



Understanding Risk

Key Concepts for Effective Risk Management

Presenter

Dr. Mary Skow – Agency Risk Management Officer, Headquarters

Value of Risk Management

- NASA can't operate without risk. Budgets, technology, environments and other factors introduce obstacles that companies must not only manage but overcome.
- Risk Management provides value by helping to identify, assess, prioritize, and manage risks that could impact goals, objectives, missions, and projects
 - Enabling better decision-making
 - Minimizing negative impacts of events and external implications
 - Increased financial performance
 - Demonstrates leadership increasing communication and stakeholder confidence
 - Ensuring compliance with rules and regulations

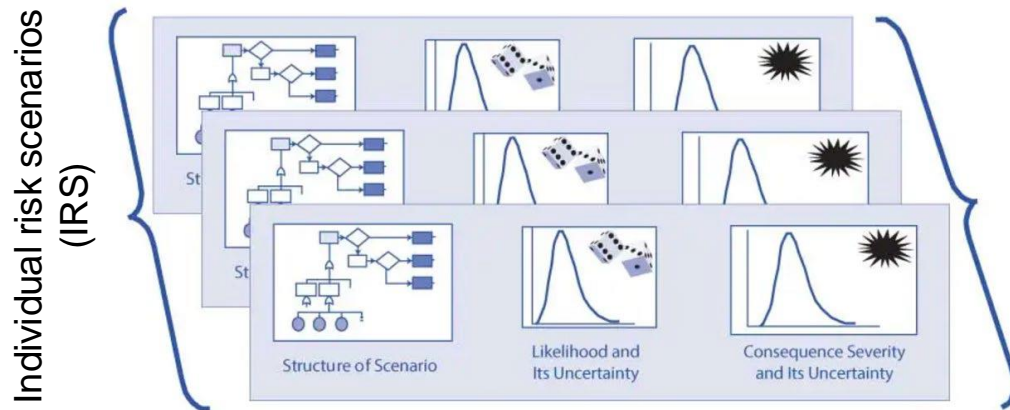
What is Risk?

Risk - The potential for shortfalls with respect to achieving explicitly established and stated objectives

- Risk is inherently **probabilistic**
 - **likelihood** that an organization's objectives will be met (or will continue to be met)
- Risk is **holistic**
 - **aggregate risk** to an organization's objectives from *all* causes
- Risk is **organization-specific**
 - Risk is defined with respect to an **organization's objectives**, Objectives -> requirements



Individual & Aggregate Risks



+ Individual risks

- + An individual risk is a scenario leading to degraded performance with respect to one or more performance measures
- + A scenario is a defined sequence of events, starting from an Initiating (Departure) Event, and leading after some set of pivotal events to an undesirable effect on a performance measure
- + Characterized by scenario, likelihood, and consequence

+ Aggregate risks (AR)

- + An aggregate risk is the accumulated effect of all relevant scenarios on the probability of not being able to meet a performance measure constraint value, target value, or other defined value or set of values
- + With inherent uncertainties in discovering or characterizing all significant individual risks, unknown and/or underappreciated (U/U) risk may also contribute to AR.
- + Produced by combining individual risks that threaten common objective or activity

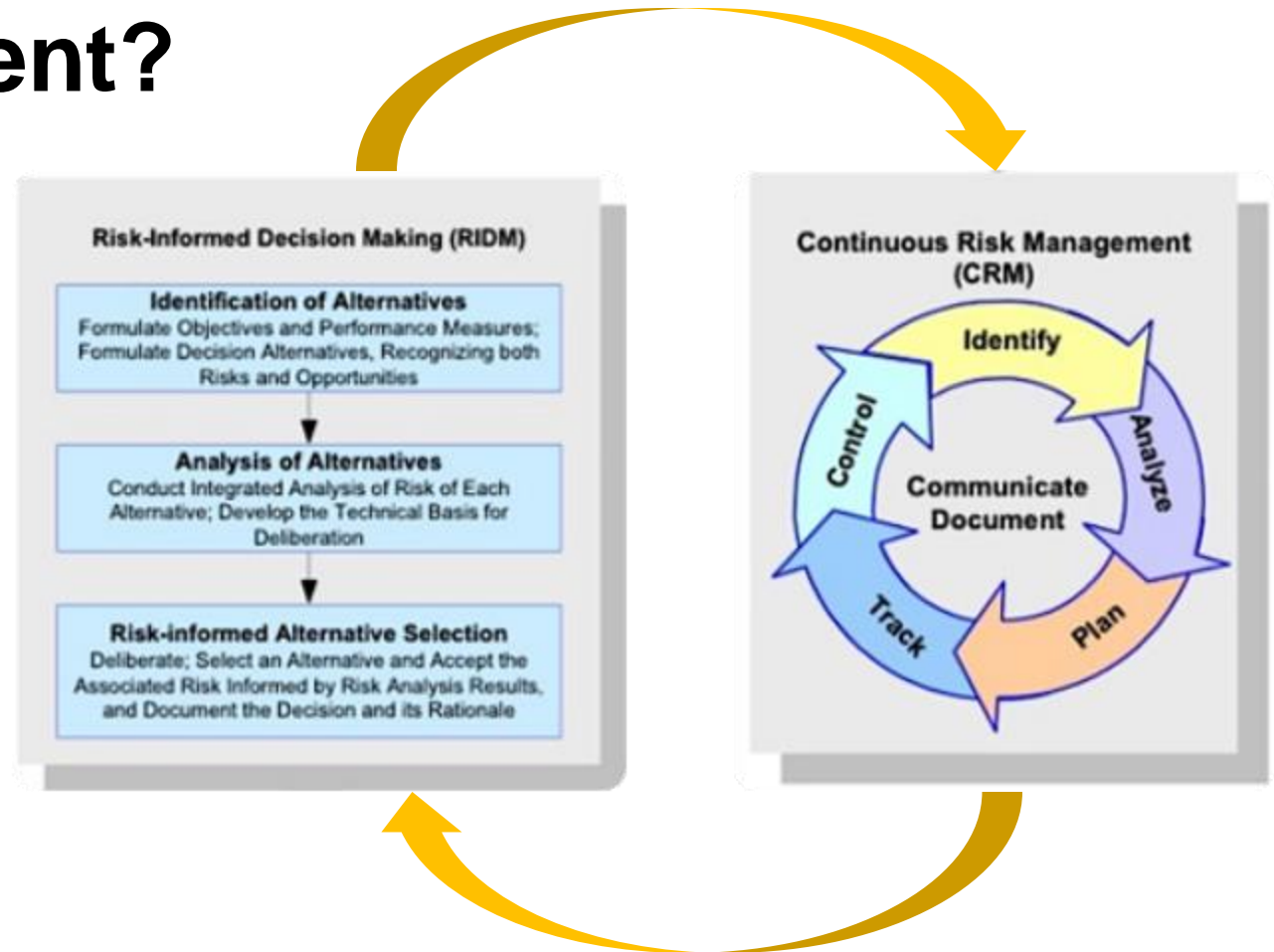
- Understanding contributors to AR provides a basis for prioritizing risk response decisions
- The ensemble of ARs across an activity's objectives constitute its risk profile. The acceptability of an activity's risk profile is based on whether it is within the risk posture

What is Risk Management?

- Risk management is a set of activities aimed at understanding, communicating, and managing risk to achieve a set of objectives
 - Applicable to all Agency activities directed toward the accomplishment of Agency strategic goals, including strategic planning and assessment; program and project concept development, formulation, and implementation; institutional management of infrastructure, including physical, human, and information technology resources; and acquisition
- Risk management includes risk-informed decision making (RIDM) and continuous risk management (CRM) in an integrated framework

What is Risk Management?

- + **Risk-informed Decision Making (RIDM)**
 - + To inform decision making through better use of risk information and establishes baseline performance requirements for program/projects and mission support organizations
- + **Continuous Risk Management (CRM)**
 - + To manage risk associated with the implementation of baseline performance requirements
 - + Keeping the potential for performance shortfalls within tolerable limits



Key Risk Management Principles

- Objectives-Driven
- Implement a Philosophy of Risk Leadership
- Conducted Throughout the Life Cycle of an Activity

Note: Additional NASA RM Principles are in back up, with complete set found on the ARMO website: [Risk Management Principles Consistent With NPR 8000.4C](#)

Objectives Driven Risk Management



An approach to risk management that focuses on ensuring that a program's / project's / Organization's risk profile is aligned with the established objectives and within the established risk posture.

NASA's 2022 Strategic Plan Themes, Strategic Goals, and Strategic Objectives

Vision: Exploring secrets of the universe for the benefit of all

Mission: NASA explores the unknown in air and space, innovates for the benefit of humanity, and inspires the world through discovery



Discover

Strategic Goal 1: Expand Human Knowledge through new scientific discoveries

- 1.1 Understand the Earth system and its climate
- 1.2 Understand the Sun, solar system, and universe
- 1.3 Ensure NASA's science data are accessible to all and produce practical benefits to society



Explore

Strategic Goal 2: Extend human presence to the Moon and on towards Mars sustainable long-term exploration, development, and utilization

- 2.1 Explore the surface of the Moon and deep space
- 2.2 Develop a human spaceflight economy enabled by a commercial market
- 2.3 Develop capabilities and perform research to safeguard explorers
- 2.4 Enhance space access and services



Innovate

Strategic Goal 3: Catalyze economic growth and drive innovation to address national challenges

- 3.1 Innovate and advance transformational space technologies
- 3.2 Drive efficient and sustainable aviation



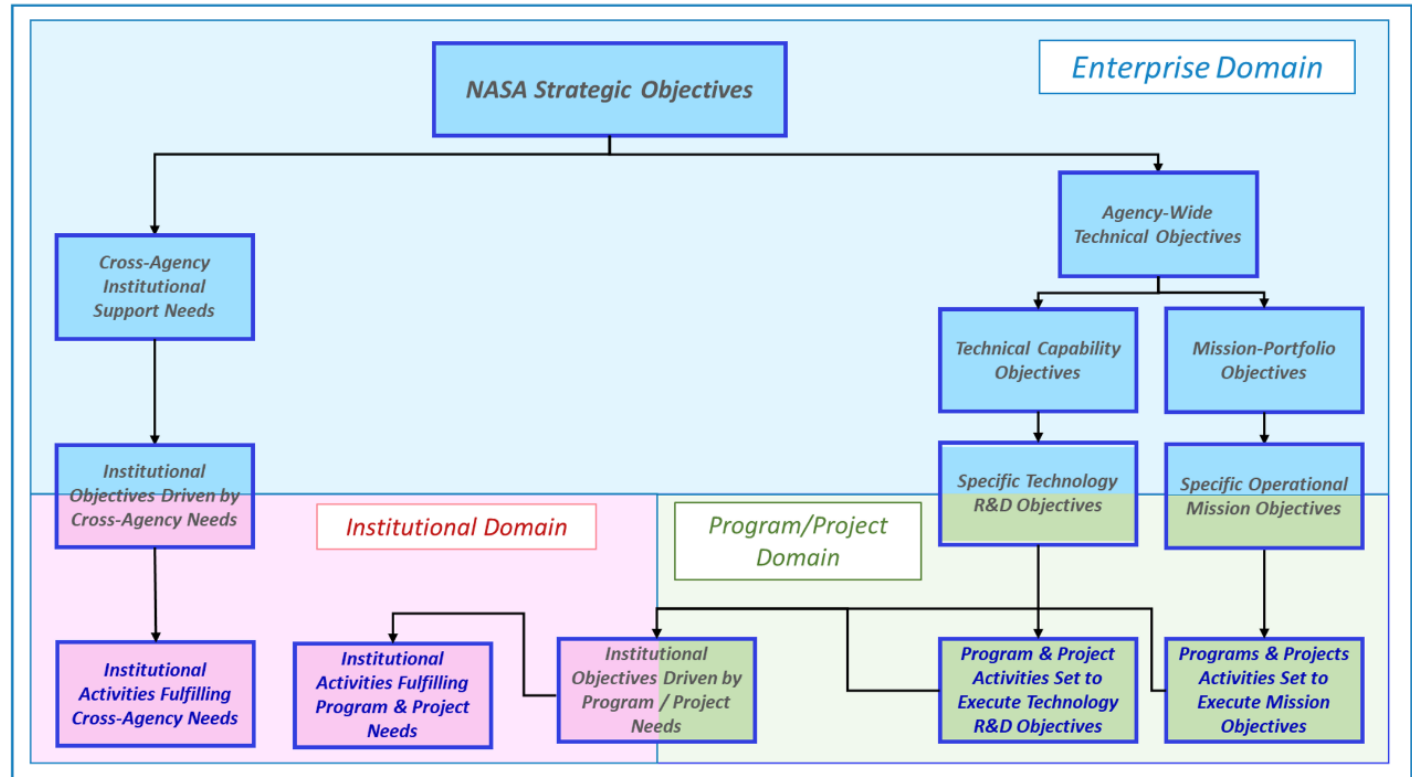
Advance

Strategic Goal 4: Enhance capabilities and operations to catalyze current and future mission success

- 4.1 Attract and develop a talented and diverse workforce
- 4.2 Transform mission support capabilities for the next era of aerospace
- 4.3 Build the next generation of explorers

Objectives-Driven Risk Management

- Each organization's objectives flow down from NASA's strategic objectives
- NASA's organizations and objectives fall into domains of:
 - **Enterprise** - Strategic programmatic and cross-Agency objectives
 - **Program/project** – Technology R&D and operational mission objectives
 - **Institutional** – Supporting cross-Agency and Program/project objectives



Objectives-Driven Risk Management

The risk management effort of each NASA organization should be focused on managing the risk to that organization's **top-level objectives**

- Top-level **Enterprise objectives** typically fall into domains such as:
 - Strategic
 - Reputational
 - Compliance
 - Operations
- Top-level **Program and project objectives** typically fall into domains such as:
 - Mission technical
 - Cost
 - Safety
 - Schedule
- Top-level **Institutional organization objectives** typically fall into domains such as:
 - Staffing
 - Facility safety
 - Facility availability
 - Cybersecurity
- Top-level objectives define the **fundamental purposes** of the organization rather than any means of achieving those purposes

Implement a Philosophy of Risk Leadership

Risk Leadership – Leading, by an accountable leader, risk acceptance decision-making within the limits of a defined risk posture, including the authority to allocate portions of the risk posture to subordinate / supporting organizations

Goal of risk leadership is to increase ‘decision velocity’ within a risk posture

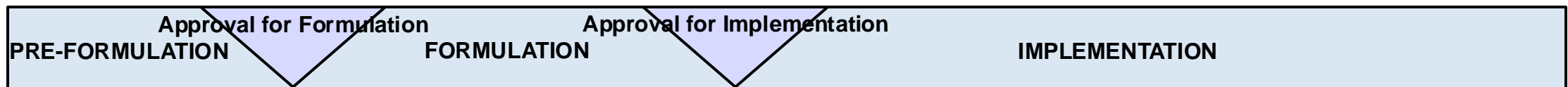
- Risk leadership entails:
 - Exercising risk management authority within an established **risk posture** consisting of **acceptable levels of risk** to the organization’s **top-level objectives**
 - Flowing down the risk posture (and associated risk management authority) to subordinate organizations, in tandem with the flow-down of objectives to those organizations
- Risk posture defined early in an activity, **in tandem with the baselining of the organization’s objectives**
 - Supports mutual understanding and defines decision space for subordinate organizations

Risk Posture – The limits of acceptable risk to the established / stated objectives whose achievement is of direct concern to stakeholders.

Conducted Throughout the Life Cycle of an Activity

- Direction-setting decisions should be risk-informed, since they determine the risks that the organization will face
- This is captured in the formulation, $RM = RIDM + CRM$
 - Risk-informed Decision Making (RIDM): Making sure that decisions are made with an understanding of the risks associated with each decision alternative
 - Continuous Risk Management: Making sure that the risks associated with the selected alternative are within the organization's established risk posture
 - E.g.,:

Activity Life Cycle



Emphasis is on RIDM

Ensuring that direction-setting decisions are risk-informed

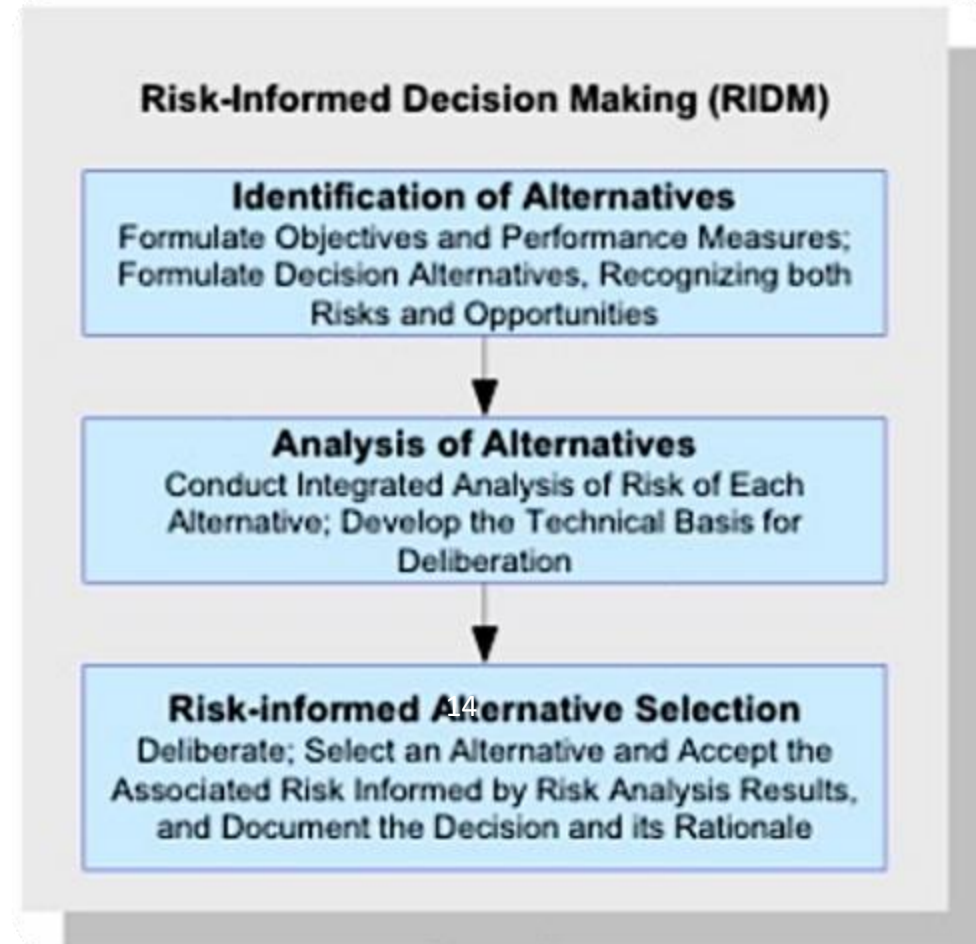
Emphasis is on CRM

Ensuring that the risk profile is within the risk posture

Risk-Informed Direction-Setting Decisions

RIDM consists of three parts:

- Identification of Alternatives
- Analysis of Alternatives
- Risk-Informed Alternative Selection

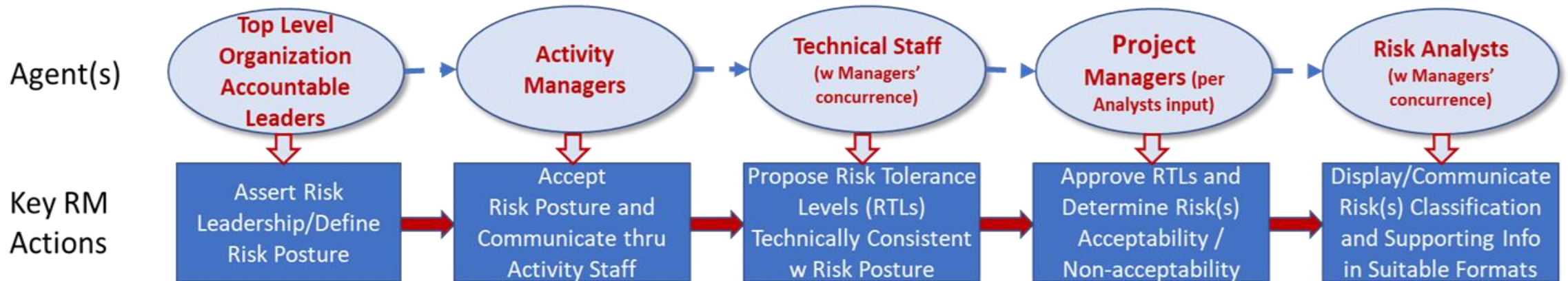


Risk Leadership

- + Organization top level defines strategic and programmatic objectives
- + Top level expresses amount of risk that is acceptable across objectives (risk posture)
- + Objectives and risk posture flow down to individual projects and activities

Objectives-Driven Risk Management

- + Objectives defined and assigned at all organizational levels
- + Objectives quantified via performance measures, goals (targets) and/or requirements
- + Risks assessed and managed based on potential impact to objectives



Successful Risk Leadership and Objectives Risk Management

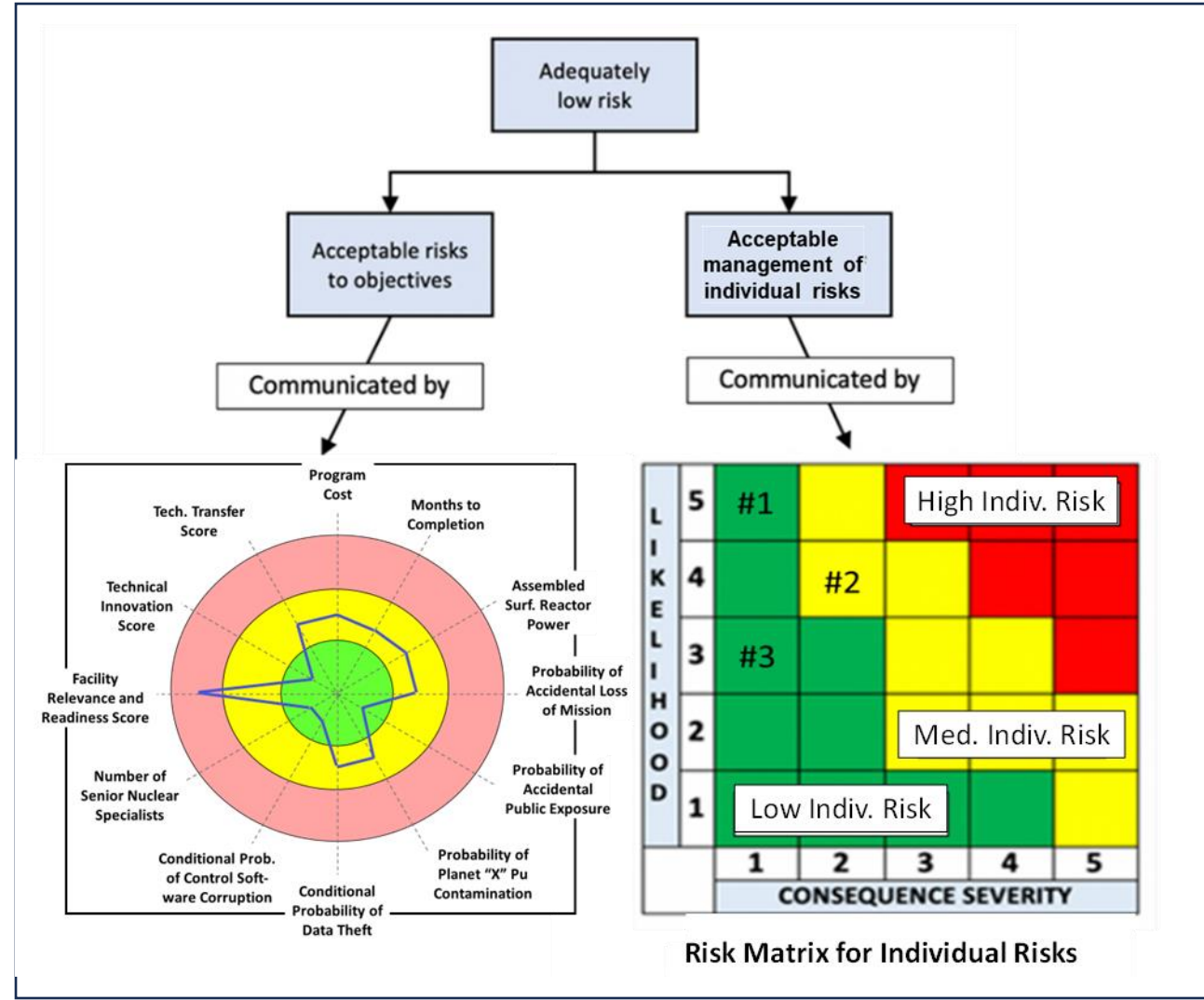
- Full commitment by managers and leaders at all levels
- Clear identification of strategic and organizational objectives
- Clear articulation and communication of risk posture in relation to the identified organizational objectives, to managers and staff at all levels of the organization
- Willingness to take-on and accept risk in activities / projects with potential high benefit returns
- Risk assessment and management practices geared toward:
 - objectively-based decision-making
 - balanced handling of individual and aggregate risks affecting the declared strategic and organizational objectives
 - formulation and implementation of effective organizational internal controls
- Effective protocols for upward and cross-organizational communication of risk management challenges, to enable the identification and effective handling of cross-cutting risks



Communication of Risk

Communication of Risk

- Risk management involves the management of both “individual risks” and “risks to objectives”
- Individual risks are traditionally displayed on a risk matrix that shows the likelihood and consequence severity of specific risk scenarios (right-hand chart)
- Risks to objectives are determined by aggregating individual risks to evaluate the cumulative effect of the scenarios on a set of performance measures (left-hand chart, with details on next slide)
- The performance measures are selected in advance to serve as quantitative surrogates for the objectives



Example Risk Matrix and Definitions

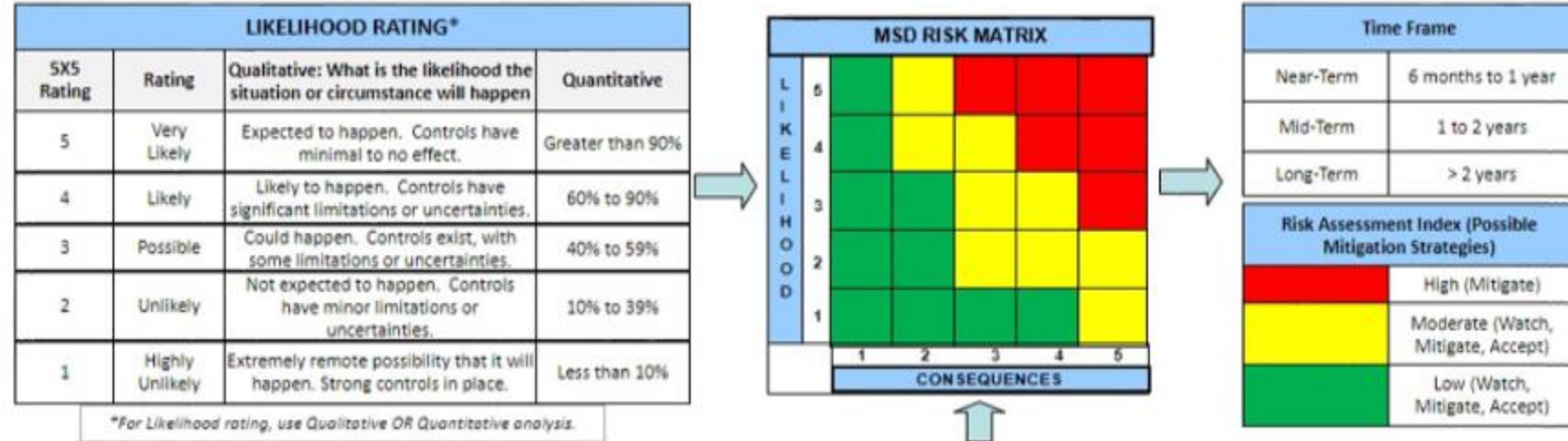
Human System Risk Board Risk Matrix and Definitions

		LIKELIHOOD RATING			L x C Matrix						Time frame Expected Need for Mitigation			
		In-Mission	Flight Recertification	Long Term Health	LIKELIHOOD	5	10	16	20	23	25	Near	0 < 2 Years	
5 Very High	More likely to happen than not during the mission or probability (P) >10%	Very likely to happen. Controls are insufficient or P > 10%	Likelihood is very high OR >10% excess risk	4		7	13	18	22	24	Mid	2-7 Years		
	Likelihood is during the mission or 1% < P ≤ 10%	Likely to happen. Controls have significant limitations or uncertainties or 1% < P ≤ 10%	Likelihood is high OR 6-10% excess risk	3		4	9	15	19	21	Far	> 7 Years		
4 High	Likelihood is during the mission or 0.1% < P ≤ 1%	Not likely to happen. Controls exist with some limitations or uncertainties or 0.1% < P ≤ 1%	Likelihood is moderate OR 3-6% excess risk	2		2	6	11	14	17				
	Unlikely to happen during the mission or .01% < P ≤ 0.1%	Not expected to happen. Controls have minor limitations or uncertainties or 0.01% < P ≤ 0.1%	Likelihood is low OR 1-3% excess risk	1		1	3	5	8	12				
3 Moderate	Nearly certain to not occur in-mission or P ≤ 0.01%	Extremely remote possibility that it will happen. Strong controls in place or P ≤ 0.01%	Likelihood is very low OR < 1% excess risk											
					1	2	3	4	5					
					CONSEQUENCE									
					1		2		3		4		5	
IN MISSION	Crew Health Impact	Temporary discomfort	Minor injury/illness that can be dealt with by crew without ground support, minor crew discomfort	Significant injury/illness or incapacitation that requires diagnosis and/or treatment support from ground, may affect personal safety	Critical injury/illness of one crew member requiring extended medical intervention and support, may result in temporary disability	Death or permanently disabling injury/illness affecting one or more crewmember (LOCL/LOC)								
	Mission Objectives Impact	Insignificant impact to crew performance and operations – no additional resources required	Minor impact to crew performance and operations – requires additional resources (time, consumables)	Significant reduction in crew performance, threatens loss of a mission objective	Severe reduction of crew performance that results in loss of multiple mission objectives	Loss of mission due to crew performance reductions or loss of crew								
FLIGHT RECERT	Crew Flight Recertification Status	Immediate flight recertification status	Flight recertification status within 3 months with limited intervention	Flight recertification status within 1 year with nominal intervention or restricted flight status	Flight recertification status requires extended medical intervention and takes > 1 year	Unable to be Recertified for Flight Status, premature career end								
LONG TERM HEALTH	Health Outcomes	Career related short term self-resolving medical conditions	Career related medical conditions manageable with outpatient medical treatments	Treatable career related medical condition that requires hospitalization for management	Chronic career related medical condition requiring intermittent hospitalization or nursing care	Career related premature death or permanent disability requiring institutionalization								
	Quality of Life	No impact on quality of life OR independence in activities of daily living	Minor, short-term impact on quality of life OR rare support required for activities of daily living	Moderate long-term impact on quality of life OR may require some time-limited support for activities of daily living	Major long-term impact on quality of life OR requires intermittent support for activities of daily living	Chronic debilitating impact on quality of life OR requires continuous support for activities of daily living								

LXC Likelihood and consequence.



Example Risk Matrix and Definitions



		Very Low	Low	Moderate	High	Very High
		1	2	3	4	5
Health, Safety, Environment (HSE)	Injury	Minor injury	Short-term Injury or illness	Injury or illness Resulting in Days Away from Work OR Hospitalization	Injury or illness Resulting in Permanent Partial Disability OR Hospitalization of 2+ People	Injury or illness Resulting in a Fatality OR Permanent Total Disability
	Property Damage	<\$20K	\$20K to \$50K	>\$50K to \$500K	\$500K to <\$2M	≥\$2M
	Compliance, Environment	Negligible impact to compliance; or Minor or Non-Reportable Hazard or incident	Minimal impact to Compliance; or Administrative OSHA Violation	Moderate Hazard or Reportable Violation; or Minor OSHA Violation	Significant Threat to Regulatory Requirement; Event Requires Immediate Remediation	Cannot Comply with Regulatory Requirement; or Catastrophic Hazard
Technical Performance	Infrastructure and Asset	Insignificant impact to Mission Support infrastructure and/or Asset	Minor impact to Mission Support infrastructure and/or Asset	Significant impact to Mission Support infrastructure and/or Asset	Major impact to Mission Support infrastructure and/or Asset	Severe impact or Loss of Mission-Critical or Agency-Unique infrastructure and/or Asset
	Organizational Objectives	Negligible impact to Objectives	Minimal impacts	Moderate impacts, workaround(s) available	Significant Threats, no feasible workaround(s)	Failure to Meet Critical Objectives
Agency Capabilities	Service Delivery	Incidental Disruption of Institutional Services or Operational Support	Short-Term Disruption of Institutional Services or Operational Support	Significant Disruption of Institutional Services or Operational Support	Major Disruption of key Institutional Services or Operational Support	Work Stoppage of Key Institutional Services or Operational Support
	Workforce	Insignificant impact / Reduced Efficiency of Mission Support Resources	Minor impact, Reduced Efficiency of Mission Support	Significant impact, Reduced Efficiency of Operational Support	Major impact to Effectiveness of Mission Operations Support	Severe impact, Loss of Critical Skills or Capabilities
Cost	Organizational Budget Impacts	\$0 to <\$500K OR <2% increase over allocated and negligible impact on reserve	\$500K to <\$1M OR 2% to 5% increase over allocated and can handle with reserve	\$1M to <\$2.5M OR 5% to 10% increase over allocated and cannot handle with reserve	\$2.5M - <\$5M OR 10% to 15% increase over allocated and exceeds reserves	>\$5M OR >15% increase over allocated and exceeds reserves
Schedule	Project Timelines	Negligible impact	Minimal impact, Slip is Within schedule Dwell Time, No impact to Milestones	Moderate impact, Project Milestone Slip, No impact to Budget	Significant impact, Project Milestone Slip impacts Budget by <3 months	Major impact, Project Milestone Slip impacts Budget by >3 Months



ARMD Consequence Severity Rating Criteria by Risk Type

Risk Type	Strategic		Operational	Financial	Reputational		Cybersecurity	Other
Consequence Severity Label (Score)	OR		Extent of activities associated with a research area or management function that are prevented from being performed	Extent of activities associated with a research area or management function that are prevented from being accomplished	OR		Extent of the unrecoverable losses to the cyber capabilities associated with a research area or a management function	Extent of the activities within an ARMD research area or management function that are affected
	Level of objective(s) that are threatened	Extent of threatened activities within an ARMD research area			Extent of ARMD's credibility within the aeronautics community, associated with a research area or management function, that is destroyed	Extent of the public goodwill toward NASA that is destroyed		
Critical (5)	Agency	Nearly all	Nearly all	Nearly all	Nearly all	Nearly all	Nearly all	Nearly all
Severe (4)	ARMD	Most	Most	Most	Most	Most	Most	Most
Serious (3)	Program	Many	Many	Many	Many	Many	Many	Many
Moderate (2)	Project	Some	Some	Some	Some	Some	Some	Some
Minor (1)	Project	Few	Few	Few	Few	Few	Few	Few

Likelihood	Score	Qualitative Guidance	Quantitative Guidance
Expected	5	Very likely	85%-100%
Probable	4	More likely than not	60%-85%
Possible	3	Equally likely as not	40%-60%
Improbable	2	Less likely than not	15%-40%
Unexpected	1	Very unlikely	0%-15%

Risk Type	Usage Notes
Strategic	Risk that would prevent the accomplishment of ARMD objectives or performance of its mission.
Operational	Risk of operational disruption due to inadequate or failed internal processes, legal or regulatory actions, failure to comply with applicable laws, regulations, or other requirements, or the accuracy or timeliness of information needed to support decision making and/or performance evaluations. Operational risks can arise from internal or external events that impair internal processes, people, or systems, limit ARMD's capacity to consummate important transactions, enforce contractual agreements, and/or meet standards, regulations, ethical requirements, and/or stakeholder expectations.
Financial	Risk that could result in a negative impact to ARMD due to financial management or actions taken by NASA, Congress, the Executive Branch, or other policy makers that could affect the achievement of the ARMD's objectives.
Reputational	Risk that a failure (whether such failure is accurately perceived) could diminish the stature, credibility or effectiveness of ARMD. Reputational risk can arise either from actions taken by ARMD or third-party partners including service providers and agents. Reputational Risk can also arise from events in one of the other risk categories.
Cyber Security	Risk that could expose ARMD to exploitation of vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by its information systems.
Other	Risk type that is distinct from the remaining categories.

Example Risk Matrix and Definitions



Thank You

KEY CONCEPTS FOR EFFECTIVE RISK MANAGEMENT

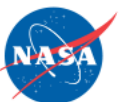
Dr. Mary Skow

Mary.coan@nasa.gov

Agency Risk Management Officer

<https://nasa.sharepoint.com/sites/osma/SitePages/Agency-Risk-Management-Office.aspx>

Please visit <https://nsc.nasa.gov/events> for upcoming virtual events



Helpful Links to Risk Management Information

- Risk Management NASA Procedural Requirement (NPR 8000.4)
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8000&s=4B>
- Enterprise Risk Management (Playbook and Greenbook)
 - <https://www.doi.gov/sites/doi.gov/files/erm-playbook-2022-update-final-508-compliant.pdf>
 - <https://www.gao.gov/assets/gao-14-704g.pdf>
- Program / Project Management NASA Procedural Requirement (NPR 7120.5)
 - <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=7120&s=5F>
- Agency Risk Management Officer's OneNASA site
 - <https://nasa.sharepoint.com/sites/osma/SitePages/Agency-Risk-Management-Office.aspx>
- NASA's Risk Management Handbook (will be updated in 2024)
 - <https://www.nasa.gov/wp-content/uploads/2023/08/nasa-risk-mgmt-handbook.pdf>
- NASA's Program / Project Management Handbook
 - https://ntrs.nasa.gov/api/citations/20220009501/downloads/PM%20Handbook%20with%20corrections-2-16-23_editorial%20corrections.pdf
- Other helpful links
 - <https://sma.nasa.gov/sma-disciplines/risk-management>

Definitions

- + **Risk** – The potential for shortfalls with respect to achieving explicitly established objectives.
- + **Risk Posture** – The limits of acceptable risk to the established / stated objectives whose achievement is of direct concern to stakeholders.
- + **Objectives-Driven Risk Management** – An approach to risk management that focuses on ensuring that a program's/project's/Organization's risk profile is aligned with the established objectives and within the established risk posture

Risk Profile: The ensemble of assessed risk to a program's/project's established objectives.

- + **Risk Leadership** – Leading, by an accountable leader or manager, risk acceptance decision-making within the limits of a defined risk posture, including the authority to allocate portions of the risk posture to subordinate / supporting organizations.



What is Risk and Risk Posture?

- **Risk is the potential for shortfalls with respect to achieving explicitly established and stated objectives**
 - Stated objectives could be related to programs and projects, institutional support for mission execution, or any other objective-driven activity and/or mission
- **Risk is operationally characterized as a set of triplets:**
 - The **scenario(s)** leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction or compromise of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).
 - The **likelihood(s)** (qualitative or quantitative; unconditional or conditional) of those scenarios.
 - The **consequence(s)** (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.
 - Uncertainties are included in the evaluation of likelihoods and identification of scenarios
- **Risk Posture is the limits of acceptable risk to the established / stated objectives whose achievement is of direct concern to stakeholders**

What are common types of risk?

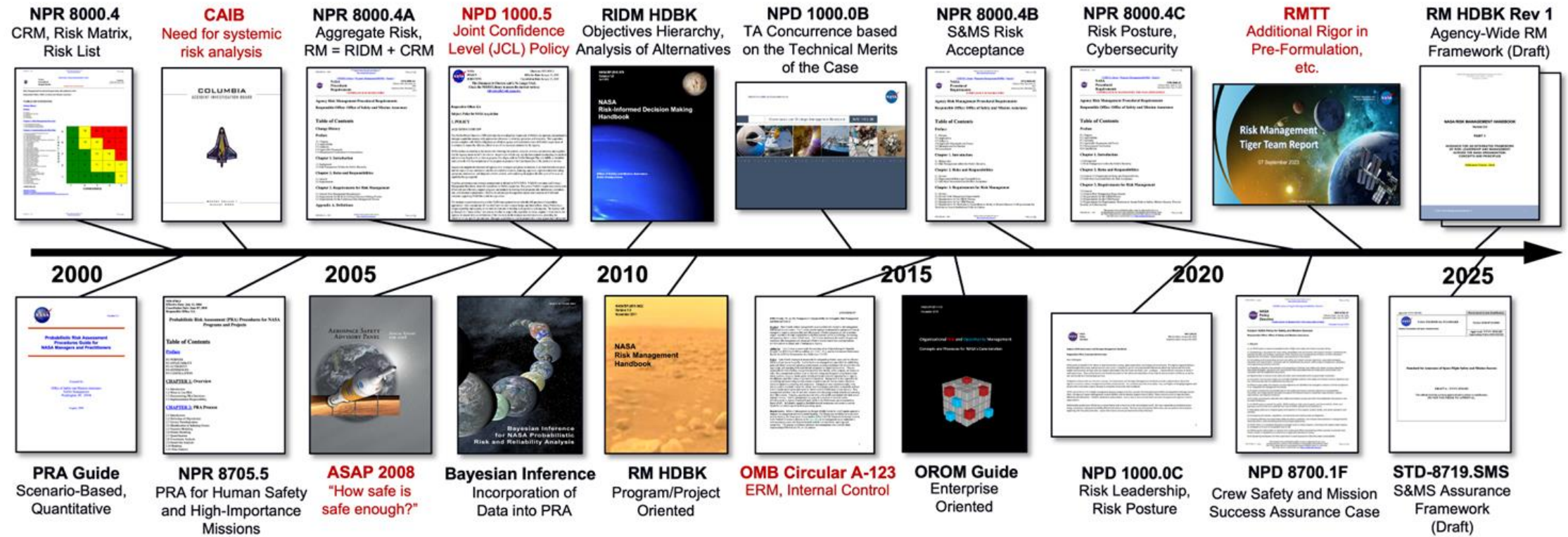
Common Risk Types Typically Assigned to Each Activity Domain		
Enterprise	Program/Project	Institutional
Strategic	Safety	Staffing
Operations	Technical	Training
Compliance	Security	Maintenance
Acquisition	Cost	Supply chain
Fraud	Schedule	Facility safety
Reputational	Etc.	Facility availability
Etc.		Etc.

Caveat: It should be emphasized that the bucketing of risk types into specific activity domains should not be taken too literally. The assignment of risk types to activity domains helps ensure that all significant risks are considered under the risk management umbrella. In actuality, however, many risk types span at least two and sometimes all three of the activity domains in the table above.

NASA's Risk Management Principles

- + Risk Management at all levels of the Agency should be Objectives-Driven.
- + Risk Management within every organization should be anchored to the activities the organization conducts in the service of meeting its objectives.
- + Every organization should adhere to an established risk posture, consisting of acceptable levels of aggregate risk to each of its objectives.
- + Risk management should be conducted in a manner that is consistent with NASA's governance model.
- + Each organization is accountable for overseeing the risk management processes of subordinate organizations, as well as for managing risks identified at its own level.
- + Risk management is conducted and overseen in a timely manner throughout the life cycle of the activity.
- + Risk management includes the identification and management of systemic, cross-cutting individual risks that threaten multiple objectives across multiple organizations.
- + The risk information communicated by subordinate organizations should support the higher-level organization's own risk management needs as well as its risk management oversight needs.

Evolution of NASA Risk Management



Risk Leadership Represents the Highest Maturity Level of Objectives-driven Risk Management*



Level 1: Ad hoc risk management addresses a specific problem when it arises.

Level 2: Targeted or initial risk management approaches risks with multiple understandings of what constitutes risk, and management occurs in silos.

Level 3: Integrated or repeatable risk management puts in place an organization-wide framework for risk assessment and response.

Level 4: Intelligent or managed risk management coordinates risk management across the business, using common tools.

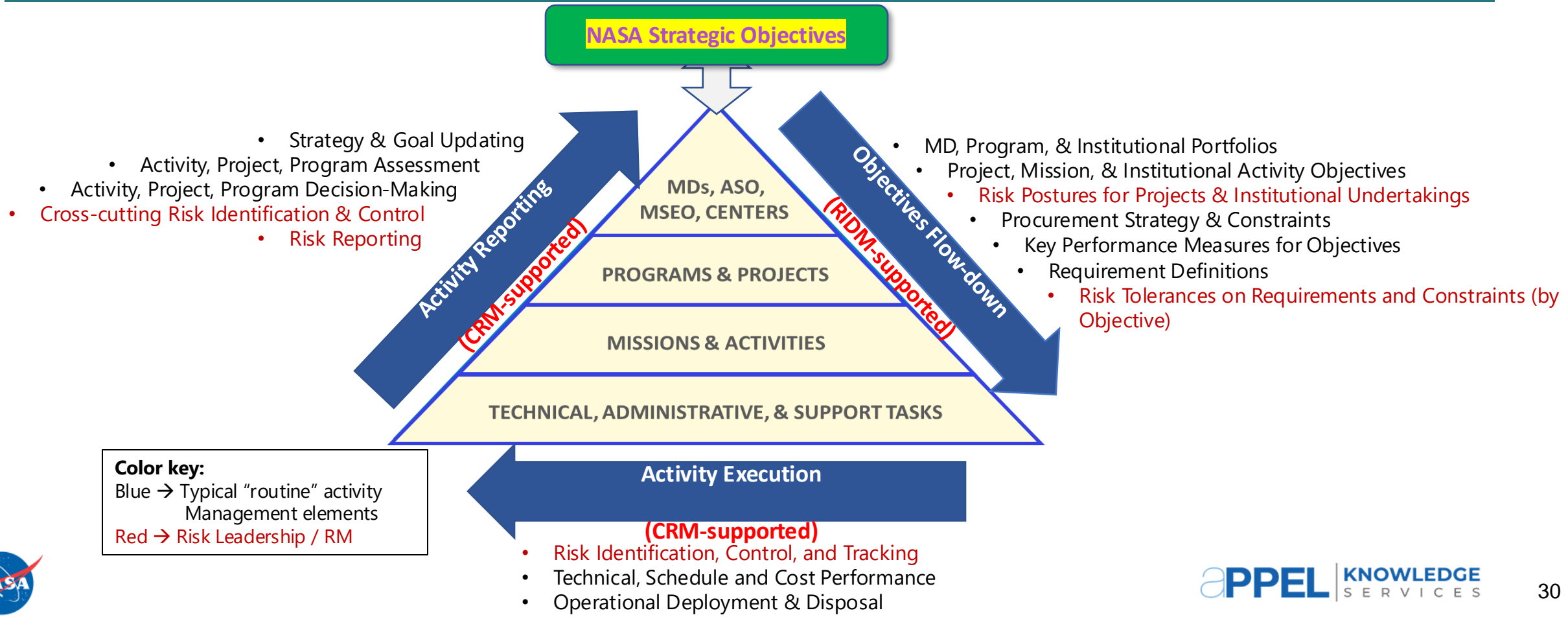
Level 5: Risk leadership incorporates risk management into strategic decision-making.

"Over its evolution, [a high-level organization should] move from narrow tactical risk management to holistic strategic, and long-term risk management"

* Case study of best practices operationalized at Intuit Corp., quoted from "Enterprise Risk Management Case Studies: Heroes and Zeros," Smartsheet, Inc., 2021.

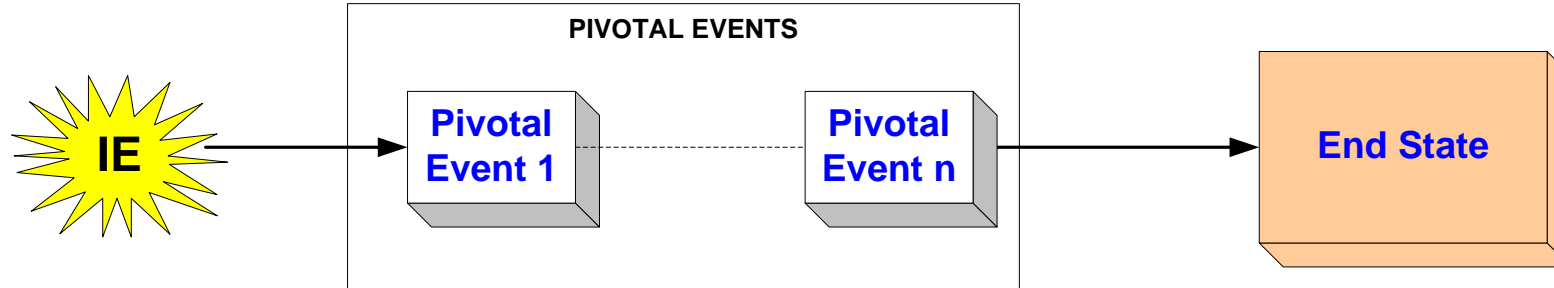
Implementation of Risk Leadership

- + Application of Risk Leadership is integrated with agency management processes at all levels
 - + Top-down definition and communication of objectives and associated risk posture and risk-tolerance in key mission / activity dimensions
 - + Bottom-up feedback on activity execution, application of risk-tolerances and effectiveness of associated risk controls



WHAT IS THE DIFFERENCE BETWEEN INDIVIDUAL RISKS AND AGGREGATE RISKS?

- **An individual risk** is a scenario leading to degraded performance with respect to one or more performance measures
- A scenario is a defined sequence of events, starting from an Initiating (Departure) Event, and leading after some set of pivotal events to an undesirable effect on a performance measure



- The characterization of an individual risk includes the scenario itself, the likelihood of the scenario occurring, and the consequence resulting from the scenario

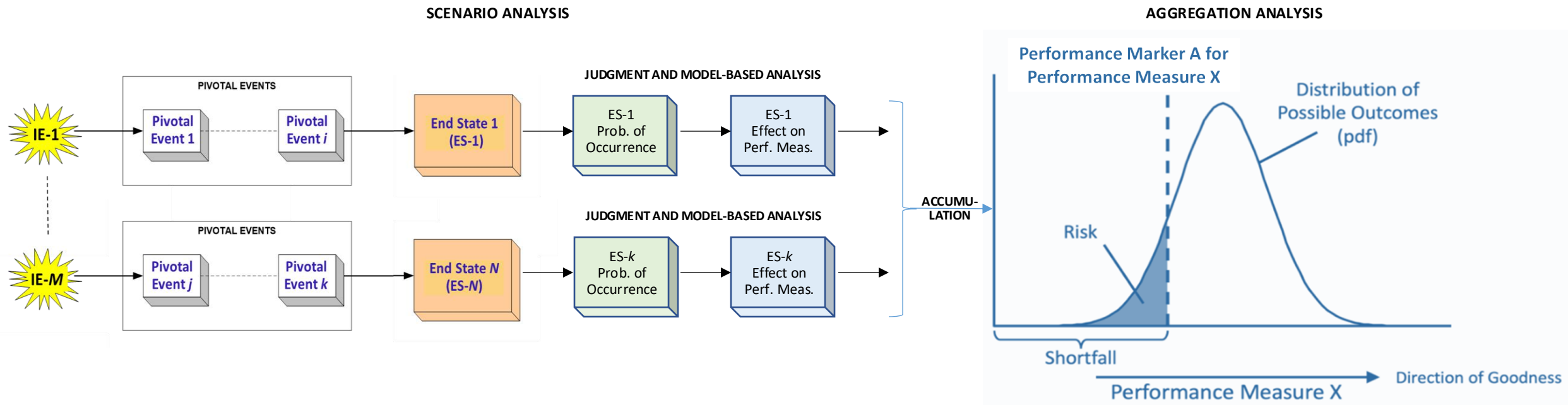
WHAT IS THE DIFFERENCE BETWEEN INDIVIDUAL RISKS AND AGGREGATE RISKS? (Cont.)

INDIVIDUAL RISK SCENARIO EXAMPLES

- Program/project example 1 (S&MS related)
 - Failure of an on-board control system during an orbital vehicle's approach to an extraterrestrial planet or moon leads to overloading of the vehicle, resulting in structural failure and loss of vehicle, release of radioactive material from its RTGs, and contamination of the planet or moon
- Program/project example 2 (cost related)
 - Unexpected results during integrated system testing of a space system in microgravity conditions lead to concern about the ability to meet mission requirements, resulting in a significant delay in the launch date with a commensurate unplanned cost increase
- Institutional example (core competency related)
 - Unanticipated retirements in a specialty critical to the Agency, stiff competition for new hires, and lack of funding for training courses lead to a poor score from an independent assessor concerning the Agency's ability to maintain a strong core competency in that specialty

WHAT IS THE DIFFERENCE BETWEEN INDIVIDUAL RISKS AND AGGREGATE RISKS? (Cont.)

- An **aggregate risk** is the accumulated effect of all relevant scenario on the probability of not being able to meet a performance measure constraint value, target value, or other defined value or set of values
- These set-point values are collectively referred to as performance measure markers



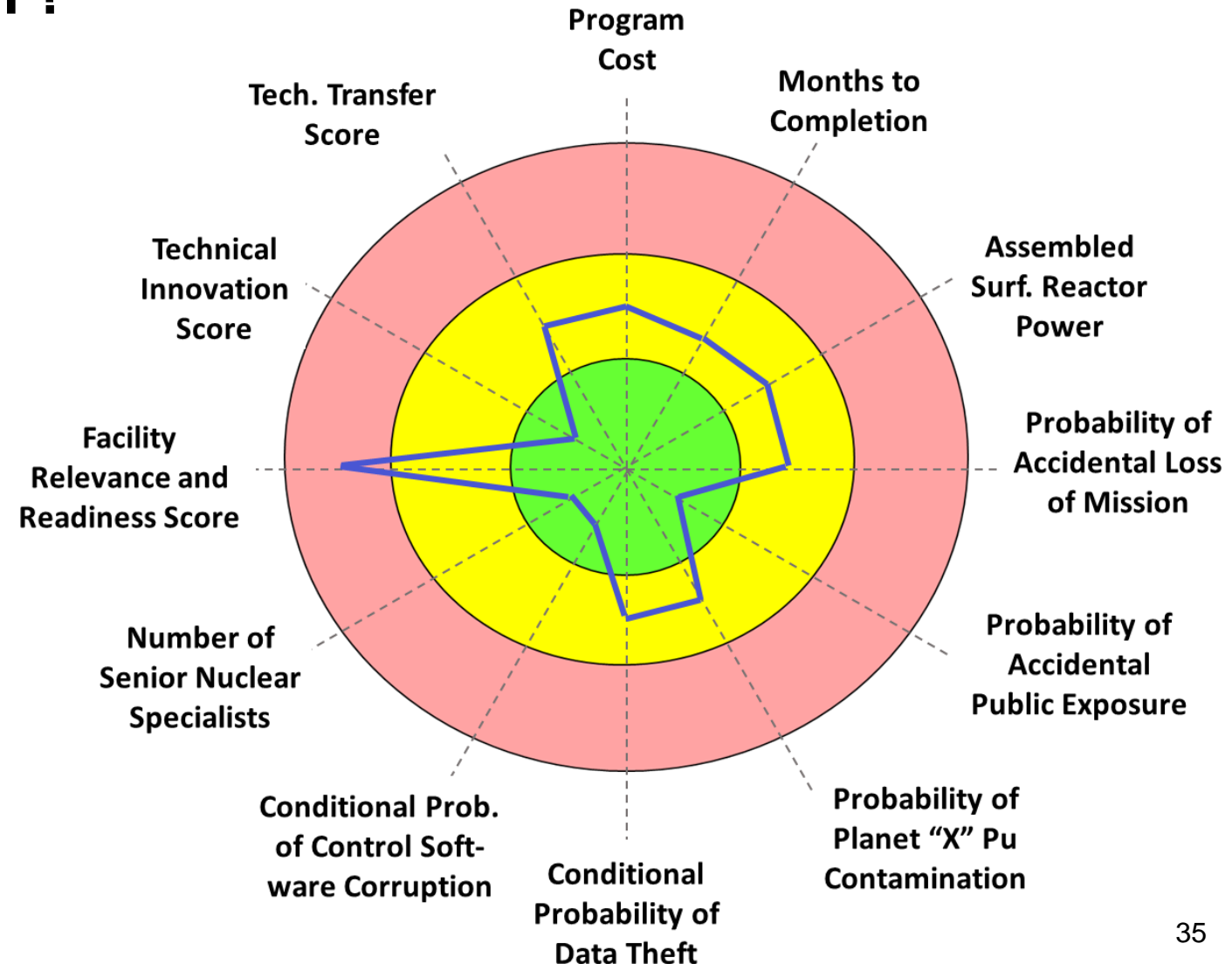
WHAT IS THE DIFFERENCE BETWEEN INDIVIDUAL RISKS AND AGGREGATE RISKS? (Cont.)

AGGREGATE RISK EXAMPLES

- Program/project example 1 (S&MS related)
 - The cumulative probability that there will be loss of vehicle during Project X in the vicinity of Planet Y resulting in an unacceptable level of planetary radioactive contamination, considering all identified accident scenarios, is less than 10%
- Program/project example 2 (cost related)
 - The cumulative probability that the total expenditure on Project Y will exceed the funding constraint allocated by Congress and the Office of the President, considering all identified cost risk scenarios, is around 30%
- Institutional example (core competency related)
 - The cumulative probability that the required staffing to maintain a core competency in cybersecurity protection across the Agency, considering all identified scenarios leading to staff attrition and replenishment difficulties, is between 15% and 25%

HOW MAY THE AGGREGATED RISKS BE DISPLAYED IN A MANAGEMENT-FRIENDLY WAY?

- **Spider Charts of Performance Measure Aggregate Risk Results (Hypothetical Illustration for 3 Discrete Rankings)**
 - This spider chart shows the rankings of the aggregate risks as
 - 1-Green (acceptable), 2-Yellow (Marginal), or 3-Red (unacceptable)
 - It includes multiple performance measures on one chart
 - The performance measures span multiple risk management domains: programmatic, institutional, enterprise, mandated requirements
 - Since the rankings are discrete and not continuous, the data points are plotted in the center of each band



Questions?