**Risk Management Concept Template**

**1. Introduction**

* **Purpose**: State the primary purpose of this document: to define the strategy, processes, and requirements for systematically managing risks across the system's entire lifecycle. It aims to anticipate and address potential threats and opportunities before they impact the project.
* **Scope**: Define the boundaries of this risk management concept, specifying that it applies from **concept development through disposal**, adapting to evolving risks.
* **System Identification**: Clearly identify the system or system element that is the subject of this risk management concept.

**2. Purpose and Scope**

* **Overall Goal**: To reduce potential risks to an acceptable level before they occur and to achieve a proper balance between risk and opportunity. This process helps understand and avoid potential cost, schedule, and technical performance risks to a system.
* **Key Objectives and Benefits**:
	+ **Proactive Uncertainty Management**: Anticipating and addressing potential threats and opportunities.
	+ **Lifecycle Coverage**: Applying the concept from concept development through disposal, adapting to evolving risks.
	+ **Decision Support**: Providing data-driven insights for trade-offs and resource allocation.
	+ **Ensuring Project Success**: Managing the risk of not delivering what is needed, late delivery, excess cost, and negative unintended consequences.
	+ **Ensuring Quality Assurance**: Assisting in managing risks associated with developing, producing, operating, and sustaining systems and capabilities.
	+ **Trustworthiness**: Contributing to building systems resilient to cyber-physical threats.
	+ **Compliance**: Helping meet regulatory standards.

**3. Core Components of Risk Management Process**

The risk management process involves several continuous activities:

* **3.1. Risk Planning**
	+ **Purpose**: To establish and maintain a strategy for identifying, analyzing, handling, and monitoring risks.
	+ **Content**: Documented in a Risk Management Plan (RMP), which defines the process, implementation, stakeholders' perspectives, risk categories, objectives, assumptions, and constraints.
	+ **Key Elements**: Define roles, tools, and reporting cadence (e.g., monthly risk review boards).
* **3.2. Risk Identification**
	+ **Purpose**: The continuous process of examining project products, processes, and requirements to identify and document candidate risks.
	+ **Methods**: Brainstorming, Delphi technique, SWOT analysis, historical data review, Work Breakdown Structure (WBS) analysis, key process evaluations, checklists, and expert judgment.
	+ **Outputs**: **Risk register** listing threats (e.g., technical failures) and opportunities (e.g., new technologies). Risk statements should be clear, unambiguous, and ideally in an "if-then" format (condition, event, consequence).
* **3.3. Risk Analysis**
	+ **Purpose**: Systematically evaluating each identified risk to estimate its likelihood and consequence.
	+ **Methods**:
		- **Qualitative**: Prioritizes risks using probability/impact matrices (e.g., 5x5 scales).
		- **Quantitative**: Computes numerical risk exposure (e.g., Monte Carlo simulations for cost/schedule variance), decision trees, probabilistic risk assessments.
	+ **Output**: Risks are prioritized based on their level or score, considering timeframe, frequency, and interrelationships.
* **3.4. Risk Handling (Treatment/Mitigation)**
	+ **Purpose**: Identifying, selecting, and implementing options to reduce a risk to an acceptable level within program constraints and objectives.
	+ **Strategies**:
		- **Avoidance**: Redesign to eliminate a failure mode. Adjust program requirements or constraints to eliminate or reduce the risk.
		- **Mitigation**: Implement actions to minimize the impact or likelihood of the risk (e.g., redundant components for reliability). This is the most common approach for higher-priority risks.
		- **Transfer**: Reassigning accountability, responsibility, and authority for a risk to another willing party (e.g., outsourcing a high-risk subsystem or insurance).
		- **Acceptance**: Deliberately accepting a risk without special efforts to control it (e.g., documenting minor schedule delays).
		- **Exploitation**: Capitalize on opportunities (e.g., adopting emerging tech for efficiency).
	+ **Output**: Mitigation plans detailing actionable steps with resources and timelines. Risk handling plans (RHPs) or risk element plans (REPs) should be developed for high and medium risks.
* **3.5. Risk Monitoring and Control**
	+ **Purpose**: Evaluating the effectiveness of risk handling activities against established metrics and providing feedback to other risk management process steps.
	+ **Key Elements**: Track progress, identify new risks, and revise plans as needed.
	+ **Triggers**: Key risk indicators (KRIs) and thresholds (e.g., "if supplier delay exceeds 2 weeks, escalate").
	+ **Tools**: Risk dashboards, audits, and periodic reviews.

**4. Types of Risks**

Risks can be categorized into various types throughout the system lifecycle:

* **Technical Risk**: Associated with achieving a technical goal, impacting performance, human health, safety, mission assets, system security, or the environment. This includes the feasibility of performance and quality based on technology maturity. Cybersecurity is considered a technical risk in NASA.
* **Cost Risk**: Potential increase in project costs beyond the original budget.
* **Schedule Risk**: Potential for a project, task, or activity to be completed outside of the planned schedule or deadline.
* **Programmatic Risk**: Risks produced by events beyond the control of the project manager.
* **Management Risk**: Concerns budget, schedule, resources, and upper-level management support.
* **Development Risk**: Problems due to failure to follow project management and SE lifecycle process activities.
* **Production Risk**: Concerns the ability to manufacture or code the system.
* **System Integration Risk**: Issues arising during the integration of various system elements.
* **System Verification and Validation Risks**: Related to test resources and ensuring the system meets needs and requirements.
* **Compliance Risk**: Concerns the ability to show compliance with applicable standards and regulations.
* **Operational Risk**: Involved in the performance of the system for its intended use by intended users in its operational environment.
* **Interface Risk**: Associated with interface boundaries in terms of stability, threats, or failures impacting system operation.
* **Human Systems Integration (HSI) Risk**: Risks related to human interaction with the system, including safety incidents, long-term health damage, or loss of life.
* **Environment, Safety, and Occupational Health (ESOH) Risk**: Risks to be accepted by Joint Authorities, including System Safety, environment, and occupational health.
* **Supply Chain Risk Management (SCRM)**: Addressing risks across the supply chain, from design to disposal.

**5. Integration with Other SE Processes and Artifacts**

Risk management is deeply integrated throughout the systems engineering lifecycle and its processes:

* **Business or Mission Analysis (Concept Stage)**: Preliminary lifecycle concepts are established, and initial uncertainties leading to risks are identified. Defining the problem/opportunity space includes understanding associated risks and constraints.
* **Stakeholder Needs and Requirements Definition**: Risks concerning product development and intended use are identified and captured, with needs derived from risk mitigation concepts having traceability to the risk.
* **Project Planning**: Risk assessment is incorporated early in the planning process to identify areas needing special attention or contingencies.
* **Measurement**: Provides indicators for risk analysis. Measures help quantify risks and provide information on the effectiveness of risk mitigation, including Technical Performance Measures (TPMs).
* **Decision Management**: Evaluates alternatives for selection and handling of identified and analyzed risks, often incorporating risk and uncertainty analysis in trade studies.
* **Configuration Management (CM)**: Proper CM is vital for managing risk, as unmanaged changes to baselines can introduce problems and risks.
* **System Safety Engineering**: Involves identifying hazards, assessing and mitigating associated risks, and tracking, controlling, accepting, and documenting risks throughout the entire life cycle, including design, development, test, acquisition, use, and disposal.
* **Technical Reviews**: Risks are assessed at key technical reviews (e.g., ASR, SFR, PDR, CDR) to ensure technical feasibility and maturity for progressing to the next phase.
* **Integrated Master Schedule (IMS)**: Risk mitigation activities should be included as tasks within the IMS, allowing for analysis of schedule and cost risks.
* **Requirements**: Risks are linked to requirement volatility or ambiguity.
* **Architecture**: Mitigations can be embedded in design (e.g., modularity for easier upgrades).
* **Verification**: Risk-based testing prioritizes high-impact scenarios.

**6. Key Considerations and Best Practices**

* **Early and Continuous Application**: Risk management should begin as early as possible in the acquisition lifecycle and be performed continuously.
* **Tailoring**: The level of detail and rigor should be tailored to the project's complexity, technology maturity, and specific risks.
* **Stakeholder Involvement**: All relevant stakeholders must be identified and included in risk identification and management, with crucial communication of risk information among them.
* **Clear Terminology**: Define and communicate risk terminology to prevent misunderstandings.
* **Distinguish Risk from Issue**: Risks are potential future events (probability < 1), while issues are unwanted events that have occurred or are certain to occur (probability = 1).
* **Focus on Root Causes**: Addressing root causes of risks is more effective than patching individual instances.
* **Margins and Reserves**: Use sufficient budget and schedule margins and reserves to mitigate risks.
* **Trade-off Analyses**: Risk is a critical criterion in trade-off analyses, balancing cost, schedule, and performance.
* **Documentation and Tracking**: Document all identified risks, their analysis, mitigation plans, and status in a **risk register or database**.
* **Culture**: A management culture that encourages and rewards risk identification from all staff levels is essential.
* **Avoid Technical Debt**: Proper SE and PM practices, including addressing risks upfront, help avoid technical debt.

**7. Tools and Metrics**

* **Tools**:
	+ **Risk Registers/Databases**: Repositories for all relevant risk information.
	+ **Risk Matrices**: Used to combine likelihood and consequence to determine risk levels and prioritization.
	+ **Specialized Tools**: RiskNav®, Risk Radar, Active Risk Manager.
	+ **Modeling and Simulation**: Used for quantitative risk analysis (e.g., Monte Carlo simulations) and to evaluate design alternatives.
* **Metrics**:
	+ **Risk Exposure Trends**: Evaluates risk exposure over time (cost, schedule, technical).
	+ **Risk Treatment Trends**: Evaluates the effectiveness of implementing risk mitigation activities.
	+ **Technical Performance Measures (TPMs)**: Assess design progress, track technical risks, and show compliance to performance requirements.
	+ **Technology Readiness Levels (TRLs) and Manufacturing Readiness Levels (MRLs)**: Measures of maturity that inherently indicate risk.

**8. Traceability and References**

* **Traceability Matrix**: (Optional but Recommended) A matrix to map identified risks to system requirements, architectural elements, and mitigation strategies.
* **Documentation and Records**: Document and retain records of all risk management activities, including risk registers, mitigation plans, and decision rationale.
* **References**: List all source documents, standards, related concepts (e.g., System Concept, Cost and Schedule Concept, Security Concept), and other artifacts that inform this Risk Management Concept.