DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

OPNAV M-5100.23 CH-2
N09F
05 Sep 2022

OPNAV MANUAL 5100.23 CHANGE TRANSMITTAL 2

From: Chief of Naval Operations

Subj: NAVY SAFETY AND OCCUPATIONAL HEALTH MANUAL

Encl: (1) Revised page 2 Table of Issuance and Revision-Changes
(2) Revised Foreword
(3) Revised page i of the Table of Contents
(4) Inserted pages Ai through Aiii
(5) Revised Pages A1-1 through A5-1

1. Purpose. This change is issued to revise the Safety Management System in its entirety including the Foreword.

2. Action. Replace enclosure (1) of the change transmittal behind cover page to Manual. Replace foreword with enclosure (2). Replace page i of the Table of Contents with enclosure (3) from the change transmittal and replace Section A with pages pages Ai through Aiii, enclosure (4), followed by pages A1-1 through A5-1 from enclosure (5) of the change transmittal.

3. Records Management

a. Records created as a result of this change transmittal, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy (DON) Assistant for Administration, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this change transmittal or the records disposition schedules, please contact the local records manager or the OPNAV Records Management Program (DNS-16).

C. M. ENGDAHL
RADM USN
Special Assistant for Safety Matters

Releasability and distribution:
This change transmittal is cleared for public release and is available electronically only via DON Issuances website, https://www.secnav.navy.mil/doni/default.aspx.

TABLE OF ISSUANCE AND REVISION-CHANGES

OPNAV MANUAL	ISSUANCE DATE
OPNAV M-5100.23	5 JUN 2020

CHANGE-REVISION HISTORY	DATE PUBLISHED
CH-1	26 May 2021
CH-2	8 July 2022

CH-1 Change Highlights:
Replaced Chapter 13 in its entirety and authorizes the Navy Fall Protection Guide.

CH-2 Change Highlights:
Replace Section A the OPNAV Safety Management System.

DEPARTMENT OF THE NAVY
CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

OPNAV M-5100.23 CH-2
N09F
05 Sep 2022

CNO FOREWORD

The principles of safe naval operations are unchanged since the days of the sail and steam: profound competence in our work, strict compliance to proven safe practices, and engaged leadership that provides critical oversight and emphasizes safety as a responsibility of every Sailor from E1 to O10. As leaders, our focus on safety and risk mitigation is a pact we make with every Sailor, every Marine, and every civilian on our team that we will do everything possible to make their workplace safe and bring them home unharmed. Safety is generated and earned through a relentless focus and mindset of all involved. Furthermore, safety is not a department, it is a responsibility borne by every Sailor, Marine, and leader. Safe operations requires continual investment in training; as well as, a culture that clearly assigns responsibility and demands accountability to deliver safe processes and mitigation of risk. Safety demands competence and procedural compliance at every level, and a deep commitment by leadership to prioritizing safety. By delivering a safety management system that underpins and keeps pace with a rapidly evolving Navy, we will benefit from greater resilience against unnecessary harm to people, damage to equipment, and loss of capability.

Safety is an all-hands commitment, from the deckplate to the highest levels of command – we all are responsible for safety, including me. The Navy is a "can do" organization, but we must guard against slipping into a "must do" at all costs where risks are not adequately recognized or reported. We do that proactively by establishing a day-to-day culture where all personnel are empowered to provide backup, small problems are actively addressed (thereby preventing larger problems from developing), processes provide defense-in-depth, and leaders communicate unabated significant risk up the chain of command.

The aim of this safety management system (SMS) is to set conditions for success, not prescribe or regulate all aspects of safety and risk across the Navy. This SMS is the concept of operations for controlling risks. As such, this SMS is not an exhaustive list of specific responsibilities, processes, orders, or routines. The specifics are designed, managed, and owned by the echelon 2 commands (and subordinates) to control specific risks in the operating context. This is a 'plug and play' SMS. It is adaptable – and therefore flexible – so that its requirements and standards are translated locally to ensure controls are in place to mitigate risks and issues and assure such controls are effective and appropriate to keep people safe and ensure the Navy remains effective at achieving successful naval outcomes across all spectrums of operations including combat operations.

Our safety management system is led by me, defined and enabled by the Naval Safety Command, and executed and owned by teams across the entire Navy. Safety is everyone's responsibility and I expect our leaders to fully embrace decisive risk management. I expect the entire team to aggressively identify and communicate risk. We must emphasize to our teams the

critical importance of self-assessment and self-correction so that we are able to identify, communicate, and control risk up and down the chain of command to ensure unnecessary risks are not accepted. Risk shall be mitigated at the appropriate level in the chain of command – risks must not blindly cascade down to the unit level.

M. M. GILDAY

TABLE OF CONTENTS

SECTION A. SAFETY MANAGEMENT SYSTEM

REFERENCES

(a) CFR 29-1960, Basic Program Elements for Federal Health Occupational Safety and Health Programs and Related Matters

(b) E.O. 12196, Occupational Safety and Health Standards for Federal Employees

(c) DoDI 6055.01 of 14 October 2014 DoD Safety and Occupational Health (SOH) Program

(d) SECNAVINST 5100.10L, Department of the Navy Safety Program

(e) ISO 4500, International Standards Organization Occupational Health and Safety Management Systems

(f) OPNAVINST 3500.39D, Operational Risk Management

(g) OPNAVINST 3500.37D, Navy Lessons Learned Program

GLOSSARY

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.

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 or mitigation efforts and other societal and socioeconomic considerations, in relation to mission accomplishment. "Reasonable" requires the degree of risk (likelihood × 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.

Available Resources. Manning, training, equipment, time and funding.

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.

Defense-in-Depth. A layered approach to designing and sustaining a system involving the use of successive compensatory measures that prevents accidents and mitigates 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 conditions 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 within the system (unsafe behaviors carried out by individual parties).

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.

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.

Risk. Chance of adverse outcome 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 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 Register. A repository for capturing and recording risks and associated information. Accountable Persons should document risks and issues in a risk register, using a consistent template to enable oversight, decision making and risk communication up and down the chain of command.

Safe to Operate. The as-designed safety for places, property/materiel, people and processes/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 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 or bottom-up, organization-wide approach to managing safety risk and assuring the effectiveness of risk controls. Safety management systems often involve a systems of systems approach that inculcates procedures and policies throughout the organization working together to achieve the safety management system desired outcomes.

CHAPTER 1

INTRODUCTION

A0101. Purpose and Aim. Establish a framework for a unified and resilient safety management across the Navy, predicated on a risk control system that delivers decisive management of risks and issues to ensure operational excellence through continuous improvement. The aim is an effective Safety Management System (SMS) that avoids unnecessary harm to people or damage to equipment across the entire scope of Navy activities. Avoiding unnecessary loss is paramount to maintaining the readiness of our force and preserving our nation's assets.

A0102. Legal Requirement. References (a) and (b) establish the requirement for the Department of Defense (DoD) to comply with workplace and worker safety rules except for rare exceptions regarding military unique operations. References (c) and (d) establish DoD and Department of the Navy (DON) policy for compliance with references (a) and (b) respectively. Section B of this manual establishes the requirements for Navy to comply with references (a) through (d). Based on their unique nuclear and radiological authorities, the Director, Naval Nuclear Propulsion (OPNAV N00N) and the Director, Naval Nuclear Weapons Program (OPNAV N00NW) will solely determine how to and the extent of implementation of SMS under their authority.

A0103. Applicability. This SMS is applicable to the entire Navy, comprised of Sailors, civilians, contracted employees and industry partners. These principles apply to all Navy activities in air, land, sea and space -- at all times and in all operating environments. Deliberately, this SMS is not overly prescriptive; to make it so would lead to limited applicability and freedom to individual command chains to apply safety management in the context of their operations. The principles of this document apply across the entire spectrum of operations regardless of the operational or administrative chain of command.

A0104. Desired Outcomes. Chapters 2 through 4 describe the organization and arrangements for unified and resilient SMS that applies a formal, top-down and bottom-up approach to ensure and assure we are Safe-to-Operate and Operating Safely. There are four desired outcomes: Safe Place, Safe People, Safe Property/Materiel and Safe Processes/Procedures (the 4Ps).

a. Outcome 1: Safe **Place**. Safe workplace or working environment from a benign office environment through high-risk operational environments. Ensure safe entry, safe working and safe egress, including in an emergency. Ensure emergency protocols and systems are operable and tested regularly.

b. Outcome 2: Safe **People**. People and their supervisors are trained and qualified on all aspects of conducting their work properly and who are experienced, proficient, current, procedurally compliant, risk-aware and fit to work (general health and wellbeing). This outcome includes working safely, regardless of role, level or position in the Navy.

c. Outcome 3: Safe **Property/Materiel**. Proper and available tools, equipment, machinery, infrastructure and whole equipment systems that are Safe-to-Operate and Operated Safely.

d. Outcome 4: Safe **Processes/Procedures**. Proper and accessible standard operating procedures, emergency procedures, safety procedures, maintenance standards, etc.

CHAPTER 2

RESPONSIBILITIES AND ACCOUNTABILITY

Responsibilities. Below are the key responsibilities and requirements of this manual. All other sections of this manual are provided to teach and guide the execution of actions required to fulfill responsibilities delineated. Echelon 2 commanders and their subordinate commands **must** use the SMS framework in Figure 2-1 to design and execute an effective safety system within their command to deliver the 4Ps described in Chapter 1. Echelon 2 commanders are responsible for executing an effective echelon 2 SMS based upon reference (e) Plan, Do, Check, Act (PDCA) principles as an acceptable means of compliance with this instruction.

Accountability. For unity of effort, risk accountability and authority for overall SMS oversight, the echelon commander is the designated Accountable Person (AP) personally accountable to the CNO through the chain of command for effective execution of the SMS or Safety Management Plan (SMP).

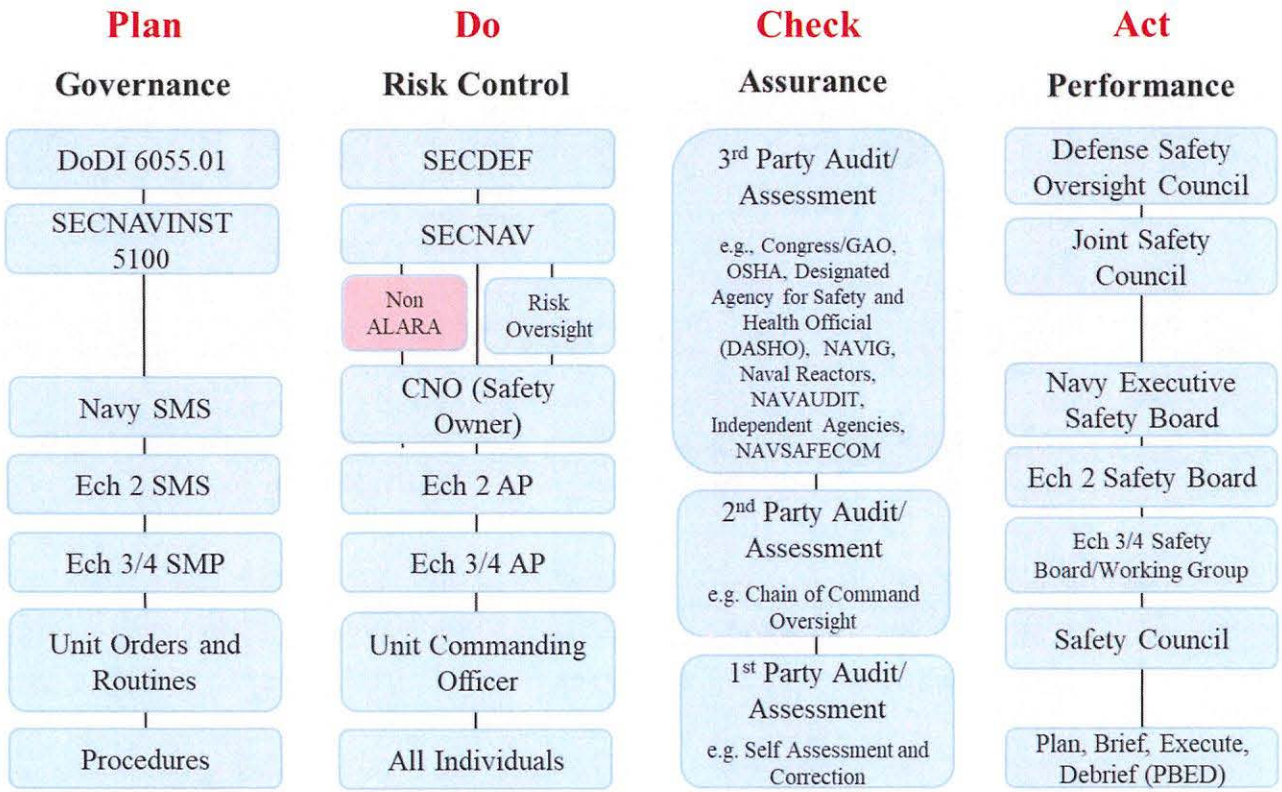

Figure 2-1. Overview of SMS Responsibility Structure based on the ISO 45001 Principles.

A0201. Chief of Naval Operations (CNO)

a. Most senior accountable person for the Navy and therefore ultimately responsible and accountable for a Navy that is Safe-to-Operate (across the 4Ps) and Operates Safely (execution of hazardous activities).

b. Ultimate decision maker on the time, cost and other resourcing factors (people, training, equipment and mission) needed to reduce risk or mitigate risk to As Low As Reasonably Achievable (ALARA) throughout the Navy.

c. Ultimate ownership and accountability for risk throughout the Chain of Command via the SMS.

d. Where resources within the Navy to mitigate an unacceptable risk to ALARA are exhausted, the CNO **must** raise the risk and proposed solution outside of CNO control to higher command or authority.

A0202. Echelon 2 and other Headquarters Commander as the Accountable Person

a. Accountable Person for the echelon 2 or other headquarters' activity and therefore ultimately responsible and accountable for Safe-to-Operate (across the 4Ps) and Operates Safely (execution of hazardous activities).

b. Produce echelon 2 SMS directives that specify risk communication thresholds and guidelines for SMS implementation throughout their command, unit or activity and lower echelons based on the principles and requirements contained in this manual.

c. Ensure their SMS provides a resilient, defense-in-depth based system that:

(1) Inculcates continuous learning;

(2) Identifies and corrects problems while they are small before growing into deeper, more systemic issues;

(3) Clearly indicates risk ownership;

(4) Elevates risks if unacceptable;

(5) Formally communicates hazards and near misses;

(6) And establishes accountability at the appropriate level.

d. Assess the effectiveness of the SMS throughout the command including lower echelons.

e. Ensure all leaders and managers understand the responsibility for the proper training of their people, identifying and fixing problems under their control, communicating and taking account for unmitigated risk at the appropriate level in the chain of command.

f. Identify and address potential risks to readiness and operations by collecting and analyzing organizational-wide mishap, near-miss, hazard, exercise, operational and related data.

g. Openly communicate risks and uncorrected hazards up and down the chain of command.

h. Where available resources prevent mitigating a risk to ALARA, commanders **must** raise the risk to higher command or authority's AP.

A0203. Echelon 3 and 4 Commander as the Accountable Person

a. Accountable Person for their activity and therefore ultimately responsible and accountable for Safe-to-Operate (across the 4Ps) and Operates Safely (execution of hazardous activities).

b. Produce a complementary SMS or SMP to meet the echelon 2 SMS requirements.

c. Assess the effectiveness of the SMS and SMP throughout the command, unit or activity including lower echelons.

d. Ensure the organization is properly resourced to execute unit level safety programs.

e. Where available resources prevent mitigating a risk to ALARA, commanders **must** raise the risk to higher command or authority's AP.

A0204. Commanding Officers and Officers in Charge (Unit Level)

a. Accountable Person for the Command activity and therefore ultimately responsible and accountable for Safe-to-Operate (across the 4Ps) and Operates Safely (execution of hazardous activities).

b. Perform unit level auditing to measure how well the requirements and controls of higher authority echelon 3 SMS or SMP are being maintained.

c. Ensure risk controls are in place and effective to prevent unnecessary harm or loss.

d. Where available resources prevent mitigating a risk to ALARA, Commanding Officers and Officers in Charge **must** raise the risk to higher command authority's AP.

A0205. Personal Accountability

a. All individuals and teams have a personal responsibility to work safely, according to established standards and authorized regulations, instructions, orders, routines, procedures and processes.

b. Individuals and teams are to take reasonable care of themselves and others that are affected by their actions.

c. All Navy personnel are accountable for their deliberate risk taking.

d. All Navy personnel are accountable for risk communication and **must** raise all known, discovered or perceived risks and issues to their immediate supervisor or chain of command.

A0206. Office of the Chief of Naval Operations, Special Assistant for Safety Matters (CNO (N09F)/ Commander, Naval Safety Command (NAVSAFECOM)

a. Serve as the principal advisor to the CNO and Assistant Secretary of the Navy (Energy, Installations and Environment) Safety on policy and administration of the Navy SMS Program, including policy guidance, accountability and assurance.

b. Act as the echelon 1 SMS Authority. Establish a standardized echelon 1 SMS framework that provides an acceptable means of compliance with the 4Ps.

c. Continually assess the Navy's risk control system and overall safety performance of the Navy and report to the CNO.

d. Assure proper and effective accountability of safety management across the Navy.

e. Conduct data collection and independent analysis to assess the effectiveness of the Navy SMS.

f. Compel corrective action by activity owners of unsafe practices and, when warranted, suspend those activities until corrected.

g. Compel the inclusion of Navy SMS requirements in all training courses, personnel qualification standards, job qualification requirements, events and evolutions across the Navy.

h. Advocate for the inclusion of Navy SMS principles throughout the Planning, Programming, Budgeting and Execution activities.

A0207. Safety Officers and Safety Professionals

a. Designated Safety Officers and assigned Safety Professionals in each command are responsible for supporting AP's to execute an effective SMS or SMP (as applicable). These safety personnel must be and remain independent of those responsible for safely executing work to provide another layer of defense-in-depth to the AP.

b. Provide advice to other leaders, supervisors and individuals on safety-related matters.

c. Ensure generic and specific Risk Assessments (RA) are completed and formally recorded in accordance with reference (f) for hazardous activities in the command.

d. Provide advice and guidance to the command on carrying out dynamic RAs, as required.

e. Nominated Safety Officers in each command maintain a Risk Registry (or other formal mechanism) of risks and issues impacting the 4Ps and overall execution of an effective SMS.

CHAPTER 3

RISK CONTROL SYSTEM

This chapter sets out basic philosophy and concepts for a systems approach to controlling risks to protect people and materiel from unnecessary harm. This instruction does not advocate for a particular SMS structure (e.g., the Federal Aviation Administration's 4-pillar SMS model), but rather presents principles for echelon 2 leaders to create their own SMS that is tailored for their operations. Reference (e) is a recognized international standard employed by High Reliability Organizations and provides additional information for developing an effective SMS.

A0301. Risk Leadership and Accountability

a. All aspects of effective safety management are predicated on properly informed leadership and supervision at all levels throughout the Navy.

b. Leaders and supervisors must be confident and competent to ensure proper standards are being executed in the conduct of work. Leaders and supervisors must also be confident and competent to make properly informed risk-based decisions, not be risk averse and not be risk blind due to lack of knowledge or training.

c. All individuals have an inherent responsibility to work safely to protect themselves and others affected by their actions. Critically, this means that individuals must ensure that they are competent to carry out the work tasked of them and they must follow established procedures and processes. Individuals are empowered to question established procedures and processes if they cannot be properly or safely executed.

A0302. Resilience: A Systems Approach to Risk

a. Resilience is the ability of a system to adjust so that it can sustain normal functioning in the face of disturbances; in other words, 'bounce-back from' or 'absorb' disturbances. Risk resilience is a systems view of risk controls that protects people and materiel and also effectively prevents or de-escalates issues leading to increased severity of harm (e.g., effective emergency response, correcting smaller issues through self-assessing, self-correcting). No one goes to work intending to cause a mishap, yet error is a normal by-product of human performance especially in demanding, repetitive, dynamic and complex operating environments associated with naval and industrial activities. Mishap analysis invariably reveals complex paths of system failures linked to organizational factors, competence of personnel and local conditions that promote unsafe behaviors in our various operating environments. System failures occur when risk controls are absent, disregarded, ineffective or fail to account for the inevitability of human error. The mishap therefore, often comes as a complete surprise, as the organization is not likely aware of its actual cumulative risk level. The lack of resilience is borne out in mishap investigations that invariably reveal weaknesses in the organization's ability to identify, assess or control risks. The findings from an investigation often come as no surprise (we knew or should have known the problems).

b. Situational Awareness (SA) is the conscious recognition and ability to respond correctly to all factors that may degrade successful outcomes in an operating environment. The inescapable presence of multiple inter-related networks of latent and active safety failures, found in complicated workplaces or

complex military operations, results in near impossibility to maintain sufficient risk SA. Sometimes our personnel are inadvertently oblivious to an unsafe condition with only luck separating success from failure. To claim we are safe, in absolute terms, is therefore challenging. We merely aspire to resiliency by working coherently and consistently across the whole safety enterprise to remove or reduce the likelihood of safety issues occurring and have the preparedness and resources to respond decisively when they occur. This effort requires a resilient network of system controls that work in concert to protect people and the mission from recognized and unrecognized risks. These system controls include the 4Ps – safe places, people, property/materiel and processes/procedures.

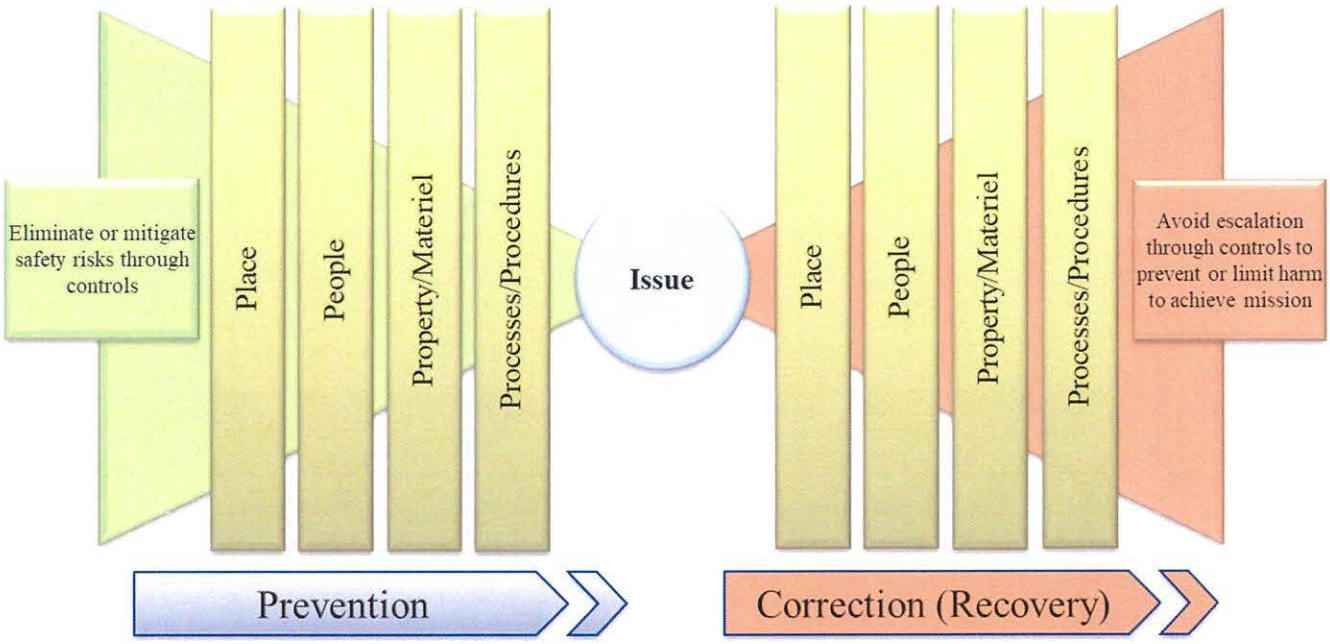

Figure 3-1. Resilience Model

c. The resilience model in Figure 3-1 is a simple method of organizing and understanding system safety performance in terms of risks controls. Figure 3-1 is an end-to-end pictorial representation of the safety system for an activity or group of activities. The left side of safety resilience highlights the process of preventing or reducing safety risks to an acceptable level or ALARA. This reduction/prevention is achieved through mitigation controls, but it supports the desired outcomes (4Ps). These generalized controls are designed to prevent or reduce the likelihood of an incident or capture errors when they inevitably occur. No control should be a single-point of failure, thus the diagram is drawn purposely to depict controls working together as multiple barriers to uncontrolled risk (defense-in-depth), in isolation or as an unintended network of risks, to prevent them from transitioning to a safety issue.

Example: On the left side of the model, many different types of controls are expected to prevent or reduce the likelihood of a fire occurring (e.g., storage of combustible materials, fire watches, operable fire suppression and hot work controls). No system of controls is infallible, so the right side of safety resilience is the 'insurance policy' that should detect and respond effectively to the fire, ensuring the safety issue does not escalate to cause harm to people or the mission. Typical controls to limit the spread or damage caused by fire include: fire detection systems, fire suppression, ventilation, dewatering, rescue teams or ready firefighting teams, as well as effective supervision and leadership. If all aspects function

as intended and further harm is avoided, then the system is resilient. Thus, safety resilience describes a whole system view of identifying and controlling risks, while also having the resources in place to recover successfully from emergent safety issues, thereby avoiding further harm to people, equipment, readiness and the overall mission.

d. A resilient system is 'Safe to Operate' and 'Operating Safely'. A resilient system also offers additional benefits in terms of reduced equipment damage and financial gains, as well as intangible socio-political effects and non-technical attributes, such as improved job satisfaction and wellbeing. Resilience thinking is a systems approach (not a human error approach) to protecting complex environments (e.g., a ship, submarine, air system, etc.). Resilience provides a formal method of organizing leading and lagging indicators to judge the level of assurance and overall safety performance from prevention [of issues] through to correction [to avoid additional harm]. For example, a safe system of work and training in a ship should prevent or reduce the likelihood of incorrectly torqued engine mounting bolts. If system induced human error occurs, resulting in incorrectly torqued bolts, this generates an unsafe condition. If undetected during the maintenance procedure, subsequent vibration in the power turbine becomes a safety issue with the potential to cause damage or fire. A whole system view of safety resilience recognizes the need to ensure further mitigation reduces escalation in harm to people, extended equipment damage, readiness or mission failure. Resilience thinking also captures the need for vibration detection systems, alarms, fire suppression and emergency training and effective human supervision of the emergent safety issue.

e. Good safety leadership and management are regarded as integral parts of generating and maintaining global warfighting effectiveness and lethality. A healthy culture exhibits a focus on continual checks and feedback at all levels. Teams or individuals feel ownership for safety and take responsibility for themselves and others. People do not accept low standards. They believe meaningful improvement can only be achieved as a group and that preventing unnecessary harm to people, equipment and the environment is an attainable vision. They feel confident to report their concerns and the supervisory chain will act. They instinctively work hard to avoid safety failures but always remain ready to respond effectively should things go wrong to limit any potential harm. Training and education have embedded a self-sustaining, healthy attitude towards safety that requires only occasional direction from senior management. Informed risk-based safety behavior is intuitive and proportionate to the safety threat.

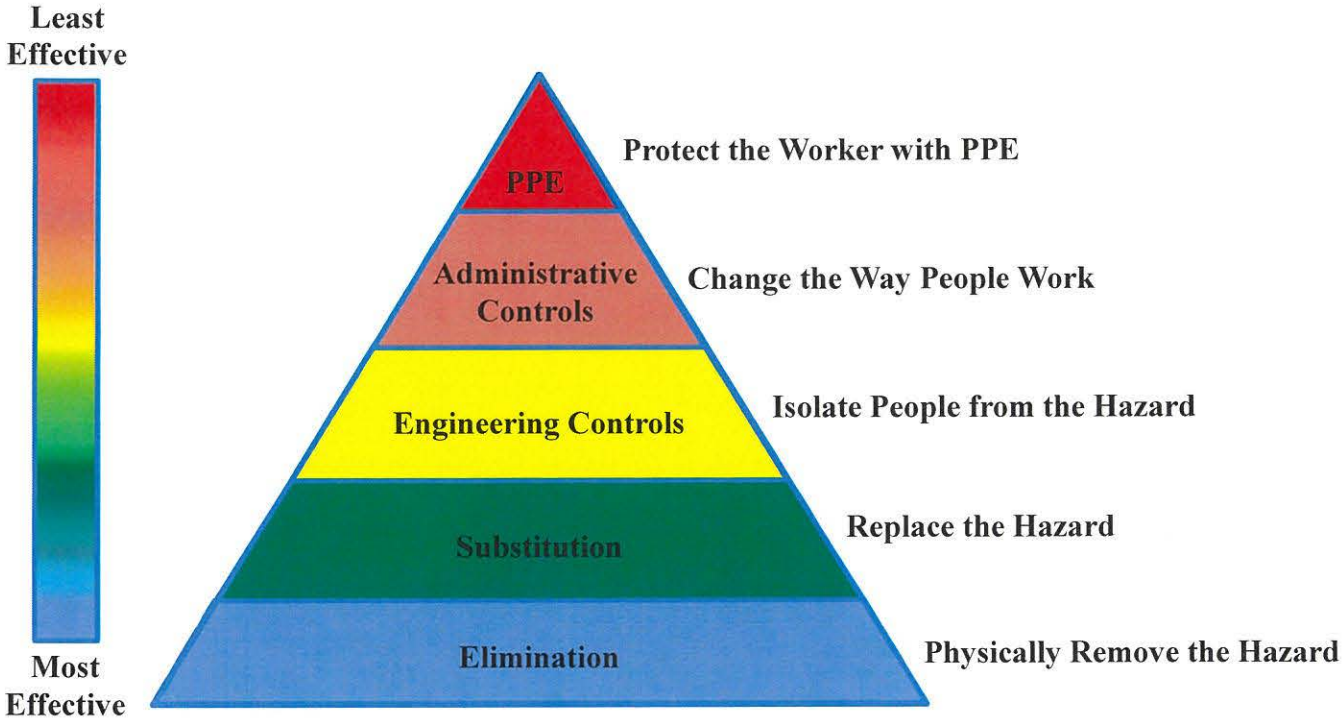

Figure 3-2. Hierarchy of Hazard Control

f. The strategic level pillars or barriers shown in Figure 3-1 are derived from analyses of mishaps that invariably revealed the same 'usual suspects' of human factors across all mishaps and the basic need to ensure a safe place, people, property (equipment) and processes/procedures exist. As the risk system is the same to control risk and recover from issues, the pillars are the same for both sides of the safety resilience concept. Each pillar is equally important in which you should follow the traditional hierarchy of hazard control to control specific risks (Figure 3-2). The sequence of the pillars is not critical. Of note, Figure 3-1 is drawn for clarity of the concept, but we must recognize the diagram belies the complexity of all potential hazards in the operating system and infinite ways their associated risk can network to create a path to harm.

g. In addition to assurance activity, resilience is determined through reporting, analysis and capitalizing on safety information. This information is gained from mishaps (lagging indicators) but more importantly, everyday hazard observations, near misses and safety successes (leading indicators). **Data cannot predict the next mishap, but it can infer the level of resilience to risk.** To determine whether sufficient resilience exists within the safety system, the efficacy of risk controls in each pillar shown in Figure 3-1 should be regularly measured and assessed.

h. Pillars defined

(1) **Safe Property/Materiel** (Echelon 1 through 3). The high-level management of safety includes resourcing to ensure compliance with Federal Law, DoD and DON policy. Organizational factors also include, deciding on the mission, structure of the organization, provision, allocation of resources and risk appetite. In summary, this category encompasses all factors needed for a safe workplace (applicable to the entire spectrum of workplaces from a benign office environment through frontline warfighting in a ship, submarine or other forward deployed operating base).

(2) **Safe People** (Echelon 3 through Unit level). The absolute safety-critical need for individuals and teams to behave safely. To facilitate this, the organization must ensure enough appropriately trained personnel are qualified, experienced and current for the tasks required of them; that they are also physically, psychologically and mentally prepared (akin to warrior toughness program); and human limitations are accounted for (anthropometric reach, vision, hearing, etc.).

(a) Organizational drift or becoming blind to risk (and issues) is the most significant causal factor found in mishaps. Leaders, supervisors, managers, teams and individuals must remain responsive to risks and issues in the workplace and empowered to raise concerns without fear of retribution or dismissal by their chain of command.

(b) The organization provides competent personnel while local commanders, leaders and supervisors must preserve competence in their personnel (this includes welfare support). Degraded competency will directly impact safety performance since competence is vital to countering the effects of other absent or ineffective controls (e.g., ineffective procedures, lack of supervision, unplanned or novel situations, etc.). A lack of competence (from the designer or decider through the operator) is the highest risk factor leading to mishaps. Competence is therefore characteristic of professionalism and is especially important where safety processes (controls) are exhausted through exceptional conditions. Control exhaustion can include occasions where personnel are exposed to unplanned and unexpected hazards, which may necessitate novel and spontaneous solutions to achieve and maximize operational benefit.

(c) Leadership must specify the competency requirements for persons in hazardous activities. Personnel must be suitably qualified, proficient (current) and experienced based on the required task for declared competency. Mishap analysis and surveys often reveal people were employed in positions, which they were not qualified, proficient or suitably experienced. This human competency gap erodes the safety margin, which also occurs when people deviate or drift from a standard as they become de-sensitized or blind to danger. This behavior is not complacency; it is simply a natural human response to risk.

(d) The final component of competence relates to non-technical skills, which are also key to ensuring people can act safely in the workplace. These include, but are not limited to: physical/mental limitations (i.e., decision-making, leadership, anthropometric reach, cognitive ability, vision, strength, etc.); physiological conditions (i.e., extremes of weather, heat stress, vibration, noise, ship roll, physical fatigue, etc.); and psychological conditions (i.e., managing perceived stress, fear, mental fatigue, etc.).

(3) **Safe Place** (Echelon 3 through Unit Level). Safe place refers to the condition of the physical operating (and operational) environment. A safe place is a workplace that is free from unnecessary hazards. The chain of command (Echelon 2 through Unit-Level) must ensure a safe place, equipment and practices are in place and effective to control risks in the workplace, which includes working in warfighting and crisis conditions. The workplace should also be populated with a sufficient number of competent personnel to maintain designed workplace safety. Commands need to evaluate the entire system to ensure resources are correct to safely complete tasking.

(4) **Safe Processes/Procedures** (Unit Level). This condition supports resilience at the 'sharp-end' of naval operations by prompting safe behaviors in the work environment. Safe actions are dependent on effective leadership and supervision so that personnel routinely work safely and are resourced and

empowered to respond to emergent risks and issues. At this level, it is about individuals and teams working within a safety system's boundaries as defined by established standards and procedures. Risks and issues requiring mitigation beyond unit-level resources are elevated to the next higher AP.

A0303. Safety Case. One method of executing a risk control system is a safety case. A safety case is a structured argument, supported by a body of evidence that provides compelling, comprehensive and valid case that a system is safe for a given application in each operating environment and that risks have been mitigated to ALARA through appropriate and effective safety controls.

A0304. Proven Work Model

a. Operations across the spectrum of naval operations require procedures, supervision, training and oversight. Successful operations rely on implementing the watchstanding principles of formality, ownership, level of knowledge, forceful backup, questioning attitude, procedural compliance and integrity. All these principles play a vital role in providing the defense-in-depth required to successfully deal with the dynamic nature of naval operations. Most operations are planned evolutions (formality), conducted by trained personnel (level of knowledge or training), using a formal written procedure (procedural compliance or engineering) and applying an adequate level of supervision (forceful backup and level of knowledge or supervision). For dynamic operations such as response to casualties that are not specifically addressed by procedures, watchstanding principles ensure a large degree of training and on-watch supervision to compensate for the inability to engineer a procedure in advance of the unexpected event. The existence of constant tearing-down forces knocking crews off-peak necessitate a distinct focus on problem prevention. One tool to help crews avoid problems or otherwise investigate problems after they occur, is the work model presented in Figure 3-3. The work model is a tool to ensure the essential aspects of any nuclear job are considered during planning and are continually assessed during execution. The model can also be easily applied across the full spectrum of naval operations.

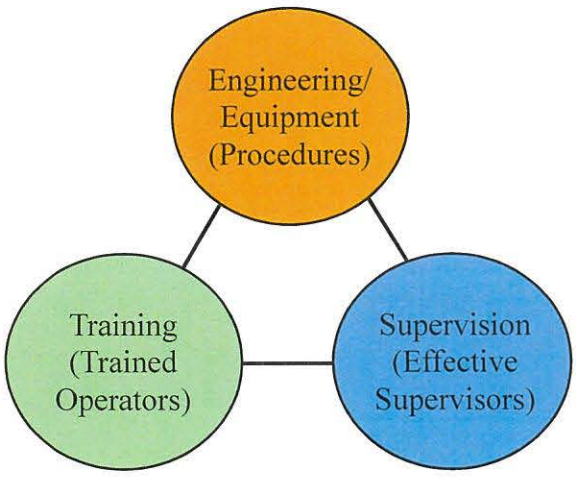

Figure 3-3. Work Model

b. There are always at least three elements necessary for the successful execution of work or operations – engineering (equipment), training and supervision. If fewer resources are invested in training, this likely must be compensated for by investing more in either engineering or supervision (or both). Similarly, if a procedure cannot be very detailed because there are too many different paths to take and

decisions need to be made in a timely manner, this must be compensated for by increasing the training of the operators or through increased supervision. The work model can be used as a problem prevention tool to think through the crew's strengths and weaknesses in each element and make adjustments as necessary. A conscious effort can then be made to adjust the size or detail of engineering, training and supervision based on the complexity of the task, level of training or experience, precision needed for the job and impact on safety.

c. When assessing an unplanned event or problem, the work model is a tool that could be used when determining the facts and problems associated with the event to thoroughly understand all sides of a problem. Probing the facts associated with each element will result in capturing the more significant problems and causes. When a problem occurs, there will always be a breakdown or weakness, in at least one of the three primary elements of the model, as well as a potential breakdown in oversight elements (those responsible for the safe conduct of the evolution not directly supervising). Continuing to use the model during causal analysis should result in the identification of causes that can be addressed with actions to correct and prevent similar problems. When problems are assessed through the "lens" of the work model, commands are able to identify how the evolution would have been successfully performed by a properly functioning work team. Focusing on differences or systematically grouping the associated facts in the work model format leads to supervisors and crews developing a mental model that continually assesses operations and maintenance evolutions by identifying and correcting imbalances real-time based on the skills, procedures and available supervision. The ideal balance should then be compared to the actual balance in place at the time of the problem to determine the "gaps" and focus on these differences as the major weaknesses in the planning and execution of the task.

CHAPTER 4

ASSURANCE

A0401. Assurance

a. Safety assurance involves routine and formal assessment through which justified confidence is provided that the safety requirements and standards are being met. In terms of resilience, assurance means that the risks and issues associated with equipment and resources, competent persons, infrastructure and compliance have been identified, controlled and owned at the appropriate level by an accountable person.

b. The Navy collectively assures the Risk Control System (RCS) is effective and is self-improving and self-correcting. The RCS involves problem solving, risk ownership and mitigation at the right level delivering a resilient Fleet. Therefore, Fleet and other echelon 2 organizations should conduct certifications, assessments and standards checks using a requirements-based, layered defense system or defense-in-depth. They should develop a system that effectively identifies and corrects problems while they are small – before they grow into larger, more systemic issues. We must place greater reliance on assuring successful naval outcomes through leading indicators or Key Risk Indicators than reactively learning and correcting from lagging indicators or Key Performance Indicators (see section A0403 below). Operating Safely is the natural product of risk management excellence.

A0402. Layered Defense System of Auditing and Assessment

a. First-party audits or assessments are self-awareness, self-assessment and self-correction. It is compliance with policy (orders, routines and processes) and risk management practices. The first-party audits/assessments assure the Commanding Officer (CO) and their immediate chain of command that the unit is Safe-to-Operate and Operating Safely. Emergent risks or issues discovered at this level should be registered locally and mitigations actively tracked by the CO and communicated up and down the chain of command. When first-party auditing detects an unsafe condition, the leaders must ensure the activity is stopped, where reasonably practicable, to assess the risk of harm and not restart the activity until protective controls are in place that meet the ALARA condition or the benefit of the operational (not operating) imperative justifies continuing the activity.

b. Second-party audits or assessments must be conducted by APs in the chain of command to ensure compliance with the principles of this instruction and other legislation, regulation and policy relevant to the echelon 2 environment. The second-party audits or assessments assure the echelon 2 Accountable Person and their subordinate commands that they are Safe-to-Operate, Operating Safely and resilient. Second-party auditing provides a formal mechanism for the chain of command to engage risks and issues (e.g., building a risk picture via risk registry (collection of risks)), assess readiness for the mission and confirm the SMS or SMP is effective at identifying, controlling and owning risks and issues. This method includes checking if risks are held at the appropriate level depending on the Risk Assessment Code (RAC) and whether the nominated risk owner has the proper levers to mitigate the risk (i.e., it is inappropriate for a person to own a risk or issue if they do not have the authority or resources to mitigate the risk to an ALARA condition).

c. First and second party auditing and assessment are inherent responsibilities to the chain of command to ensure that they and their subordinates are safe to operate and operating safely. The ability to identify and correct deviations from the expected standard is paramount to meeting the SMS desired outcomes ("4Ps").

d. Third-party audits or assessments are an independent assessment of the overall resilience-level of echelon 2 (and below) commands conducted periodically by NAVSAFECOM on behalf of the CNO. Third-party audits or assessments ensure that subordinate APs are effective at generating safe operations, controlling risks and issues and are compliant with this manual and other relevant legislation, regulations and policies. This audit is a systems level assessment that the SMS is performing as designed; it is resilient and therefore Safe-to-Operate and Operating Safely. Third-party oversight provides justified confidence to the CNO that safety practices underpin and enable readiness and successful naval outcomes.

A0403. Key Indicators

a. The key indicators (measures) of risk management and safety performance that can be used for assurance are identified in subparagraphs A0403a(1) – A0403a(3).

(1) Key Performance Indicators (KPI). Primarily a lagging indicator of the effectiveness of the overall SMS. It's a lag indicator because metrics are based on historical data showing how well the SMS functioned at keeping people and materiel free from harm. KPIs comprise metrics derived from: number and rate of mishaps; enforcement action, lost work time, lost equipment availability, lost capability, financial losses, etc.

(2) Key Risk Indicators (KRI). Primarily a leading indicator of the effectiveness of a risk control system (or risk management system). KRIs inform and update risk models to reduce uncertainty and judge impact against a capability need. KRIs comprise metrics derived from: audits, inspections, hazard reports, health and medical surveillance, competence availability, benchmarking, surveys, etc.

(3) KRIs are metrics that can provide an early signal of increasing risk exposure in a particular risk area. KRIs are indicators that provide an early warning system around the potential for a KPI to be missed. KRIs differ from KPIs in that the latter is a measure of how well something has done historically, whereas the former is an indicator of the possibility of future impacts. KRIs can be developed in tandem with KPIs and linked to the DON's strategic planning, Enterprise Risk Management Concept of Operations and performance management processes. For each performance activity, KPIs are set to identify the performance target for that activity's completion. Management further identifies the acceptable variation in performance with respect to the target outcome, typically so that these performance levels are consistent with the organization's risk appetite. KRIs are then set to serve as leading indicators of when performance is operating outside of acceptable tolerance ranges and therefore indicating risk to the achievement of the desired outcome. KRIs provide an opportunity to proactively identify risks to meeting objectives and take corrective action to meet the performance target. The development of KRIs and KPIs require a collaborative effort at various levels in the organization.

b. Examples include, but are not limited to:

(1) KPIs (lagging indicators; how well have we done?)

- Deaths (zero, % by affected population)
- Mishaps, by class (number reported, % by Fleet)
- Occupational Safety and Health Administration (OSHA) reportable personal injuries number, downward trend, % by affected population)
- Lost workdays due to personal injury, primary role (xx days per month)
- Occupational health referrals (number)
- Equipment damage ($$)
- Lost mission, directly attributable to safety failure (xx missions per month)
- Lost equipment availability, attributable to safety failure (xx days per month)
- Cost of occupational injuries and illnesses, litigation ($$)
- Non-compliance with law or policy
- Regulatory enforcement notices
- Prosecutions

(2) KRIs (leading indicators; how resilient are we?)

- Redefining the pinnacle events below the mishap level thresholds and designing systems to prevent redefined pinnacle events from ever occurring (i.e., critiquing events to understand causality).
- Organization
    - Echelon 1 SMS, compliant with legislation and policy
    - Echelon 2/3 SMP, compliant with SMS and domain specific legislation and policy
    - Echelon 4/5 orders, standard operating procedures (SOP) and safety programs: available, effective, compliant with higher guidance
    - Compliance with OSHA, non-unique military activity
    - Compliance with DoD policy, uniquely military activity
    - Risk Registry (oversight and efficacy)
    - Risks, RAC 1-2 formally reviewed at least annually
    - Non-ALARA (insufficiently mitigated/controlled) risks held (number)
    - Mishap and hazard recommendations closed-out within agreed times (number, %)
    - 2nd & 3rd Party independent audits carried out (% completed against number planned)
    - Audits or inspections corrective actions executed within agreed timings and scope
    - Safety governance boards (by echelon, attendance, % achieved against planned)

- Benchmarking, horizon scan for lessons identified (LI) from similar High Reliability Organizations and OSHA

- Competence (see competency definition for logic)

  - Fit or fill (trained, qualified, suitably experienced & current in task. (i.e., aviation maintenance experience (AMEX))
  - Operational career experience
  - Non-Tech skills (welfare, general health and wellbeing)
  - Hazard observations or dangerous occurrences (number reported, upward trend)

- Operating Conditions

  - Operational change rates (i.e., frequency of transition periods)
  - Safety specific training and education completed (% of personnel)
  - Safety stand-downs
  - Safety critical positions filled with competent persons
  - Infrastructure fit for purpose
  - Suitable and sufficient emergency response plan in place and exercised
  - Safety noticeboard present, overtly accessible and updated

- Local Actions (work as done)

  - Suitable and sufficient workplace risk assessments carried out, in date, with risks mitigated
  - Safety induction brief, new personnel and visitors carried out
  - First-party self-audit (% completed against number required or alignment with 2nd Party assessments)
  - Safety committees or council held (monthly)
  - Climate surveys completed and responded to
  - Safety awards (number, % by number available)
  - Lessons identified briefed (at shift handover, flyers, posters, etc.)

A0404. Organizational Learning (Report, Analyze and Get Better)

a. Rarely is an accident or serious occurrence the result of a single factor or due to the actions of a lone individual. Invariably an incident is the confluence of multiple organizational safety failures and local actions that creates a path to cause harm to people, damage equipment or impact the environment. People manage risks and hazards every day during normal operations and in exceptional circumstances. Effective organizational learning is dependent upon gathering and capitalizing on lessons learned from others' experiences. Continuous self-evaluation to the recognized standard is required to prevent organizational drift and the normalization of deviation from safe practices.

b. Organizational learning is also about responsive and flexible organizations working hard to identify shortfalls and enact improvements to maintain resilience. Individuals and leaders at all levels need to self-correct; find and fix small problems before they become larger, systemic issues; fix the root causes,

not just symptoms. The higher in the chain of command the deviations from the standard are detected, the larger the problems are likely to be. Our people need to apply problem solving tools and best practices to shift from more activity to better outcomes. A learning mindset is essential. Leaders need to transparently share what they learn to make others more successful and iterate to find the best solution, adjusting the plan based on learning.

c. The Report, Analyze and Get Better (RAG) cycle shown in Figure 4-1 supports this need by perpetually gathering reports from all available sources, analyzing risk control efficacy and then capitalizing on that knowledge. The RAG of safety mishaps and hazard observations permits organizational learning to improve existing risk controls or identify new controls. When sufficient quality data is reported and analyzed effectively to identify lessons, this knowledge can be utilized to enhance resilience in the workplace and support informed risk-based decisions. Reference (g) provides requirements for this process.

Figure 4-1. Report, Analyze and Get Better

(1) Report. There are many ways to learn – from mishap investigations, routine reporting and analysis of safety occurrences, benchmarking, audits or just taking time to discuss safety with colleagues and supervisors. Risk Management Information (RMI) is used for the mandatory reporting of mishaps and is also used for other reporting such as near misses and hazard observations.

(2) Analyze. Learning from safety reports can be grouped as lagging and leading indicators. Lagging indicators include lessons gained from major or minor occurrences as shown in Figure 4-2. Mishap investigations are carried out to learn why things did not go as expected and so the learning opportunity lags these types of occurrences. Unidentified non-compliance that results in a mishap is a lagging indicator whereas non-compliance identified through self-assessment is a leading indicator. Figure 4-2 also highlights how lag indicators often expend significant resources to investigate the occurrence and deliver improvements. Simply learning from lagging indicators demonstrates a reactive organization and is representative of an immature organization. Conversely, leading indicators capitalize

on safety intelligence gained from hazard observations, dangerous occurrences, near misses, confidential reports, first, second or third-party safety assessments or audits and safety learning from benchmarking to gain early warning of weaknesses in the safety system. An organization that routinely invests in the widespread analysis of leading indicators is often seen as a proactive or resilient safety organization. Here, there is a collective effort to improve safety, for which the investment in organizational learning is now shared throughout the Navy. Significantly, leading indicators allow the reporting of everyday safety successes, which can be exploited for wider learning. Measuring safety behaviors in the workplace (as done) is also a leading indicator. Leading indicators can also include lessons from successful failures; where the safety system failed yet decisive leadership acted to direct resources to limit harm, e.g., The National Aeronautics and Space Administration (NASA) considered the ill-fated Apollo 13 to be a successful failure as the crew returned to Earth unharmed.

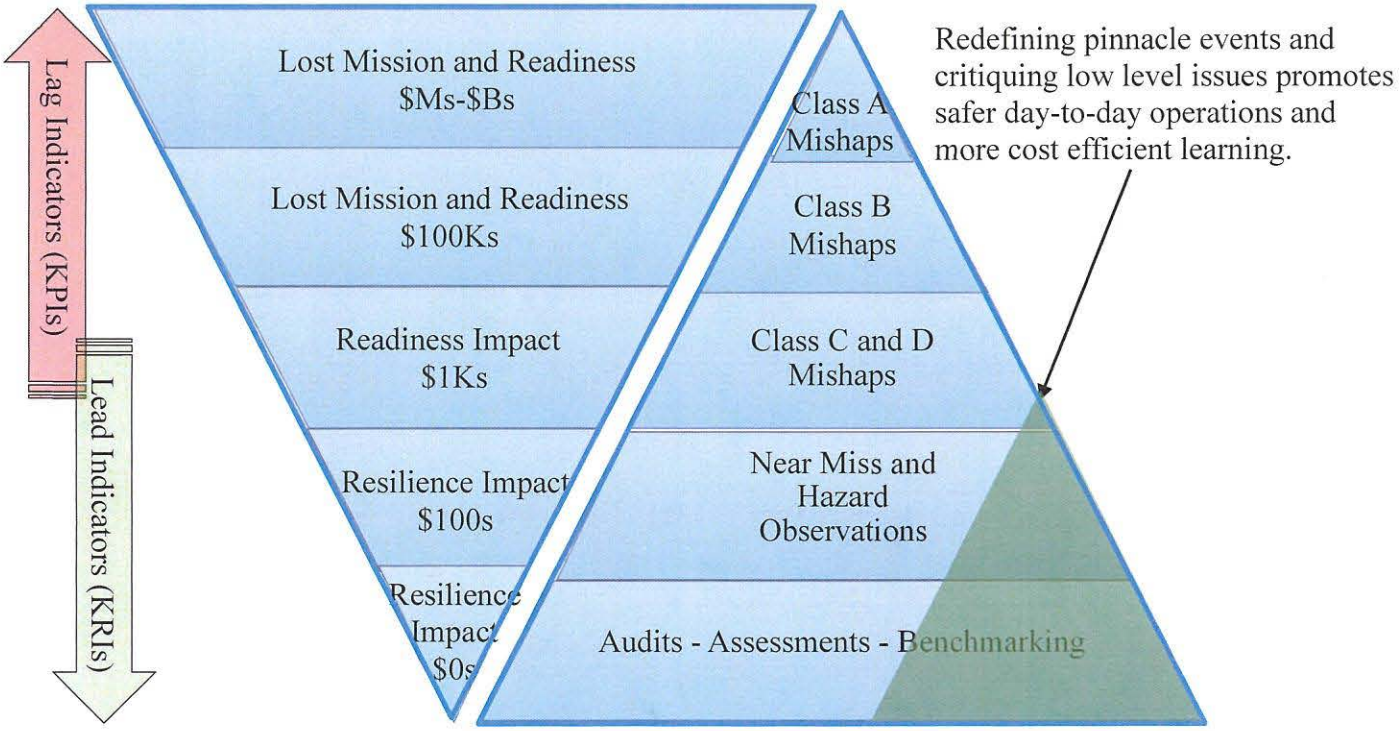

Figure 4-2. Human, Operational Availability (A_o) and Monetary Costs of Ineffective Learning

(3) Get Better. An effective organizational learning system exploits the safety intelligence gained from the analysis component. At the strategic level, intelligence gained from organizational learning can be mapped to one or more of the strategic controls described by the resilience model in Figure 3-1 to identify the efforts needed to mitigate weak risk controls. Using leading and lagging indicators in this manner is more likely to provide overall assurance of a safe working environment, rather than simply reacting to individual hazards. Knowledge or intelligence can also be utilized to update or raise new risks or issues and develop training and education. Critically, how we capitalize on lessons must be fed back to the affected community to ensure people learn to appreciate the real value of transparent reporting. The Naval Safety Command monitors safety events in RMI for good practices as well as oversight of risks relevant to the wider affected communities. Our Fleet's organizational risk management resilience will then be achieved through updates to policy and safety promotions.

(4) Refining Pinnacle Events. Echelon 2 SMS or SMPs must have systems and procedures to ensure we get better at learning in the green area shown in Figure 4-2 (i.e., we must invest in learning earlier where the cost is less therefore the overall return on investment is greater). An example of this methodology is to redefine pinnacle events at a lower mishap threshold and applying the same rigor and status of analysis that would normally be afforded a high impact pinnacle event (i.e., class A/B mishaps). Echelon 2 and 3 leadership needs to ensure these lessons learned are capitalized on in accordance with procedure outline in reference (g).

CHAPTER 5

OPERATIONAL RISK MANAGEMENT

Reserved for Future Use