality, and priority
4. **Risk Planning & Mitigation** – Establishing an actionable plan for risk handling; reflecting the effort’s activities related to risk mitigation within the effort’s schedule
5. **Risk Monitoring & Control** – A continuous effort to implement plans, and capture, compile, track, and report risks’ plans and statuses

1.2.4 Risk Management Stakeholders, Roles & Responsibilities

Key stakeholders with a role in RM include:

- Organization, Program or Project Manager, or Assigned Lead
- Team Members
- Project Management Office (PMO)
- Responsible Management Official (RMO)
- Management/Senior Leadership with authority over the effort
- Customer(s) and Affected Stakeholders

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

The table that follows provides an overview of key roles and responsibilities for RM stakeholders:

Table 1: Risk Management Stakeholders Roles & Responsibilities

Stakeholder Roles	Responsibilities
Organization, Program or Project Manager, Assigned Lead	<ul style="list-style-type: none"> ✓ Complies with RM PG / documents effort-specific RMP ✓ Establishes the Risk List tool ✓ Ensures the effort follows CRM and RIDM processes ✓ Schedules and manages recurring RM activities; ensures these activities are reflected in the effort's schedule ✓ Identifies, documents, and periodically reviews assumptions ✓ Identifies and analyzes risks ✓ Identifies and documents realized risks as issues; manages issues to closure ✓ Assigns ownership of risks and issues ✓ Approves risk approach and related mitigation or contingency plans ✓ Monitors execution of approved mitigation or contingency plans ✓ Regularly communicates and reports risk status to PMO, RMO, Management, Senior Leadership, and other appropriate stakeholders ✓ Escalates risk to PMO, RMO, and Management/Senior Leadership when appropriate
Team Member(s)	<ul style="list-style-type: none"> ✓ Participates in recurring RM activities ✓ Identifies and documents assumptions ✓ Identifies and analyzes risks ✓ Identifies and communicates realized risks as issues ✓ Supports risk approach selection and helps define related mitigation or contingency plans ✓ Executes approved mitigation or contingency plans ✓ Regularly communicates and reports risk status; identifies realized risks in a timely manner ✓ Escalates risk when appropriate

Table 1: Risk Management Stakeholders Roles & Responsibilities

Stakeholder Roles	Responsibilities
Project Management Office (PMO)	<ul style="list-style-type: none"> ✓ Offers RM support and guidance via available RM tools, including: the RMP template, Risk List template, training, and mentoring ✓ Receives and reviews risk status with PMs or Assigned Leads on a regularly recurring basis, i.e., Project Status Reviews ✓ Integrates and aggregates risk information across ITCD for DSR risk status reporting to Management/Senior Leadership ✓ Confirms compliance to RM PG (or effort-specific RMP) requirements ✓ Ensures risks are discussed at Stage Gate reviews and other major milestones for the effort ✓ Validates RM artifacts/work products that are the outcome of executing against the approved RM PG or effort-specific RMP ✓ Reviews, approves (or rejects) RM tailoring or waiver requests ✓ Escalates risk to Management/Senior Leadership when appropriate
Responsible Management Official/Office (RMO)	<ul style="list-style-type: none"> ✓ Reviews and approves risk baseline(s) ✓ Reviews and approves mitigation plans; reviews and approves related budget or schedule impacts ✓ Authorizes expenditures of resources for mitigation ✓ Reprioritizes all risks to determine the Top risks for the effort ✓ Makes control decisions (analyze, decide, execute) for Top risks ✓ Coordinates communication with Management, Senior Leadership, Center Leadership, and NASA HQ, as appropriate
Management/Senior Leadership	<ul style="list-style-type: none"> ✓ Reviews and approves risk baseline(s) ✓ Reviews and approves mitigation plans; reviews and approves related budget or schedule impacts ✓ Authorizes expenditures of resources for mitigation ✓ Reprioritizes all risks to determine the Top Three risks ✓ Makes control decisions (analyze, decide, execute) for Top Three risks ✓ Coordinates communication with Management, Senior Leadership, Center Leadership, and NASA HQ, as appropriate
Customer(s) and Affected Stakeholders	<ul style="list-style-type: none"> ✓ Identifies and communicates risk information ✓ Is informed or consulted about risks ✓ Is informed or consulted (and provides approval, when appropriate) in mitigation planning

For all IT efforts, the organization, program or project managers, and team members are responsible for all RM activities and shall make sure the team members identify, categorize, and assess risks in accordance with the RMP.

1.3 NASA RISK MANAGEMENT PROCESS OVERVIEW

NASA leverages an integrated approach by using the following two processes to identify and manage risks:

- Continuous Risk Management (CRM)
- Risk-Informed Decision Making (RIDM)

CRM is a process for the management of risks associated with the implementation of designs, plans, and processes. The CRM functions of identify, analyze, plan, track, control, and communicate and document provide a structured environment for assessing risks, determining priorities, and implementing mitigation strategies.

Risks shall be identified and ranked according to likelihood, or probability of occurrence, together with the urgency or the seriousness of the impact.



Figure 1. NASA's CRM 5-Step Process

RIDM is a process that uses a diverse set of performance measures, along with other considerations within a deliberative process to inform decision-making on a set of alternatives. RIDM supports decision-making at each management level by applying quantitative and qualitative risk information to achieve specific requirements. RIDM uses an evaluation process to analyze solutions against established criteria and consider alternatives to determine a decision. RIDM allows stakeholders to identify opportunities and reduce the subjective nature of decision-making as it relates to selecting which option to pursue. Once a risk-informed alternative is selected the CRM process takes over.

CRM and RIDM are integrated into the RM lifecycle to foster proactive risk management that enables decision-making through better use of risk information.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

Page 11 of 47

IT organizations, programs and projects shall use CRM and RIDM processes to record and report details of all risks and decisional opportunities identified.

ITCD organizations, programs or project managers shall reflect recurring risk management activities and risk mitigation-related activities within their efforts' schedule.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

2 RM PROCESSES: CRM, RIDM, COMMUNICATION & CLOSURE

ITCD organizations, programs, and projects shall use the two RM processes iteratively: CRM and RIDM. These unique processes are integrated throughout the RM lifecycle to foster proactive risk management that enables decision making through better use of risk information across ITCD’s organizations, programs, and projects.

ITCD’s application of CRM and RIDM will ensure risk mitigation strategy is commensurate with the severity. These factors dictate the rigor applied to making a risk-informed decision.

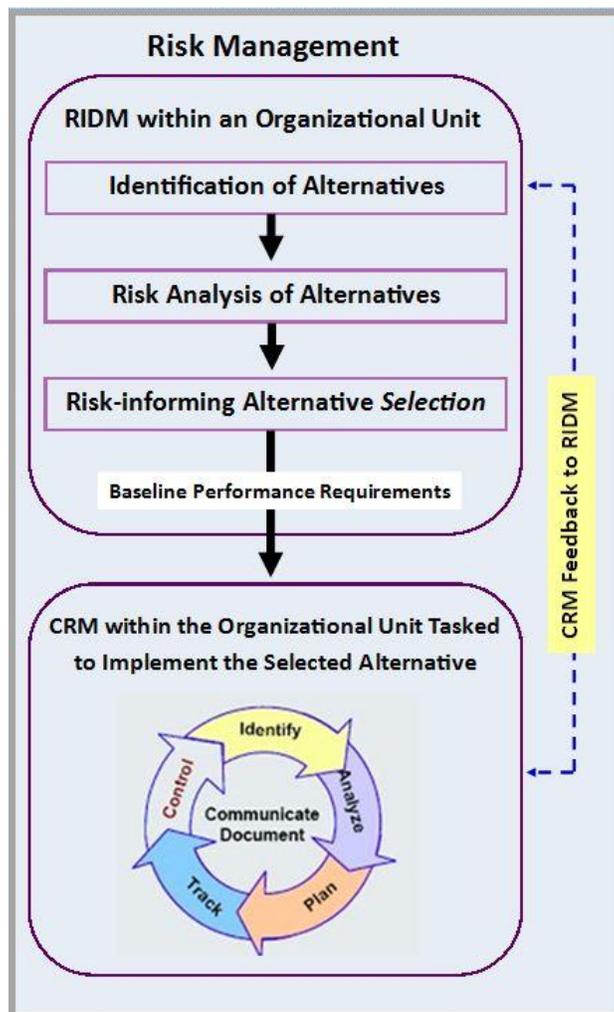


Figure 2: CRM & RIDM – Two Integrated Processes for Effective Risk Management

ITCD organizations, programs, and projects shall also employ the two processes that occur continuously throughout the RM lifecycle: risk communication process to engage and inform stakeholders, and the risk closure process when the criteria for risk closure has been met.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

2.1 CRM PROCESS

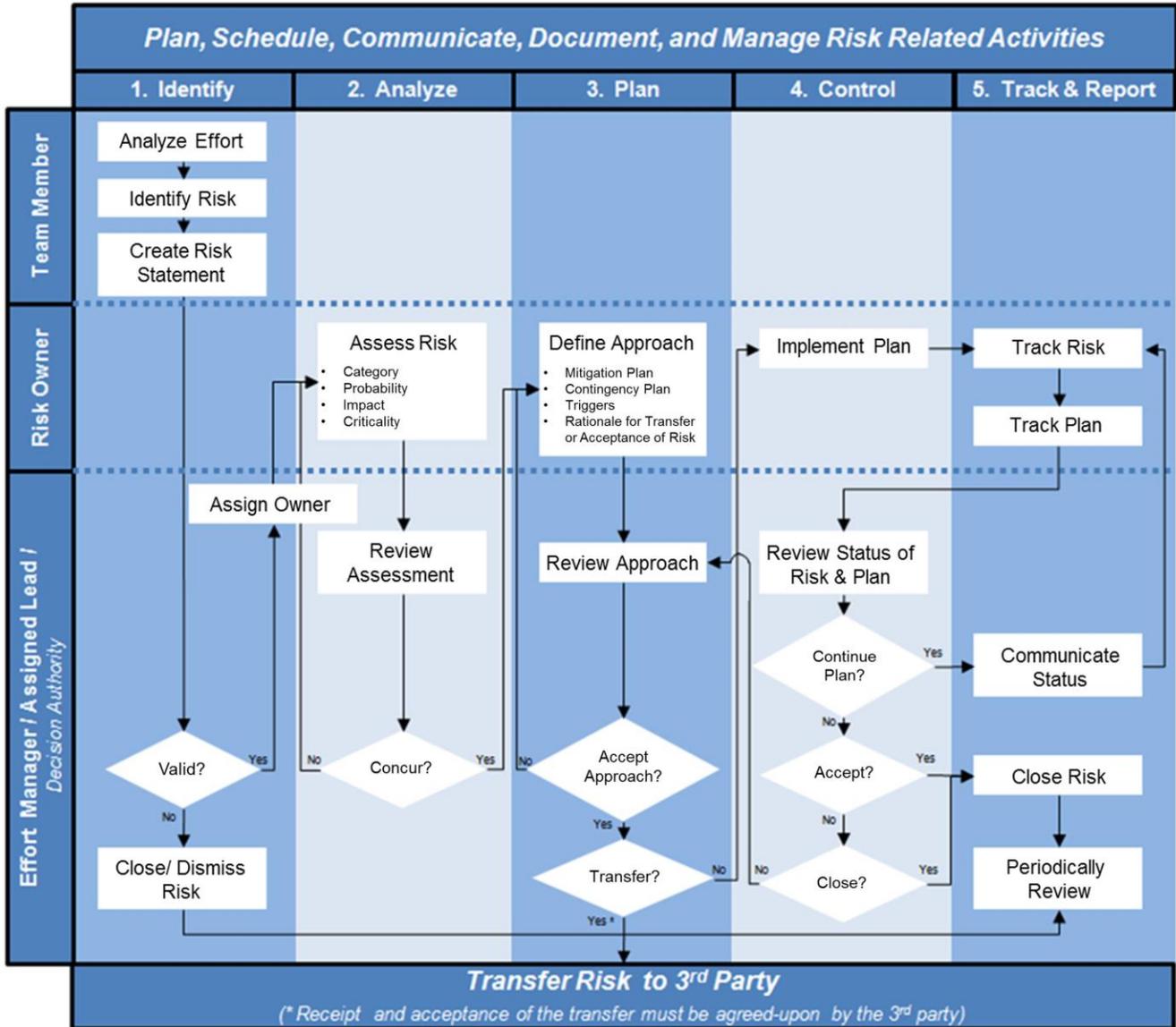


Figure 3: CRM Process Overview

*Transferring a risk to an external party outside the effort, and having the external party accept the risk, means the effort is no longer responsible for handling or managing that risk.

2.1.1 CRM Step 1: Identify Risks

2.1.1.1 Analyze the Effort

The initial step in risk management is risk identification. The designated authority and potential risk owner shall consider the following to help identify risks:

- What could go wrong?
- How and when will we know something has gone wrong, or is about to?
- What could we do to prevent it altogether, or at least lessen any negative impact?
- What will we do about it?

2.1.1.2 Document Identified Risks

Risk identification and documentation activities shall occur as soon as a team member articulates a new or different risk. All team members are highly encouraged to communicate possible risks upon discovery.

Tools that may be used to help identify risks include:

- Brainstorming Sessions
- Interviews
- SWOT (Strength, Weakness, Opportunities and Threats) Analysis
- Diagramming
- Prior Lessons Learned (risks realized or mitigated by similar efforts)
- List of Additional Risk Types & Categories (refer to: [Appendix C: Additional Risk Types & Categories](#))

In addition, assumptions should be periodically reviewed to see if the assumptions remain true. Assumptions that are no longer true will typically become risks that should be managed accordingly.

2.1.1.3 Create Risk Statements

As part of risk identification, descriptions of each risk shall be documented in a **Risk Statement**. Risk statements are brief and objective. Risk statements are comprised of two components: **Conditions** (“If...”) that describe the circumstances or cause for concern; and, **Consequences** (“...then...”) that describe the possible negative outcomes due to the concern.

Table 2: Sample Risk Statements

Risk Name	Conditions and Consequences
SME Resources	IF ITCD Subject Matter Expert (SME) resource availability is impacted by other duty responsibilities, THEN delivery and quality of the service may be negatively impacted.
Mission Schedules	IF the impacts of Mission freezes exceed the ability of the project to compensate, THEN the project schedule may be negatively impacted and one or more networks may not be included within the baseline border assessment.
Failover Capability	IF a recovery site is not established to support failover capability, THEN there will be outages to production systems (in the event of significant hardware failures) resulting in lack of access and delayed delivery of critical mission services.

The designated authority and risk owners will use multiple sources of data to formulate cause and effect risk statements. Potential causes, effects, or impacts may be identified by analyzing items in the following list of potential records and artifacts:

- Formulation Authorization/Agreement Document (FAD)
 - Does the effort have an appropriate level of advocacy from its sponsor?
- Organization, Program or Project Charter or Scope Document
 - Does the project have the appropriate buy-in from the key stakeholders across the organization?
 - Is the scope feasible, given available resources?
- Work Breakdown Structure (WBS)
 - Is the definition of work (WBS) consistent with the scope?
 - Is the project schedule defensible?
- Schedule Estimates
 - Are the resources adequate given the milestone schedule?
- Budget Estimates
 - Does the project have adequate funding?
- Resource or Staffing Plan
 - Are there an adequate number of resources?
 - Do the personnel have the necessary skill sets?
- Procurement Needs
 - Has the time to acquire contract resources been taken into consideration?
- Assumptions and Constraints
 - Are all of the critical assumptions likely to be resolved?
- Business Case
 - Will this yield a reasonable return on investment or breakeven point in competitive timeframe relative to other investment possibilities?

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- Historical Information such as: metrics, costs, resource levels, estimated durations, etc. from similar efforts
 - Is the environment suitable for an effort of this scope?
 - Does the organization have a positive track record for similar efforts?

The organization, program, or project manager shall lead risk identification, ranking, and documentation activities with the team members to identify and record potential risks in the effort’s Risk List.

The organization, program, or project manager shall also select and assign risk ownership as part of this step.

2.1.2 CRM Step 2: Analyze Risks

2.1.2.1 Select Risk Categories

Risks shall be categorized for reporting and mitigation purposes and to create a knowledge base for future risk planning. NASA Flight Projects traditionally use three risk categories, each with its own unique criteria for evaluating probability and severity.

NASA’s Flight Projects have three risk categories: Safety, Technical, and Programmatic. NASA’s Flight Projects have three risk categories: Safety, Technical, and Programmatic. Each of these three high-level categories has unique criteria for quantitatively and qualitatively evaluating probability and severity. Each of the flight project categories (safety, technical, and programmatic) associates its unique percentage variable to risk valuations: very low, low, medium/moderate, high, and very high along a number of subcategories.

Table 3: Flight Project Risk Type Categories

Category	Description
Safety	Relates to the avoidance of injury, fatality, or destruction of key assets
Technical	Relates to the system(s), technologies, capabilities, or science related to the effort
Programmatic (Cost/Schedule)	Cost: Relates to ability to execute within allocated costs or budget Schedule: Relates to ability to meet defined milestones and associated dates

Ground-based, general purpose IT efforts, however, will simplify risk evaluation by using a single set of criteria for quantitatively and qualitatively evaluating probability and severity regardless of the risk category. This single set of numeric values to express IT efforts' risk criteria are provided in *Table 5: Likelihood & Consequence – Qualitative & Quantitative Values* found in *Section 2.1.2.3 Assign Risk Evaluation Criteria*. Additional information on standardized scoring for ITCD risks has been provided in [Appendix D – Risk Scoring & Ranking](#). Frequently used IT risk categories are provided in the table that follows.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

Table 4: Sample IT Risk Type Categories

Category	Description
Cost	Relates to ability to execute within allocated costs or budget
Schedule	Relates to ability to meet defined milestones
Resources-Staffing	Represents risks related to personnel - e.g., unavailability, attrition, necessary skills, knowledge transfer, etc.
Requirements	Relates to the need for or lack of a defined requirements; may require the capture, analysis, documentation, and approval of requirements
Environment	Relates specifically to the environment of the customer, the effort, or the solution; may be technical in nature (i.e., a development, test, or production environment)
External Event-3rd Party	Represents a risk that is outside the control of team
Management-Programmatic	Relates to the management of the sponsor, customer, the team, or the organization, program or project; requires management decision and/or intervention to proceed
Policy Development-Implementation	Requires the development, re-engineering, or implementation of a business or enterprise-wide policy
Process	Relates to the need for or lack of a consistent, documented, and/or followed process; may require the development, re-engineering, adherence to, or implementation of a process or set of processes
Procurement	Represents the need to procure items or services to proceed; impact is typically to the schedule and relates to turnaround time and/or duration of time required to complete required acquisition lifecycle activities
Regulatory	Represents risks (to cost, schedule, or quality - and/or technical challenges) that may be imposed by regulatory changes that occur during the lifecycle
Security	Relates to the need to comply with Information Security standards, training, and accessibility (and the impact to time/accessibility/resource availability that may ensue)
Stakeholder	Represents the need for stakeholder input and/or approval to proceed
System-Integration	Relates to the availability, accessibility, and/or suitability of a designated system or integration points needed to support the client, the product, or the effort

Additional categories and types of risks for consideration are provided in [Appendix C: Additional Risk Types & Categories](#).

2.1.2.2 Assess Risk Probability, Consequence, Criticality and Priority

Likelihood or **Probability** of an event is used to describe a measure of the possibility that a risk will occur, which accounts for the frequency of the risk within a specified timeframe.

Consequences or **Impact** describe possible negative outcomes of conditions that create uncertainty or risk and the severity of the effect on the effort if the risk occurs.

Probability and Impact of a risk may be assessed qualitatively (e.g., low, medium, or high) and may also be quantifiably expressed in terms of frequency, i.e., 50% chance of occurring.

A risk’s exposure value or **Criticality**, frequently synonymous with **Severity** and often (but not always) synonymous with **Priority**, is based upon both the probability of the risk occurring and the severity of its impact. The numeric value associated for criticality is calculated by multiplying likelihood and consequences (“Likelihood x Consequence” or “LxC”). The resulting value denotes a low, medium, or high level of importance that shall be expressed using green, yellow, or red stoplight descriptors.

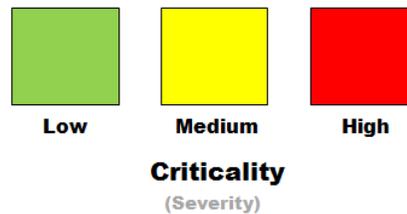


Figure 4: Risk Criticality “Stoplight Description”

While most often a high criticality risk (also referred to as a “red risk”) is synonymous with a high priority risk, occasionally a risk’s priority may differ from its criticality, based on resources, requirements, or constraints. For example: a risk that has a high likelihood and consequence and a numeric value of 4 or 5 will likely be the number one priority. However, a red risk that requires funding or expertise that is not readily available may not be the top priority to address; the effort may need to establish priorities that are counter-intuitive to risk criticality, if there are constraints or circumstances that require it.

2.1.2.3 Assign Risk Evaluation Criteria

The organization, program or project manager and team members shall assign the likelihood and consequences using the values associated with Goddard’s 5x5 matrix approach, which is depicted in the following tables.

Table 5: Likelihood & Consequence – Qualitative & Quantitative Values

Qualitative Value	Quantitative Value	5x5 Mapping Value <i>(on X, Y axes)</i>
Very High	Greater than 75% chance of occurring (> 75%)	5
High	Between 50% to 75% chance of occurring	4
Medium	Between 25% to 50% chance of occurring	3

Table 5: Likelihood & Consequence – Qualitative & Quantitative Values

Qualitative Value	Quantitative Value	5x5 Mapping Value (on X, Y axes)
Low	Between 10% to 25% chance of occurring	2
Very Low	Less than 10% chance of occurring (< 10%)	1

Additional information on standardized scoring for ITCD risks has been provided in [Appendix D – Risk Scoring & Ranking](#).

The organization, program or project manager shall review and approve all risk assessments, including assigned values for each risk. All approved risk assessments shall be recorded in the Risk List.

Table 6: Risk Criticality on the 5x5 Matrix

Item	Definition
Likelihood Probability	(L) = The likelihood (or probability) of occurrence
Consequence Severity and Impact	(C) = The consequences of the effect (severity and impact) on the effort if the risk occurs
Criticality Severity Ranking	Result of the multiplication of the values for Likelihood (Probability) and Consequence (Severity and Impact)
	<p>5x5 Matrix - Mapping Values: Where: LxC = Criticality...</p> <p>1 - 6 map to: Low Green²</p> <p>6 - 12 map to: Medium Yellow¹</p> <p>13 - 25 map to: High Red</p>

In cases where risks have the same numeric mapping value, risks with the higher consequence value are weighted more heavily, and therefore ranked higher. For example, on the 5x5 matrix the criticality value of “5” may be either green or yellow, when: L5xC1 = green and L1xC5 = yellow. Similarly the criticality value of “6” can be either green or yellow, when: L3xC2 = green and L2xC3 = yellow. Additional information on ranking criticality of ITCD risks has been provided in [Appendix D – Risk Scoring & Ranking](#).

2.1.2.4 Map Risks Using the 5x5 Matrix

The organization, program or project manager and team members shall use the Goddard 5x5 matrix approach² to document and describe the probability, severity, and criticality characteristics for risks.

¹ On NASA’s 5x5, the criticality value of “5” can be either green or yellow: L5xC1 = green and L1xC5 = yellow. Similarly the criticality value of “6” can be either green or yellow: L3xC2 = green and L2xC3 = yellow.

² Reference: GPR 7120.4D

This matrix reflects the mapping of a risk’s probability and severity values and derives the criticality of each risk from that mapping.

For example, if a team member identifies a risk that has a High likelihood of occurring (L = 4) and a Very High consequence anticipated (C = 5), then the resulting numeric value of “20” will categorize the risk as “Red” or a “High” level of criticality, as depicted by the “★” (star) in the figure that follows.

This same risk would receive a ranking value of “24” – see the figure provided in [Appendix D – Risk Scoring & Ranking](#) for a graphical depiction of the ranking values associated with each of the 5x5 twenty-five quadrants.

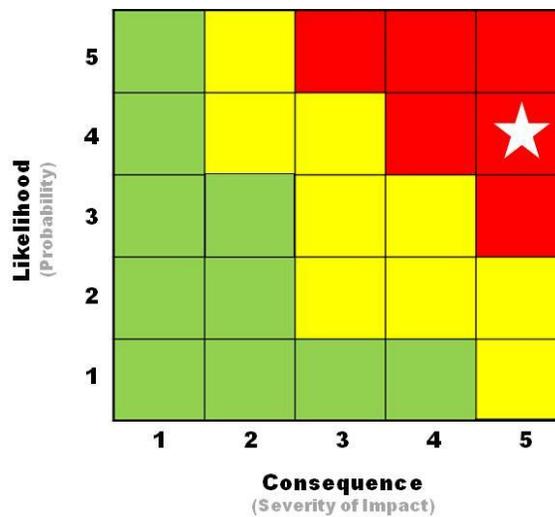


Figure 5: The 5x5 Risk Matrix

2.1.3 CRM Step 3: Plan Each Risk

2.1.3.1 Define the Approach

When planning, the members shall decide on an appropriate disposition, handling, or response **Approach** for each risk. These approaches include whether to **Research, Watch, Mitigate, Elevate,** or **Accept** the risk.

2.1.3.2 Identify Actionable Mitigation Plan

The team members shall develop actionable steps that can be taken to help avoid the risk or reduce the consequences of the risk were it to occur. This is the **Mitigation Plan** for this risk.

Risk mitigation plans are based on the assessed combination of the likelihood of occurrence and severity of the consequence for an identified risk. This approach requires development of a plan that is implemented and monitored for effectiveness.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

The organization, program or project manager works with the appropriate stakeholders to ensure that the necessary approval and buy-in for any mitigation or contingency plan(s) is obtained. The organization, program or project manager and team members shall document and update agreed-upon plans and maintain current status of the plans in the Risk List.

When risks are identified, a “cost” may be associated with the mitigation or contingency plans. When this occurs, the organization, program or project manager and team members shall review constraints (requirements, staffing, budget, time, etc.) and communicate, determine how the current funds can cover the risk migration/contingency or escalate any requirements that may adversely affect the budgeted resources (funding or staffing).

The organization, program or project manager shall seek appropriate approvals with their immediate manager when additional resources are deemed necessary.

2.1.3.3 Identify Possible Contingency Plan

If a risk cannot be avoided or mitigated (e.g., because the risk is outside the control of the organization, program, or project) then the team members shall develop steps that can be taken to minimize the impact were the risk to occur. This is the **Contingency Plan** for this risk.

Contingency planning involves coming up with a good alternative if a mitigation approach and plan is not feasible or is determined to be ineffective. Determining a contingency plan involves:

- Analyzing the risks and warning signs
- Identifying, defining and prioritizing contingencies
- Developing scenarios for possible contingencies
- Selecting the most effective contingency
- Developing the plan for the new scenario
- Maintaining and updating the contingency plan

2.1.3.4 Identify Risk Triggers

Risk Triggers are the warning signs that an identified risk may be about to occur. Identifying these triggers helps to know when it is time to implement the mitigation or contingency plan for a risk. Risks can have many triggers. Triggers may be discovered in the risk identification process and watched in the risk monitoring and controlling process. The identification and documentation of triggers early in the process will help proactively manage risks.

The organization, program or project manager and team members will consider and document what activities or events can trigger a need for follow-on action(s); i.e., the implementation of a mitigation or contingency plan.

2.1.3.5 Develop Rationale for Transfer

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

Risk *Transfer* is a risk mitigation strategy that shifts responsibility for risk handling, often to a third party external to the team. Risk transference changes the party responsible for handling or managing the risk. An example might include transference of a particular risk to a higher authority, i.e. the NASA Agency, for risk response or resolution.

2.1.4 CRM Step 4: Control Risks

A crucial part of the RM process is the monitoring and control of identified risks and the effectiveness of the plans put in place to eliminate or mitigate those risks. To do so, organization, programs and projects shall:

- Regularly update risk status
- Execute control measures (i.e., mitigation or contingency plans)
- Monitor the effectiveness of the mitigation or contingency plans underway
- Confirm risks meet acceptance and closure criteria before changing risk status to “Closed”

2.1.4.1 Regularly Update and Status Each Risk

The organization, program or project manager and team members shall review and update each risk status monthly, at the minimum, or more frequently as needs dictate.

2.1.4.2 Execute Control Measures

The designated authority shall execute “control measures” by implementing the agreed-upon approach and mitigation or contingency plan(s) for identified risks and managing these plans through closure or resolution of the risk.

2.1.4.3 Monitor Effectiveness of Plan(s)

The organization, program or project manager and team members shall re-assess each risk monthly (at a minimum) to evaluate the effectiveness of the related mitigation or contingency plan(s), and assess the effect of the execution of these plans on statuses and performance.

The organization, program or project manager shall take appropriate action when mitigation or contingency plans do not produce the desired result of risk reduction or avoidance. Appropriate steps may include, but are not limited to:

- Reassign risk ownership, tasks, etc.;
- Invoke contingency plan if/when the mitigation plan proves inadequate; or
- Replan risk approach and handling (e.g., change the approach; create new mitigation plan, etc.)

2.1.4.4 Replan When Necessary

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

The organization, program or project manager shall replan when the mitigation plan is not achieving the desired outcome or conditions have changed. Replanning entails taking action to:

- Re-evaluate risk approach;
- Develop an alternative plan;
- Attain necessary approvals and buy-in; and,
- Implement the new plan to ensure that effort objectives will be met.

2.1.5 CRM Step 5: Track & Report Risks

Another key aspect of risk monitoring and control is the tracking, reporting, and communication of risk status. Risks shall be tracked, reported, and communicated on a monthly basis, at a minimum.

The PM shall report the status and effectiveness of important risk mitigation action activities and current risk status to the key stakeholders, the PMO and Directorate on a monthly basis, or more frequently as needs dictate.

The organization, program or project manager and team members shall:

- Conduct risk status updates on a regularly recurring basis and document these activities within the effort's schedule
- Review, reevaluate, and modify the probability and impact for each risk item on a regular basis, at a minimum monthly, and prior to any formal status reporting/presentation
- Update the Risk List to reflect review of results or new risks identified and ensure the effort's Risk List is up-to-date
- Analyze any new risks that are identified
- Report risks using required forums and formats: Project Status Report (PSR), Directorate Status Report (DSR) and Monthly Status Review (MSR)
- Review the baseline set of risks with the team prior to significant milestones
- Communicate the baseline set of risks with stakeholders during formal reviews, milestones, or gateways.
- Escalate risks to appropriate management levels, when appropriate
- Confirm criteria has been met prior to risk closure

2.1.5.1 Track Risks

An up-to-date risk list shall be maintained by the organization, program and project, and shall be used to record and track risk management data. The organization, program or project manager will be responsible for ensuring the risk list remains current throughout the lifecycle.

The risk list shall be filed on the appropriate SharePoint site within the ITCD SharePoint portal.

Copies of ITCD risk lists shall be provided to the PMO for creation of a centralized Directorate risk list.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

2.1.5.2 Report Risks

The specified format for the appropriate reporting forum shall be used to report ITCD risks.

This is the required template to communicate risk status on a monthly basis. This format succinctly shows the risk, rank, identifier, and trending for top risks along with their current status. A sample of this format is depicted in the following figures.

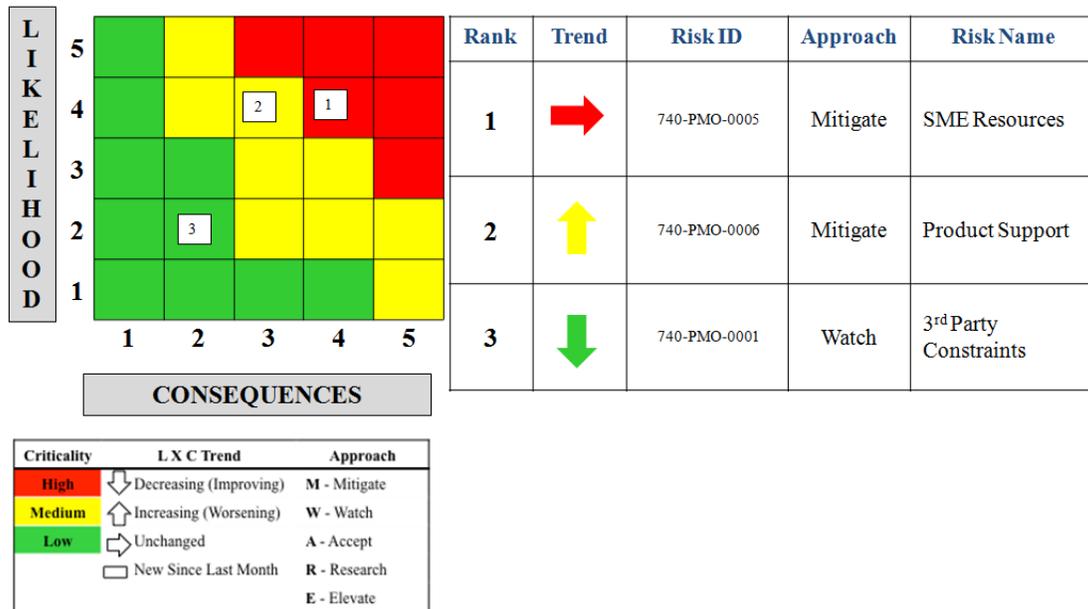


Figure 6: Risk Reporting Format (1st Slide)

Rank #	Risk ID	LXC Trend	Risk Statement <i>If...Then</i>	Approach & Plan	Status/Comments <i>Show last month's then this month's status</i>
1	740-PMO-0005		If: SME Resources are not available in time to support scheduled activities, Then: the project schedule will likely be negatively impacted, causing schedule slippages.	Mitigate Discuss SME requirements with Code 760 and CISO managers; obtain agreement to support	<u>December 2012: Involving affected parties in development of project activities and schedule.</u>
2	740-PMO-0006		If: Product Support can not be obtained or procured in a timely manner, Then: the project schedule will likely be negatively impacted, causing schedule slippages.	Mitigate Negotiate Product Support cost, availability, and cycle time.	<u>December 2012: Negotiations underway.</u> <i>Possible contingency: Determine level of support in-house resources can provide.</i>
3	740-PMO-0001		If: A recovery site for failover capability is not established by the responsible (3 rd) party, Then: there will be outages to the Production system in the event of a significant hardware failure.	Watch Follow scheduled progress of (responsible party).	<u>December 2012: 3rd Party progress to install failover capability being monitored.</u>

Figure 5: Risk Reporting Format (2nd Slide)

The top three risks and any other high priority risks shall be summarized and reported on monthly basis. In addition, monthly risk reporting shall report on the effectiveness of mitigation/contingency plan activities underway.

2.2 RIDM PROCESS

Throughout the lifecycle of any effort, it is common to encounter circumstances where alternatives become known and decisions must occur. When this happens, the alternatives must be decided upon and the process documented. The RIDM process goal is to arrive at a clear selection of an alternative over all others, and then act upon that selection.

RIDM is also used when the effort identifies risk that entails high stakes, complexity, uncertainty, multiple attributes or competing objectives, or a diverse range of stakeholders. The RIDM process will inform the mitigation strategy and ensure that the rigor applied to make decisions for risk handling, approach, mitigation, and management is appropriate for that risk.

The figure that follows provides an overview of the RIDM process using a hypothetical depiction of three alternatives: A, B, and C. This scenario supports the objective decision to pursue Alternative C, analysis of A, B, and C’s pros, cons, and risks.

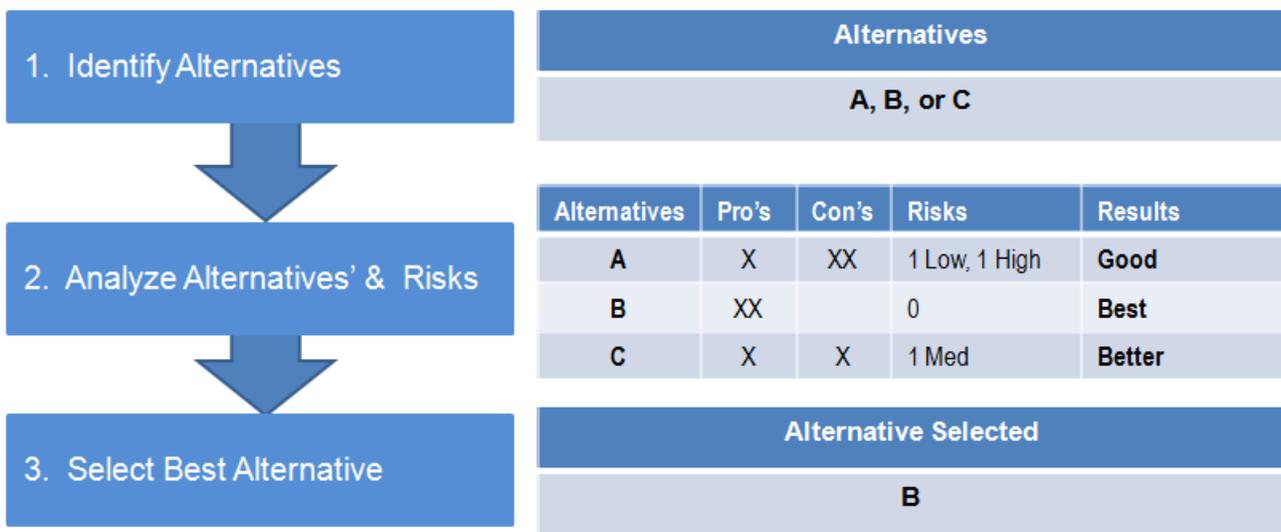


Figure 6: RIDM Process Depiction

ITCD shall document and describe the possibilities that have presented themselves as opportunities or alternatives to be considered and decided upon during an effort’s lifecycle.

ITCD shall follow the RIDM process to arrive at a clear selection of a single alternative over all others, and act upon that selection.

RIDM should start with the identification of Performance Objectives from Top-Level objectives and corresponding Performance Measures. For example, Minimize Cost, which would be measured in dollars; Maximize Adoption, which is measured in the number of active users of a new system, as a percentage of total users.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

2.2.1 RIDM Step 1: Identify Decision Alternatives

ITCD shall consider challenges and opportunities based on the effort's stated objectives, and document the possibilities that have presented themselves as opportunities or alternatives to be considered and decided upon.

2.2.2 RIDM Step 2: Analyze Decision Alternatives

After identifying and documenting alternatives, ITCD shall apply subject matter expertise across disciplines, as needed, to bound risk scenarios, integrate all key drivers and impacts, and consider performance measures.

The organization, program or project manager and team members shall evaluate each alternative.

The organization, program or project manager and team members shall identify pros and cons for each, assess the risks associated with that alternative (using the CRM process to do so), and objectively rank the alternatives based on the evaluation and assessment of that information.

2.2.3 RIDM Step 3: Select the Alternative

After ranking alternatives, the organization, program or project manager and team members shall select the best alternative informed by (though not solely based on) risk analysis results.

After a deliberative review informed by risk analysis results, the organization, program or project manager and team members shall select a decision alternative and develop risk mitigation strategies, if needed.

2.2.4 Implement the Selected Alternative

ITCD organizations, program or project managers, or assigned leads and team member shall take the necessary actions to proceed with the scheduling and implementation of the effort's selected alternative (and any related mitigation plans, as needed).

2.3 RISK COMMUNICATION PROCESSES

There is a difference between communication and escalation. Communication seeks to inform the target audience of routine status and information, while escalation intends to seek resolution from the target audience.

2.3.1 Communicate Risks

Risks that are deemed as a high criticality ("Yellow" or "Red") shall be communicated to the PMO, the RMO, Directorate managers, and to other appropriate stakeholders in a timely manner.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

The organization, program or project manager shall ensure that the appropriate leadership, management, and affected stakeholders are informed about significant changes in risk status, in a timely manner.

At a minimum, priority risks shall be reviewed (or re-reviewed) with stakeholders at the following points in the lifecycle:

- Project status reporting forums
- Directorate status reporting forums
- Formal reviews, including but not limited to:
 - Change control board (CCB) meetings
 - System Requirements Review (SRR)
 - Preliminary/Critical Design Reviews (PDR/CDR)
 - Test Readiness Review (TRR)
 - Operational Readiness Review (ORR)
- Gateway decisions or major milestones, such as:
 - Phase A through F gateway reviews
 - Other Go/No Go decision points in the project lifecycle, including: Authority to Proceed/Authority to Operate (ATP/ATO)
 - Start and/or Finish of key activities noted in the effort's Work Breakdown Structure (WBS)

Stakeholder acceptance or approval of mitigation or contingency plans shall be sought, whenever appropriate.

2.3.2 Elevate Risks

Elevate is used to describe a specific NASA risk handling approach that entails following an escalation path to communicate the risk and seek resolution to and from the next level of management; the terms “elevate” and “escalate” in this context are synonymous.

When the “elevate” approach is necessary, escalation paths differ depending on whether it is an organization, program or project. Project managers elevate risks to the RMO, with the next elevation level being the RMO's organization. Organizations, programs and projects then escalate next to the Directorate organization that is responsible for the effort, followed by the Directorate, Center, and NASA governance boards, beginning with the Directorate governance board. Reasons to elevate a risk may include:

- Additional resources are needed to mitigate the risk.
- Direction, assistance, or a decision is needed from the next level of management or senior leadership.
- The risk has cross-cutting significance or impact across Branches, Divisions, Directorates, Centers, etc.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

Table 7: Risk Communication & Escalation Summary

Communication & Escalation Path	Risk Description	Frequency & Forum
Project Team Member(s) → Program or Project Manager, or Assigned Lead	Any risk that impacts performance of the effort	Monthly via PSR
	Any risk that impacts >10% of the budget	
	Any risk that exceeds schedule milestones	
		Any risk that needs to be transferred to another directorate, division, branch, or other 3 rd party
Program or Project Manager, or Assigned Lead → RMO / PMO RMO / PMO → Management (as needed)	Top 3 (+/-) “Yellow” or “Red” risks, status, and trends	Monthly via PSR
	Any risk that impacts performance or success of the effort, including but not limited to: <ul style="list-style-type: none"> • Any risk that causes major slips of schedule milestones • Any risk that impact the technical aspects of the effort • Any risk that impacts the resource budget (people and funding) • Any risk that needs to be transferred to another directorate, division, branch, or other 3rd party 	Monthly via PSR, DSR, and/or MSR, as appropriate
	Mitigation activity status	

Table 7: Risk Communication & Escalation Summary

Communication & Escalation Path	Risk Description	Frequency & Forum
Program or Project Manager, or Assigned Lead → Management <hr/> Management → Leadership (as needed)	Top 3 (+/-) “Yellow” or “Red” risks, status, and trends	As Needed (daily, weekly, monthly, other)
	Mitigation activity status	
	Any risk that impacts effort success	
	Any risk that impact the technical aspects of the effort	
	Any risk that causes major slips of schedule milestones	
	Any risk that causes the budget to be exceeded by more than 10%	
	Any risk that negatively impacts the organization’s, Center’s, or NASA’s reputation	

2.4 RISK CLOSURE PROCESS

2.4.1 Confirm Criteria Before Risk Closure

The organization, program or project manager is authorized to close risks.

Prior to recording risk closure, the organization, program or project manager shall confirm appropriate criteria have been met.

A risk shall be deemed “Closed” when no further action is required or warranted because the risk has either been:

- Rejected (i.e., dismissal of a proposed non-risk)
- Accepted as-is
- Transferred to another party (a 3rd party not part of the project or project team)
- Realized (i.e., has been noted as an Issue)
- Resolved successfully (i.e., has been effectively avoided, mitigated, eliminated, or transferred)

2.4.1.1 Risk Rejection

An organization, program or project manager has discretion to reject a proposed risk and close this non-risk within the risk list at the time of rejection.

DIRECTIVE NO.	<u>740-PG-8000.1.1A</u>
EFFECTIVE DATE:	<u>August 12, 2013</u>
EXPIRATION DATE:	<u>August 12, 2018</u>

2.4.1.2 Risk Acceptance

Prior to risk acceptance, the organization, program or project manager will confirm that further mitigation is not cost-effective and that residual risk is at an acceptable level. The organization, program or project manager shall ensure that the acceptance rationale for the risk is approved by the owning organization and key stakeholders. The ITCD PMO must review accepted risks periodically to determine acceptance rationale remains applicable.

2.4.1.3 Risk Transfer

When risk transfer is appropriate, the organization, program or project manager shall identify and document the rationale for transferring the risk and communicate the risk transfer to the third party before changing the risk status within the Risk List.

2.4.1.4 Risk Realization

An organization, program or project manager shall record risks that have been realized (100% likelihood has occurred), and shall update the risk list to reflect this status.

Realized risks become issues that shall be submitted through the Directorate's Top Ten Issues process.

2.4.1.5 Resolved Risk

A risk is considered "resolved" when the implemented plans have been successfully executed and the risk has been either avoided or mitigated and there is no longer any probability that the risk or event will occur or have impact.

2.4.2 Complete Risk Closure

The organization, program or project manager shall confirm that the closure rationale is sound, is documented, and is approved, when necessary, at the appropriate management levels to demonstrate that the risk has been:

- Eliminated;
- Residual risk is negligible such that further steps are unnecessary; or that
- The threat that the risk formerly presented has been subsumed by a new or different risk.

When a risk is closed, the disposition shall be noted in the risk list and it shall remain on the risk list in a closed state for historical purposes throughout the duration of the lifecycle.

Closed risks shall be periodically reviewed by the organization, program or project manager. When warranted, closed risks may be either re-opened (returned to an open state) or be recreated as a new risk within the risk list to track risk recurrence.

3 RISK MANAGEMENT TOOLS

The following tools shall be used to manage and track risks through their lifecycle:

- Risk List
- Status Reporting forum(s) and designated format(s) for the Project, Division, and Directorate
- ITCD SharePoint Portal as the preferred repository for ITCD risk records

The IT *Risk List* is an RM tool that manages, tracks, reports risks and is used to help reduce risks identified before and during execution. It details risk mitigation strategies, contingency plans, and/or triggers for identified risks and records risk evaluations in terms of probability and severity. Data within the Risk List³ quickly and concisely conveys essential risk-related information including, but not limited to:

Identification Data:

- Risk ID
- Title
- Ownership
- Risk Statement

Management Data:

- Approach
- Mitigation Plan
- Contingency Plan
- Trigger(s)

Reporting Data:

- Ranking
- Priority
- Status
- Trending

ITCD organizations, programs or project managers, and team members shall use the PMO-developed Risk List tool to capture, document, status, rank, and trend ITCD risks.

The Risk List tool data requirements have been provided for reference within [Appendix B: Risk List Data Requirements](#).

³ For a complete list of required data elements please refer to: [Appendix B: Risk List Data Requirements](#).

APPENDIX A –TERMS, DEFINITIONS & ACRONYM LISTS

Terms & Definitions

- A.1 Accept** – (Acceptance of Risk) Formal process of justifying and documenting a decision not to mitigate a given risk associated with achieving given objectives or given performance requirements; determination that the consequences of an identified risk, should they occur, are acceptable without further mitigation. No further resources are expended in managing this risk except periodic review to ensure assumptions or circumstances have not changed.
- A.2 Acceptable Risk** – An acceptable risk is a risk that is understood and agreed to by the program/project, Governing Program Management Council (GPMP), Enterprise and other customer(s) sufficient to achieve the defined success criteria within the approved level of resources.
- A.3 Approach** – Disposition or handling strategy selected for a risk; options include: accept, elevate, research, mitigate, and watch.
- A.4 Artifact** – A document, work product or tool that is a non-record and may include such things as extra copies of a record, working files, technical reference materials.
- A.5 Assumption** – A statement accepted or supposed true without proof or demonstration, and that if proven false may become a risk.
- A.6 Authority to Operate** – Approval to move into an operational state based on meeting certain conditions primarily relating to meeting security requirements. The Director of ITCDD must approve ATOs.
- A.7 Conditions** – The (“If...”) component of a risk statement that describes the circumstances or cause for concern.
- A.8 Consequence** – Possible negative outcomes of conditions that create uncertainty and/or risk.
- A.9 Contingency Plan** – Planned course of action to be followed if a preferred *Mitigation Plan* fails or an existing situation changes.
- A.10 Criticality** – The probability of the risk occurring and the severity of its impact.
- A.11 Continuous Risk Management** – A specific process for the management of risks associated with implementation of designs, plans, and processes. The CRM functions of identify, analyze, plan, track, control, and communicate and document provide a disciplined environment for continuously assessing what could go wrong, determining which issues are important to deal with, and implementing strategies for dealing with risk.
- A.12 Elevate** – A process to increase the visibility of a risk, and to transfer the decision for the management of an identified source of risk to the risk management structure at a higher organizational level; synonymous with “escalate”
- A.13 Impact** – Severity of the effect on the project if the risk occurs.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- A.14 Issue** – A risk that has occurred and that has impacted a project; an event or incident that is impacting the organization which may be a risk that has been realized or identified
- A.15 Likelihood** – Probability of occurrence; a measure of the possibility that a risk will occur, which accounts for the frequency of the risk and the timeframe in which the risk can occur. For some purposes, it can be assessed qualitatively (e.g., High, Low). For other purposes, it is quantified in terms of frequency or probability (50% chance of occurring)
- A.16 Mitigate** – Modification of a process, system, or activity to reduce a risk by reducing its probability, consequence severity, or uncertainty, or by shifting its timeframe.
- A.17 Mitigation Plan** – Actionable plan for reducing the impact from the occurrence of a specific risk event. Defines the plan and steps that will achieve the desired risk handling approach: to proactively avoid, eliminate, reduce or transfer the risk.
- A.18 Organization Manager** – Director of ITCD, Associate Director of ITCD, all other Associate Directors, Division Chief, and Associate Division Chief.
- A.19 Program Manager** – The person responsible for managing multiple projects within a given functional area. This person is typically an Associate Director or Division chief.
- A.20 Priority** – Criticality of a risk, based upon the **Risk Value**; options include: Low/Green, Medium/Yellow, and High/Red
- A.21 Research** – Investigation of a risk to acquire sufficient information to support another disposition of the risk (i.e., close, watch, mitigate, accept, or elevate).
- A.22 Residual Risk** - Residual risk is the remaining risk that exists after all mitigation actions have been implemented and/or exhausted in accordance with the RM process.
- A.23 Risk** – Risk is the combination of the likelihood (or probability) that an organization/program/project will experience an undesired event (e.g., failure to achieve success criteria, cost overrun, schedule slippage, etc.) and the consequences (or severity and impact) of the undesired event were it to occur.
- A.24 Risk Informed Decision Making** – A process that uses a diverse set of performance measures (some of which are model-based risk metrics) along with other considerations within a deliberative process to inform decision making.
- A.25 Risk List** – The Risk List is the listing of all identified risks in priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the project; a register, database, spreadsheet, or other tool used by the organization, program or project to identify, analyze, plan, track, control, communicate, and document the risks and current risk status.
- A.26 Risk Management** – An organized, systematic decision-making process that efficiently identifies, analyzes plans, tracks, controls, communicates, and documents risk to increase the likelihood of achieving organization/program/project goals. Includes Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM) in an integrated framework.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

- A.27 Risk Statement** – A narrative description of a risk framed within an IF...THEN context where: the “If...” portion of the risk statement describes the condition that may occur; it describes the circumstances or cause(s) for concern, and the “Then...” portion of the risk statement describes what will be affected if the condition is not addressed and what the consequences will be; it describes the possible negative outcomes due to the concern(s).
- A.28 Risk Status** – Current state of the risk and approach.
- A.29 Risk Value** – Numerical value used to calculate criticality, and supports ranking, based upon the multiplication of the value for likelihood (L) by the value for consequence (C): Likelihood (ranging in values from 1 to 5) * Consequence (ranging in values from 1 to 5) = Value (may also be stated as: L×C); options include the values of 1 through 25.
- A.30 Transfer** – The act of allocating authority, responsibility, and accountability for a risk to another person or organization; a mitigation strategy that shifts responsibility for risk response, handling, and management to a third party.
- A.31 Trigger** – The warning sign(s) or description of possible events that may signal the risk is about to occur, and will “trigger” the need to take action.
- A.32 Watch** – The monitoring of an identified risk and its attributes for early warning of critical changes in consequences, likelihood, timeframe, or other indications that might reveal a risk event is imminent.
- A.33 Work Product** – See “Artifact.”

Acronym List

AA	Alternative Analysis
APPEL	Academy of Program/Project & Engineering Leadership
ATO	Authority to Operate
ATP	Authority to Proceed
CDR	Critical Design Review
CMMI	Capability Maturity Model Integration
COTS	Commercial-Off-The-Shelf
CRM	Continuous Risk Management
DSR	Directorate Status Review
FAD	Formulation Authorization Document or Formulation Agreement Document
GDMS	Goddard Directive Management System
GPR	Goddard Procedural Requirement
ID	Identifier / Identification
IT	Information Technology
ITCD	Information Technology & Communications Directorate (Code 700)
KDP	Key Decision Point
MIS	Management Information System (a Goddard in-house developed multi-function tool)
MSR	Monthly Status Report
NASA	National Aeronautics and Space Administration
NGIN	Next Generation Intelligence Networks (a COTS product used to develop a Goddard in-house multi-function tool)
NHBK	NASA Handbook
NPR	NASA Procedural Requirement
NRRS	NASA Records Retention Schedule
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PG	Procedural Guidance
PIMD	Program Integration & Management Division (Code 740)
PM	Project Manager
PMI	Project Management Institute
PMO	Project Management Office
PMP	Project Management Professional

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

Page 37 of 47

PP	Project Plan
PRA	Probabilistic Risk Assessment
PSR	Project Status Review
RIDM	Risk-Informed Decision Making
RM	Risk Management
RMO	Responsible Management Official/Office
RMP	Risk Management Plan
SATERN	System for Administration, Training, and Educational Resources for NASA
SE	Systems Engineering
SEI	Software Engineering Institute
SME	Subject Matter Expert
SP	Special Publication
SRR	System Requirements Review
STD	Standard
SWOT	Strength, Weakness, Opportunity, and Threat (a standardized format for assessment or analysis)
TRR	Test Readiness Review
WBS	Work Breakdown Structure

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

APPENDIX B – RISK LIST DATA REQUIREMENTS

Data Required	Description	Format / Explanation
Risk ID	The unique identifier for each risk	ITCD-ABC-#### Where: <u>ITCD</u> represents the Directorate (Code 700), <u>ABC</u> represents the organization program or project name (e.g., 740, ACES, DAR, PMO, HPP, etc.) reporting the risk, and <u>####</u> represents unique sequential numbering from 0001 through 9999
Date Opened	The date the risk is identified and entered into the risk list	MM/DD/YYYY
Risk Title	The summary name, or title, that describes the risk	(Free-form Text)
Risk Owner	The individual, role, or organization that is assigned responsibility for handling the risk	(Free-form Text)
Originator	The name of the individual who identified the risk	(Name, Free-form Text)

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

Data Required	Description	Format / Explanation
Risk Type	<p>A: Categories for Flight Project risk types</p> <p>B: Categories for IT risk types⁴</p>	<p>A. Flight Project risk types:</p> <ul style="list-style-type: none"> • Safety • Technical • Programmatic • Cost • Schedule <p>B. IT Project risk types may include, but are not limited to:</p> <ul style="list-style-type: none"> • Cost • Schedule • Resources-Staffing • Requirements • Environment • External Event-3rd Party • Management-Programmatic • Policy Development-Implementation • Process • Procurement • Regulatory • Security • Stakeholder • System
Risk Statement	<p>A narrative description of a risk framed within an IF...THEN context</p>	<p>(Free-form Text)</p> <p>IF: The “If...” portion of the risk statement describes the condition that may occur; it describes the circumstances or cause(s) for concern</p> <p>THEN: The “Then...” portion of the risk statement describes what will be affected if the condition is not addressed and what the consequences will be. It also describes the possible negative outcomes due to the concern(s)</p>

⁴ For a list of additional possible IT Project risk types and categories, please refer to Appendix C.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

Data Required	Description	Format / Explanation
Approach	The selected disposition or handling approach for the risk	Options include: <ul style="list-style-type: none"> • Accept • Elevate • Mitigate • Research • Watch
Likelihood	The probability of occurrence	Options include: 1 ... 5 Where: 1 = Very Low 2 = Low 3 = Medium 4 = High 5 = Very High
Consequences	The severity of impact	Options include: 1 ... 5 Where: 1 = Very Low 2 = Low 3 = Medium 4 = High 5 = Very High
Risk Value	The numerical value used to calculate Priority based upon the multiplication of the value for likelihood (L) by the value for consequence (C): <i>Likelihood * Consequence = Value</i> May also be stated as: LxC Note: The Risk Value is used to determine Risk Rank for reporting purposes; the risk with the highest numerical value is ranked “1”, next highest “2” (and so on).	Where numeric value of LxC equals: 1 - 6 map to: Low Green ⁵ 6 - 12 map to: Medium Yellow ⁵ 13 - 25 map to: High Red

⁵ On NASA's 5x5, the criticality value of “5” can be either green or yellow: L5xC1 = green and L1xC5 = yellow. Similarly the criticality value of “6” can be either green or yellow: L3xC2 = green and L2xC3 = yellow.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

Data Required	Description	Format / Explanation
Priority	The criticality of the risk, based upon the <i>Risk Value</i>	Options include: Low = Green Medium = Yellow High = Red Where: 1 - 6 map to: Low Green ⁶ 6 - 12 map to: Medium Yellow ⁶ 13 - 25 map to: High Red
Trending	Records priority trending across reporting period(s).	Options include: <ul style="list-style-type: none"> • New • No Change • Raised <i>Priority</i> • Lowered <i>Priority</i>
Trigger Event	The warning signs or description of possible events that may signal the risk is about to occur, and will “trigger” the need to take action	(Free-form Text)
Mitigation Plan	The actionable plan for reducing the impact from the occurrence of a specific risk event. Defines the plan and steps that will achieve the desired risk handling approach: to proactively avoid, eliminate, reduce or transfer the risk.	(Free-form Text)
Contingency Plan	The planned course of action to be followed if a preferred Mitigation Plan fails or an existing situation changes	(Free-form Text)

⁶ On NASA’s 5x5, the criticality value of “5” can be either green or yellow: L5xC1 = green, and L1xC5 = yellow. Similarly the criticality value of “6” can be either green or yellow: L3xC2 = green, and L2xC3 = yellow.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

Data Required	Description	Format / Explanation
Risk Status	The current state of the risk and approach.	Options include: <ul style="list-style-type: none"> • Research Underway • Being Watched • Contingency Active • Mitigation Pending Approval • Mitigation Underway • On Hold • Realized Risk • Closed_Accepted • Closed_Rejected (dismissed) • Closed_Resolved • Closed_Transferred
Update Date	The date the risk was last updated	MM/DD/YYYY
Reported Status	The documented status presented at the appropriate forum/format (e.g., PSR, DSR, etc.) for the reporting period	(Free-form Text)
Comments	Additional details, explanations, or notes that provide clarity about the risk	(Free-form Text)
Closure Date	The date the risk was deemed “No further action required or warranted” because it has either been: <ul style="list-style-type: none"> • Accepted • Realized (<i>and noted as an Issue</i>) • Resolved successfully (<i>avoided, mitigated, eliminated, etc.</i>) • Dismissed / Closed 	MM/DD/YYYY
Risk/Issue	Flag to indicate whether this item is a risk or an issue for tracking and reporting purposes	Options include: <ul style="list-style-type: none"> • Risk • Issue

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

APPENDIX C – ADDITIONAL RISK TYPES & CATEGORIES

The following data is provided to assist in identifying risks.

Note: Some risk types may map to multiple categories and therefore may be repeated intentionally.

Business-Related Risks

- 3rd Party Relationship
- Business Disruption
- Compliance / Governance Requirements
- Lost Opportunity Costs
- Policy Development / Requirements
- Political Discord
- Reduction in Competitiveness
- Regulatory Requirements
- Strategic [Competition]

Constraint-Based Risks

- Budget
- Contract Dependencies
- Contract Restrictions
- Contractor / Subcontractor Relations
- Customer | Availability
- Customer | Engagement
- Customer | Responsiveness
- Customer Satisfaction
- Facilities
- Management
- Partners
- Project / Program Interfaces
- Resources | \$
- Resources | Staff
- Schedule

Environment-Related Risks

- Configuration Management
- Configuration Management | Change Control
- Development | Environment
- Development | Process
- Development | Tools
- Management Process | Planning
- Management Process | Project Organization
- Personnel Management
- Quality Assurance

Implementation-Related Risks

- Business Disruption
- Configuration Management Maturity
- Organizational Change Management
- Production Environment Readiness
- Coordination
- Schedule

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

Management-Related Risks

- Duplication of Efforts
- Estimation Accuracy | Activities
- Estimation Accuracy | Costs
- Estimation Accuracy | Resources
- Inadequate Change Process
- Inadequate Testing Process
- Inadequate Top Management Sponsorship/Support
- Inadequate Communication
- Inadequate Training
- Internal or External Priority Competition
- Lack of Stakeholders' Commitment
- Limited Project Experience (similar effort)
- Procurement
- Scope Management

Technical Risks

- Adequacy of Code and Unit Test
- Application Security
- Data Integrity
- Data Security
- Design | Difficulty
- Design | Functionality
- Design | Interfaces
- Design | Performance
- Design | Testability

Technical Risks, Continued

- Hardware Availability
- Hardware Capability
- Hardware Capacity
- Hardware Reliability
- Infrastructure Security
- Integration Test | Adequacy
- Integration Test | Environment
- Integration Test | Product / Tools
- Integration Test | System
- Requirements | Clarity
- Requirements | Completeness
- Requirements | Feasibility
- Requirements | Precedent
- Requirements | Scale
- Requirements | Stability
- Requirements | Validity
- Software Availability
- Software Capability
- Software Reliability
- Software Security
- System Availability
- System Capability
- System Reliability
- System Security
- Technical Interface
- Technical Interface | Design
- Technical Interface | Documentation
- User Acceptance Test | Adequacy
- User Acceptance Test | Environment
- User Acceptance Test | Product / Tools

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

APPENDIX D – RISK SCORING & RANKING

This guidance will be used to standardize the scoring of ITCD risks, and to ensure that risk consequence values are weighted in favor of risk likelihood values when ranking ITCD risks.

ITCD Standard Risk Scorecard

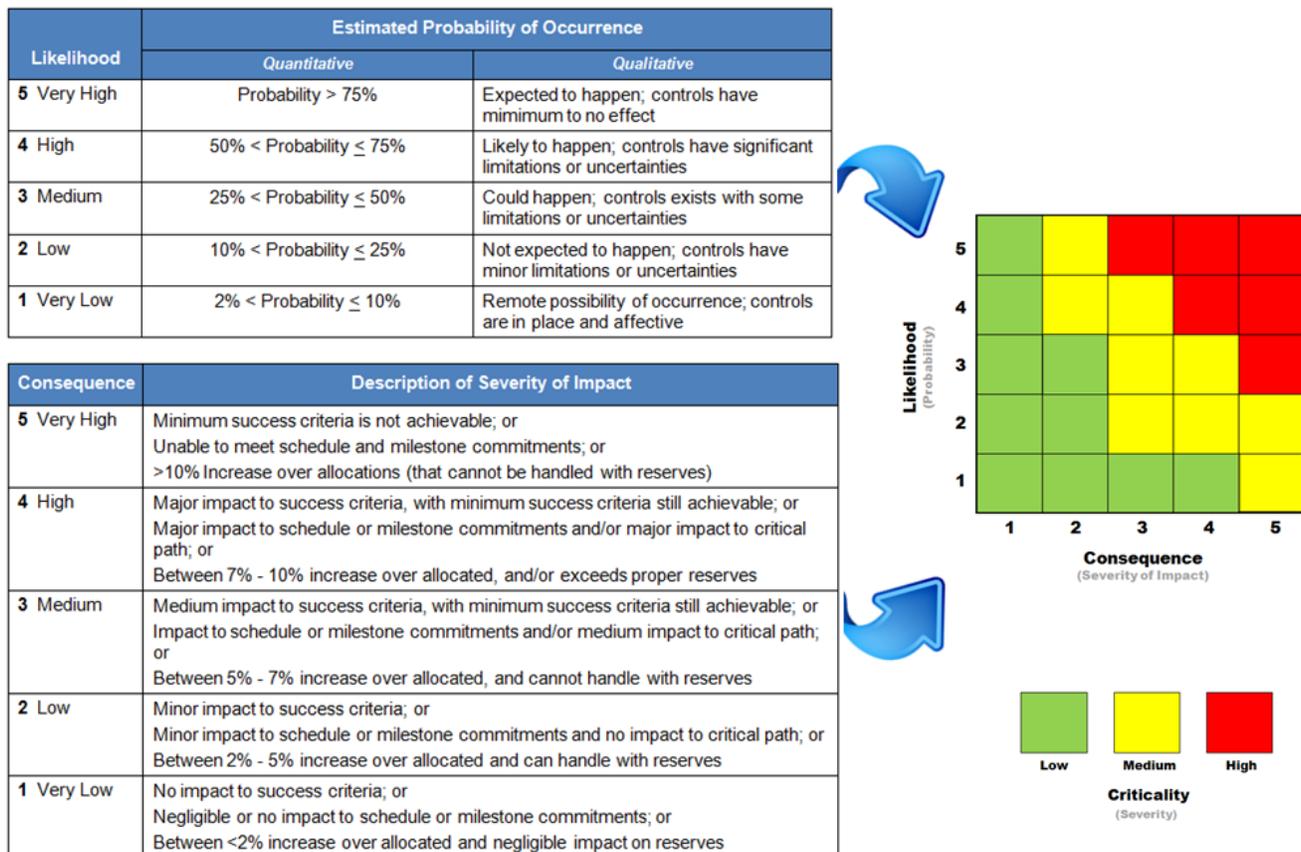


Figure 7: Standard Risk Scorecard

The figure that follows provides a depiction of the risk 5x5, and unique ranking values.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

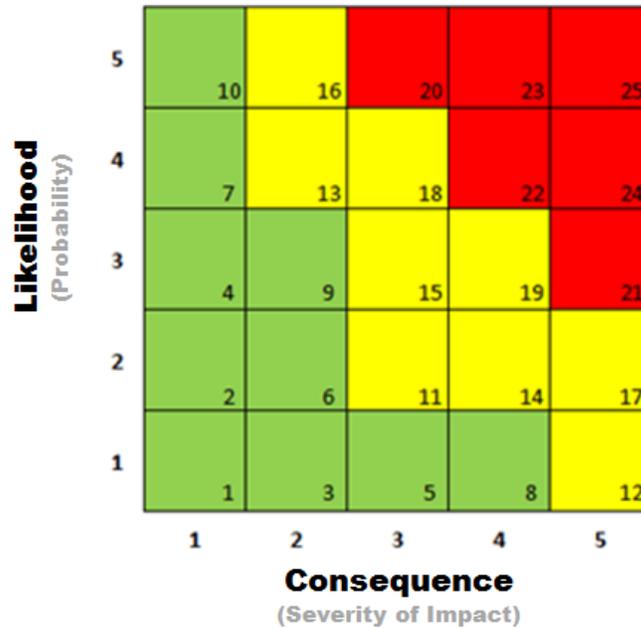


Figure 8: Risk Criticality Ranking Values of 1 (lowest) to 25 (highest)

This figure provides the unique value (1 – 25) assigned to each of the quadrants of the 5x5 risk matrix. The higher the assigned value, the higher the ranking of the risk is. The value assigned to each quadrant reflects the preferential weighting of consequence over likelihood, and removes the ambiguity for ranking risks that have the same total risk value. For example L3xC1 and L1xC3 both result in a risk mapping value of 3 (3x1 and 1x3, respectively). However, notice the assigned value for L1xC3 is higher (5) versus L3xC1 (4).

DIRECTIVE NO. 740-PG-8000.1.1A
EFFECTIVE DATE: August 12, 2013
EXPIRATION DATE: August 12, 2018

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	August 12, 2013	Initial Release
A [if this is the baseline version, leave this and the remaining Revision blocks blank]		

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.