NASA 2023 Cost & Schedule Symposium

Risk Management

Overview

Agenda

✓ **What is Risk Management?**
Elements of why we use risk management

✓ **RIDM & CRM Framework**
Strategic and tactical approach managing risks

✓ **Risk Defined**
What is risk?

✓ **Risk Identification**
Risk identification methods

✓ **Characterization of Risks**
Discuss scenario, likelihood and consequence

✓ **Risk Appetite**
How much risk can we take?

✓ **Risk Tolerance**
How much risk are we willing to accept?

What is Risk Management?

- Risk Management is a deliberative, systematic process to analyze and communicate the risk of **performance shortfalls**. This process involves the development of risk handling plans, and implementation of approved strategies to reduce or eliminate the **likelihood** of occurrence and severity of **consequence**.

- Risk management includes risk-informed decision making (RIDM) and continuous risk management (CRM) in an integrated framework.

Risk Defined

Basic Definition of Risk*

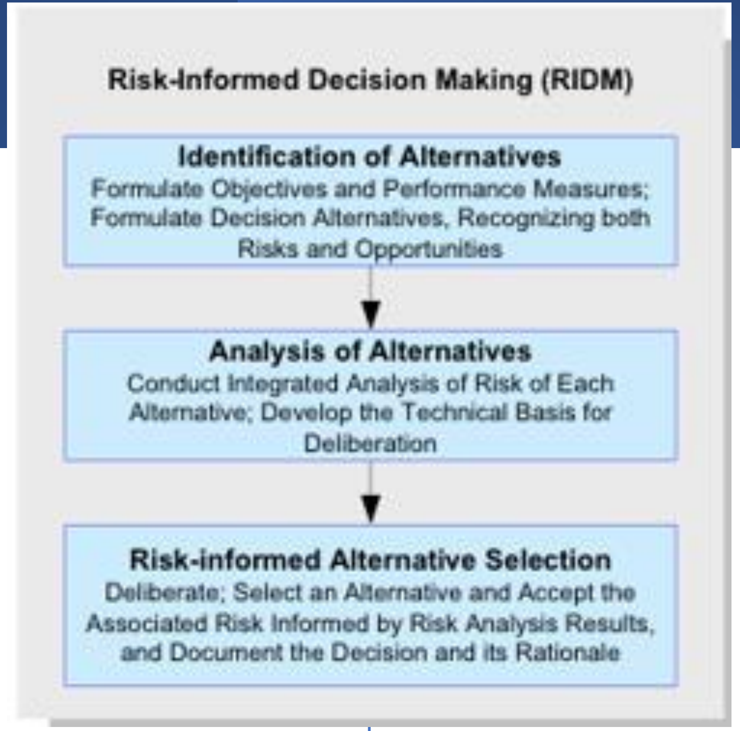
- **Risk** is the potential for shortfalls with respect to achieving explicitly established and stated objectives.
- Objectives are translated into **performance requirements** for programs and projects related to the mission execution domains:
    - Safety
    - Mission success
    - **Cost**
    - **Schedule**
    - Cybersecurity

*NPR 8000.4C, Agency Risk Management Definition of Risk is Based on Meeting Performance Objectives

RIDM & CRM Framework

Risk-informed Decision Making (RIDM)

- ➢ To inform decision making through better use of risk information
  - ➢ Establishes baseline performance requirements for program/projects and mission support organizations.



Risk-Informed Decision Making (RIDM)

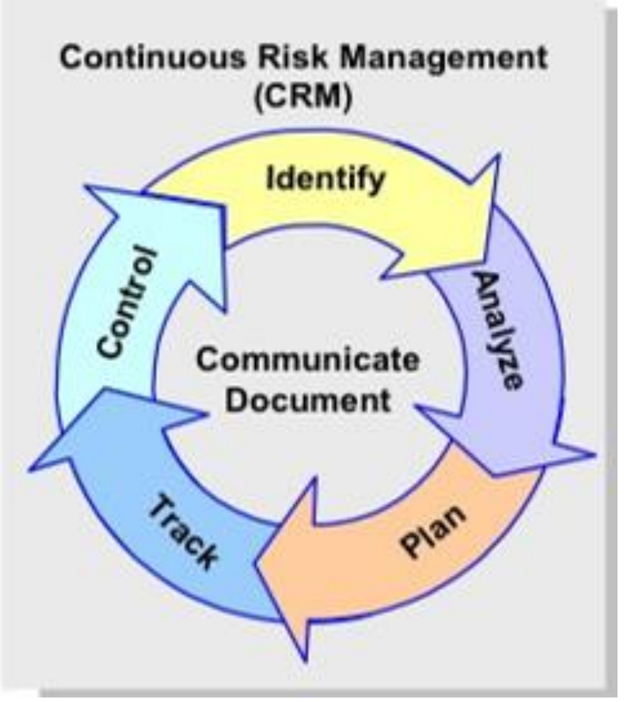
Identification of Alternatives
Formulate Objectives and Performance Measures; Formulate Decision Alternatives, Recognizing both Risks and Opportunities

Analysis of Alternatives
Conduct Integrated Analysis of Risk of Each Alternative; Develop the Technical Basis for Deliberation

Risk-informed Alternative Selection
Deliberate; Select an Alternative and Accept the Associated Risk Informed by Risk Analysis Results, and Document the Decision and its Rationale

Continuous Risk Management (CRM)

- ➢ To manage risk associated with the implementation of baseline performance requirements. In other words, the <u>CRM process is oriented toward keeping the potential for performance shortfalls within tolerable limits</u>.



Continuous Risk Management (CRM)

Risk Identification

- Risks are identified by the project team, reviews, lessons from past projects, and experience.
- Lessons from past projects are captured via ‘trigger questions’, or questions that challenge a development strategy or design solution

Project risk status and top ten risks are reviewed periodically - usually monthly - and at the project milestone reviews.

Risk Characterization

- 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 budget overruns)
  - Schedule (scenarios leading to timeline/milestone slippage)
  - Cybersecurity (damage to computers, electronic communications systems, etc.)
- The **likelihood** (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

NPR 8000.4C, Agency Risk Management Procedural Requirement

Risk Appetite

- **What is Risk Appetite**
  - Risk appetite is the amount of risk a project is willing to accept to achieve its objectives. NASA recognizes that they cannot remove all risk and achieving program/project goals requires accepting some of those risks while taking actions to mitigate, avoid or transfer other risks.
  - The task facing programs/projects is determining which risks fit within the organization's risk appetite and which require additional controls before they are acceptable. You can think of an organization's risk appetite as its **risk capacity** -- the maximum residual risk that the organization will accept after controls are put in place.

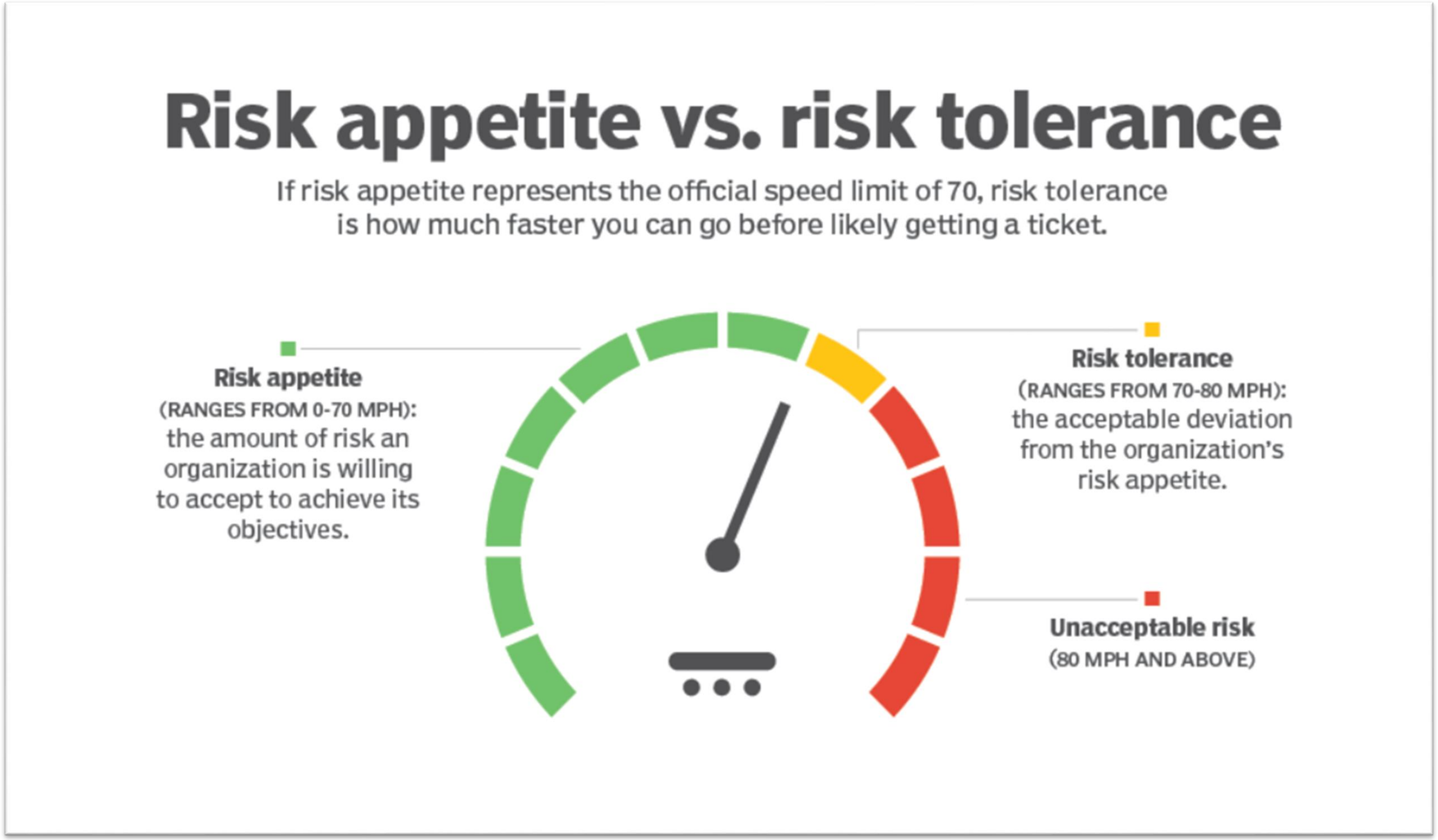
NPR 8705.4A Risk Classification for NASA Payloads

Risk Tolerance

- **What is Risk Tolerance?**
  - Risk tolerance is the amount of acceptable deviation from the established risk appetite. While risk appetite is a broad, strategic philosophy that guides an organization's risk management efforts, risk tolerance is a much more tactical concept that identifies the risk associated with a specific initiative and compares it to the organization's risk appetite.
  - You can think of a NASA's risk tolerance for a specific initiative as its willingness to accept the risk that remains after all relevant controls are put in place.
- The risk tolerances established during the RIDM process indicate the levels of acceptable initial risk that the CRM process commits to managing during implementation.

NPR 8705.4A Risk Classification for NASA Payloads
NASA/SP-2011-3422 NASA RM Handbook

Risk Appetite vs. Risk Tolerance



Risk appetite vs. risk tolerance

If risk appetite represents the official speed limit of 70, risk tolerance is how much faster you can go before likely getting a ticket.

🟩 **Risk appetite**
(RANGES FROM 0-70 MPH):
the amount of risk an organization is willing to accept to achieve its objectives.

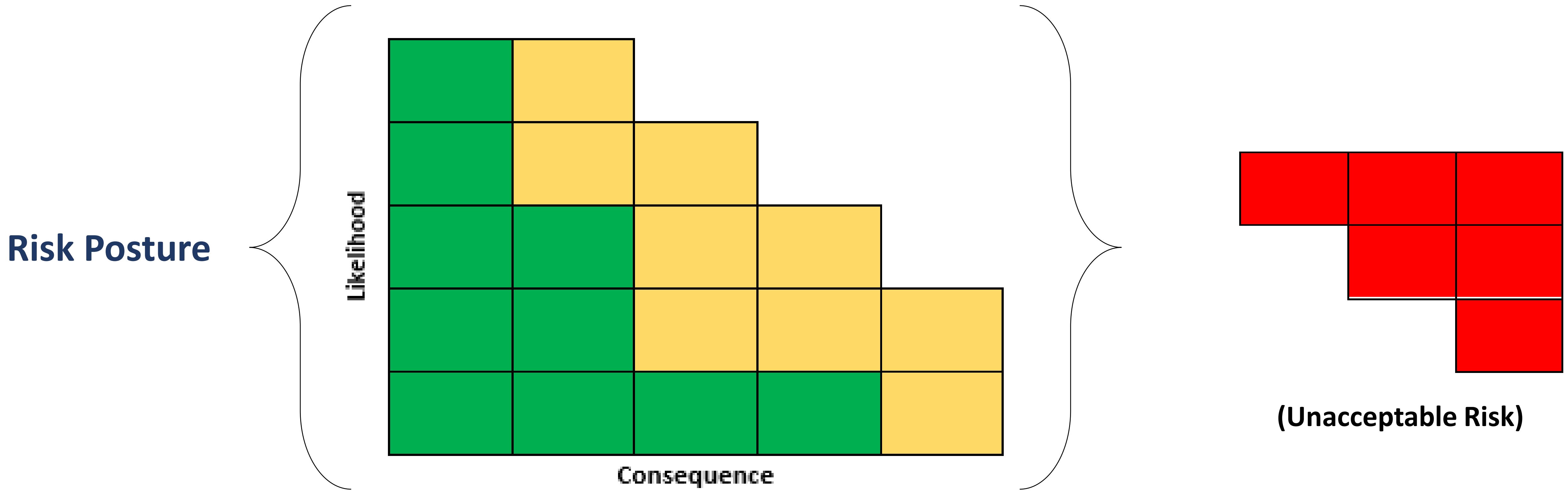
🟨 **Risk tolerance**
(RANGES FROM 70-80 MPH):
the acceptable deviation from the organization's risk appetite.

🟥 **Unacceptable risk**
(80 MPH AND ABOVE)

Risk Posture

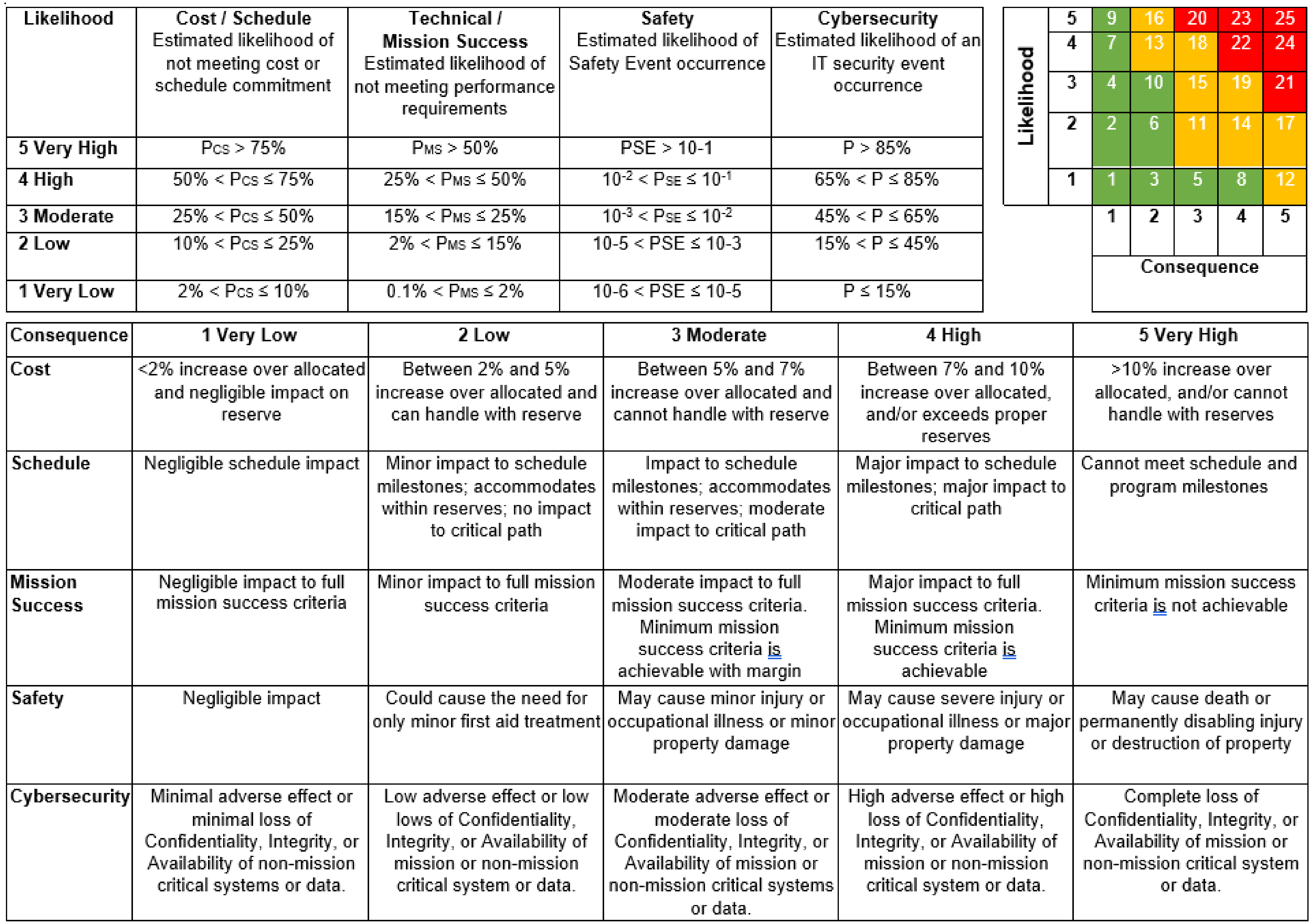
- **Risk Posture**
  - Risk appetite and risk tolerance **combined** define the organization's risk posture.

Risk Appetite + Risk Tolerance = **Risk Posture**



Sample Risk Scoring Criteria

- Langley standard risk scoring criteria for Space Flight projects



Likelihood	**Cost / Schedule** Estimated likelihood of not meeting cost or schedule commitment	**Technical / Mission Success** Estimated likelihood of not meeting performance requirements	**Safety** Estimated likelihood of Safety Event occurrence	**Cybersecurity** Estimated likelihood of an IT security event occurrence
5 Very High	$P_{CS} > 75\%$	$P_{MS} > 50\%$	PSE > 10-1	P > 85%
4 High	$50\% < P_{CS} \le 75\%$	$25\% < P_{MS} \le 50\%$	$10^{-2} < P_{SE} \le 10^{-1}$	65% < P ≤ 85%
3 Moderate	$25\% < P_{CS} \le 50\%$	$15\% < P_{MS} \le 25\%$	$10^{-3} < P_{SE} \le 10^{-2}$	45% < P ≤ 65%
2 Low	$10\% < P_{CS} \le 25\%$	$2\% < P_{MS} \le 15\%$	10-5 < PSE ≤ 10-3	15% < P ≤ 45%
1 Very Low	$2\% < P_{CS} \le 10\%$	$0.1\% < P_{MS} \le 2\%$	10-6 < PSE ≤ 10-5	P ≤ 15%

Likelihood						
	5	🟩 9	🟨 16	🟥 20	🟥 23	🟥 25
	4	🟩 7	🟨 13	🟨 18	🟥 22	🟥 24
	3	🟩 4	🟩 10	🟨 15	🟨 19	🟥 21
	2	🟩 2	🟩 6	🟨 11	🟨 14	🟨 17
	1	🟩 1	🟩 3	🟩 5	🟩 8	🟨 12
		1	2	3	4	5
		Consequence				

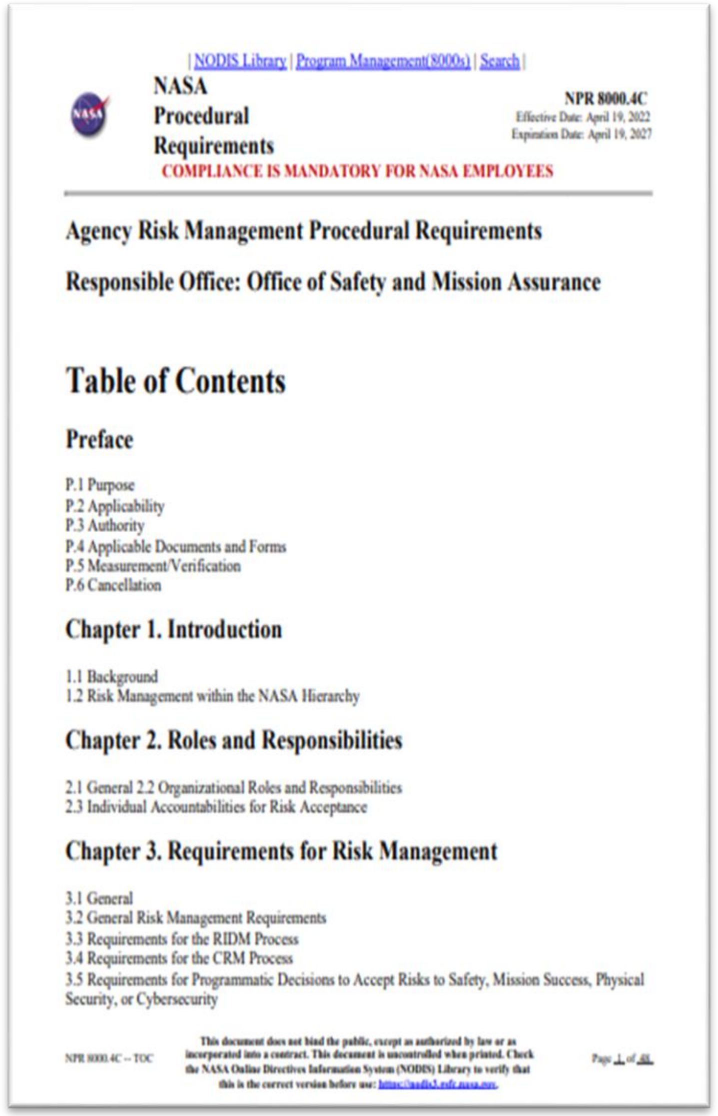
Consequence	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Cost	<2% increase over allocated and negligible impact on reserve	Between 2% and 5% increase over allocated and can handle with reserve	Between 5% and 7% increase over allocated and cannot handle with reserve	Between 7% and 10% increase over allocated, and/or exceeds proper reserves	>10% increase over allocated, and/or cannot handle with reserves
Schedule	Negligible schedule impact	Minor impact to schedule milestones; accommodates within reserves; no impact to critical path	Impact to schedule milestones; accommodates within reserves; moderate impact to critical path	Major impact to schedule milestones; major impact to critical path	Cannot meet schedule and program milestones
Mission Success	Negligible impact to full mission success criteria	Minor impact to full mission success criteria	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin	Major impact to full mission success criteria. Minimum mission success criteria is achievable	Minimum mission success criteria is not achievable
Safety	Negligible impact	Could cause the need for only minor first aid treatment	May cause minor injury or occupational illness or minor property damage	May cause severe injury or occupational illness or major property damage	May cause death or permanently disabling injury or destruction of property
Cybersecurity	Minimal adverse effect or minimal loss of Confidentiality, Integrity, or Availability of non-mission critical systems or data.	Low adverse effect or low lows of Confidentiality, Integrity, or Availability of mission or non-mission critical system or data.	Moderate adverse effect or moderate loss of Confidentiality, Integrity, or Availability of mission or non-mission critical systems or data.	High adverse effect or high loss of Confidentiality, Integrity, or Availability of mission or non-mission critical system or data.	Complete loss of Confidentiality, Integrity, or Availability of mission or non-mission critical system or data.

Will it make us look bad?

- All projects have risks, denial does not make them go away, it just makes you unprepared for them if they occur.
- Risk in itself is not bad, it is how well the project plans for and reacts to risks that counts.
- Formal risk management is a cornerstone of good project management. Stakeholder visibility into project risks makes it easier to get additional resources and organizational support when risks do occur.

Acknowledgements

This presentation was partly derived from the following sources:



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

NASA
Procedural
Requirements

NPR 8000.4C
Effective Date: April 19, 2022
Expiration Date: April 19, 2027

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

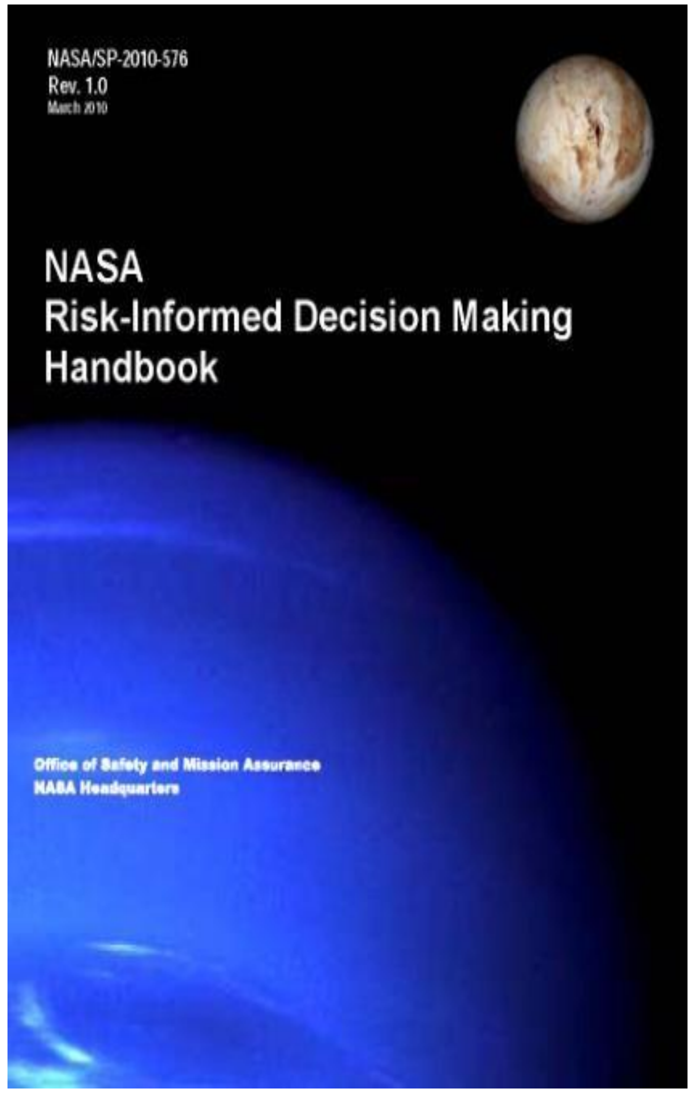
Table of Contents

NPR 8000.4C -- TOC

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 Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Page 1 of 48

NPR 8000.4C

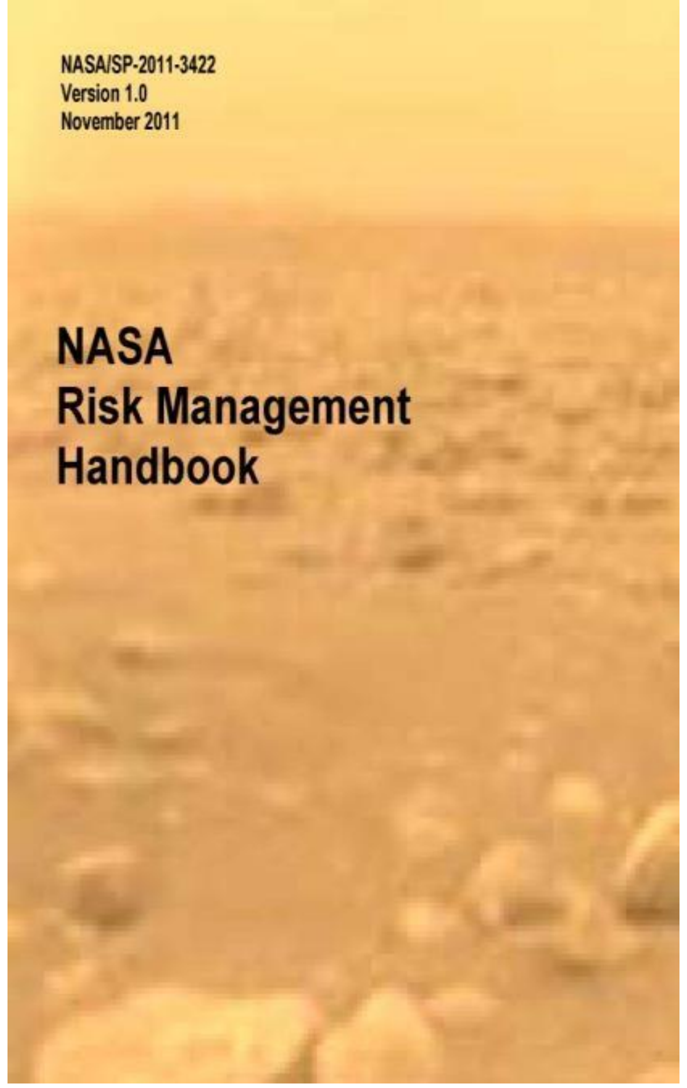


NASA/SP-2010-576
Rev. 1.0
March 2010

NASA
Risk-Informed Decision Making
Handbook

Office of Safety and Mission Assurance
NASA Headquarters

NASA/SP-2010-576



NASA/SP-2011-3422
Version 1.0
November 2011

NASA
Risk Management
Handbook

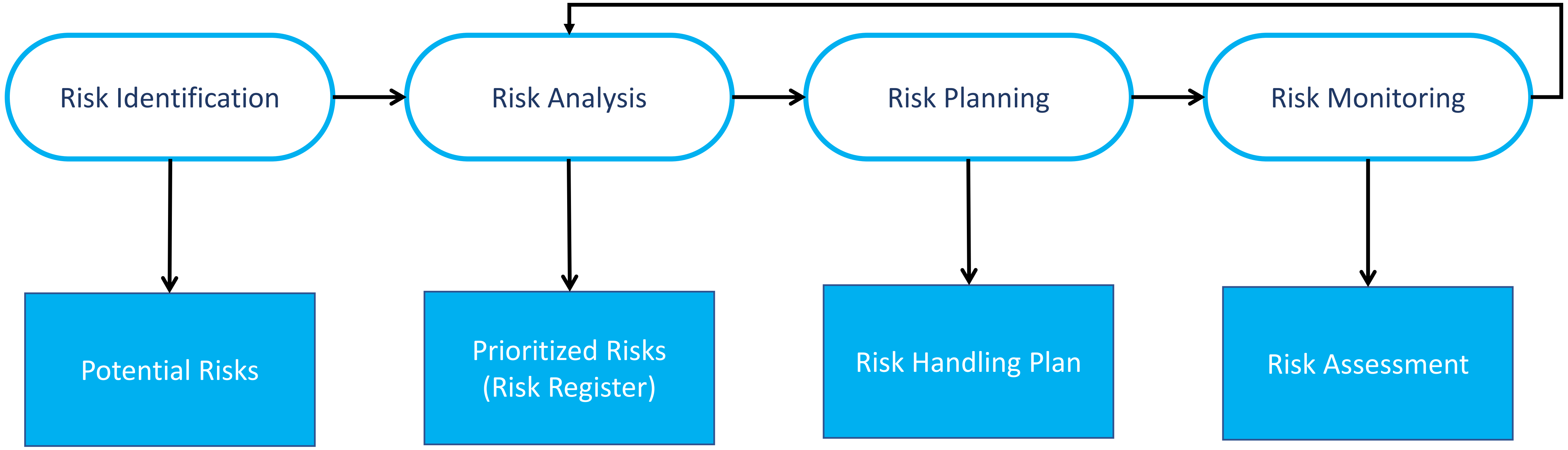
NASA/SP-2011-3422

Thank You

for the opportunity

to present to you today!

Risk Management Process



Risk Identification

Risk Analysis

Risk Planning

Risk Monitoring

Potential Risks

Prioritized Risks (Risk Register)

Risk Handling Plan

Risk Assessment

Risk Analysis

- **Assess probability, seriousness, and urgency of each risk**
  - **Probability may be low, moderate or high**
  - **Risk effect(s) may be catastrophic, serious, tolerable or insignificant**
  - **Urgency might be defined as immediate, short-term or long-term**

Analyzing Risk - Qualitative

- **Qualitative – the process of scoring or rating risk based on a team member's perception and/or experience**
  - **First step in risk analysis**
  - **Subjective**
  - **High, Medium, Low**
  - **Red, Yellow, Green**
  - **Prioritized/Ranked list of ALL identified risks**
  - **Top 10 risks**

Analyzing Risk - Quantitative

- **Quantitative – a more formal and systematic risk analysis approach to quantifying the risks**
  - **Numerical/Statistical Analysis**
  - **Determines probability of occurrence and consequences of risks**
  - **Should be focused to highest risks as determined by Qualitative Risk Analysis and Risk Threshold**

Risk Response

- **Planning**
  - **What are we going to do?**
  - **Strategies**
    - **Avoidance – Eliminate it**
    - **Transference – Elevate/Escalate risk**
    - **Mitigation – Reduce probability or impact**
    - **Acceptance – Do nothing or mitigate to a level of acceptance**
  - **Strategies should align with return on investment (ROI). Don’t spend more money mitigating a risk than the amount of impact a risk will have on the project.**

Monitoring Risks

- **Assess risks:**
  - **Regularly to determine handling plan impact, and whether it is working to burn down the risk**
  - **To determine if strategy plan is having the expected effect on the risk**
  - **To determine your Top 10 and most critical risks**
  - **To open new risks, and close or accept risks that have been reduced down to acceptable levels**