RISK MANAGEMENT GUIDE

PURPOSE: The Risk Management Guide is intended to provide amplifying procedures and applicable instructions and resources to assist Naval personnel in implementing risk management principles in day-to-day operations. This guide is designed to supplement OPNAVINST 3058.1.

1. Introduction

a. Risk management is a proactive and systematic process that identifies, assesses and mitigates potential risks that could impact an organization's assets, operations, reputation and overall success. Effective risk management involves a structured approach that enables organizations to anticipate, respond and manage potential threats and opportunities, ultimately ensuring resilience, sustainability and long-term viability.

b. Risk management is an inherent part of decision-making at all levels. Exercising a robust risk management process is key to our culture and must be continuously taught and mentored. This guide provides the tools required to assist in risk management training and mentorship. OPNAVINST 3058.1 Navy Risk Control System contains all requirements.

c. OPNAVINST 3500.39 was cancelled upon release of OPNAVINST 3058.1, removing the requirements to assign an Operational Risk Management (ORM) Manager and Assistant ORM Managers, supervisor and annual training requirements. This cancellation was a conscious decision to align to the cultural foundation of the Navy's Risk Control System (RCS) Program where risk management is a day-to-day, all hands activity. Risk management is a skill that requires application and regular mentorship to hone; it cannot be mastered through formal instruction. Although periodic training requirements have been removed, the training is kept current and is still available to teach the fundamentals on the Navy E-Learning platform. Commands are encouraged to use available products and tailor their risk management training needs to fit their mission requirements.

2. Risk Discussion

a. What is a Risk? A Risk is an uncertain future event that could affect the organization's ability to achieve its objectives.

(1) A risk:

- is forward-looking (not a current issue),
- has an element of uncertainty,
- could affect the achievement of objectives,
- must be credible and reasonably foreseeable, and
- can have both positive and negative effects.

(2) Risk is the likelihood and potential impact of an event within a specific time horizon that could cause harm to something of value, often aligned with objectives outlined in the strategic guidance. The risk management framework provides a standardized and consistent approach to evaluating, managing and communicating risk, enabling leaders to make informed decisions across various processes. Risk assessment and prioritization is a qualitative process that incorporates commander's judgment, while quantitatively expressing probability and severity when relevant. The dynamic nature of the strategic environment means risk assessment has to be a continual process requiring periodic reassessment. The risk management framework is flexible and adaptable and allows risk-related processes to incorporate relevant components while maintaining the base components of probability, consequence, time, organizational integration and risk level. This foundation ensures a consistent and structured approach to risk assessment, enabling effective decision-making and risk mitigation.

b. What is an Opportunity? An occurrence where risk is present but managing the risk could potentially lead to a positive impact on objectives is classified as an Opportunity.

(1) OPNAVINST 3058.1 focuses on the identification and management of risks that can have a negative impact on objectives, often referred to as threats; however, the same process and activities can be applied to identifying and managing opportunities. This approach enables organizations to leverage potential benefits and enhance their chances of success, in addition to mitigating potential downsides.

(2) When evaluating each aspect of risk, organizations should consider how risk identification, assessment and management can be leveraged to identify and capitalize on opportunities that create an advantage. This opportunity-focused approach begins with the identification and assessment steps, where organizations intentionally look for potential benefits and advantages. However, it is during the assessment and prioritization phases that the balance of risks versus opportunities becomes relevant. By deliberately managing risk and determining acceptable levels of exposure, decision-makers can create an environment that fosters opportunities aligned with strategic objectives.

(3) Recognizing risk is not solely the presence of a threat, but also reveals opportunities to exploit, innovate and gain a strategic edge. By integrating an opportunity-minded perspective into the risk management process, the organization can adopt a more holistic approach, one that balances risk mitigation with proactive efforts.

c. Role of Risk Management in the Navy's Resilience Model

(1) Modern safety takes into account not only mishap prevention but includes the ability to recover from an adverse event while minimizing loss and impact. This is called resilience or the ability of the system to bounce back without unnecessary additional harm. *(Figure 1)*

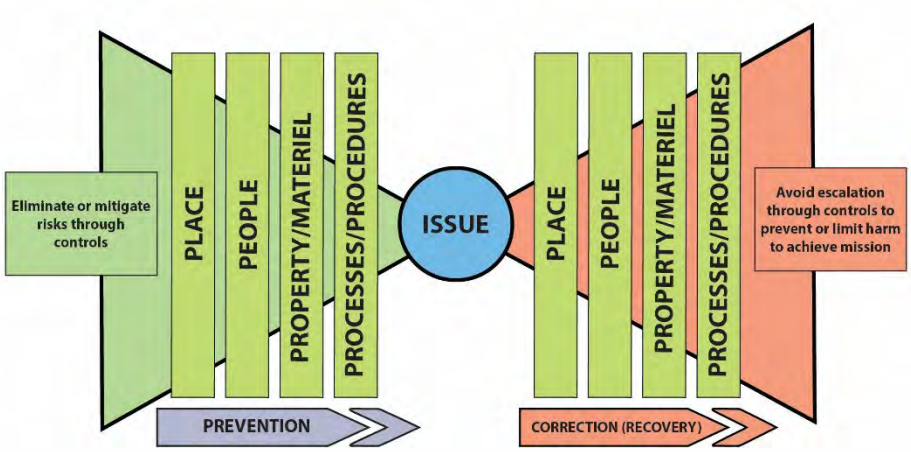
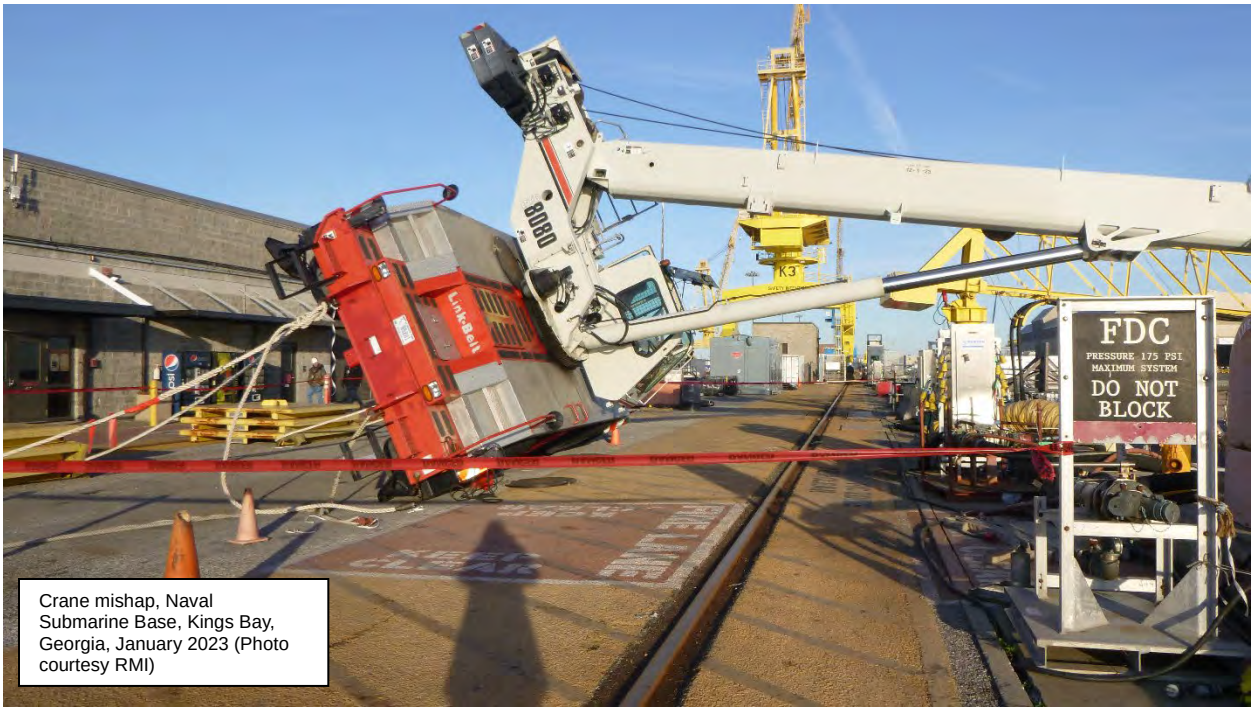


Figure 1. Resilience Model

(2) Risk management is a critical component of ensuring the safety and success of complex systems, and resilience plays a vital role in this process. Resilience refers to the ability of a system to absorb and recover from disturbances, such as unexpected events or failures, without suffering significant harm or degradation. In the context of risk management, resilience is about creating a system that can prevent, mitigate or respond to potential risks and threats, thereby minimizing their overall impact. There are several key aspects of resilience in risk management:



Crane mishap, Naval Submarine Base, Kings Bay, Georgia, January 2023 (Photo courtesy RMI)

(a) Risk resilience: This involves implementing a systems view of risk controls that protects people, material and the environment from harm. It requires a proactive approach to identify and mitigate potential risks, as well as develop effective emergency response plans to address unexpected events. Building a robust defense-in-depth (multiple means to prevent and respond to adverse events) is key to building a resilient system.

(b) System Failures: System failures occur when risk controls are absent, disregarded, ineffective or fail to account for human error. These failures can lead to significant harm and degradation of the system, highlighting the importance of robust risk management and resilience strategies.

(c) Situational Awareness: Situational awareness is critical in complex operating environments, where multiple inter-related networks of latent and active safety failures can exist. Situational awareness involves conscious recognition and response to factors that may degrade successful outcomes and it is essential for maintaining sufficient risk awareness and resilience.

(d) The 4Ps: A resilient system relies on a network of system controls that work in concert to protect people, places, property and processes. The 4Ps (safe places, people, property and materiel, and processes and procedures) provide a framework for organizing and implementing these controls. Note the 4P pillars are often interdependent.

(e) Safe to Operate and Operating Safely: A resilient system is characterized by its ability to operate safely and maintain a high level of safety performance. This requires a proactive approach to risk management, as well as a commitment to continuous improvement and learning.

(f) Benefits of Resilience: Resilience offers numerous benefits, including reduced equipment damage, financial gains, and improved job satisfaction and wellbeing. It also provides a formal method

for organizing leading and lagging indicators to judge the level of assurance and overall safety performance.

(3) To achieve resilience in risk management, organizations should adopt a systems approach that focuses on protecting complex environments from recognized and unrecognized risks, as outlined in OPNAVINST 3058.1. This involves:

By adopting a resilience-based approach to risk management, organizations can reduce the likelihood and impact of adverse events, improve their overall safety performance and maintain a competitive advantage in complex and dynamic operating environments.

(a) Proactively identifying and assessing potential risks and threats to the system.

(b) Implementing effective risk controls, such as safety protocols, emergency response plans and mitigation strategies.

(c) Maintaining a high level of situational awareness to recognize and respond to potential risks and threats.

(d) Continuously monitoring and improving the system's resilience and safety performance.

(e) Fostering a culture of resilience within the organization, where employees are empowered to identify and report potential risks and threats.

(4) By adopting a resilience-based approach to risk management, organizations can reduce the likelihood and impact of adverse events, improve their overall performance and maintain a competitive advantage in complex and dynamic operating environments.

3. Levels of Risk Management

a. Risk management is a decision-making process to systematically evaluate possible courses of action, identify risks and benefits, and determine the best courses of action for any given situation. As such, risk management enables commanders, functional managers, supervisors and individuals to maximize capabilities while limiting risks through application of a simple, systematic process appropriate for all personnel and functions in both on and off-day situations. Appropriate use of risk management increases an organization's and individual's ability to safely and effectively accomplish their mission and activity while preserving lives and limited resources.

b. The risk management process is applied on three levels: **in-depth**, **deliberate** and **time critical**. The primary distinguishing factor between these levels is the amount of time available for preparation and planning of missions or tasks. The risk management process is flexible and scalable, allowing it to be tailored to the specific time constraints and requirements of each situation.

Sailors and Airmen search for foreign objects and debris (FOD) during a FOD walkdown on the NAVSTA Rota airfield, May 2024. (U.S. Navy photo by Mass Communication Specialist 2nd Class Drace Wilson)

(1) **In-depth**. The in-depth level of risk management is a meticulous and comprehensive approach that is employed when time is not a limiting factor, and the accuracy of the outcome is crucial for the success of a mission or task. This level of risk management is characterized by a thorough and systematic process that involves:

(a) Thorough research, analysis and a detailed examination of all relevant data, including historical records, industry benchmarks and expert opinions, to gather a comprehensive understanding of the risks involved.

(b) Use of diagrams and analysis tools, such as:

- Fault trees: a graphical representation of the possible causes of failure or hazard.
- Event trees: a graphical representation of the possible sequences of events that could lead to failure or hazard.
- Decision trees: a graphical representation of the possible decisions and their potential outcomes.
- Failure mode and effects analysis: a systematic approach to identify and evaluate potential failures in a system or process.
- Reliability block diagrams: a graphical representation of the reliability of a system or process.

(c) Formal testing or long-term tracking associated hazards. Conduct thorough testing and evaluation of systems, equipment and processes to identify potential hazards and monitor their performance over time. This may include:

- Simulation modeling: the use of computer models to simulate the behavior of a system or process under various scenarios.
- Prototype testing: the testing of a prototype or pilot version of a system or process to identify potential hazards and evaluate its performance.

- Long-term monitoring: the ongoing monitoring of a system or process over an extended period to identify potential hazards and evaluate its performance.

(d) The in-depth level of risk management is applied in a variety of situations including:

1. Long-term planning of complex or contingency operations, such as:

- The planning and execution of military operations, including the identification of potential risks and the development of contingency plans.
- The planning and execution of complex engineering projects, such as the construction of a new building.
- The planning and execution of response and recovery efforts in the event of a natural disaster or other crisis.

2. The application of technical standards and system hazard management principles during the engineering design phase of new equipment and systems to:

- Identify potential hazards associated with the design and operation of a system or equipment.
- Evaluate the risks associated with the design and operation of a system or equipment.
- Develop strategies to mitigate or eliminate identified hazards and risks.

3. The development of tactics, techniques and procedures and training curricula for personnel to:

- Ensure they are equipped with the necessary skills and knowledge to handle complex and high-risk situations.
- Respond to emergencies, such as fire and medical, guided by effective procedures and protocols.

4. The planning and execution of major maintenance or repair activities, such as:

- Overhaul of an aircraft carrier.
- Repair of critical infrastructure such as a bridge or a highway.

(2) **Deliberate**. The deliberate level refers to situations when there is ample time to apply the risk management process to the detailed planning to obtain the "best" answer or course of action required of a mission or task. This type of risk management is typically done at the operational level. At this level, the planning primarily uses experienced personnel and brainstorming and is most effectively accomplished in a group setting. The Navy Planning Process is a good example of risk management application integrated at this level. Other examples include the planning of unit missions, tasks, or events; review of standard operating procedures (SOPs), maintenance or training procedures, recreational activities and the development of damage control and emergency response plans.

Steps in deliberate risk management

- Identify hazards: Identify the potential risks associated with an operation
- Assess hazards: Evaluate the risk level of each identified hazard
- Make risk decisions: Decide how to manage the risks
- Implement controls: Put controls in place to reduce the risk
- Supervise and evaluate: Monitor the controls and assess their effectiveness

(3) **Time Critical**. This is the level at which personnel operate daily on- and off-duty. The time critical level is best described as being at the point of commencing or during execution of a mission or task. At this level there is little or no time to plan. An on-the-run mental or verbal assessment of the new, changed or changing situation is the best one can do. Time is limited in this situation, so the application of the five-step process has proven impractical and ineffective. The Navy has adopted the ABCD Model to facilitate use of risk management at the time critical level.

(a) The ABCD Model provides a common language and structure for a measured response when an individual, team or crew is executing a routine task or when they are under duress from a more complex situation resulting from additive conditions, crew factors or task loading. Training to the ABCD Model will embed a set of patterns that will help personnel recognize and recall a set of actions to counter risk even when distracted. This simple and easy to remember mnemonic provides individuals with a means to evaluate risks and formulate mitigation strategies while on-the-run and can easily be applied in on- and off-duty situations.

(b) Using the ABCD Model, Figure 2, daily creates a habit and trains the brain to continue thinking under duress or stress. The model is designed to assist when:

- Working in a dynamic environment
- Monitoring a static or routine situation to capture errors
- Making a decision with partial information

(c) In all three situations, it is necessary to develop habits that trigger the TCRM process to "Assess" the situation, "Balance" resources, "Communicate" to others, "Do and Debrief" the event.

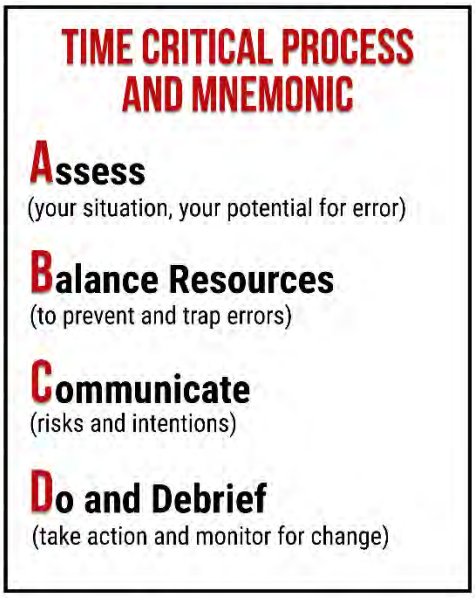


Figure 2. ABCD Model

(d) Additionally, these situations require the continuous use of "Assess," "Balance," "Communicate," "Do and Debrief" as necessary. An added benefit and value of the ABCD Model is the continuous improvement of skills and knowledge which occurs with self-assessment.

(e) Time critical decision-making requires a unique set of skills, which must be practiced.

(f) TCRM relies on the decision maker's previous experience, training and availability to recall resources from the in-depth or deliberate processes.

(g) Standardizing the communication structure in a time critical situation reduces conflicts and errors and improves the ability to manage risk and resources.

4. Responsibilities

a. All personnel are integral to the risk management process, contributing at every stage from identifying and assessing potential hazards, to implementing controls and mitigations and ultimately evaluating the effectiveness of risk decisions. Their active participation and collective ownership of risk management are essential to ensuring a robust and resilient safety culture.

b. Leaders and supervisors have the responsibility to:

- Make informed risk decisions.
- Establish and communicate levels of risk decision authority.
- Assign accountability for controls.
- Ensure risk decisions are documented and reassessed periodically.
- Provide resources to support the growth and sustainment of a proactive, mature and resilient risk-aware culture.

5. Risk Communication

a. Effective risk communication is the foundation of any successful risk management effort. It is an ongoing process that requires continuous attention and effort. It involves the exchange of information, ideas and concerns between all stakeholders, including personnel at all levels, to ensure that everyone is aware of the risks and their potential impact. Risk communication is a two-way process that should flow both from the bottom up, where personnel identify and report potential hazards, and from the top down, where leaders and managers inform personnel of potential risks and provide guidance on mitigation strategies.

b. Open and transparent communication between risk stakeholders is critical to reducing misunderstandings, minimizing potential surprises, and fostering a culture of trust and cooperation. When personnel are informed and engaged in the risk management process, they are more likely to take ownership of risk mitigation efforts and make informed decisions that support the organizations overall risk management goals.

c. To ensure effective risk communication, organizations should establish clear channels of communication, provide regular updates and feedback and encourage active participation and feedback from all personnel. This includes:

- Providing timely and accurate information about potential risks and hazards.
- Encouraging personnel to report concerns or incidents without fear of retribution.
- Fostering an open-door policy where personnel feel comfortable approaching leaders and managers with questions or concerns.
- Using multiple communication channels, such as training sessions, meetings and written notifications, to reach all personnel.
- Ensuring that communication is clear, concise, and easily understood by all stakeholders.

d. By prioritizing risk communication and making it an integral part of the risk management process, organizations can:

- Improve situational awareness and reduce the risk of surprises.
- Enhance collaboration and cooperation among personnel.
- Increase personnel engagement and ownership of risk mitigation efforts.
- Support informed decision-making and reduce the risk of errors.
- Foster a culture of transparency, trust and accountability.

e. Ultimately, effective communication is essential to building a robust and resilient risk management framework that supports the organization's overall mission and objectives.

f. An important aspect of risk communication is the relationship between the command's RCS risk registry (or register) and Integrated Risk Management (IRM) and the flow of information. Risk registries flow information to the CNO *(Figure 3).* Echelon II organizations funnel mission-critical risks (captured by subordinate commands) to the CNO's Risk Management and Internal Control Program Office as part of the IRM program. Risks from the organization's risk registry are typically reported in the operations section of the IRM report. This process enables senior leadership to see "bottom-up" risks with potential impact. The risk registries ultimately inform the CNO, under the auspices of the IRM program, of what risks are out there, what needs to be resolved and what has been fixed or mitigated. This upward line of communication and reporting ensures all levels of command are better informed and aware of all mission-critical risks.

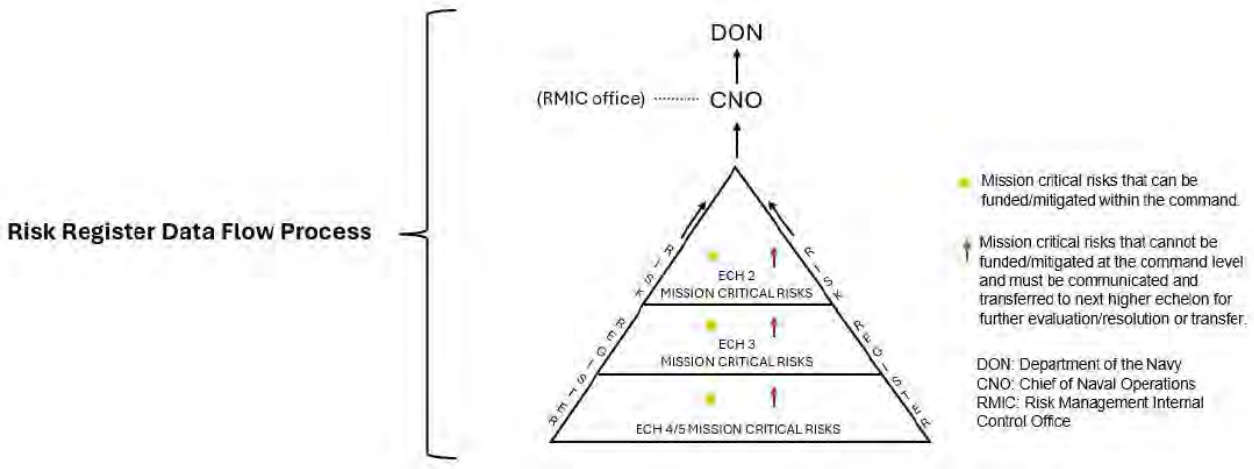


Figure 3. Risk Registry flow of information to CNO

6. Risk Management Process

a. The risk management process is a dynamic and iterative cycle, where each step builds upon and informs the other, ensuring that risk management is a continuous and ongoing effort. This cyclical process involves a series of interconnected steps that are repeated, with each iteration refining and improving over time, as well as the overall risk management approach.

b. The benefits of an iterative and continuous risk management process include:

- Improved risk awareness and understanding, enabling more informed decision-making
- Enhanced risk mitigation and control, reducing the likelihood and impact of adverse events
- Increased agility and adaptability, allowing the organization to respond quickly to changing circumstances and new risks
- Better allocation of resources, focusing on the most critical risks and opportunities
- Improved stakeholder (internal and external) confidence and trust, demonstrating a proactive and responsible approach to risk management

c. Risk Management Process Steps

(1) Risk and Hazard Identification

(a) The first critical step in the risk management process is to identify potential risks and hazards that could impact the organization, its mission, or personnel. This involves a systematic and structured approach to recognize and document potential risks and hazards that may affect the organization's strategic objectives, operations, or personnel. *(Figure 4)*

Figure 4. Risk Management Process Steps

(b) Risks versus Hazards. The words “risks” and “hazards” are often used interchangeably, but they have distinct meanings. Risks refer to the potential consequences of an event or situation that may impact the organization's strategic objectives, whereas hazards refer to the specific conditions or situations that may lead to harm or damage. Risks are typically identified through planning and assurance activities such as strategic planning, business continuity planning and audit activities. Hazards, on the other hand, are most often identified through day-to-day operations and compliance monitoring, such as workplace inspections, incident reporting and regulatory compliance audits.

(c) There are many documented approaches and methodologies that can be applied when conducting risk identification. Some of the most common techniques are described below.

1. **Deliberate Planning** (i.e., Operational Evolution Planning). A workshop-like session planned well in advance with affected parties to identify significant risks to the organizations. Deliberate planning consists of the following activities:

- To ensure alignment with the organization's overall goals and objectives, obtain the long-term strategy and in-year objectives for the risk area(s) under review.
- Conduct in-depth briefs with selected participants involved in the process to gather insights and perspectives on the most significant risks to the organization's operations and mission achievements.
- During the interview, seek to ascertain what the risks are and explore why participants deem them to be significant. Asking open-ended questions can help identify the risk event, followed by asking what could trigger the event (e.g., lots of 'why' questions). Participants typically find the identification of the cause or root cause of the risks the most challenging aspect of risk identification. Then consider the consequences of the risk and how they impact the objectives and strategy.
- If unable to conduct briefs or for participants who are unable to attend any briefs, it is recommended to send a read-ahead document in advance of the session, explaining the purpose of the planning session, asking them to review the risk area objectives and strategy and to e-mail you what they consider to be the key risks in advance of the planning session.
- Analyze the results of the briefing responses and create a preliminary list of key risks. Identifying any common themes and outliers.
- Start with the preliminary list of risks and ensure the list is complete. Are any significant risks missing? There may be too many risks identified at this stage to realistically discuss them all in a single session. An initial meeting will need to be completed to prioritize those that should be the focus of the planning session and that are appropriate to be owned at this level or if there are risks that need to be elevated.
- Once the preliminary risks are identified and agreed upon, each risk should be discussed to come to an agreement on the descriptions, which should be structured in a cause-event-consequence format. Ensure that the event has an element of uncertainty to it and ensure the real root cause of the risk is identified. Consider the full range of consequences that could result from the risk event, and ensure all significant consequences are described.
- Ensure the accountable person is aware of each risk and is the appropriate person to accept the risk at their level.
- Identify and record the key controls and mitigations in place, the initial and residual risk levels, and the response plan.
- Once the risks have all been assessed, and response plans created and accepted by the accountable person, the risks should be communicated with all personnel to ensure appropriate risk communication and awareness.

2. **Bowtie Method** (not to be confused with the resilience model from OPNAVINST 3058.1). The bowtie method is a visual risk assessment technique that provides a comprehensive and structured approach to identifying and analyzing potential risks. This method results in a visual tool, known as a bowtie diagram, which diagrammatically represents the various elements of a risk in a bowtie-shaped risk picture. The bowtie method is a widely used and effective technique for risk assessment and management, and its visual representation makes it easy to understand and communicate complex risk information.

a. The Bowtie Shaped Risk Picture. The bowtie shaped risk picture is a unique and intuitive visual representation of the risk, allowing users to easily identify and understand the relationship between different elements of risk *(Figure 5).* This risk picture is divided into two main sections:

- Left Side- Potential Causes: The left side of the bowtie represents the potential causes of an adverse event, including the underlying hazards, threats, and vulnerabilities that could lead to the event. This section helps to identify the potential triggers and contributing factors that could lead to an adverse event.
- Right Side- Potential Consequences: The right side of the bowtie represents the potential consequences of the adverse event, including the potential impacts, effects and outcomes that could result from the event. This section helps to identify the potential harm, damage, or loss that could result from an adverse event.

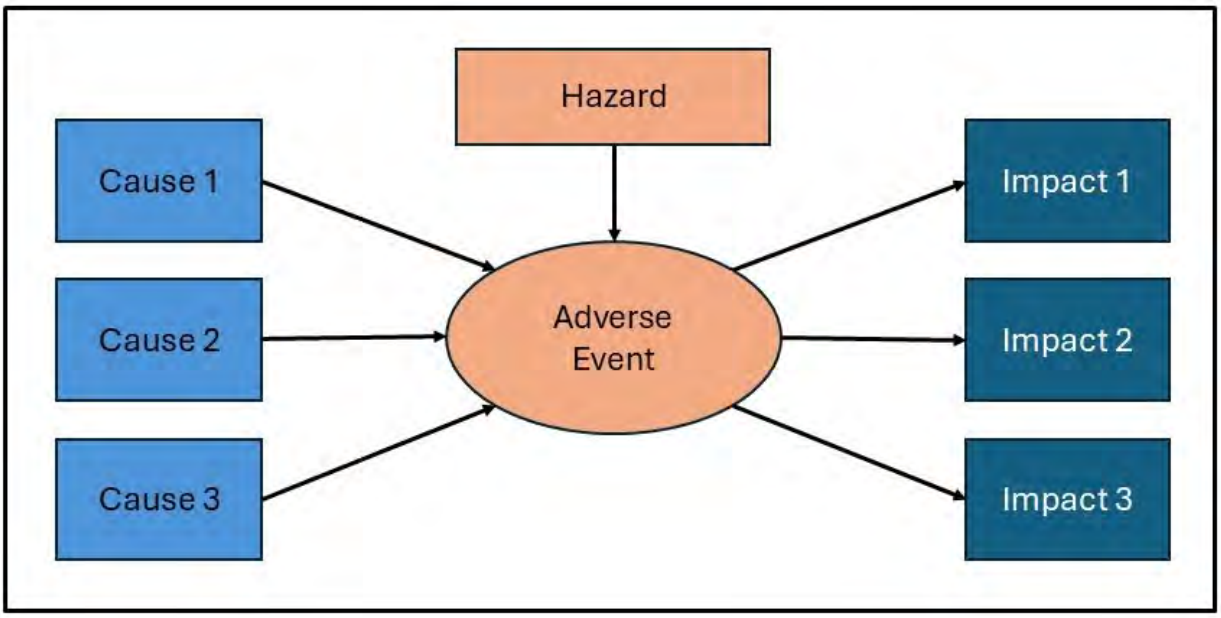


Figure 5. Bowtie Diagram

b. The Bowtie Method: A Common Language Framework. The bowtie method provides a common language and framework for discussion and analyzing risks. By using the bowtie method, organizations can:

- Gain a deeper understanding of the risks they face, including the potential causes and consequences of adverse events.
- Develop effective strategies to manage and mitigate risks, including identifying and implementing controls, safeguards and mitigation measures.
- Improve communication and collaboration among stakeholders, including risk managers, subject matter experts and decision-makers.
- Enhance risk awareness and culture within the organization, including promoting a risk-informed decision-making approach and encouraging a proactive and preventive approach to risk management.

3. **Fault Tree Analysis (FTA) Method**. Fault tree analysis is a systematic, top-down, deductive approach to evaluating the potential failures of a complex system. This methodical process begins with the identification of an undesired top-level event, often referred to as the "top event," which represents a critical failure or hazard within the system. The primary objective of FTA is to identify and understand the potential causes and contributing factors that could lead to the occurrence of this top event, thereby enabling proactive measures to mitigate or prevent such failures. The logical relationships between these events are represented using logical gates, such as AND, OR, and NOT gates, which define how the occurrence of basic and intermediate events can lead to the occurrence of higher-level events. For instance, an AND gate indicates that all the input events must occur for the output event to occur, while an OR gate indicates that the output event will occur if any of the input events occur. *Figure 6* illustrates a simplified example of a fault tree diagram.

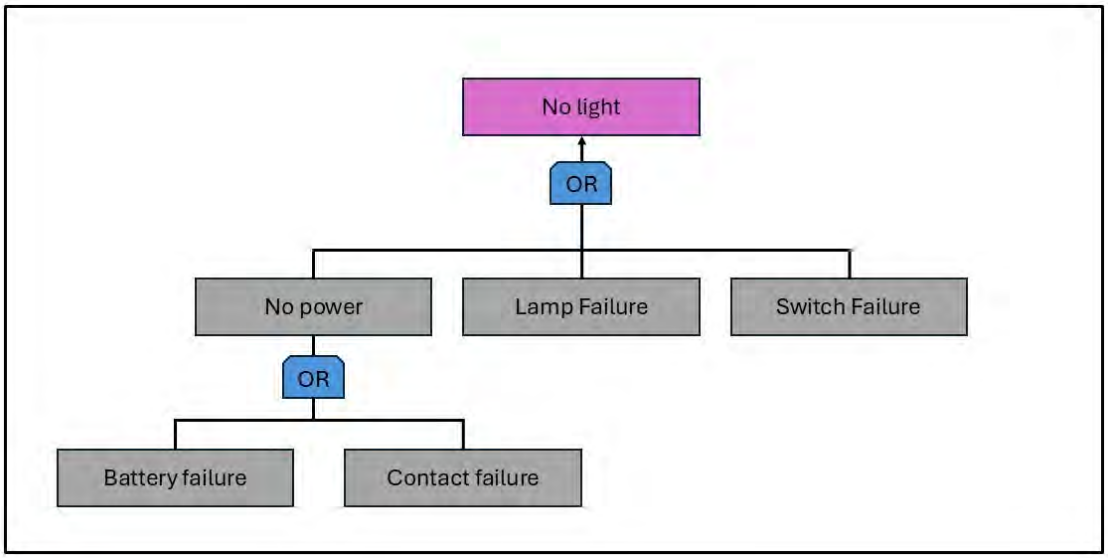


Figure 6. Fault Tree Diagram

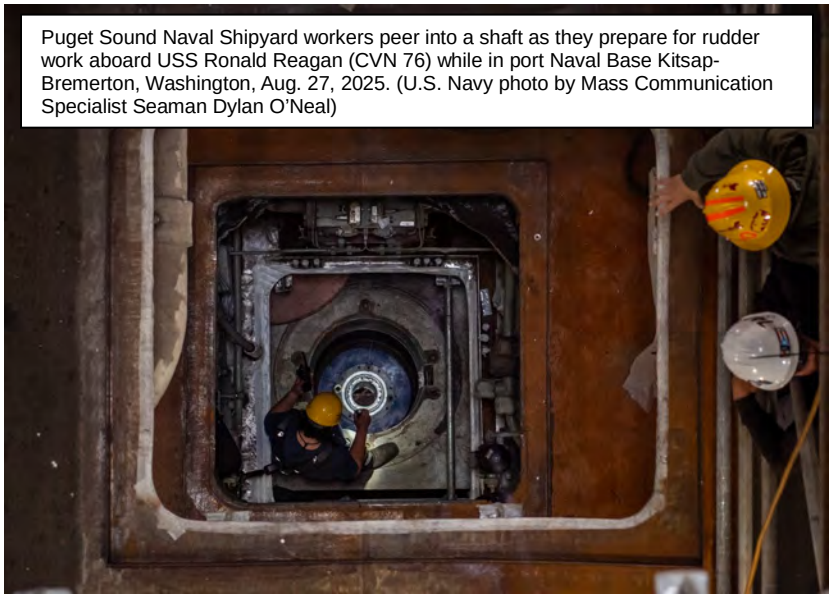
a. FTA is widely applied in various fields, including system reliability, maintainability and safety analysis, due to its ability to provide a comprehensive and visual representation of the potential failure paths. By using FTA, personnel can:

- Identify the potential causes of system failures, allowing for proactive measures to mitigate or prevent such failures.
- Provide a quantitative assessment of the system's reliability, enabling the evaluation of the likelihood of failure and the identification of critical components or factors.
- Inform the design process, enabling the development of more reliable and fault-tolerant systems.
- Prioritize maintenance activities and develop targeted maintenance strategies to minimize downtime and reduce maintenance costs.
- Enable the identification of potential hazards and the evaluation of the likelihood and potential consequences of accidents.

(d) Risk Ownership and Acceptance

1. Once a risk or hazard has been identified and recorded, a designated risk owner, or Accountable Person (AP), assumes accountability for overseeing and managing it. By assigning a risk owner, organizations can ensure that risks are properly managed, and that accountability and transparency are maintained throughout the risk management process. The AP's responsibilities encompass all aspects of risk management, including:

- Ensuring the risk is accurately and clearly described to facilitate understanding and communication.
- Identifying and implementing controls and mitigations to manage the risk, as well as evaluating their effectiveness.
- Verifying that controls and mitigations are operating as intended and making adjustments as needed to ensure their ongoing effectiveness.
- Conducting accurate assessments of both the initial (raw) and the residual (mitigated) risk to inform decision-making.
- Continuously monitoring the risk for changes in its severity, likelihood, or impact, and updating risk assessments and mitigation strategies accordingly.
- Communicating risk information to relevant stakeholders, including those who may be impacted by the risk, as well as reporting up and down the chain of command to ensure that leadership and other key stakeholders are informed and engaged.



Puget Sound Naval Shipyard workers peer into a shaft as they prepare for rudder work aboard USS Ronald Reagan (CVN 76) while in port Naval Base Kitsap-Bremerton, Washington, Aug. 27, 2025. (U.S. Navy photo by Mass Communication Specialist Seaman Dylan O'Neal)

2. When a risk is identified that falls outside the organization's direct control or is more appropriately owned by another organization, it is essential to establish a clear understanding of risk ownership and management responsibilities. In such cases, the organization that initially identified the risk should engage with the organization capable of eliminating the risk to discuss and acknowledge the transfer of risk ownership. This communication in no way alleviates the unit affected by the risk to implement adequate mitigations (including ceasing operations) to ensure the safety of operations and personnel. It is incumbent on the risk owner to communicate down the chain of command when risk decisions affect a subordinate command. For example, if a risk is accepted in the acquisition process, that risk must be formally communicated to the end user.

U.S. Marine Corps Cpl. Kelvin Adjei, an airframes mechanic with Marine Attack Squadron (VMA) 231, stands in front of an AV-8B Harrier II at Naval Air Facility El Centro, California, Feb. 24, 2025. (U.S. Marine Corps photo by Cpl. David Ornelas Baeza)

3. If the risk is deemed to be the responsibility of another organization, the following steps should be taken:

- Notification: The organization that identified the risk should notify the relevant organization of the potential risk and provide sufficient information to enable them to understand the risk and its potential consequences.
- Acknowledgement: The relevant organization should acknowledge receipt of the risk information and confirm their acceptance of risk ownership.
- Risk Management Plan: The relevant organization should provide a risk management plan that outlines how they intend to manage the risk, including any controls or mitigations they will implement.
- Ongoing Communication: The organization that initially identified the risk should establish a communication plan to ensure that they receive regular updates on risk management activities and any changes to the risk profile.

(e) Risk Categories. Risk categories are a crucial framework for identifying, assessing, and prioritizing potential risks that can impact an organization's ability to achieve its objectives. By categorizing risks, organizations can better understand the potential threats and opportunities and develop targeted strategies to mitigate or capitalize on them. Below is a list of risk categories:

- Strategic: Risks associated with the overall management and direction of the organization. Strategic risks can have a significant impact on the organization's long-term success and viability.
- Operational: Risks associated with the day-to-day operations of the organization. Operational risks can disrupt the organization's ability to achieve its objectives.

- People: Risks associated with the management of human capital. People risks can impact the organization's ability to attract, retain and develop talented personnel, which is critical to achieving its objectives.
- Warfighting Capability: Risks associated with the ability to project and deliver military power to achieve strategic and tactical objectives.
- Infrastructure: Risks associated with all support services.
- Finance: Risks associated with the accounting and reporting of naval activity and spending
- Information: Risks associated with information security including cybersecurity and resilience
- Reputational: Risks associated with the possibility that an organization's actions or inactions could cause a negative public perception that damages the organization's reputation.

U.S. Navy Aviation Boatswain's Mate (Handling) Airman Autumn Salvador paints in the hangar bay of the Nimitz-class aircraft carrier USS Theodore Roosevelt (CVN 71). (U.S. Navy photo by Mass Communication Specialist 3rd Class Aaron Haro Gonzalez)

(f) Tips for Identifying Risks

- Do not identify issues as risk. An issue is already occurring or has happened, therefore has no uncertainty. There may be a risk that this issue will worsen or will remain if no action is taken to manage the issue.
- When considering risks to achieving objectives, do not simply describe the opposite of the objective.
- Be as specific as possible when describing risks.

- When identifying risks, consider near misses. A near miss is an adverse event or set of circumstances that had the potential for significantly more severe consequences than were experienced.
- Do not state impacts as risks, use the cause-event-consequence approach to describe the risk properly.
- Consider any dependencies, milestones, activities, timescales and resources that will be used to achieve objectives.

(g) Risk Identification Worked Example. Below is a hypothetical example of the risk identification process:

A Commander has a conversation with a colleague that mentions that their team is under a lot of pressure to resolve an issue in their team, which has resulted from the bankruptcy of a critical supplier. This triggers the Commander to think whether such an event could occur on her team, so she decides to be proactive and investigate this, and think about any other adverse events that could impact the ability of her team to deliver its objectives.

She organizes a deliberate planning session, to which she invites her entire team of 10 people. She asks each team member to think about all risks and hazards that could negatively impact the team's ability to meet its objectives and asks them to email their responses to her in advance.

On receipt of these e-mails, she finds there are a few themes emerging where several team members have raised similar risks. There are also a few outliers where only one person has raised some risks. She collates these into a draft list of risks facing her team, which she uses to kick off the planning session.

After an initial update to this list, she then goes through each risk to ensure the description is correct and in the right cause-event-consequence format and is communicated to the Accountable Person.

A risk that caused significant debate was centered around the risk that the supplier of critical equipment Y could become insolvent. Several reasons why the supplier could become insolvent were discussed, including the fact that the supplier recently lost a major contract with another one of their customers, however it was determined that the primary cause of why the supplier may go bankrupt was due to a downturn in the economy. It was also agreed that this was a key risk because at the time, the DON could only source critical equipment from this supplier.

The risk description is agreed to be a "a downturn in the economy causes Company X, the only supplier of critical equipment Y to become insolvent, resulting in significant disruption to DON operations."

(2) Risk Assessment and Prioritization. Risk assessment determines the significance of a risk by considering two factors, the potential impact (severity) and the likelihood (probability) of the risk occurring.

- Severity (impact). The severity of a risk is established by considering its potential effects on the achievement of the organization's objectives. Objectives can vary widely in their nature and significance; a standard measurement scale is typically used to consistently evaluate risks. (*See Table 1 and Figure 7*)

- Probability (likelihood). The likelihood of a risk occurring is determined by estimating the probability or expected frequency of the risk occurring in a given timeframe.

Hazard Severity		Mishap Probability			
Description	Code	A Likely to occur immediately or in a short time	B Probably will occur in time	C Possibly will occur in time	D Unlikely to occur in time
Death, permanent total disability, or loss of facility or asset	I	1 Critical	1 Critical	2 Serious	4 Minor
Permanent partial disability or major property damage	II	1 Critical	2 Serious	3 Moderate	4 Minor
Lost workday injury or compensable injury, or minor property damage	III	2 Serious	3 Moderate	4 Minor	5 Negligible
Injury involving first aid or minor supportive medical treatment, a minimal threat to personnel or property, or a violation of a standard	IV	4 Minor	4 Minor	5 Negligible	5 Negligible

Table 1. Risk Assessment Code Matrix from DoDI 6055.01.

(a) How to Assess Initial and Residual Risk. To understand the true nature and potential of a risk exposure and determining the most appropriate response requires accurate assessment of the initial (raw) and residual (mitigated) risk. Mitigations are activities and/or measures put in place to reduce the impact of an adverse event.

1. Initial (raw) Risk Assessment. The assessment of initial risk is based on the assessment of a pre-mitigated impact and likelihood. The initial risk assumes that controls and mitigations are not in place or do not function as intended. This assessment determines the reasonably foreseeable, plausible worst-case scenario for the risk. Assessing risk on an initial basis provides a view of how bad a risk could be if the existing controls and mitigations in place do not work as intended or do not exist. This is important as when compared to the residual risk exposure it provides an understanding of the amount of reliance being placed on current activities, focusing scrutiny and challenge by management on their effectiveness and adequacy in light of reasonably, plausible worse case consequences.

2. Residual Risk Assessment. The assessment of residual risk is based on the assessment of the mitigated impact and likelihood of a risk. It assumes that the specific and significant controls and mitigations that are in place are working as intended. Residual risk assessment tells the current severity of a risk's existing controls and mitigations to manage the risk are in place and are working as intended. Residual risk allows for the current aggregated risk exposure to be considered when determining

whether to take on more risk or where the balance of investment should be focused. In addition to assisting in focusing the risk owners and management towards the most significant risks, understanding the difference between initial and residual assessments also helps inform the assurance focus and in can determine risk reporting requirements

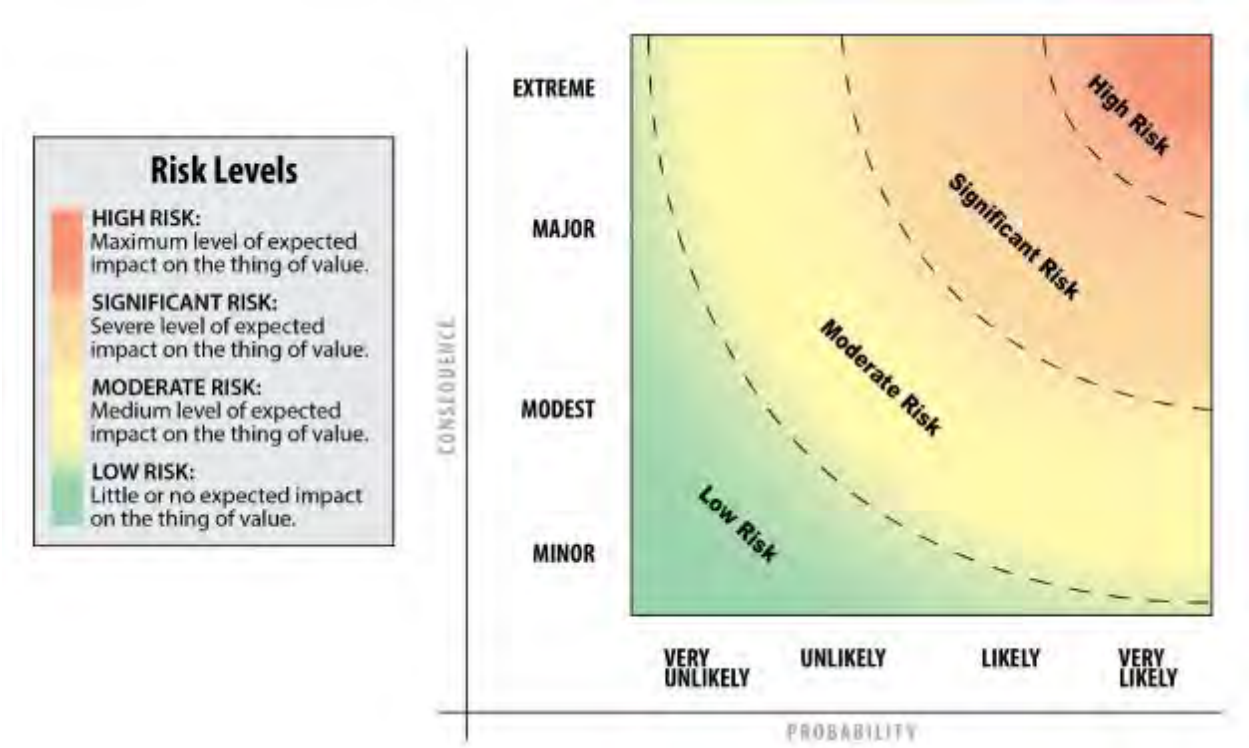


Figure 7. Risk Characterization graphic from CJCSM 3105.01B. This graphic is an alternative method to visualize risk characterization.

(b) How to Assess Risk. Once a risk has been identified, the following steps should be carried out, to assess the severity of the risk:

Step 1: Establish the controls and mitigations currently in place. Detail all significant controls and mitigations that are specifically applied to actively manage the risk at present and consider their effectiveness. The following should be considered:

- What component(s) of the risk do the controls and mitigations affect? How and by how much? Do they fully prevent a cause leading to an adverse event? Are they independent or do they rely on other processes or activities to work effectively?
- How reliable are the controls?
- What are the limitations of the controls?
- If a control fails, is there a back-up?

Step 2: Assess the initial risk. What would the likelihood and impact of the risk be if controls and mitigation did not exist? The following should be considered:

- What could happen?

- How severe could the impact be and what is the reasonably foreseeable, plausible worst-case scenario?
- How likely is it that the risk will occur? Is what causes the risk a permanent state or intermittent?

Step 3: Assess the residual risk. Taking into account the controls and mitigations in place, estimate the residual risk size. What are the likelihood and impact based on the effectiveness of the controls and mitigations in place? The effectiveness and reliability of the controls and mitigations should be considered when estimating residual risk

Step 4: Differences. What are the differences between the initial risk, the residual risk and the acceptable level of risk exposure? Consider the following to capture the differences:

- Capture activities that have been agreed upon, where funding (if applicable) has been approved and where the activities will be implemented and effective within five years.
- Identify activities that could be put in place with the existing funding available.
- Consider whether those funded activities and those which could be funded within existing budgetary constraints would decrease the risk exposure to an acceptable level.
- Where risk exposure remains unacceptable, the risk owner should communicate the risk to higher level of authority and ensure consequences of the remaining risk exposure are fully understood.

(c) Risk Prioritization. If multiple risks require a response, it may be necessary to prioritize the order in which the risks are managed due to time and resource constraints. The following points should be considered when prioritizing risks for response:

- Risks that have the greatest residual risk impact. Likelihood should be a secondary consideration after impact for prioritization as it can be the more subjective measurement in risk assessment.
- Risks with the largest difference between initial and residual risk, where management wants more levels of control as current controls may not be reliable.
- The proximity of risk, i.e., a risk which could occur in the near future may warrant prioritization over those that are longer-term. Care should be taken to ensure that imminent risks are not continuously prioritized at the expense of adequate management of longer-terms risks, and that the longer-term risks also receive sufficient resources and focus to ensure they are responded to before they turn into imminent risks.
- Consideration of feasibility, cost, resources and time required to further manage the risk.
- The prioritization/importance of the objective that will be affected, should the risk occur.
- Accountable Person manages priorities and focus.

(3) Risk Mitigation. The purpose of risk management is not to eliminate all risk but to manage or mitigate the risk to an acceptable level. Where the risk is not acceptable, appropriate actions

(mitigations) will need to be selected and implemented to bring the residual risk to an acceptable level. Risk mitigation should be based on their effectiveness, cost and feasibility. *Figure 8* describes risk mitigation options.

Risk Mitigation Type	Definition
Avoidance	Forgo the activity that would produce intolerable risk
Reduction	Implement measures (risk mitigation activities) that decrease the probability or consequence of harm
Transfer	Take action to change where and when the risk is incurred and potentially who or what incurs it
Acceptance	Make an informed decision to act without mitigating the risk
Take the opportunity	Action taken to exploit an opportunity

Figure 8. Risk Mitigation Options

(a) Where "reduction" is selected as the appropriate risk mitigation, consideration should be given to the different types of controls available and the overall control environment created to manage the risk. The following factors should be considered:

- Effectiveness of the proposed response in actually reducing the probability and/or impact of the risk.
- Efficiency of the proposed mitigation compared to other options.
- Reliability of the proposed controls.
- The type of control required.
- Cost and resource requirements of the proposed response.
- Timeframe to implement the response compared to how rapidly a response is needed.

(b) Hierarchy of Controls. The Hierarchy of Controls is a fundamental concept in risk management, particularly in the context of occupational health and safety. It provides a framework for controlling and mitigating risks in the workplace by ranking control measures in order of their effectiveness.

1. The Hierarchy of Controls *(Figure 9)* is typically depicted as a pyramid, with the most effective controls at the base and the least effective at the top. The hierarchy is as follows:

a. Elimination: This is the most effective control measure, which involves removing the hazard or risk altogether. For example, if a particular chemical is hazardous, eliminating its use in the workplace would be the best way to control the risk.

b. Substitution: If elimination is not possible, the next best option is to substitute the hazardous material or process with a safer alternative. For instance, replacing a toxic chemical with a less toxic one or using a different process that reduces the risk of injury.

c. Engineering Controls: These controls involve modifying the workplace or equipment to reduce the risk of injury or illness. Examples include:

- Ventilation systems to remove airborne contaminants.
- Machine guards to prevent accidental contact with moving parts.
- Safety interlocks to prevent equipment from operating when a guard is open.

d. Administrative Controls: These controls involve implementing policies, procedures and training to reduce the risk of injury or illness. Examples include:

- Developing SOPs for hazardous tasks.
- Provide training on safe work practices and emergency procedures.
- Implementing rotation of workers to reduce exposure to hazardous tasks.

e. Personal Protective Equipment (PPE): This is the least effective control measure, which involves providing workers with equipment to protect themselves from hazards. Examples include:

- Hard hats and safety glasses to protect against physical hazards.
- Respirators to protect against airborne contaminants.
- Gloves and safety vests to protect against chemical and physical hazards.

2. The Hierarchy of Controls is important because it:

- Encourages a proactive approach to risk management, focusing on eliminating or controlling hazards at the source.
- Provides a framework for evaluating and prioritizing control measures.
- Helps to minimize reliance on PPE, which can be less effective and more prone to human error.
- Supports a culture of safety and risk awareness in the workplace.

3. By applying the Hierarchy of Controls, organizations can effectively manage risks and reduce the likelihood of injuries and illnesses in the workplace. *(Figure 9)*

(c) Developing a Risk Response Plan. A risk response plan should be prepared once the risk mitigation options have been assessed, prioritized and the appropriate risk controls/responses have been determined. The plan should be reviewed by the Accountable Person to consider whether its implementation will change the assessed risk level to an acceptable level of risk. If the risk is not acceptable, then consideration needs to be given as to whether there are additional activities (within resource constraints) that could be added to the response plan to reach the acceptable level.

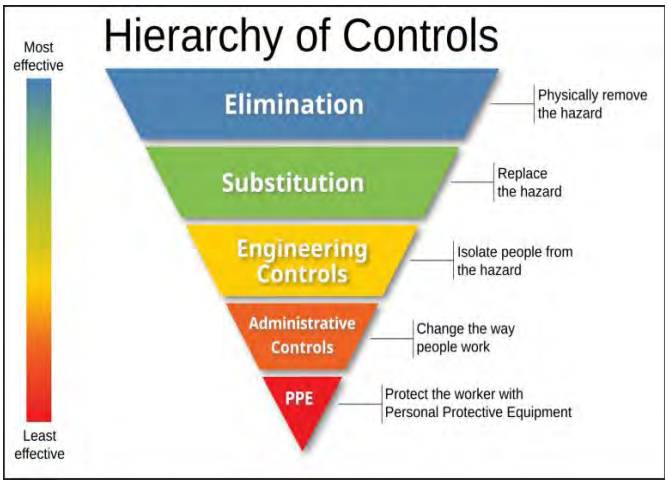


Figure 9. Hierarchy of Controls

Risk Response and Mitigation Worked Example. Below is a hypothetical example of the risk response and mitigation process.

Previously identified risk: a downturn in the economy causes Company X, the only supplier of critical equipment Y to become insolvent, resulting in significant disruption to operations.

A previously established risk already being managed through:

- Financial due diligence during supplier selection.
- Monthly operational KPI checks.
- Regular contact of sourcing staff with supplier.
- Business continuity planning has identified an alternative provider and describes a process for transition.
- Spares are warehoused.

However, the risk is still deemed to be unacceptable, therefore further response options are considered.

The business decides to dual source the product, so a plan is put in place to work with an alternative provider (the one identified in the business continuity planning) and to contract with them to deliver 20% of the volume of equipment required.

The volume of equipment delivered by Company X therefore needs to be reduced by 20%; this introduces a knock-on risk that the reduced volume (and therefore reduced revenue for Company X) causes financial stress, which could increase the likelihood of Company X going into insolvency.
To mitigate this unintended consequence, and to minimize any potential business disruption in case Company X goes into insolvency before the alternative supplier is on board, two proposals are suggested:

- Change the payment terms to improve Company X's cash flow.
- Obtain approval to support and finance Company X if it goes into insolvency

Both proposals are approved, and funding is allocated from within existing budgets. Action owners are appointed by the Accountable Person to implement each of the agreed-upon response plans.

(4) Monitor and Review Risks. Capture, tracking and review of risk information is required to be able to identify changes to risks and notify leadership to those changes to support understanding and decisions on mitigations.

(a) Risk Monitoring. Organizations should implement monitoring and review processes to track the status of individual risks, aggregated risks and the effectiveness of their risk management risk process. Risk monitoring provides leadership with the necessary risk information to:

- Detect changes in risk profile and status of risks, supporting decisions on prioritization, reporting up the management line, and response activities as well as providing evidence to support assessments of future performance.
- Allow oversight of the completeness and quality of the risk information produced and the robustness of the risk management approach.

- Ensure that risk mitigations are effective and efficient in both design and operation.
- Monitor the progress of risk response plans.
- Obtain further information to improve the identification and analysis of risks.
- Analyze risk issues, changes, trends, leadership successes and failures to capture lessons learned and ensure continuous improvement.

Risk Monitoring Worked Example. Below is a hypothetical example of the risk monitoring process:

Previously identified risk: a downturn in the economy causes Company X, the only supplier of critical equipment Y to become insolvent, resulting in significant disruption to operations.

A number of monitoring activities are put into place:

- <u>Monitoring the response plan:</u>
- Each of the response plans is closely monitored to ensure that they get completed on time and to budget, and to check that they adequately mitigate the risk as expected.
- For example, the project plan and progress on securing a contract with, and on boarding, the alternative supplier is monitored on a weekly basis to ensure the activity is completed on time. The ability for the new supplier to deliver the required volumes of critical equipment Y to schedule is also closely monitored.
- <u>Monitoring whether there are any changes to the risk's likelihood or impact:</u>
- The economy is monitored to identify whether a downturn is likely to occur, and how severe it will be, to establish whether this increases the risk of Company X becoming insolvent.
- Wider performance of Company X is also monitored, including whether it is winning new work with other customers, to help strengthen its financial position.
- Turnover of management and staff is also monitored, as indicators of further financial distress.

- <u>Monitoring the existing controls and mitigations:</u>
- Checks are put in place to ensure that there are sufficient spares being warehoused, and that the buffer stock is not being depleted.
- The Accountable Person checks that the operational KPI checks and regular contact of sourcing staff with the supplier are actually taking place.
- The Accountable Person reviews the business continuity plan and ensures it is up-to-date, appropriate and fit for purpose.

(b) Risk Review. The Accountable Person should establish the frequency of review and monitoring for each risk. The Quarterly Hazard Review Board process defined in OPNAV M-5102.1 Chapter 6 is an example of this process. Regular risk monitoring enables the Accountable Person to:

- Confirm that the controls and mitigations implemented to manage the risk are operating effectively.
- Adjust controls and mitigations as required.
- Identify changes to the risk including deterioration in status or circumstances that can affect risk severity and probability and report as necessary.

- Ensure any significant changes are communicated both up and down the chain of command.

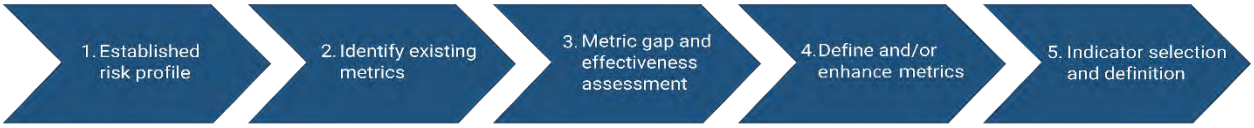
7. Key Risk Indicators

a. Key Risk Indicators (KRIs) are forward looking information points and metrics that when tracked can provide an early warning of the occurrence of a risk and/or change in its potential severity or probability. Typically, for metrics to make effective indicators they should have strong relationships with the cause and drivers of specific risks to be predictive, as well as being able to be practically tracked.

b. Benefits to KRIs. An effective KRI-based risk monitoring system will produce the following benefits.

- Establishes the basis for developing a robust early warning risk management system focused on avoidance of risk occurrence as opposed to crisis management.
- Promotes a 'no-surprise' environment through continuous monitoring of risk exposures.
- Communicates the acceptability of risk through aligned escalation thresholds.
- Increases awareness of risk among all personnel and the importance of effective monitoring and reporting.

c. Defining KRIs - The Process. Detailed below is a five-step process to define robust KRIs.



(1) Establish Risk Profile. This can be done by identifying risks and associated response activities and allocating weight to risk drivers and risk responses.

(a) Identify risks and associated response activities. Conduct a thorough review of relevant risk registries, collaborating with SMEs as needed, to comprehensively identify and assess all potential risks and their corresponding response activities. This review will enable the development of KRIs that are targeted, forward-looking and predictive, by:

- Identifying critical risks: Focus on the most significant risks that have the greatest potential impact on the organization.
- Understanding cause-and-effect relationships: Analyze the relationships between risks, their causes, and potential consequences to develop a deeper understanding of the risk landscape.
- Evaluating response activity effectiveness: Assess the reliability and effectiveness of existing response activities to ensure they are adequate and can be improved upon.
- Informing KRI development: Use the insights gained from this review to develop KRIs that are relevant, measurable, and actionable, enabling proactive risk management and mitigation.

(b) Allocate weight to risk drivers and risk responses. Assign relative weights to risk drivers and response activities based on a thorough analysis of their relationships and effectiveness. To do this:

- Assess the strength of relationships. Evaluate the correlation between identified risk drivers and risk causes and allocate weights accordingly. Focus on drivers with medium strength relationships (these drivers have a notable impact on the risk cause should be closely monitored) and high strength relationships (these drivers have a significant impact on the risk cause and should be prioritized for mitigation and management).
- Evaluate response activity effectiveness. Assess the reliability and effectiveness of identified response activities in managing the likelihood or impact of the risk. Allocate weight based on their ability to prevent or mitigate the risk. Focusing on response activities that can significantly reduce the likelihood or impact of the risk and their potential consequences of failure. Prioritizing response activities that, if they fail, would have the most significant effect on the risk occurring or increasing in impact.
- Prioritize critical response activities. Identify response activities that are crucial to preventing or mitigating the risk and allocate higher weights to these activities. Consider scenarios where failure would have a significant impact as well as where success would have a substantial benefit.

Seaman Joshua Bunnell climbs down a ladder after conducting a routine maintenance check on the king post aboard USS Kidd (DDG 100). (U.S. Navy photo by Mass Communication Specialist 2nd Class Mason Congleton)

(2) Identify existing metrics. Conduct a thorough review of existing risk management and performance information/reporting to identify metrics that are currently being tracked against each risk in focus. These metrics may have the potential to be effective KRIs and can provide valuable insight into the organization's risk profile. To facilitate this review, consider the following steps:

- Gather relevant information: Collect and review existing risk management and performance reports, dashboards and metrics to identify potential KRIs.

- Identify metrics with KRI potential: Determine which metrics have the potential to be effective KRIs, based on their ability to measure and monitor risk drivers, likelihood, impact or other relevant risk factors.
- Create a metrics mapping matrix: Develop a matrix to map the identified metrics against the drivers of the organization's key risks. This matrix can help to illustrate the relationships between metrics and risk drivers, highlighting potential correlations and areas of focus as well as identify metrics with multiple risk relationships. An example of a metric mapping matrix is provided below *(Figure 10).*

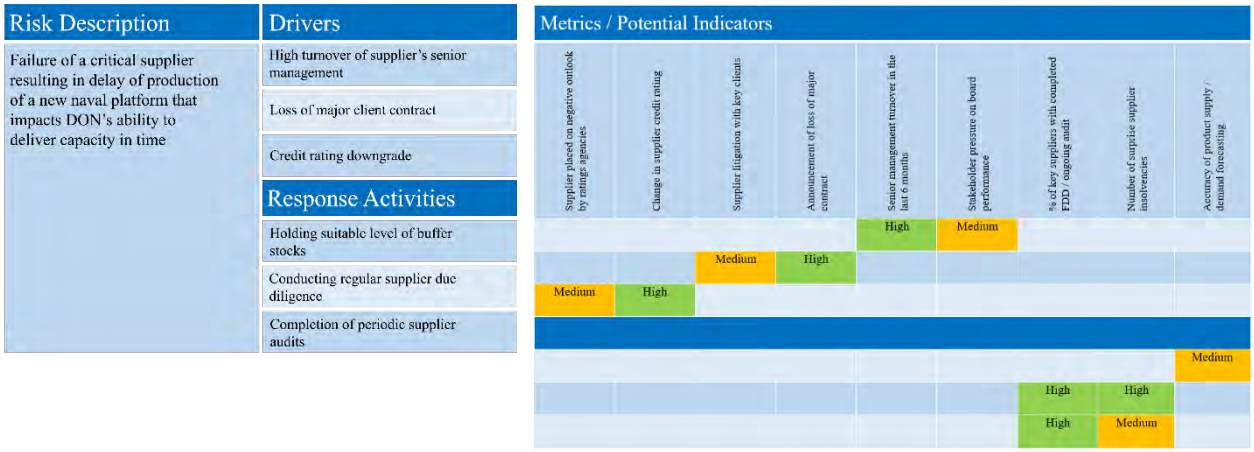


Figure 10. KRI metric mapping matrix

- Metric gap and effectiveness assessment. Analyze the relationships between risk drivers, risk responses and metrics to identify potential gaps in indicator coverage. Specifically, focus on risk drivers or risk responses that have multiple high or medium strength relationships with multiple metrics. This analysis can help identify areas where there may be insufficient metrics to support the development of robust predictive indicators.

- Gaps in indicator coverage can compromise the effectiveness of an early warning system in several ways such as insufficient data, inadequate risk monitoring and reduced predictive power. To address these gaps, identify risk drivers or risk responses with limited metric coverage, assess the potential impact of gaps in indicator coverage and develop a plan to address gaps in indicator coverage.

- By addressing gaps in indicator coverage, organizations can ensure that their early warning systems are effective in identifying potential risks, providing timely warnings and supporting informed decision making. Besides conducting a gap assessment, a KRI-effectiveness assessment should be conducted as well. Table 2 can assist in conducting a thorough assessment of KRI effectiveness. *Figure 11* provides an example of KRI effectiveness assessment.

Two MH-60S Sea Hawk helicopters, assigned to Helicopter Sea Combat Squadron (HSC) 14. (U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Daniel Kimmelman)

KRI Effectiveness Criteria				
Criteria	Question	Low	Medium	High
Ease and cost of tracking	Can the metric be easily and cost effectively tracked?	The metric is external to the organization and is difficult to obtain.	The metric can be obtained but requires new / additional work to do so. Potential measurement error is perceived to be low.	Metric is obtainable internally through a reliable, repeatable procedure. Measurement error is very low
Tracking frequency	Can the metric be tracked with sufficient frequency to facilitate early intervention?	Unable to track the metric at the required frequency to enable timely intervention.	Metric can be tracked at an acceptable, but not optimized frequency, which will support timely intervention.	Tracking frequency can be optimized to maximize early warning and intervention time.
Predictive value (leading or lagging)	Is the metric leading or lagging in nature?	The metric has a low strength relationship with the cause / drivers and/or response activities.	The metric has at least a moderate strength relationship with the cause / drivers and/or response activities but may	The metric has a strong relationship with the cause / drivers and/or response activities, maximizing

			not be sufficiently leading to facilitate early intervention.	opportunity for early intervention.
Source integrity and data accuracy/completeness	How reliable is the information source and is the data accurate and complete?	Information source is not perceived to be reliable and/or data is generally incomplete.	Information source is reliable, but data may not be wholly complete and/or metric accuracy / reliability is moderate.	Information source is verified as reliable and data and metric accuracy / reliability is very high.

Table 2. KRI Effectiveness Criteria

Metric Description	Ease of Tracking	Tracking Frequency	Predictive value (leading or lagging)	Data / source accuracy
Supplier placed in negative outlook by ratings agencies	Medium	High	Medium	High
Change in supplier credit rating	Medium	High	High	High
Supplier litigation with key clients	Low	Medium	Medium	Medium
Announcement of loss of major contract	Medium	High	High	High
Senior management turnover in last 6 months	Medium	Medium	Medium	Medium
Stakeholder pressure on board performance	Low	Medium	Medium	Low
% of key suppliers with completed FDD / ongoing audits	Medium	High	High	High
Number of 'surprise' supplier insolvencies	Medium	High	Medium	Medium
Accuracy of product supply / demand forecasting	High	High	Medium	High

Figure 11. Example KRI Effectiveness Assessment

(3) Define and/or enhance metrics. Completion of the gap and effectiveness assessment will provide a view of any coverage gaps or existing metrics that are ineffective, supporting an understanding of where focus on defining new and making enhancements to existing metrics is needed.

- Enhance existing metrics. Having conducted the effectiveness review, evaluate the potential of existing metrics that do not have strong scores to be made more reliable and effective as KRIs (i.e. consider eh feasibility and cost of changes that would need to be made to the metric, such as tracking frequency, to achieve a high score).
- Define new metrics. Where coverage gaps were identified in the previous stage, consideration should be given to whether new ones are required, what these could be to provide early warning of changes in the risk and the feasibility and cost of tracking. All

new metrics should be assessed against the effectiveness criteria to ensure they will be practical and useful and the KRI matrix updated with any new metrics.

(4) Indicator selection and definition. Select metrics that can be cost effectively and reliably tracked to provide predictive insights into the imminent occurrence of a risk or an increase in its severity as KRIs. To optimize the KRI selection process, take into consideration the following:

- Cost effectiveness: Choose metrics that can be tracked at a reasonable cost, taking into account the resources required to collect, analyze and report the data.
- Reliability: Select metrics that are reliable, accurate and consistent, ensuring that they provide a true representation of the risk landscape.
- Predictive insight: Focus on metrics that provide predictive insights into the risk, enabling proactive management and mitigation.
- Comprehensive coverage: Ensure that the selected KRIs provide comprehensive coverage of all key risks and response activities, minimizing gaps in risk monitoring and management.

(a) To minimize the effort required to track KRIs, follow these best practices:

- Keep it simple: Select the fewest number of metrics necessary to provide effective and comprehensive coverage of all key risks and response activities.
- Avoid duplication: Eliminate redundant or duplicate metrics that do not add significant value to the risk management process.
- Focus on key risks: Prioritize metrics that are most relevant to the organization's key risks and response activities.

(b) Define escalation thresholds and actions for each KRI to promote consistent risk communication and effective risk management. This includes:

- Clear thresholds: Establish specific, measurable thresholds for each KRI, indicating when the risk is escalating or requires attention.
- Defined actions: Specify the actions to be taken when escalation thresholds are exceeded, including notification procedures, mitigation strategies and contingency plans.
- Communication protocols: Establish communication protocols to ensure that risk information is shared consistently and effectively across the organization, facilitating timely decision-making and action.
- Review and revision: Regularly review and revise escalation thresholds and actions to ensure they remain relevant, effective, and aligned with the organization's risk management objectives.

AFFF discharge, VMA 223, North Carolina, January 2023. Photo courtesy RMI.

8. The Risk Registry

a. A risk registry (also known as the risk register) is a repository for capturing and recording risks and associated information to provide a holistic portfolio of major risks to allow for prioritization of resourcing and efforts to achieve strategic objectives.

b. APs should document risks and issues in their command risk register using a consistent template to enable oversight, informed decision making, and risk communication up and down the chain of command.

c. Risk registers are not a simple list of hazards and risks; risk registers should address the common and repeated causes or drivers of hazards and risks. This approach enables addressing root causes vice tracking deficiencies for closure.

d. What is causing or inducing the risk? Can it be corrected locally or is it the outcome of higher headquarters (at any level) decisions? If it can be corrected locally, commands should immediately address it to remove the risk. If it cannot be corrected locally, commands should abate to the best of their abilities and report the issue up the chain of command for resolution or acceptance. Any risk that can only be abated should be reported up the chain of command for resolution. These risks should be documented on a risk registry. A good example is the gap in a critical command billet where a loss or potential mission degrade is possible due to the gap.

e. As a best practice, risk registries should be reviewed and reassessed periodically by leadership in a group setting. This allows the Commander or Commanding Officer to weigh in on the risks identified and broadens the command's leadership's understanding of the command's overall risk picture and how their teams may or may not be affected. Each risk should be reevaluated for priority based on current updates and environment.

f. A risk registry example with descriptions is provided in Figure 12.

Index Number	Risk	Risk Description	Category	Probability	Severity	Initial RAC	Residual RAC	Risk Owner	Affected Command	Risk Response	Update
Note (1)	Note (2)	Note (3)	Note (4)	Note (5)	Note (6)	Note (7)	Note (8)	Note (9)	Note (10)	Note (11)	Note (12)

Figure 12. Sample Risk Registry

Note (1) The **Index Number** is for local communication and tracking. Several risks are multi-year risks and tracking by FY may be beneficial (e.g., 26-001).

Note (2) The **Risk** column is a short description or title to the risk.

Note (3) The **Risk Description** is where you define the risk in detail providing sufficient information to understand the risk without additional voiceover.

Note (4) **Category** of what is driving the risk (e.g., Manning, Resourcing, External Support, Reputation, Internal Process). Commands should also annotate risks as "Retired" when they are eliminated.

Note (5) **Probability** as taken from calculating the risk assessment code (e.g., Frequent, Probable, Possible, or Unlikely).

Note (6) **Severity** as derived from calculating the risk assessment code (e.g., Catastrophic or Extreme, Significant or Major, Minor or Modest, or Minimal).

Note (7) **Initial Risk Assessment Code** (RAC) assigned (e.g., Critical, Serious, Moderate, Minor, or Negligible).

Note (8) **Residual RAC** is the risk that remains after implementing local controls.

Note (9) The **Risk Owner** is the person that can correct or eliminate the risk. This person is also the person that can formally accept the risk.

Note (10) **Affected Command** column is provided to communicate who is affected. Is this a single command issue or multiple? This column is important and used as risks are aggregated up the chain of command.

Note (11) The **Risk Response** are pre-planned action(s) that provides an overview of how the risk is being abated (if possible) and what is planned to occur if the risk manifests. This column should provide the organizational leader enough detail to develop a solid overview of intended command actions.

Note (12) **Updates** should be provided to track risks over time.

Glossary

Abate. To eliminate or reduce permanently an unsafe or unhealthful working condition by coming into compliance with the applicable OSH standard.

"ABCD." The mnemonic for the four actions of TCRM.

Acceptable Risk. The portion of identified risk that is allowed to persist during the mission or task.

Accountable Person. The individual who is personally accountable with the authority and responsibility for the effective execution of the Safety Management System or Safety Management Plan. This individual owns the risks within their command. This responsibility cannot be delegated.

Activity. A physical location shore, under a single higher authority command, where business is conducted or where services or operations are performed.

Acute. Momentary, usually severe or crucial often dangerous in which rapid changes are occurring. An acute exposure runs a comparatively short course (24 hours or less).

Additive Condition. Refers to all items that compete for an individual's or crew's attention during the execution of a mission or task. Examples include equipment malfunctions, change in weather, multiple players, unpredictable information and change to mission. Additive conditions may increase task loading or uncertainty and lead to distraction or channelized focus.

Adverse Event. Any event that indicates that a consumer product (1) fails to comply with an applicable consumer product safety rule or with a voluntary consumer product safety standard; (2) fails to comply with any other rule, regulation, standard or ban under the CPSA or any other Act enforced by CPSC; (3) contains a defect that could create a substantial product hazard described in section 15(a)(2) of the CPSA (15 U.S.C. § 2064(a)(2)); or (4) created an unreasonable risk of serious death or injury.

ALARA. ALARA is an acronym for "as low as (is) reasonably achievable," which means making every reasonable effort to maintain risk exposure as low as practical, consistent with the purpose for which the activity is undertaken, taking into account the state of equipment, competency of the workforce, expense of elimination and mitigation efforts or other societal and socioeconomic considerations, in relation to mission accomplishment. "Reasonable" requires the degree of risk (likelihood x severity) of a particular activity or environment to be balanced against the costs to both avoid the risk and potential outcome of failure. The greater the risk, the more likely it is that it will be reasonable to go to very substantial expense to reduce it. If the consequences and the extent of a risk are small, the same substantial expense would be considered disproportionate to the risk and it would be unreasonable to have to incur them to address a small risk.

Chronic. Persistent, prolonged, repeated.

Commander. The Navy official in charge of a naval shore command, activity or installation office or unit. Unless specified to the contrary, the term is synonymous with commander, commanding officer (CO), Officer in charge (OIC), director or other title for the head of the organization.

Competence. A person who is trained and qualified on all aspects of conducting their work properly. Competent persons are experienced, proficient, procedurally compliant, current, risk-aware and fit to work (general health and wellbeing). Competent persons must understand the established standards for their work.

Controls. Actions take or measures put in place to eliminate a hazard or reduce the associated identified risk. Some types of controls include engineering controls, administrative controls and physical controls. Also called mitigations.

Crew Factors. Refers to human factors which affect the capabilities of the individual, crew, or team, and can increase the potential for errors. This includes such things as attitudes, personalities, level of training, experience, fatigue and physiological factors.

Defense-in-Depth. A layered approach to designing and sustaining a system involving the use of successive compensatory measures that prevent accidents and mitigate the severity of smaller issues. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures or unexpected or undesired changes in condition so that no single layer, no matter how robust, is exclusively relied upon to prevent an accident. This approach defends against latent, unrealized weaknesses in a system or mistakes made by humans working with the system (unsafe behaviors carried out by individual parties).

Effectiveness of Corrective Action. The degree to which the proposed hazard abatement system can be expected to reduce the cited hazard. For health hazards, this would typically be expressed at the intensity of the hazardous chemical or physical agent remaining, in appropriate units, after the proposed abatement measure is operational. For safety hazards, effectiveness is expressed as "in full compliance" or "not in full compliance" with the applicable standard, if any.

Exposure. An expression that considers the frequency, length of time, and percentage of people or assets subjected to a hazard. Exposure is a component of risk but not directly used to assign a level of risk. Rather, it is a consideration in determining probability and severity.

Hazard. Any real or potential condition that can cause injury, illness or death to personnel; damage to or loss of equipment or property; degradation of mission capability or impact to mission accomplishment; damage to the environment (synonymous with the term threat).

Issue. An issue is an event or situation that has occurred or will definitely happen, which is certain or likely to affect a safe task or mission outcome.

Mishap. Any unplanned or unexpected event, or series of events, causing death, injury, occupational illness; damage, including days away from work, job transfer or restriction; or unexpected event, or series of events, causing materiel or assets to be lost or damaged, where if some or all causal factors that might have been corrected, the event or series of events would have been unlikely to occur

Navy Planning Process. The process by which a commander can effectively plan for and execute operations, ensure the employment of forces is linked to objectives and integrate naval operations seamlessly with the actions of a joint force.

Operate Safely. The CO, unit leadership team and operators all have a duty to Operate Safely by preserving the Safe to Operate conditions. Operate Safely is executing the mission within the designed safety envelope, while controlling unforeseen anomalies as they arise. The safety envelope is normally maintained by operating within established procedures. When unplanned or unforeseen safety risks manifest outside of the approved Safety Case and the military benefit (operationally defined objective) of taking the risk outweighs the cost of the risk exposure, then commands should apply the principles of operational risk management to control risk.

Opportunity. A potential positive outcome or gain that arises from an uncertain situation.

Plan of Action and Milestones (POAM). Document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks and scheduled completion dates for the milestones.

Proactively. By taking action to control a situation rather than just responding to it after it has happened.

Probability. A measure of the likelihood that given exposure to a hazard, a potential consequence mishap will occur.

Residual Risk. Risk remaining after controls have been identified and selected.

Requirement. A condition or capability that must be met or possessed by a solution or solution component to satisfy a contract, standard, specification or other formally imposed documents.

Resource. In general, a resource is something that can be used to develop controls and include time, money, people or equipment.

Risk. Chance of adverse outcome or bad consequence, such as failed or degraded mission, injury, illness or loss. Risk level is expressed in terms of hazard probability and severity.

Risk Assessment. A structured process to identify and assess hazards. An expression of potential harm, described in terms of severity, probability and exposure to hazards.

Risk Assessment Code (RAC). An expression of the risk associated with a hazard that combines its severity and probability into a single code which can be used to help determine hazard abatement priorities. This is typically accomplished through the use of a risk assessment matrix.

Risk Control. An activity or measure that is expected to reduce the likelihood of a risk event occurring.

Risk Control System. Risk control system is a collective term encompassing the risk identification and assessment, the management of risk, response to emergent threats and issues, measures to preserve established risk controls including record keeping and the continual self-assessment and correction. All of these efforts enable a resilient system.

Risk Decision. The decision to accept or not accept the risk(s) associated with an action made by the commander, leader, or individual responsible for performing the action.

Risk Management. A formal system of hazard identification, risk assessment, risk acceptance, control implementation and risk monitoring to control risk to acceptable levels.

Risk Management Information - Streamlined Information Reporting (RMI-SIR). RMI-SIR is a web-enabled, role-based single integrated mishap reporting and analysis system for reporting aviation, afloat, ground and motor vehicle mishaps.

Risk Registry. A repository for capturing and recording risks and associated information. Accountable Persons should document risks and issues in a risk registry, using a consistent template to enable oversight, decision-making and risk communication up and down the chain of command. Also known as a risk register.

Root Cause. Any basic underlying cause that was not in turn a result of more important underlying causes. Describes the depth in the causal chain where an intervention could reasonably be implemented to change performance and prevent an undesirable outcome. The analysis of a hazard may identify multiple causes. However, applying controls to the root cause is ultimately more effective than merely addressing an intermediate cause.

Safe to Operate. The as-designed safety for places, property, materiel, people, processes and procedures. It is the defining design, policy, engineering, resourcing and expectation management that sets the safety risk envelope for the hazardous activity or activities for a given operating environment. Original Equipment Manufacturers, Systems Commands, Program Offices and upper echelon commands are primarily responsible for the Safe to Operate criteria.

Safety. Protection in depth from those condition that can cause depth, injury, occupational illness or damage to or loss of equipment or property.

Safety Management Plan. Policy framework for implementing the safety management system to achieve the desired outcomes of the safety management system. Safety management plans are the documents that implement the desired outcomes of the safety management system. Safety management plans define and communicate performance expectations and may include additional guidance on risk accountability and communication expectations. Note safety management plans include most policies, procedures and guidance documents that guide operations across the full spectrum of activities including combat actions.

Safety Management System. A formal, top-down, bottom-up, organization-wide approach to managing safety risk and assuring the effectiveness of risk controls. Safety management systems often involve a systems or systems approach that inculcates procedures and policies throughout the organization working together to achieve the safety management system desired outcomes.

Severity. This is an assessment of the potential consequence that can or could occur as a result of a hazard and is defined by the degree of injury, illness, property or environmental damage, loss of asset (time, money, personnel), or effect on the mission or task. When analyzing risk, it is based on the worst credible outcome.

Situational Awareness (SA). SA refers to the degree of accuracy by which one's perception of the current environment mirrors reality.

Task Loading. The number of tasks to complete given a set period of time. Higher task loading increases the potential for error. Task loading can be reduced by either reducing the number of tasks or taking more time.

Threat. See "Hazard."

Unacceptable Risk. The risk when measured versus the benefit or value of the mission or task that cannot be tolerated and must be eliminated or controlled.