Aerospace Systems "A Risky Business" Understanding the Need for a Mature Risk Management Framework

NSBE Aerospace Systems Conference
August 2016

Prepared By:
Jeneene Suttle
Marshall Space Flight Center

Understanding the Need for a Mature Risk Management Framework

Purpose: To share basic risk management principles and philosophy, as well as, NASA approach to risk management procedures.

Background

Madelyn Jeneene Suttle

30 years of Aerospace/Technical Management experience with NASA including SMA Risk Manager, Export Control, Independent Assessments, System Safety, Environmental, Earned Value Management & Risk Management and Project Manager for Space Product Development

Training Objectives

After completing this training, you will be able to:

▸ Understand the general definition of risk

▸ Understand the Risk Management (RM) Philosophy

▸ Explain the importance of RM

▸ Perform risk identification, analysis, and mitigation
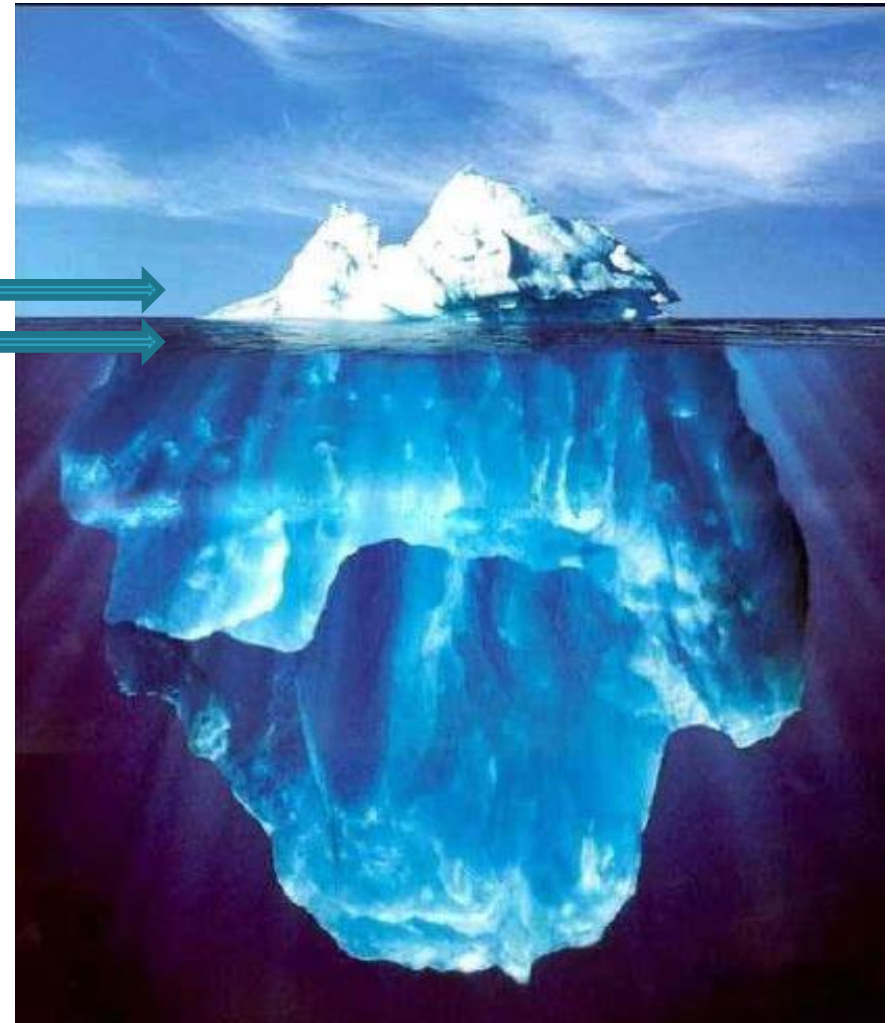
▸ Ability to communicate RM to others

What is Risk

- Risk is the intentional interaction with uncertainty.

- The likelihood of suffering a negative consequence.

Known

Unknown

What is Risk

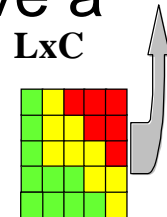▸ The potential inability to achieve success within defined cost, schedule, and technical constraints, measured using two components:

• The likelihood (or probability) of failing to achieve a desired outcome, and

LxC

• The consequence (or impact) of failing to achieve that desired outcome.

What is Uncertainty

▸ Uncertainty is a potential, unpredictable, and uncontrollable outcome; risk is a consequence of action taken in spite of uncertainty.

Risk vs Uncertainty

Risk

- Consequence of action taken in spite of uncertainty

- The effect of uncertainty on objectives)

- Risks are uncertainties that have an impact on the goals

- All risks are uncertainty

All risk are uncertainty that matter

Uncertainty

- Potential, unpredictable, and uncontrollable outcome

- Risks, Unknowns, Threats, Traps, Danger, Variables, Ambiguity, Gain and Opportunities

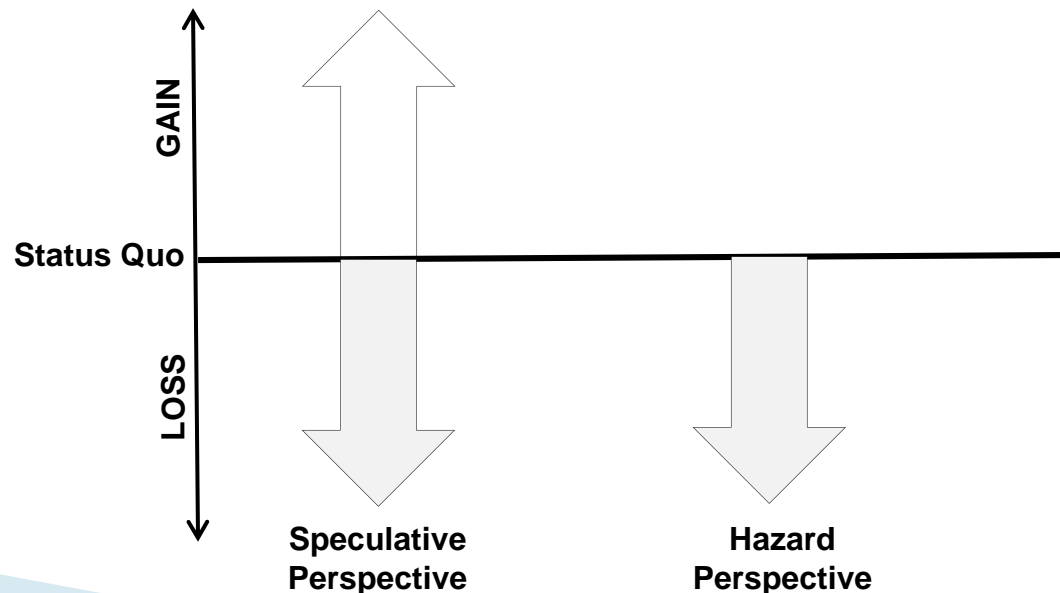- All uncertainties are not risks

Some uncertainties do not matter

Types of Risk

❑ Speculative
- Provides the potential for gain as well as the potential for loss
- Brings the potential to improve the current situation relative to the status quo

❑ Hazard
- Provides no opportunity to improve upon the current situation
- Brings only the potential for loss

9

Opportunity

❑ The likelihood of realizing a gain from an allocation or reallocation of resources
  - ▪ Defines a set of circumstances that provides the potential for a desired gain
  - ▪ Requires an investment or action to realize the desired gain (i.e., take advantage of the opportunity)

❑ Tactical opportunity provides a localized gain (e.g., to program or part of a program)

❑ Business opportunity is a gain for the organization

An opportunity is an uncertain event or condition that, if it occurs, will have a positive effect on one or more of the project objectives, such as cost, schedule and/or technical performance objectives.

What is Opportunity

Strategies for Identifying Opportunities

- ❑ **Strategies for identifying opportunities**: A number of strategies exist to help identify new opportunities and to give consideration to those that have been neglected because of perceived, but unexamined, risk. Some of these strategies include:

  - ▪ **Learning from the past**: While past experience cannot necessarily be a predictor of future performance, signals that were ignored, missed opportunities, and business surprises can provide insight into organizational blind spots

  - ▪ **Customer sensitivity**: Trying to understand customers in a way that the competition does not, and creating systems to exploit this information, can lead to great gains

  - ▪ **Learning from others**: The adage, "A wise person learns from experience, but a wiser person learns from the experience of others," holds as true in business as it does in life

  - ▪ **Scanning**: Active scanning of the business environment, potential competitors, or rival technologies is critical to successfully seizing opportunities and combating risk
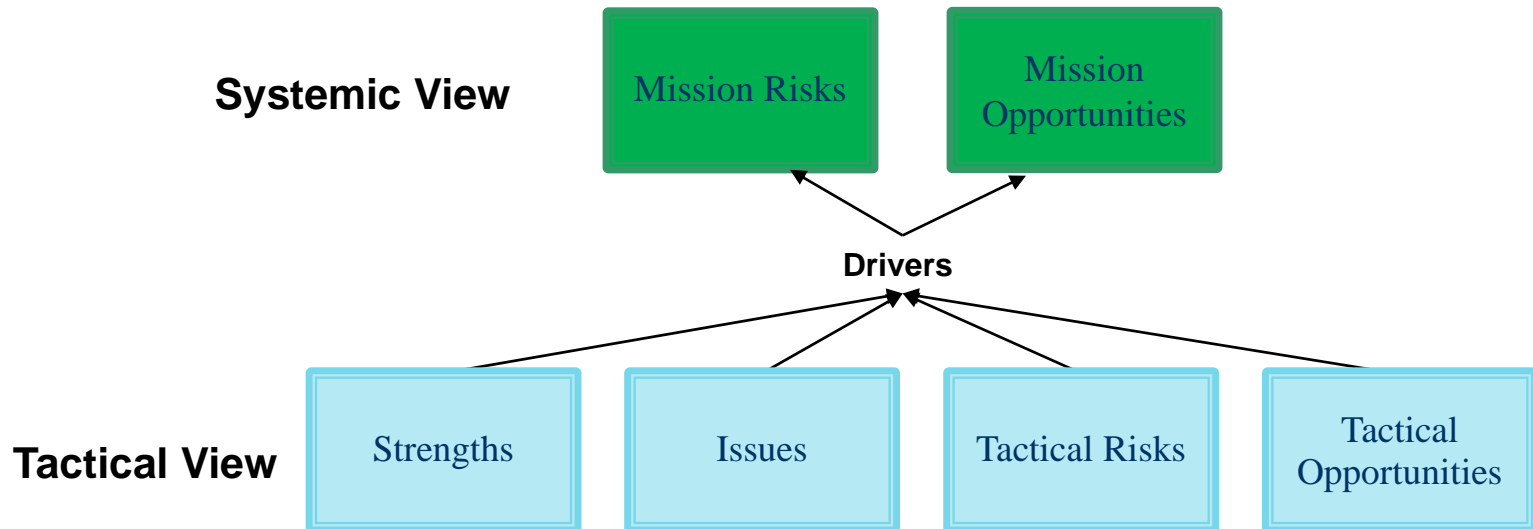
Integrated Risk and Opportunity Analysis

Systemic View

Mission Risks	Mission Opportunities

Drivers

Tactical View

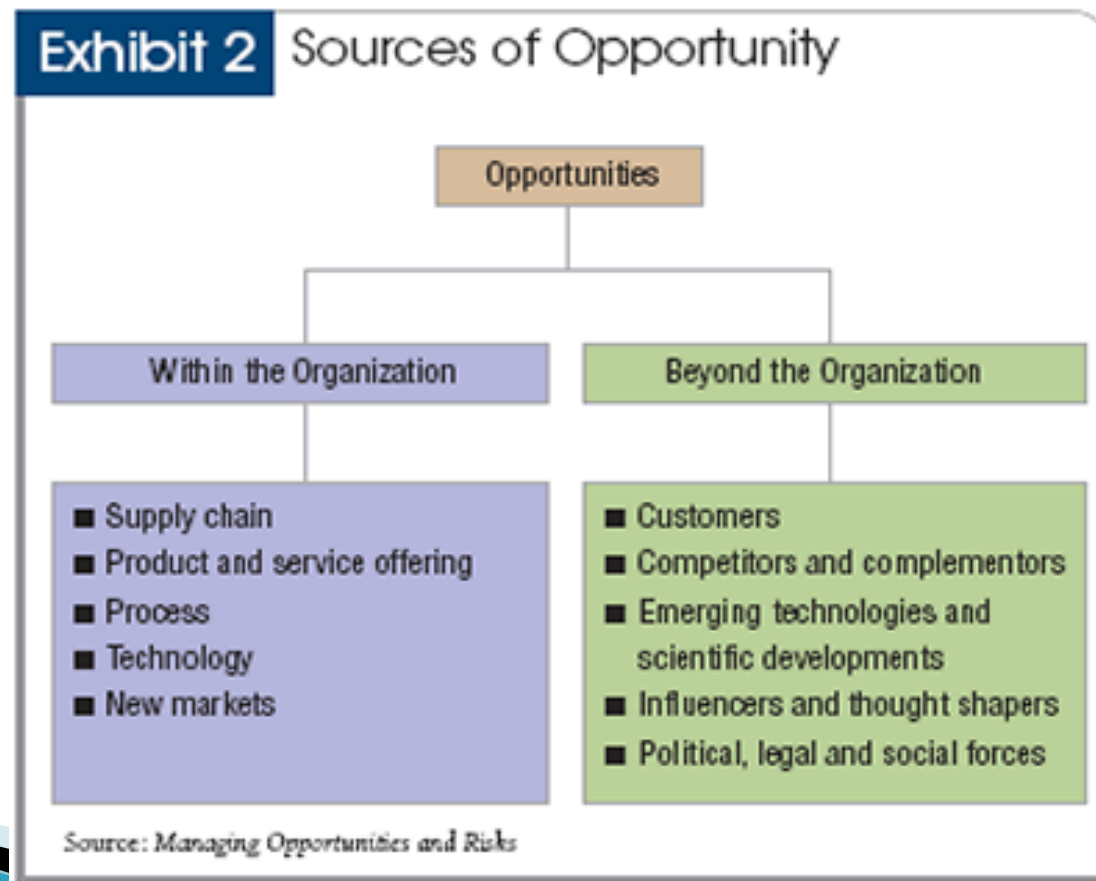| Strengths	Issues	Tactical Risks	Tactical Opportunities

- ❑ A mission risk is a circumstance that has the potential to cause loss from the business or mission perspective

- ❑ A mission opportunity is a circumstance that has the potential to provide a gain from the business or mission perspective

Sources of Opportunity

❑ **Sources of Opportunity**: Opportunities can arise from areas within the organization and externally, as illustrated in Exhibit 2.

Exhibit 2 Sources of Opportunity

Opportunities

Within the Organization

- Supply chain
- Product and service offering
- Process
- Technology
- New markets

Beyond the Organization

- Customers
- Competitors and complementors
- Emerging technologies and scientific developments
- Influencers and thought shapers
- Political, legal and social forces

Source: *Managing Opportunities and Risks*

Managing Opportunities

❑ Assessing, and potentially altering, the organization's risk appetite is a first step in managing opportunities related to risk.

❑ A program/project/organizational unit's risk appetite is heavily influenced by its culture and changes over time.

❑ Risk appetite should be defined and agreed upon at least annually, and ahead of assessing individual risks and opportunities.

❑ Sometimes shifting risk appetite is necessary to capturing opportunities. This shift can be accomplished by developing the capacity to accept more risk, thereby shifting the risk appetite boundary in Exhibit 3.

Exhibit 3 Risk Appetite Tolerance

UNMITIGATED RISK

ALTERED RISK APPETITE
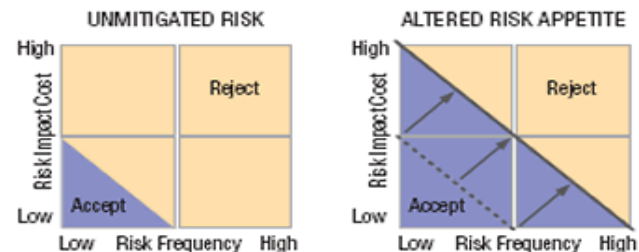
The diagonal line represents the company's risk appetite.

The diagonal line represents the company's risk appetite, shifted through experience, superior tools, etc.

Source: "A Building-Block Approach for Implementing COSO's *Enterprise Risk Management—Integrated Framework*," by Brian Ballou and Dan Heitger, *Management Accounting Quarterly*, Winter 2005.

Negative vs Positive

Risk

A risk is a circumstance that has the potential to cause loss from the business or mission perspective

Create a list the will block the path to success

Opportunity

A opportunity is a circumstance that has the potential to provide a gain from the business or mission perspective

Create a list the will enhance the path to success

The process of identifying, assessing, controlling, risks arising form operational factors and making decisions that balance the risk cost with mission benefit.

The identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[1] or to maximize the realization of opportunities.

Risk Management

Risk management refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.

According to ISO 31000 2009, the term risk management also refers to the architecture that is used to manage risk. This architecture includes risk management principles, a risk management framework, and a risk management process.

Risk Management

- A discipline and science that has developed processes, procedures and tools.
- A look at the future and the goal with focus on what really matters.
- Risk management's objective is to assure uncertainty does not deflect the endeavor from the goals.

❑ **<u>Risk & Opportunity Management Process</u>**: The risk and opportunity management process provides a model with tools and techniques to foster and manage innovation within the risk management context for improved decision making as illustrated in Exhibit 1.

❑ This model builds on the knowledge and systems already employed in other risk management tools to focus on risks and opportunities to create growth and innovation.

Exhibit 1 Risk & Opportunity Management Process

Source: Managing Opportunities and Risks
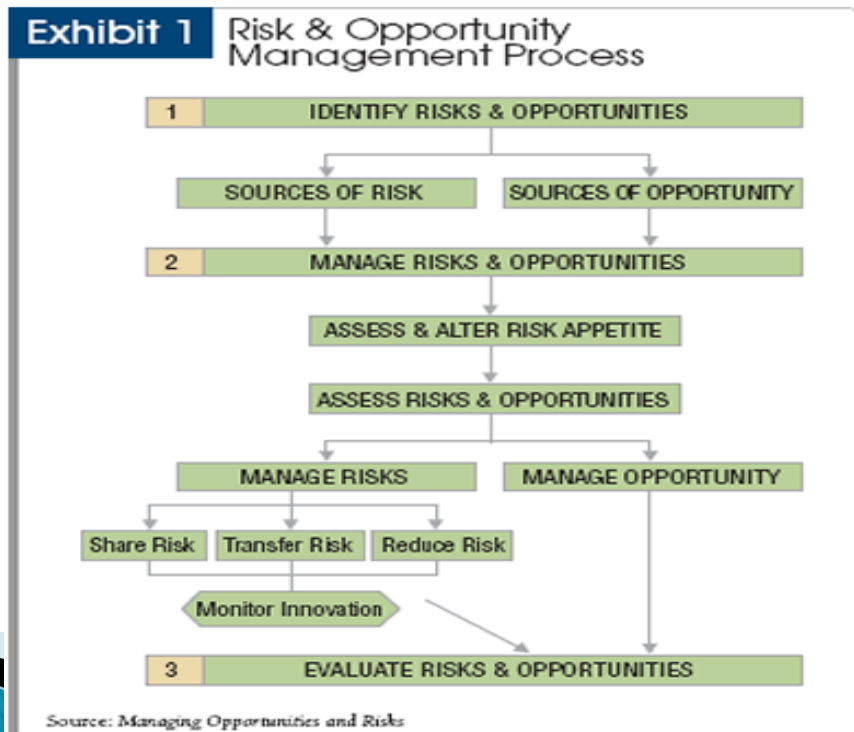
▸ Enterprise Risk Management (ERM) and Enterprise Risk and Opportunity Management (EROM) are synonymous terms used to address the natural desire of an organization to strike a reasonable balance between minimizing the potential for loss (risk) and maximizing the potential for gain (opportunity). These risks and opportunities are addressed within the context of implementing the organization's strategic goals.

Additional Governance and Tools

Risk Management Framework

Risk Management Policy

Risk Management Plan

Risk Management Flowchart

Risk Management Tools

Risk Management Metrics

- Surprises
- Stuff happens
  ◦ Nearly two thirds of all projects fail.

- Intuitive
- What really matters
  ◦ The difference between success and failure.
  ◦ Risk Management is too important not to do well!

Success vs Failure

- We must understand the Risk Level of the event or objective.
- Overall Program Risks are more than the sum of all risks.
- We think the process manages risks. People manage risk.
- We must understand risks and how people within the organization respond to risks.
- We can plan and monitor but **we must make decisions.**
- **We must understand both Risk Informed Decision Making and Continuous Risk Management.**

Columbia Accident Investigation Report (over 300 references to risks)

"There is great risk in placing human beings atop a machine that stores and then burns millions of pounds of dangerous propellants. Equally risky is having humans then ride the machine back to Earth while it dissipates the orbital speed by converting the energy into heat, much like a meteor entering Earth's atmosphere. No alternatives to this pathway to space are available or even on the horizon,
so we must set our sights on managing this risky process using the most advanced and versatile techniques at our disposal."

It all starts with the decisions we make and the uncertainty in those decisions

The first airplane fatality in history occurred September 17, 1908, when Lt. Thomas Selfridge was killed in a plane accident caused by propeller separation.

"All flight entails some measure of risk, and this has been the case since before the days of the Wright Brothers."

CAIB

One of the 300+ references to risks in the CAIB
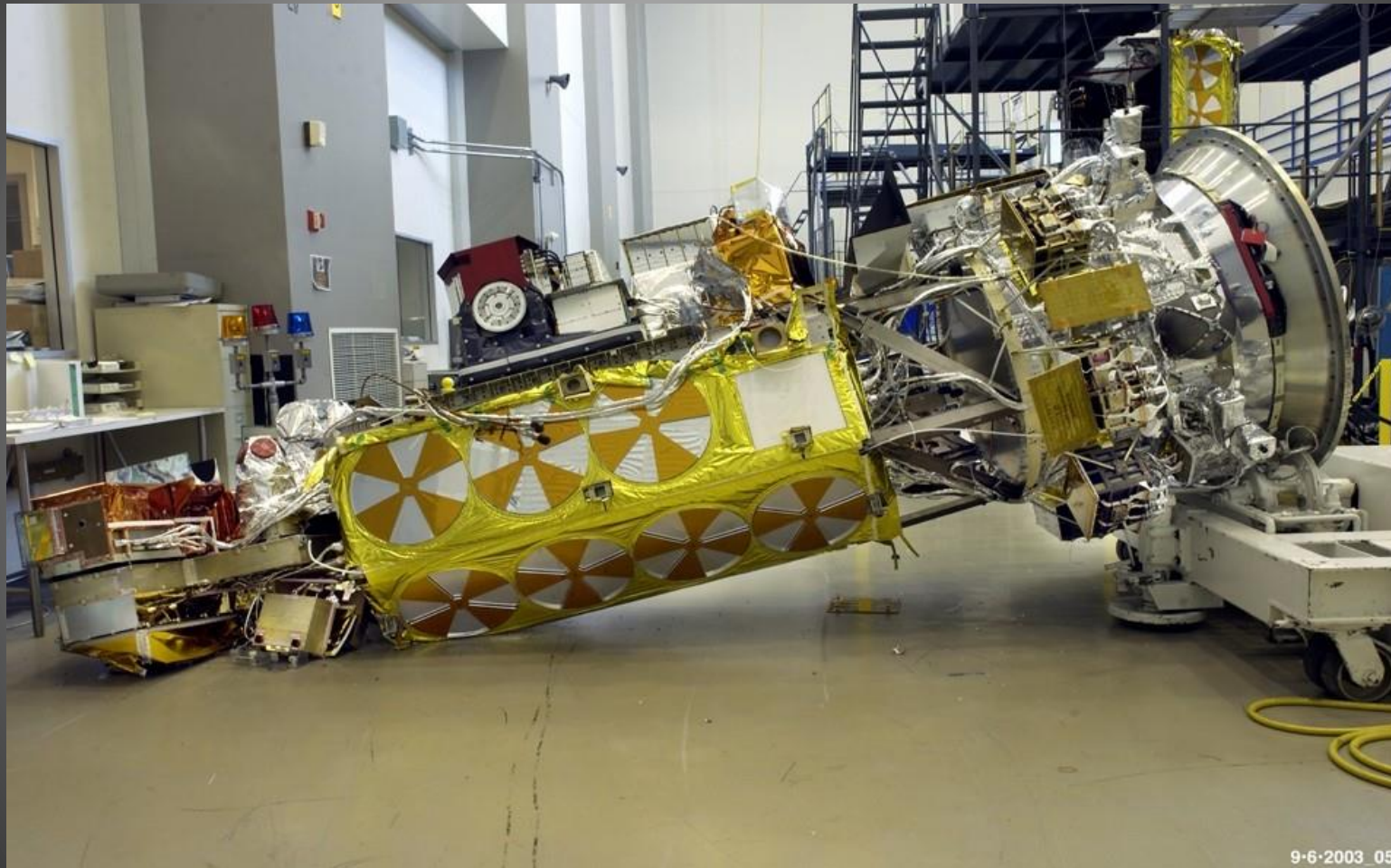
Risk Management Forum

Risk Management Forum

Risk Level vs Risk List

Implicit

‣ Risk Informed Decision Making (RIDM)

‣ To inform decision making through better use of risk information establishing requirements

Explicit

‣ Continuous Risk Management (CRM)

‣ To manage risk associated with the implementation of requirements

How Risky is the Program?	What are the Program Risks?

▸ The subjective judgment people make about the severity and probability of a risk, and may vary person to person. Any human endeavor carries some risk, but some are much riskier than others.

- Responses to risk or uncertainty are directed related to the people.

- Risk tolerance, attitude, awareness, assessment, assertion and acceptance effect the process.

- Pursuit of an opportunity can produce new risks or issues and/or change existing risks or issues.

◦ Stakeholders
◦ Partners
◦ Management
◦ Contractors
◦ NASA HQ
◦ Centers
◦ Program Offices
◦ Projects
◦ Teams
◦ Everyone

▸ People manage risks not Processes.

◦ Key Players

- Risk Manager: Shepherds the risk management process

- Risk Owner: Leads implementation of agreed-upon risk disposition or escalation

- Risk Initiator/Identifier: Identifies a potential risk concern

- Program Manager: Critical player in making decisions concerning resources

- Decision Maker: Makes risk-informed decisions

RIDM Functional Roles

❑ **Stakeholder** – An individual or organization that is materially affected by the outcome of a decision or deliverable but is outside the organization doing the work or making the decision.

❑ **Risk Analyst** – Applies probabilistic methods to the quantification of performance in the mission execution and institutional domains of safety, technical, cost, or schedule.

❑ **Subject Matter Expert** – An individual or organization with expertise in one or more topics within the mission execution domains of safety, technical, cost, or schedule.

❑ **Technical Authority (TA)** – The individuals within the technical authority process who are funded independently of a program or project and who have formally delegated TA traceable to the Administrator. The three organizations who have TA are Engineering, Safety & Mission Assurance, and Health and Medical.

RIDM Functional Roles (2)

❑ **Decision Maker** – A decision-maker is an individual with responsibility for decision-making within a particular organizational scope.

❑ **Risk Manager** – An individual with experience in risk and decision analysis and CRM who facilitates the implementation of RIDM and CRM, ensures staff members have adequate training, develops and maintains the RM Plan and other risk documentation, and coordinates RM matters with higher and lower-level organizations.

Risk Management

Two Complementary Processes for Risk Management

☐ **Risk-Informed Decision Making (RIDM)**
- ▪ To inform decision making through better use of risk information in establishing baseline performance requirements (e.g., safety, technical, cost, and schedule requirements) for program/projects and mission support organizations

☐ **Continuous Risk Management (CRM)**
- ▪ To manage risk associated with the implementation of baseline performance requirements

Risk Management

The RIDM Process Begins with Strategic Goals

❑ Within a organizational
hierarchy, high-level objectives
(Strategic Goals) flow down
in the form of progressively more
detailed performance requirements
whose satisfaction assures that
objectives are met

❑ RIDM is designed to maintain
focus on strategic goals as decision
are made throughout the hierarchy

In December 2014, the Journey to Mars took
a huge leap forward with Orion's first flight,
Exploration Flight Test-1.
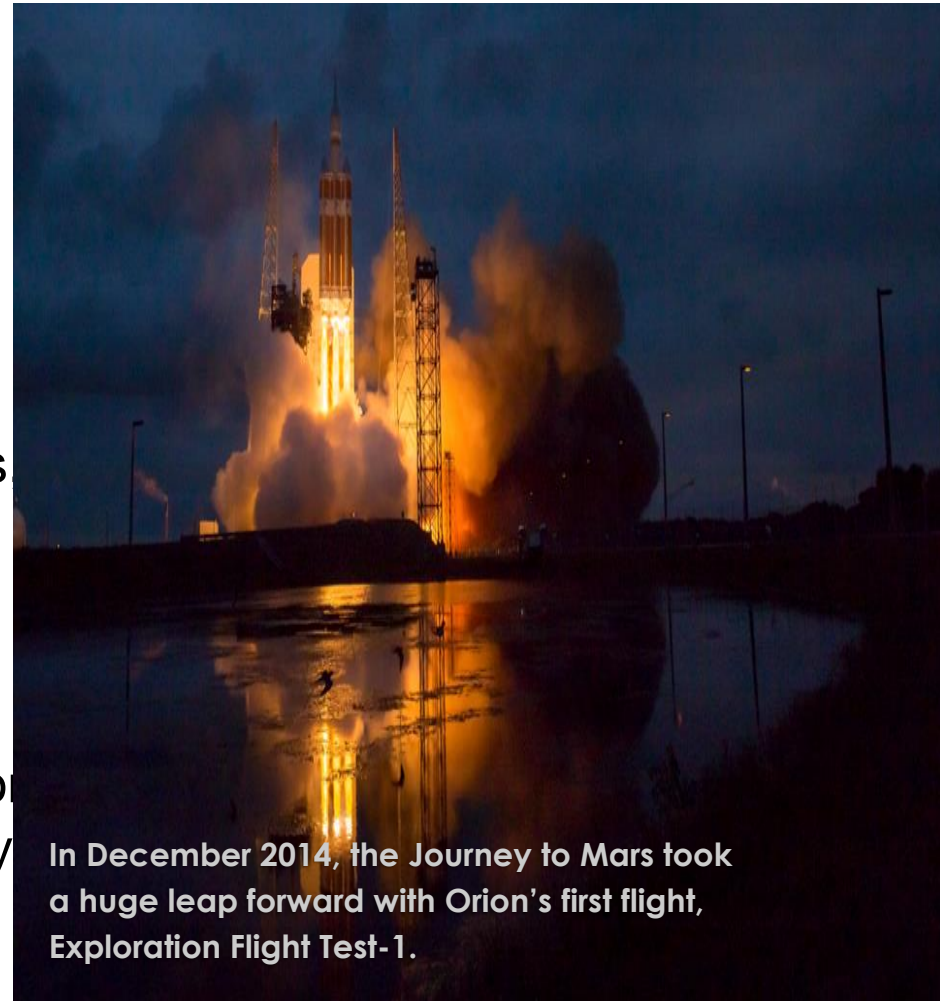
Risk Management

The Risk-Informed Decision Making (RIDM) Process

Risk-Informed Decision Making (RIDM)

Identification of Alternatives
Identify Decision Alternatives (Recognizing Opportunities) in the Context of Objectives

↓

Risk Analysis of Alternatives
Risk Analysis (Integrated Perspective) and Relative Ranking of Decision Alternatives

↓

Risk-informing Alternative Selection
Deliberate, Select an Alternative Informed by (*not solely based on*) the Risk Analysis Results and Set Baseline Performance Requirements

↓

To CRM

40

The RIDM Process

□ **Identification** of decision alternatives (decision context) and considering a sufficient number and diversity of Performance Measures to constitute a comprehensive set for decision-making purposes

□ **Risk analysis** of decision alternatives is defined as uncertainty analysis of performance associated with the alternative

□ **Selection** of a decision alternative informed by (not solely on) Risk Analysis results
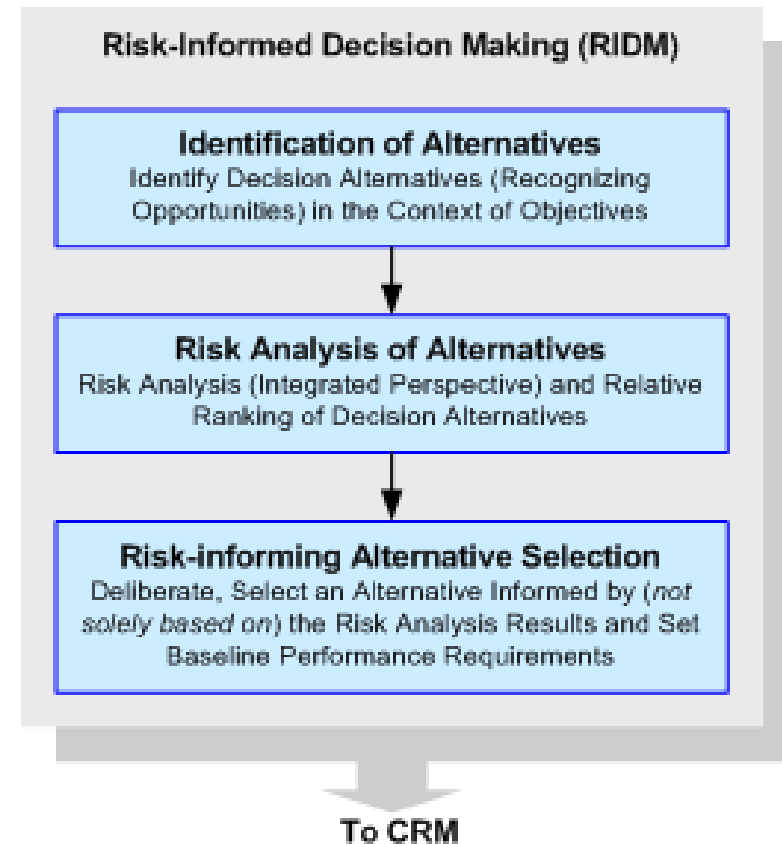
Risk-Informed Decision Making (RIDM)

Identification of Alternatives
Identify Decision Alternatives (Recognizing Opportunities) in the Context of Objectives

↓

Risk Analysis of Alternatives
Risk Analysis (Integrated Perspective) and Relative Ranking of Decision Alternatives

↓

Risk-informing Alternative Selection
Deliberate, Select an Alternative Informed by (*not solely based on*) the Risk Analysis Results and Set Baseline Performance Requirements

↓

To CRM

Risk Management

The Continuous Risk Management (CRM) Process

From RIDM

Continuous Risk Management (CRM)

Identify
Control
Analyze
Communicate
Document
Track
Plan

Steps in the CRM Process

Identify
Identify Risk Contributors (Shortfall in Performance Relative to Baseline Performance Requirements)

Analyze
Estimate Likelihood and Consequence Components of the Risk Through Analysis (Including Uncertainty Evaluation), Estimate Aggregate Risks if Feasible

Plan
Decide on Risk Disposition and Handling, Develop and Execute Mitigation Plan, and Decide What Will be Tracked

Track
Track Observables Relating to Performance Measures (e.g., performance data, schedule variance, etc.)

Control
Control Risk by Evaluating Tracking Data to Verify Effectiveness of Mitigation Plans. Make Adjustment to the Plans, and Execute Control Measures

CRM Feedback

Risk Management

Continuous Risk Management (CRM)

A systematic and iterative process that efficiently identifies, analyzes, plans, tracks, controls, and communicates and documents risks associated with implementation of designs, plans, and processes.

Source: NPR 8000.4A Agency Risk Management Procedural Requirements

What Does the CRM Risk Paradigm Represent?

NASA has adopted the CRM Risk Paradigm which represents a six step, methodical, process for identifying and managing risks.
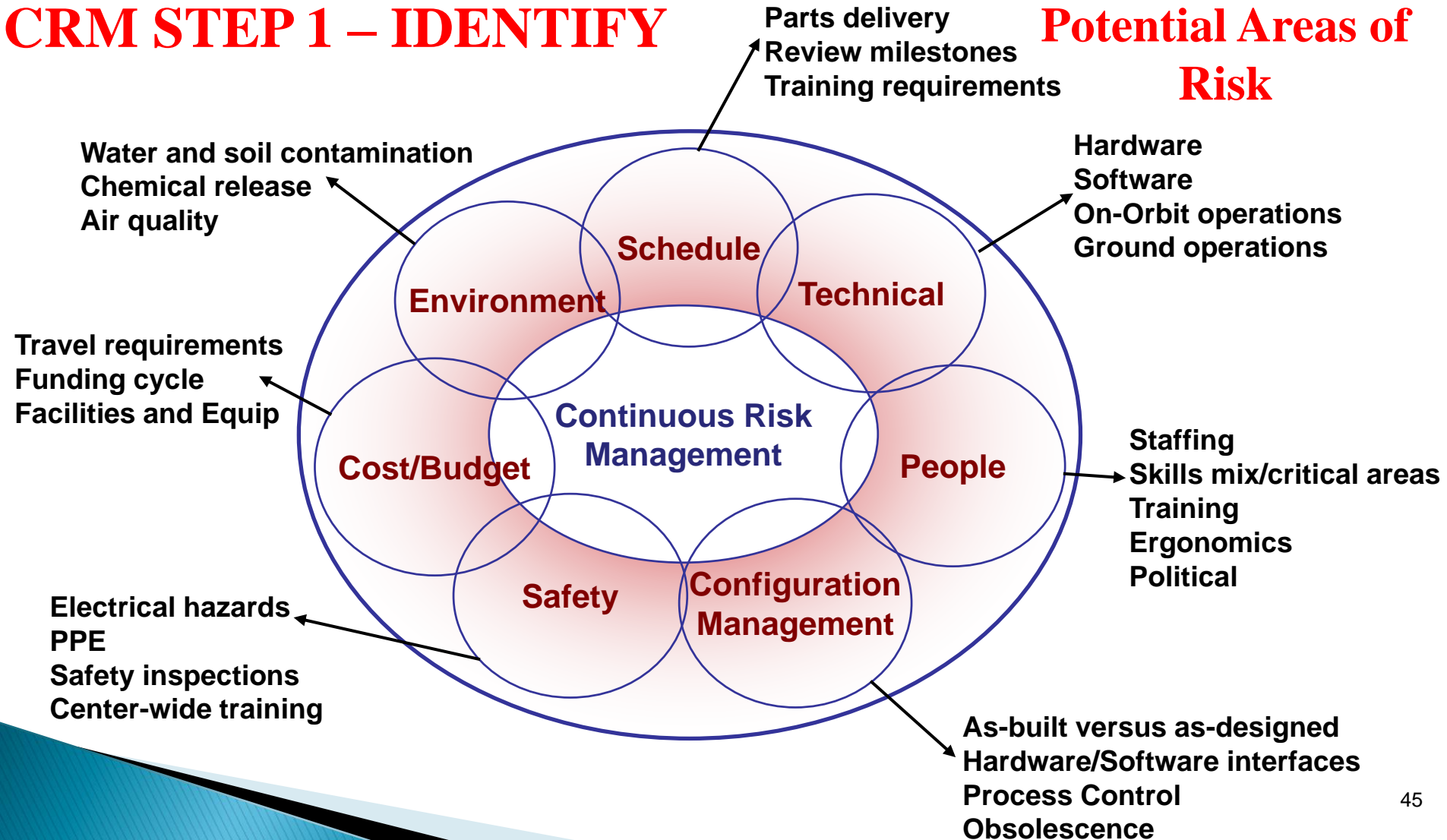
Risk Management

CRM STEP 1 – IDENTIFY

Potential Areas of Risk

Parts delivery
Review milestones
Training requirements

Water and soil contamination
Chemical release
Air quality

Hardware
Software
On-Orbit operations
Ground operations

Travel requirements
Funding cycle
Facilities and Equip

Schedule

Environment

Technical

Continuous Risk Management

Cost/Budget

People

Safety

Configuration Management

Staffing
Skills mix/critical areas
Training
Ergonomics
Political

Electrical hazards
PPE
Safety inspections
Center-wide training

As-built versus as-designed
Hardware/Software interfaces
Process Control
Obsolescence

45

Risk Management

CRM STEP 1 – IDENTIFY

Risk Statement

> ❑ Must be a Fact or perceived to be Fact
>
> ❑ Must be reality based

GIVEN → **CONDITION** → there is a **POSSIBILITY** that, → **CONSEQUENCE** **will occur.**

> ❑ Must have a Negative impact to the Condition
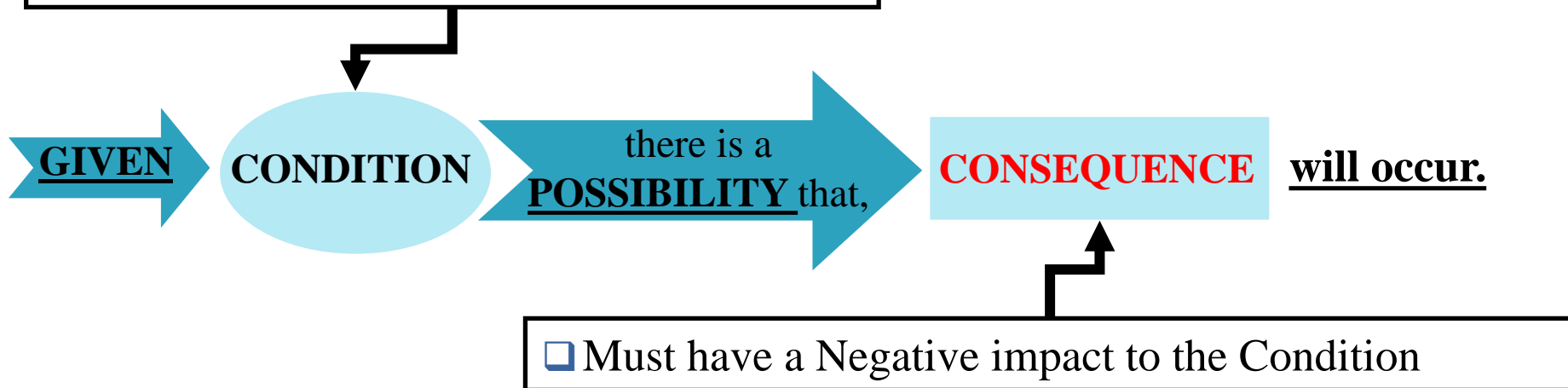
> The condition-consequence format is more concise and gets closer to an actionable statement that gets the risk management activity moving in the right direction. A good risk statement must be ACTIONABLE and have ONE condition and ONE consequence per statement. The "Risk Statement" should be 25 words or less.

CRM STEP 2 – ANALYZE (4)

Timeframe

❑ An estimate of the earliest time that the CONSEQUENCE can possibly occur so that mitigation can be accomplished sooner.

❑ Based on relevant documentation, including schedule information, and individual or group expert knowledge.

❑ Aids the prioritization of individual "risks" – near-term "risks" must be worked first.

TIMEFRAME	Near	Mid-Term	Far
	Less than four months of a Program Milestone	Between four to eight months of a Program Milestone	Between eight to twelve months of a Program Milestone

CRM STEP 4 - Plan

Decision	Rationale for Decision
Accept	A "risk may be accepted when: • It is not significant enough to justify expenditures • The Project is willing to accept the consequence • It meets the organizational unit's criteria for acceptance
Invoke a Contingency Plan	A contingency plan is invoked when a trigger has been exceeded or when some other related action needs to be taken. The "risk" and its mitigation plan continue to be tracked after the contingency plan has been executed
Mitigate	A new or modified plan is required when: • The threshold value has been exceeded • Analysis of the indicators shows that the action plan is not working • An unexpected adverse trend is discovered
Watch	No action is taken when the analysis of the tracking data indicates that all is going as expected and when the project personnel decide to continue tracking the "risk" or mitigation plan as before

Risk Management

Decision	Rationale for Decision
Research	More research is warranted when: • The uncertainty is so large that a reasonably robust decision cannot be made • The uncertainties can be reduced through research sufficiently to make a robust decision
Elevate	A "risk" decision should be elevated when: • The "risk" can no longer be controlled within the present organizational unit • The new or modified plan requires significant changes that affect multiple organizational units • A change in performance requirements may be required in order to retire a "risk"
Close	A "risk" is closed when it no longer exists or it is no longer cost-effective to track as a risk. This occurs when: • The probability has been reduced below a defined threshold • The impact has been reduced below a defined threshold • The "risk" has become a problem and is now tracked as such

Notional Risk Scorecard

LIKELIHOOD RATING

Level	Probability	
5	Very Likely	Expected to happen
4	Likely	Could happen. Controls have significant limitations or uncertainties.
3	Possible	Could happen. Controls exist, with some limitations or uncertainties.
2	Unlikely	Not expected to happen. Controls have minor limitations or uncertainties.
1	Highly Unlikely	Extremely remote possibility that it will happen. Strong controls in place.

RISK MATRIX

LIKELIHOOD / CONSEQUENCES

TIMEFRAME

Near	0 to 6 months
Mid	6 to 12 months
Far	> 12 months

Consequence Rating	Minor	Moderate	Significant	Major	Catastrophic
Level	1	2	3	4	5
SAFETY Health, Safety, Quality & Environment	-First aid incident or damage to minor asset - - Release to the environment causing insignificant to no impacts or damage to natural or cultural resources.	- Short-term injury, impairment or incapacitation. Minor damage to major asset or loss of minor asset. Minor OSHA violation - Release to the environment causing moderate impacts or damage to natural or cultural resources or a Regulatory warning.	- Long-term injury, impairment or incapacitation. Significant damage to major asset or loss of major asset. Moderate OSHA violation - Release to the environment causing significant impacts or damage to natural or cultural resources or a violation with minor fine.	- Permanent serious injury, impairment or incapacitation. Loss of major asset. Major OSHA violation - Significant release to the environment causing substantial impacts or damage to natural or cultural resources or a violation with major fine.	- May cause loss of life - Significant release to the environment causing irreparable impacts or damage to natural or cultural resources or violation resulting in loss of environmental permit
Mission Success/ Supportability (Human Capital, Facilities, Infrastructure)	Minor impact to programmatic and technical support, human capital, capability and diversity. Minor impact to facilities and infrastructure	Moderate impact to programmatic and technical support, human capital, capability and diversity. Minor impact to facilities and infrastructure	Significant impact to programmatic and technical support, human capital, capability and diversity. Significant impact to facilities and infrastructure	Major impact to programmatic and technical support, human capital, capability and diversity. Significant impact to facilities and infrastructure	Failure to meet customer requirements. Failure to meet major goal or objective
SCHEDULE	Minor milestone slip < 1 week: Critical Path slip 1 week	Minor milestone slip > 1 week to <1 month: Critical Path slip 1 week -1 month	Major milestone slip > 1 month to <2 months: Critical Path slip 1 - 2 months	Major milestone slip > 2 months: Critical Path slip 2 - 6 months	Cancellation of project due to schedule overruns
COST	< 1% increase of budget or < $100K increase	1-5% increase of budget or $100K to $1M increase	5-10% increase of budget or $1M to $10M increase	10-20% increase of budget or $10M to $50M increase	Cancellation of project due to budget overruns

CRM STEP 4 – TRACK
Tracking & Reporting on Risk Mitigation

- ❑ Risk mitigation plans are often broken down into specific actionable steps.
- ❑ Risk reduction associated with each step is evaluated and progress tracked over time.
- ❑ Best practice is to track both predicted and actual effect of each step as well as anticipated and actual data of step completion.
- ❑ Examples below show various methods of presenting this information
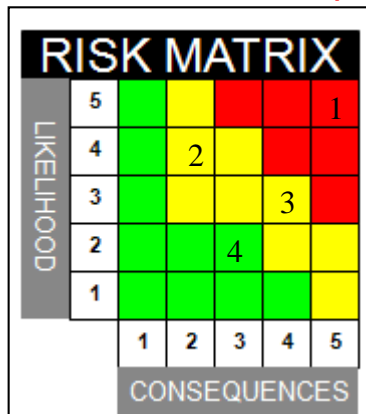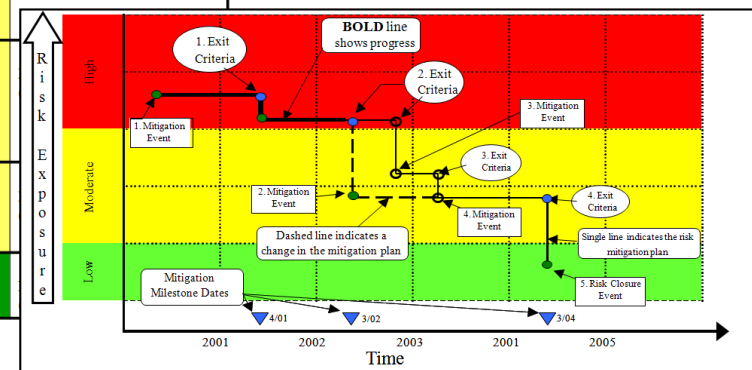
Risk Assessment Code (RAC)

Table Format

Timeline Waterfall Chart

Different Interpretations of Communication

If told to "Secure the building" …

▸ **The Army will establish a guard post and post sentries…**

▸ **The Marines will assault the building, capture the occupants, and set up a defensive perimeter…**

▸ **The Navy will turn out the lights, lock the doors and leave…**

▸ **The Air Force will take out a three year lease with an option to buy…**

▸ **NASA will form a committee to: conduct a study on how to word the Request For Proposal (RFP) & issue a contract to determine if the building is needed…**

CRM – Learning Points

❑ RIDM initializes CRM w/selected alternative and performance measures, constraints, thresholds, and requirements

❑ Step 1: **IDENTIFY**
- Risk Statements
- Risk Scenarios

❑ Step 2: **ANALYZE**
- Likelihood
- Consequence
- Uncertainty
- Timeframe

❑ Step 3: **PLAN**
- Accept
- Mitigate
- Close
- Watch
- Research
- Elevate

CRM – Learning Points

❑ Step 4: **TRACK**
- ▪ Continuously acquire and compile observable data for mitigated and watched "risks."
- ▪ Periodically run the risk analysis models with current data
- ▪ Periodically issue a Tracking Report

❑ Step 5: **CONTROL**
- ▪ Re-plan (go back to CRM Step #3)
- ▪ Close the "risk(s)"
- ▪ Invoke a contingency
- ▪ Continue tracking the "risk(s)"
- ▪ Elevate

❑ Step 6: **COMMUNICATE & DOCUMENT (throughout CRM)**
- ▪ Risk database (or list)
- ▪ Reporting to the next higher organizational level
- ▪ Cross-cutting "risks"
- ▪ Elevation of risk decision-making

Risk Management

➤ **Questions for Determining Risks and Escalating Risks:**

❑ **Trend: Does this issues or concern affect multiple organizations (horizontal/vertical)?**

❑ **Visibility: Does the mitigation require higher level decision maker(s) approval?**

❑ **Comfort Level: What is your comfort level in mitigating this risk?**

❑ **Comfort Level: What is your comfort level in accepting this risk?**

❑ **Resources: Do you require resources outside your authorization?**

❑ **Impact: Is there a potential impact other organizations (horizontal/vertical)?**
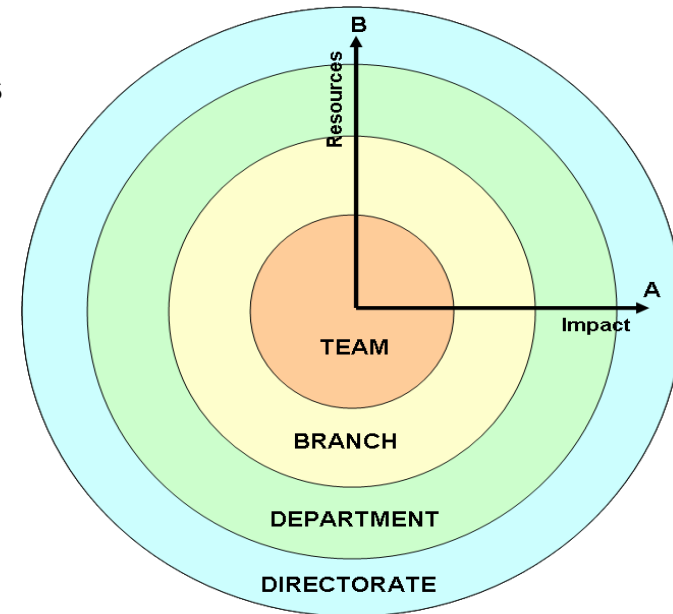
➤ **If Yes to one of the above :**

❑ **Risk must be escalated**

Note: This checklist can be utilized for Issues and Opportunities

Key Take-aways

- Most risks are below the surface; there are always indicators.
- Understanding our decisions helps us manage the uncertainty and identify the risks.
- RM process starts with understanding decisions and managing uncertainty from those decisions.
- RM is a structured process that ensures consistency and increases credibility to include planning, tracking & controlling your risks.
- Recognize that meeting objectives involves making decisions and decisions generate risks.
- Risk Management Plans are required for formal projects, very useful on others.
- Everyone is involved in managing risks.
- Make managing risks part of your job.
- Documentation and communication are essential parts of managing risks.
- Communicate your risks to all of your stakeholders.
- Risks have been and always will be with us.
- Understanding the program risks is just as important as understanding "how risky is the program".

Risk Management

References:

- ❑ Continuous Risk Management (CRM):
  - ▪ Software Engineering Institute (SEI) – Carnegie Mellon http://www.sei.cmu.edu/risk/
  - ▪ Office of Safety & Mission Assurance:
    - • Risk Management Training Course (STEP Level II): Course #SMA-Risk-OSMA-0016

- ❑ Risk Informed Decision Making (RIDM)
  - ▪ NASA/SP-2010-576, Version 1.0 April 2010: NASA Risk-Informed Decision Making Handbook
    - • http://www.hq.nasa.gov/office/codeq/doctree/NASA_SP2010576.pdf
  - ▪ Office of Safety & Mission Assurance:
    - • Risk-Informed Decision Making Training Course (STEP Level II): Course #SMA-Risk-OSMA-0013
    - • Enterprise Risk and Opportunity Management for Nonprofit Organizations and Research Institutions

- ❑ Risk & Opportunity Management :
  - ▪ Software Engineering Institute (SEI) – Carnegie Mellon http://www.sei.cmu.edu/risk/

- ISO 31000 Risk Management - The Free Dictionary - Wikipedia