

RTTUZYUW RUOIAAA0001 0981921-UUUU--RHSSSUU.
ZNR UUUUU
R 081921Z APR 26 MID320018632939U
FM COMNAVSAFECOM NORFOLK VA
TO ALSAFE
BT
UNCLAS

ALSAFE 014/26

MSGID/GENADMIN/COMNAVSAFECOM/20/APR//

SUBJ/RISK ACCOUNTABLE PERSON AND OPR//

REF/A/DOC/OPNAV M-5100.23//

NARR/REF A IS OPNAV M-5100.23, NAVY SAFETY AND OCCUPATIONAL HEALTH MANUAL//

POC/JONATHAN WILSON/CIV/NAVSAFECOM/NORFOLK/757-444-3520 EXT
7156/JONATHAN.D.WILSON2.CIV@US.NAVY.MIL.//

GENTEXT/REMARKS/1. The Navy has updated our approach to risk management. Some of the fundamental changes include a single Accountable Person (AP) for all identified risks and a new methodology for assignment of the AP or Office of Primary Responsibility (OPR) in the program of record for safety management called Risk Management Information (RMI). The new approach will be codified in chapter B5 of the next revision of reference (a).

2. Navy defines "risk" as an uncertain future event that could affect the organization's ability to achieve its objectives. A risk is forward-looking (not a current issue), has an element of uncertainty, could affect the achievement of objectives, must be credible and reasonable foreseeably, and can have both positive and negative effects. 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.

3. Once a risk or hazard has been identified and recorded, a single 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:

a. Ensuring the risk is accurately and clearly described to facilitate understanding and communication.

b. Identifying and implementing controls and mitigations to manage the risk, as well as evaluating their effectiveness.

c. Verifying that controls and mitigations are operating as intended and making adjustments as needed to ensure their ongoing effectiveness.

d. Conducting accurate assessments of both the initial (raw) and the residual (mitigated) risk to inform decision-making.

e. Continuously monitoring the risk for changes in its severity, likelihood, or impact, and updating risk assessments and mitigation strategies accordingly.

f. 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.

4. The nature of the identified risk aids in determining the correct OPR in RMI. In RMI, the OPR is assigned to a command instead of individual to ensure that risks are not lost as personnel move. The AP for the recommendation is the AP at the assigned UIC. The following methodology is required and must be followed by all warfare communities:

a. System Related Risk: The applicable SYSCOM is the OPR if abatement of the identified risk requires modification of a system, to include changes or modifications to a system or process/procedure issued by the SYSCOM.

b. Facility Risk: The property owner or organization that funds repairs (Maintenance UIC) is the OPR if the identified risk requires facilities repair or modifications outside of self-help.

c. Manning, Funding, or Headquarters Risk: The Immediate Superior in Charge (ISIC) is the OPR if abatement of the identified risk requires modification to manning, funding, or other headquarters-controlled functions.

d. Risk with action at the inspected command: The accounting organization or the inspected command is the OPR if abatement of the identified risk requires internal action from the accounting organization or inspected command, such as training, local SOP modification, or self-help.

5. 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 must 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.

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

a. Notification: The organization that identified the risk must notify the relevant organization of the potential risk and provide sufficient

information to enable them to understand the risk and its potential consequences.

b. Acknowledgement: The relevant organization must acknowledge receipt of the risk information and confirm their acceptance of risk ownership.

c. Risk Management Plan: The relevant organization must provide a risk management plan that outlines how they intend to manage the risk, including any controls or mitigations they will implement.

d. Ongoing Communication: The organization that initially identified the risk must establish a communication plan to ensure that they receive regular updates on risk management activities and any changes to the risk profile.//

BT

#0001

NNNN