



Integrating Risk Management and Nonconformance & Deviation Management

August 27, 2020

NASA Ames Research Center
Jonathan Demboski



Agenda

- Overview of Risk
- Overview of NASA's Risk Management Process
- Connecting Risk Management and Nonconformance & Deviation Management

Objective

- Have you think about how to connect Risk Management and Nonconformance & Deviation Management within the context of YOUR Organization

Basic Definition of Risk*


Risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives

These objectives are translated into **performance requirements** for programs and projects related to the mission execution domains

- Safety
- Mission success
- Cost
- Schedule
- Institutional support for mission execution

NPR 8000.4B — TOC Page 1 of 22

[NODIS Library | Program Management(8000s) | Search]

 **NASA**
Procedural
Requirements
COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

NPR 8000.4B
Effective Date: December 06, 2017
Expiration Date: December 06, 2022

Agency Risk Management Procedural Requirements
Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

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

Chapter 1. Introduction

1.1 Background
1.2 Risk Management within the NASA Hierarchy

Chapter 2. Roles and Responsibilities

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

Chapter 3. Requirements for Risk Management

3.1 General
3.2 General Risk Management Requirements
3.3 Requirements for the RIDM Process
3.4 Requirements for the CRM Process
3.5 Requirements for Decisions to Accept Risks to Safety or Mission Success 3.6 Requirements for

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directive Information System (NODIS) Library to verify that this is the correct version before use: <http://nodis1.arc.nasa.gov>

NPR 8000.4B — TOC Page 1 of 22

*NPR 8000.4B, Agency Risk Management Procedural Requirements

Operational Characterization of Risk*

The **scenario(s)** leading to degraded performance with respect to one or more performance measures:

- Safety (public and workforce safety, environmental safety, and asset safety)
- Mission Success (exceedance of mass limits)
- Cost (scenarios leading to cost overruns)
- Schedule (scenarios leading to schedule slippage)
- Institutional Support (infrastructure, information technology, security, compliance with internal (e.g., NASA) and external requirements (e.g., Environmental Protection Agency or Occupational Safety and Health Administration regulations))

The **likelihood(s)** (qualitative or quantitative) of those scenarios

The **consequence(s)** (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur

Note: Uncertainties are included in the evaluation of likelihoods and identification of scenarios

*NPR 8000.4B, Agency Risk Management Procedural Requirements

Risk vs. Problem

- “Risk” cannot be treated as a problem
- Risk identification and analysis is a **prediction** activity intended to answer three basic questions:
 1. What can go wrong that may lead to loss or degraded performance (scenarios)?
 2. How likely is it (probabilities)?
 3. What is the severity of the degradation (consequences)?
- A problem may often be a **condition** that exists
- The existence of a **condition** or a **set of conditions** might affect the risk profile
 - Introduces change in the structure of scenarios
 - Introduces change in likelihoods
 - Introduces change in consequences

NASA Uses Complementary Processes for Risk Management

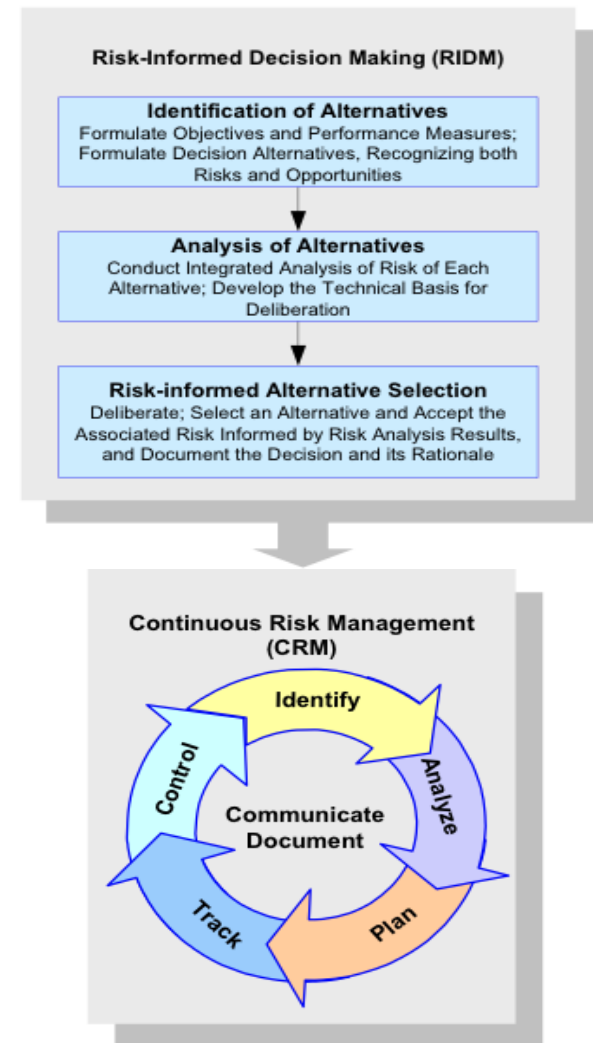
Risk-informed Decision Making*

- To inform decision making through better use of risk information
 - Establishes baseline performance requirements (e.g., safety, technical, cost, and schedule requirements) for program/projects and mission support organizations

Continuous Risk Management

- To manage risk associated with the implementation of baseline performance requirements

*“Risk-informed,” as opposed to “risk-based,” means that decision-makers base their decisions on a range of inputs, including but not over-emphasizing the predictive results of risk analysis models



Management Support and Oversight

Consider risks in relation to a quality management system and its associated processes:

- What are the risks associated with the **organization's context** and objectives - and why does each risk occur?
 - Identify the risk and the reason for its occurrence – **the Scenario**
- What would be the likely negative **consequences** of process, product, service, or system nonconformities?
- How **likely** is it that the organization will deliver nonconforming products and services in relation to the risks we have identified?
- How effective are our existing controls?
 - Identify factors that reduce the consequences or probability of the risk **in terms of what they actually need to know**

Risk Control

- Common Risk Controls
 - Inspection – more of a containment method
 - Process Validation – more of a proactive method
- Risk control as a **measure of effectiveness**
 - If the risk has been reduced and is within acceptable parameters, then it is effective
 - If the risk has not been reduced, or even if the risk has been reduced but not to acceptable parameters, it must be reworked until it is corrected
- Use historic data to build risk profile
 - Management can make more informed decisions by drawing on previous actions taken based on history of past events

L I K E L I H O O D	5	Green	Yellow	Red	Red	Red
	4	Green	Yellow	Yellow	Red	Red
	3	Green	Green	Yellow	Yellow	Red
	2	Green	Green	Yellow	Yellow	Yellow
	1	Green	Green	Green	Green	Yellow
		1	2	3	4	5
		CONSEQUENCES				

Internal Audits and Risk Management

- Internal Audits should include the following:
 - The identification of risks
 - The **evaluation** of the underlying processes, systems, and management's capabilities to manage risks
 - The **continuous monitoring and evaluation** of controls to determine their effectiveness in mitigating risks
 - Internal auditors simply must have a strong **understanding of the macro and micro risks** impacting their respective organizations

- Organizational risk assessments should include:
 - An understanding of **internal audit priorities** that drive annual audit plans
 - Information obtained and evaluated by internal auditors from continuously interacting with the organization

Finding	Risk - Informed
Met-cal: expired stickers	Inquire about which measurements have documented accuracy requirements. Check cal status of instruments used to take those measurements
ESD: Lack of ESD controls based on finding in high-risk area	Determine controls on high-risk area (beyond simply ESD) to find out if there is a clear distinction between where risks can be taken and where they can't
Use of materials beyond date (or no date)	Assess organization's understanding about expiration of materials and risks associated beyond the date
Use of standards other than those specified	Determine whether org understands the standard they use and whether they properly negotiate requirements with customer (tailoring)
Not meeting sampling rate requirements	Determine whether org makes "quality adjustments" to sampling

* Excerpt from Jesse Leitner (2017) Risk-based SMA: Audit and Assessment

Internal Audits and Risk Management

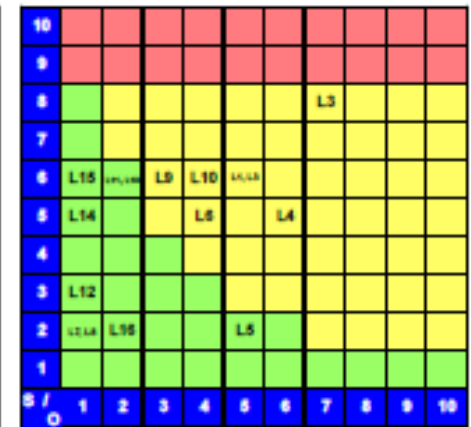
- Common example of a nonconformance classification system:
 - **Major** - Significant breakdown of the system, as indicated by the specific failure or the frequency of occurrence
 - **Minor** - An issue unlikely to have a significant impact
 - **Observation** - Something that might be a weakness but there is no requirement or objective evidence to cite
 - **Opportunity for Improvement** - Something that may enhance performance of the system
- Consider enhancing the minor and major continuum:
 - **Critical** - Potential for a severe impact on operations, stakeholders, cost, etc.
 - **Major** - High impact on operations, stakeholders, and cost
 - **Moderate** - Slight impact on operations and/or cost; no impact on stakeholders
 - **Minor** - No measurable impact on operations, cost, or stakeholders

Examples for Application of Nonconformance Classification

Impact	Risk
Minor – impact to cost, schedule, performance, institutional, etc.	Low – risks are largely acceptable, corrections may be enough to resolve the issue
Moderate – impact on impact to cost, schedule, performance, institutional, etc.	Medium – risks may be tolerable, corrections may be enough to resolve the issue; however, a CAPA should be considered
Major – Significant impact to cost, schedule, performance, institutional, etc.	High – risks are unacceptable; a CAPA should be conducted to resolve the issue

*Table based on Mark Allen Durivage (2017) *Using Risk-Based Thinking to Manage Nonconformances and Deviations*

N = No corrective actions are needed
 K = Corrective actions are needed
 # = Corrective actions are needed if the evaluation of detection (D) is equal to or greater than the one specified



Overall as result of standards and as result of analysis

*Examining Risk Priority Numbers in FMEA (2015) <http://www.Reliasoft.com/newsletter/2q2003/rpns.htm>

Connecting Risk Management and Nonconformance & Deviation Management

- Establish elevation mechanisms to CAPA process
- Link CAPA to Risk Management documentation (e.g., FMEAs, Design Control documents, etc)
- Make data reporting available and easy to users and management to establish occurrence and therefore calculate risk

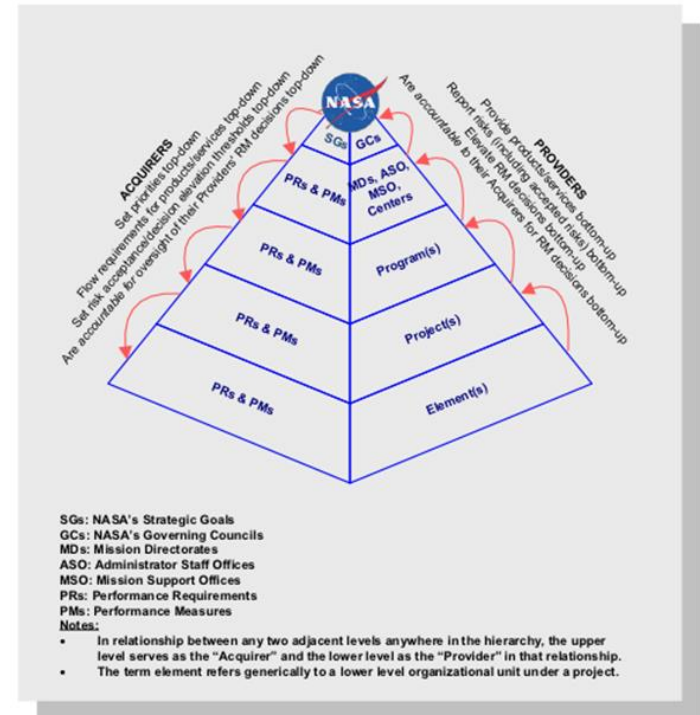
Possible Countermeasures	Effectiveness <i>(Likelihood to achieve goal/target)</i> (H, M, L)	Feasibility <i>(how realistic or practical to implement)</i> (H, M, L)	Impact <i>(what affect will the possible countermeasure have)</i> (H, M, L) (+/-)	Total Votes <i>(N/3)</i>
<ol style="list-style-type: none"> 1. How well will this countermeasure work? 2. Will this countermeasure be enough to achieve the targets or goals? 3. Will this countermeasure prevent recurrence (root cause) of the problem? 		<ol style="list-style-type: none"> 1. Quality 2. Cost 3. Safety 4. Resources 5. Time 6. Management approval 	<ol style="list-style-type: none"> 1. On others 2. The job 3. Other operations 4. The Directorate as a whole 5. The Center as a whole 	

CAPA Elevation: Connecting Risk Management and Trending

- Use a risk assessment process to allow prioritization of CAPAs and elevation to Management
- Use a risk assessment process that allows CAPAs for Preventive Action
- Critical questions for the CAPA process to determine the depth of investigation/priority of CAPA:
 - Is this a new or unknown issue?
 - Has the severity increased? Decreased?
 - Has the frequency of occurrence increased?
 - Have the causes of the issue been confirmed?
 - Are there new causes of the issue that have inadequate or no mitigation?
- Root Causes for incomplete / ineffective CAPAs
 - Is it the CAPA process?
 - the investigation process?
 - Both?
 - Other?

Strategic Alignment – Performance Measures

- Align Nonconformance & Deviation Management with organization, department, program/project goals and objectives
- Align metrics from departmental to organizational level
- Implement predictive metrics / indicators
 - CAPA metrics tend to focus on closure rates, cycle time, # of open CAPAs, etc.
 - Preventive Actions are, in most cases, longer-term solutions across processes, systems, product lines, and Quality Systems and will take more time to close
 - Examples:
 - Ambiguities per requirements page, %
 - % defects in aleatory sample (e.g. met/cal expirations)
 - Test plan coverage %



Review of Agenda

- Overview of Risk
 - Scenario, Likelihood, Consequences
 - Risk vs Problem
- Overview of NASA's Risk Management Process
 - Risk-Informed Decision Making
 - Continuous Risk Management
- Connecting Risk Management and Nonconformance & Deviation Management
 - Management oversight – Context of the organization
 - Risk Controls
 - Internal Audits input to Risk Management
 - Examples of risk analysis in the Corrective / Preventive Action process
 - Elevation process and trending of performance measures

Objective

- Have you think about how to connect Risk Management and Nonconformance & Deviation Management within the context of YOUR Organization

Reference

- NASA Procedural Requirement (NPR) 8001.4B Agency Risk Management Procedural Requirements Retrieved from <https://nodis3.gsfc.nasa.gov/>
- Safety and Mission Assurance (SMA) Technical Excellence Program (STEP) Level 1: Risk Management Overview (SMA-OV-WBT-111) Retrieved from <https://nscstep.nasa.gov>.
- Leitner, Jesse (2017) Risk-based SMA: Audit and Assessment Retrieved from <https://ntrs.nasa.gov/citations/20170011093>
- Durivage, Mark Allen (2017) *Using Risk-Based Thinking to Manage Nonconformances and Deviations*
- Examining Risk Priority Numbers in FMEA (2015) Retrieved from <http://www.Reliasoft.com/newsletter/2q2003/rpns.htm>