



DEPARTMENT OF THE NAVY

COMMANDER
FIRST NAVAL CONSTRUCTION DIVISION
1310 8th STREET, SUITE 100
NORFOLK, VIRGINIA 23521-5070

COMFIRSTNCDINST 3500.1
N02EC
16 May 2006

COMFIRSTNCD INSTRUCTION 3500.1

From: Commander, FIRST Naval Construction Division

Subj: OPERATIONAL RISK MANAGEMENT (ORM)

Ref: (a) DODINST 6055.1, Change 2 of 15 August 1998
(b) OPNAVINST 3500.39B
(c) NTTP 5-03.5

Encl: (1) Supplemental Guidance for Implementation of the Navy's Operational Risk Management Program.

1. **Purpose**. To establish policy for Operational Risk Management (ORM) as an integral part of the decision-making process for all Naval Construction Force military and civilian personnel, on and off duty.

2. **Scope**. This instruction applies to all Naval Construction Force activities, commands and personnel.

3. **Background**

a. The naval vision is to develop an environment in which every individual (officer, enlisted, and civilian) is trained and motivated to personally manage risk in everything they do on and off duty, both in peacetime and during conflict, thus enabling successful completion of all operations or activities with the minimum amount of risk.

b. ORM can become the way we do business, through leadership, accountability and integrity. Leaders at all levels are responsible for ensuring proper procedures are in place and appropriate resources are available. Only through open communication and establishing the proper command climate can ORM become effective.

4. **Discussion**. ORM is described in enclosure (1). ORM is a method to identify hazards, assess risks and implement controls

16 May 2006

to reduce the risk associated with any operation. The Navy is implementing ORM by:

a. Making ORM a major part of orientation and training of all personnel, military and civilian. The level of training should be commensurate with rank, experience and leadership position.

b. Sharing ORM assessments to reduce risk associated with all operations. Sharing documented ORM assessments can be accomplished by using the Total Risk Assessment and Control System (TRACS). TRACS link can be located at the Navy Safety Center Web Site: www.safetycenter.navy.mil.

c. Considering information available through existing safety training and lessons learned databases, and standard operating procedures whenever practicable in making risk decisions.

d. Practicing ORM at all levels within individual commands.

5. **Policy**. All NCF activities and commands shall apply the ORM process in planning, operations, and training to optimize operational capability and readiness. Commands may publish instructions or standard operating procedures to augment this instruction with command-specific applications and requirements as appropriate. Commanding Officers will be held accountable for the use of the ORM process in their command and will actively take steps to ensure that it is used at every level.

6. **Action**

a. Commanders, Commanding Officers (COs), Executive Officers (XOs) and Officers-in-Charge (OICs) shall:

(1) Incorporate ORM into their operational routines. This includes regular use of the process for crisis action and exercise planning, clear guidance in the commander's intent on the level of acceptable risk, and the discussion of risk assessment and controls at decision briefs.

(2) Conduct a Safety Climate Assessment within 60 days of assuming command and follow-up at six month intervals if the Immediate Superior in Command (ISIC) deems it necessary.

(3) Use TRACS to download available assessments or develop ORM assessments. These assessments will be made

available in TRACS for download and can be easily modified in necessary deviations to meet command specific issues.

(4) Designate the Executive Officer as the ORM Program Manager to oversee command ORM training and implementation. He or she will ensure at a minimum that:

(a) One officer and one senior enlisted are qualified as ORM instructors and be the technical experts. Additional officer and senior enlisted qualified members are encouraged based on number of personnel and unit size. They should hold significant leadership and supervisory positions such as Supply, Operations, or Company Commander.

1. ORM instructor qualification is earned by completing the OPNAV-sponsored two-day application and integration course for enlisted members and officers.

2. ORM instructors will train command personnel using NAVOSHENVTRACEN training materials, NETC GMT ORM training, videos and lesson guides, and materials provided by the OPNAV Applications and Integration Course. Venues include training in the shops, at stand-downs, Indoc classes, training syllabus events, etc.

3. Provide training to command personnel per enclosure (1). Ensure that ORM training is documented in each member's training record.

(5) Establish an Occupational Safety, Health, and Risk Over-site Council (OSHROC). The OSHROC will be chaired by the Executive Officer and be comprised of Department Heads and Company or Detachment leader. The intent of the OSHROC is to add risk over-site to the current OSH Council. The OSHROC will review and approve risk assessments developed by small unit leaders. The approved risk assessments will be published by the command for small unit leaders to use through-out the command.

(6) Incorporate, at the company or detachment level, an Operation Risk Assessment Team (ORAT). The ORAT will focus on the assessment of upcoming evolutions and produce assessments of hazards and appropriate control strategies.

(7) Incorporate identified hazards, assessments and controls into all briefs, notices and written plans.

16 May 2006

(8) Conduct thorough risk assessment for all new or complex evolutions, defining acceptable risk and possible contingencies for the task or evolution.

(9) Address the ORM process in safety, training and lessons learned reports. Reports should comment on hazards, risk assessments and effectiveness of controls implemented.

(10) Submit ORM "lessons learned" to FIRST Naval Construction Division Safety Officer, code N02EC, for inclusion in COMNAVSAFCEM ORM databases.

(11) Inform the chain of command as to what hazards cannot be controlled or mitigated at their command level.


M. H. CONAWAY
Chief of Staff

Distribution:

Electronic via Seabee Operational Portal
<https://app.ncf.navy.mil/ncf/docs/default.ctm>

SUPPLEMENTAL GUIDANCE FOR IMPLEMENTATION OF THE NAVY'S
OPERATIONAL RISK MANAGEMENT PROGRAM

COMMANDER
FIRST NAVAL CONSTRUCTION DIVISION



TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

ARTICLE	SUBJECT	<u>PAGE</u>
101	Concept	1-1
102	Training	1-1
103	Terms	1-1
104	Process	1-2
105	ORM Process Levels	1-4
106	Principals of ORM	1-5
107	Risk Assessment Matrix	1-5

CHAPTER 2

ORM AND OPERATIONAL CONSIDERATIONS

201	Background	2-1
202	Application of Risk Management	2-1
203	Integration of Risk Management	2-11
204	Analysis Models	2-12

16 May 2006

CHAPTER 1

INTRODUCTION TO OPERATIONAL RISK MANAGEMENT (ORM)

101. **Concept**. The Operational Risk Management (ORM) process:

a. Is a decision making tool used by personnel at all levels to increase operational effectiveness by identifying, assessing, and managing risks. By reducing the potential for loss, the probability of a successful mission is increased.

b. Increases our ability to make informed decisions by providing a formal operational risk management process.

c. Minimizes risks to acceptable levels, commensurate with mission accomplishment. The amount of risk we will accept in war is much greater than what we should accept in peace, but the process is the same. Correct application of the ORM process will reduce mishaps and associated costs resulting in more efficient use of resources.

102. **Training**. The following training shall be required for appropriate pay grades/job assignment. All training can be found at www.nko.navy.mil and shall be completed upon advancement to a new pay grade or assignment to a position that requires the next level of training.

a. ORM All Navy Executive Overview Course (CNET 11973)(pay grade 01-08 or assignment as Commanding Officer, Officer In Charge (OIC) or Assistant Officer In Charge (AOIC).)

b. ORM All Navy Essential for leaders (CNET 11969) (pay grade E5-E9 and 01-05.)

c. ORM All Navy Application and Integration Course (CNET 11997) (pay grade E1-E9 and 01-08.)

d. ORM All Navy Fundamentals Course (CNET 11977) (pay grade E1-E9 and 01-08.)

103. **Terms**. Operational Risk Management (ORM) terms:

16 May 2006

a. **Hazard.** Any real or potential condition that can cause personal injury or death, property damage, mission degradation or damage to environment.

b. **Hazard Severity.** An assessment of the expected consequence, defined by degree of injury or occupational illness that could occur from exposure to a hazard.

c. **Mishap Probability.** An assessment of the likelihood that, given exposure to a hazard, a mishap will result.

d. **Risk.** Chance of adverse outcome or bad consequences, such as injury, illness, or loss. Risk level is expressed in terms of hazard probability and severity.

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

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

g. **Operational Risk Management (ORM).** The process of dealing with risk associated with military operations and off duty activities, which includes risk assessment, risk decision-making and implementation of effective risk controls.

h. **Risk Assessment Code (RAC).** An expression of the risk associated with a hazard that combines the hazard severity and mishap probability into a single Arabic numeral.

104. **Process.** Page 1-9 shows the flow of the ORM process. The five-step process is:

a. **Identify Hazards (Step 1).** Begin with an outline or chart of the major steps in the operation (operational analysis). Next, conduct a Preliminary Hazard Analysis by listing all of the hazards associated with each step in the operational analysis along with possible causes for those hazards.

b. **Assess Hazards (Step 2).** For each hazard identified in step one, determine the associated degree of

16 May 2006

risk in terms of probability and severity. Although not required, the use of a matrix may be helpful in assessing hazards, described further in paragraph 107.

c. **Make Risk Decisions (Step 3).** First, develop risk control options. Start with the most serious risk first and select controls that will reduce the risk to a minimum consistent with mission/task accomplishment. With selected controls in place, decide if the benefit of the operation outweighs the risk. If risk outweighs benefit or if assistance is required to implement controls, communicate with higher authority in the chain of command.

d. **Implement Controls (Step 4).** The following measures can be used to eliminate hazards or reduce the degree of risk. These are listed by order of preference:

(1) **Engineering Controls.** When technically or economically feasible, use engineering methods to reduce risks by design, material selection, or substitution.

(2) **Administrative Controls.** Controls that reduce risks through specific administrative actions, such as:

(a) Providing suitable warnings, markings, placards, signs, and notices.

(b) Establishing written policies, programs instructions and standard operating procedures (SOP).

(c) Training personnel to recognize hazards and take appropriate precautionary measures.

(d) Limiting the exposure to a hazard (either by reducing the number of assets or personnel, or the length of time personnel is exposed).

(3) **Personal Protective Equipment.** Personal Protective Equipment (PPE) serves as a barrier between personnel and the hazard, and should be used when other controls do not reduce the hazard to an acceptable level.

e. **Supervise (Step 5).** Conduct follow-up evaluations of the controls to ensure they remain in place and have the desired effect. Monitor for changes, which may require further ORM. Take corrective action when necessary.

16 May 2006

105. **ORM Process Levels.** The ORM process exists on three levels. Deciding which of the three levels to use will be based upon the situation, proficiency level of personnel, time, and assets available. While it would be preferable to perform a deliberate or in-depth operational risk assessment for all evolutions, the time and resources to do so will not always be available. One of the objectives of ORM training is to develop sufficient proficiency in applying the process, such that ORM becomes an automatic or intuitive part of our decision-making methodology. In the operational environment, leaders should be able to employ this time-critical process to make sound and timely decisions that generate tempo and facilitate decisive results. The three levels are as follows:

a. **Time-Critical.** Time-Critical is an "on the run" mental or oral review of the situation using the five-step process without recording the information on paper. The time-critical process level of ORM is employed by experienced personnel to consider risk while making decisions in a time-compressed situation. It is the normal level of ORM used during the execution phase of training or operations, as well as in planning during crisis response scenarios. This mental process is particularly helpful in choosing the appropriate course of action when an unplanned event occurs during the execution of a planned operation or daily routine.

b. **Deliberate.** Application of the complete five-step process, as depicted on page 1-9, will aid in planning an operation or evaluating procedures. It primarily uses experience and brainstorming to identify hazards and develop controls, and is, therefore, most effective when done in a group. Examples of deliberate applications include planning of upcoming operations, review of standard operating procedures, review of maintenance or training procedures, damage control and disaster response planning.

c. **In-Depth.** In-Depth is a deliberate process involving a very thorough risk assessment, the first two steps of the five step-process. Research of available data, use of diagrams, analysis tools, formal testing, or long term tracking of the hazards associated with the operation, sometimes with assistance from technical experts, are used to identify and access the hazards. It is used to thoroughly study the hazards and their associated risk in a complex operation or system, or when

16 May 2006

hazards are not understood. Examples of in-depth applications include long term planning of complex operations, introduction of new equipment, materials and missions, development of tactics and training curricula, and major systems overhaul or repair.

106. **Principles of ORM.** ORM incorporates the following four principles:

a. **Accept Risk when Benefits Outweigh the Cost.** Naval Doctrine Publication 1 states, "Risk is inherent in war and is involved in every mission. Risk is also related to gain; normally greater potential gain requires greater risk." Our naval tradition is built upon principles of seizing the initiative and taking decisive action. The goal of ORM is not to eliminate risk, but to manage the risk so that the mission can be accomplished with the minimum amount of loss.

b. **Accept No Unnecessary Risk.** Naval Doctrine Publication 1 also states, "We should clearly understand that the acceptance of risk does not equate to the imprudent willingness to gamble. Only take risks that are necessary to accomplish the mission."

c. **Anticipate and Manage Risk by Planning.** Risks are more easily controlled when they are identified early in the planning process.

d. **Make Risk Decisions at the Right Level.** The leader makes ORM decisions due to being directly responsible for the operation. Prudence, experience, judgment, intuition and situational awareness of leaders directly involved in the planning and execution of the mission are the critical elements in making effective ORM decisions. When the leader responsible for executing the mission determines that the risk associated with that mission **cannot be controlled at his or her level**, or goes beyond the commander's stated intent, he or she **shall elevate the decision up the chain of command.**

107. **Risk Assessment Matrix.** A matrix can be used to accomplish the second step of the ORM process. Using a matrix to quantify and prioritize the risks does not lessen the inherently subjective nature of risk assessment. However, a matrix does provide a consistent framework for evaluating risk. Although different matrices may be used

16 May 2006

for various applications, any risk assessment tool should include the elements of hazard severity and mishap probability. The RAC defined in the matrix represents the degree of risk associated with a hazard considering these two elements. While the degree of risk is subjective in nature, the RAC does accurately reflect the relative amount of perceived risk between various hazards. The example matrix described below is used in Naval Occupational Safety and Health assessments. Using the matrix, the RAC is derived as follows:

a. **Hazard Severity.** Hazard severity is an assessment of the worst credible consequence that can occur as a result of a hazard. Severity is defined by potential degree of injury, illness, and property damage, loss of assets (time, money, personnel), or effect on mission. The combination of two or more hazards may increase the overall level of risk. Hazard severity categories are assigned as Roman numerals according to the following criteria:

(1) Category I. The hazard may cause death, loss of facility/asset or result in grave damage to national interests.

(2) Category II. The hazard may cause severe injury, illness, property damage, damage to national or service interests or degradation to efficient use of assets.

(3) Category III. The hazard may cause minor injury, illness, property damage, damage to national, service or command interests or degradation to efficient use of assets.

(4) Category IV. The hazard presents a minimal threat to personnel safety or health property, national, service or command interests or efficient use of assets.

b. **Mishap Probability.** The probability that a hazard will result in a mishap or loss, based on an assessment of such factors as location exposure, cycles or hours of operation, affected populations, experience or previously established statistical information. Mishap probability will be assigned a letter according to the following criteria:

16 May 2006

(1) Sub-category A. Likely to occur immediately or within a short period of time. Expected to occur frequently to an individual item or person or continuously to a fleet, inventory or group.

(2) Sub-category B. Probably will occur in time. Expected to occur several times to an individual item or person or frequently to a fleet, inventory or group.

(3) Sub-category C. May occur in time. Can reasonably be expected to occur some time to an individual item or person or several times to a fleet, inventory or group.

(4) Sub-category D. Unlikely to occur.

c. **Risk Assessment Code (RAC).** The RAC is an expression of risk that combines the elements of hazard severity and mishap probability. Using the matrix shown below, the RAC is expressed as a single Arabic number that can be used to help determine hazard abatement priorities.

RISK MATRIX

		PROBABILITY			
		A	B	C	D
<u>SEVERITY</u>	I	1	1	2	3
	II	1	2	3	4
	III	2	3	4	5
	IV	3	4	5	5

FIGURE 1

RAC Definitions:

- 1 - Critical risk
- 2 - Serious risk
- 3 - Moderate risk
- 4 - Minor risk
- 5 - Negligible risk

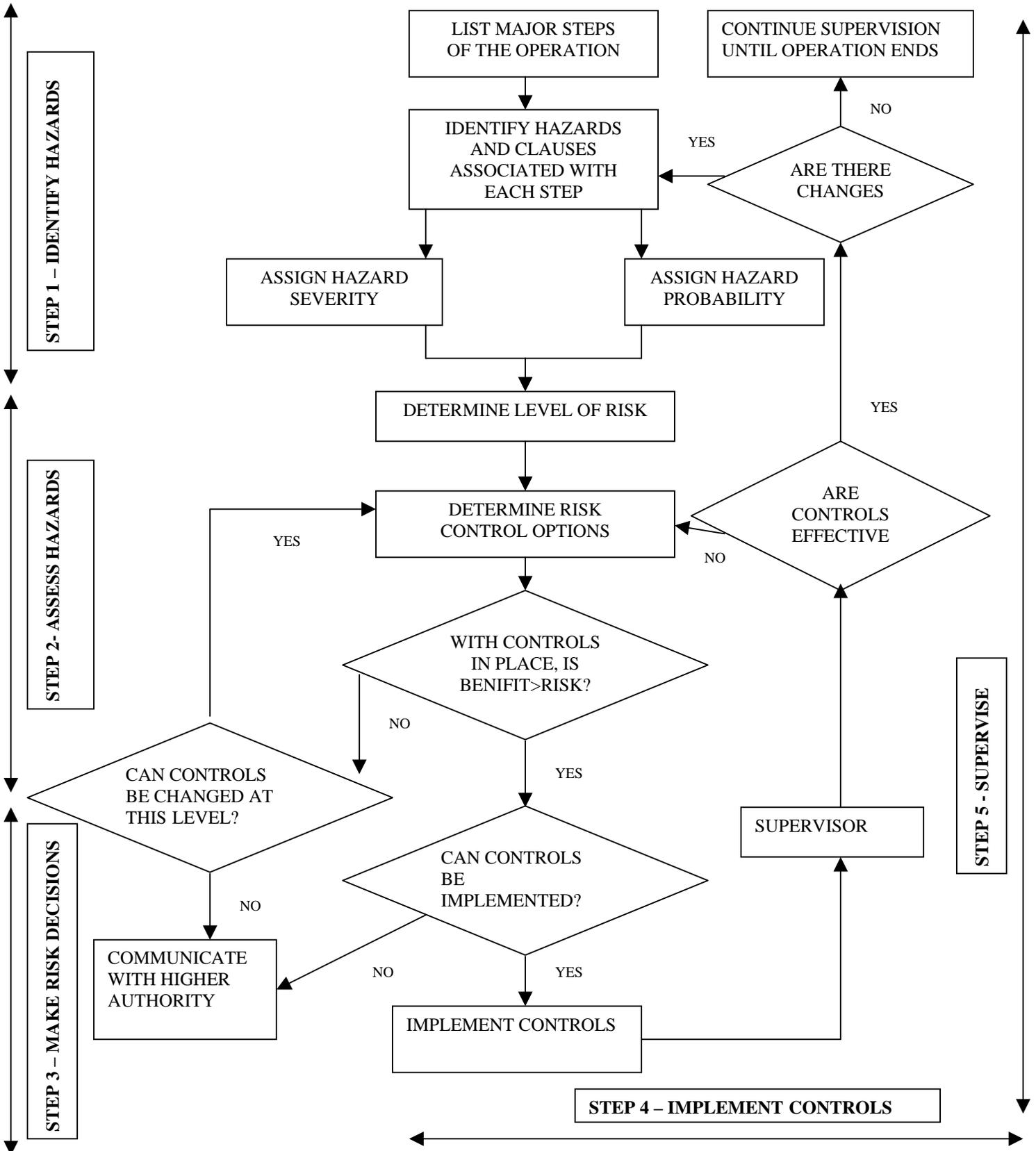
Note 1. In some cases, the worst credible consequence of a hazard may not correspond to the highest RAC for that hazard. For example, one hazard may have two potential consequences. The severity of the worst consequence (I) may be unlikely (D), resulting in a RAC of 3. The severity of the lesser consequence (II) may be probable (B),

16 May 2006

resulting in a RAC of 2. Therefore, it is also important to consider less severe consequences of a hazard if they are more likely than the worst credible consequence, since this combination may actually present a greater overall risk.

Note 2. The ORM process provides an additional tool for commanders to use in reducing risks inherent in military operations. It is not a complete change in the way we approach the operational risk management problem, but rather provides a specific methodology for personnel to anticipate hazards and evaluate risk. Just as we have trained our personnel to focus on the mission, we can train our personnel to evaluate risk as part of their decision making process. As personnel are trained in and use the process, ORM will become intuitive, being applied automatically as a means to aid in quickly developing an effective course of action to accomplish the mission.

OPERATIONAL RISK MANAGEMENT FLOW CHART



CHAPTER 2

RISK MANAGEMENT PROCESS AND OPERATIONAL CONSIDERATIONS

201. **Background**

This chapter discusses the risk management process and how it may be applied in the planning and execution phases of all operations. This enclosure also provides two situational analysis models. These models are the Mission, Enemy, Terrain and weather, Troops and support available and time (METT-T) model, and the Man, Machine, Media, Management, Mission (5-M) model. For either of these common operational planning methods, ORM should be incorporated at each step in the process.

202. **Application of Risk Management**

a. **Identify Threats.** A threat is a source of danger: any opposing force, condition, source, or circumstance with the potential to impact mission accomplishment negatively and/or degrade mission capability. Experience, common sense, and risk management tools help identify real or potential threats. Threat identification is the foundation of the entire risk management process; if a threat is not identified it cannot be controlled. The effort expended in identifying threats will have a multiplier effect on the impact of the total risk management process. Figure 2-1 depicts the actions necessary to identify threats associated with these three categories: (1) mission degradation, (2) personal injury or death, and (3) property damage.



Figure 2-1. Identify the Threats

(1) **Action 1—Analyze Mission.** This is accomplished by—

(a) Reviewing operation plans and orders describing the mission.

(b) Defining requirements and conditions to accomplish the tasks.

16 May 2006

(c) Constructing a list or chart depicting the major phases of the operation normally in time sequence.

(d) Breaking the operation down into "bite-size" chunks.

(2) **Action 2—List Threats.** Threats and factors that could generate threats, are identified based on the mission and associated vulnerabilities. The output of the identification phase is a list of inherent threats or adverse conditions, which is developed by listing the threats associated with each phase of the operation. Stay focused on the specific steps in the operation; limit your list to "big picture" threats. Examine friendly centers of gravity for any critical vulnerability. Threats may be tracked on paper or in a computer spreadsheet/database system to organize ideas and serve as a record of the analysis for future use.

(3) **Action 3—List Causes.** Make a list of the causes associated with each threat identified in Action 2. Although a threat may have multiple causes, it is paramount to identify the root cause(s). Risk controls may be more effective when applied to root causes.

b. **Assess Threats.** Each threat is assessed for probability and severity of occurrence. **Probability** is the estimate of the likelihood that a threat will cause an impact on the mission. Some threats produce losses frequently; others almost never do. **Severity** is the expected consequence of an event in terms of degree of injury, property damage, or other mission-impairing factors, such as loss of combat power. The result of this risk assessment allows prioritization of threats based on risk. The number one risk is the one with the greatest potential impact on the mission. However, the least risky issue may still deserve some attention and, possibly, risk control action. Keep in mind that this priority listing is intended for use as a guide to the relative priority of the risks involved, not as an absolute order to be followed. There may be, as an example, something that is not a significant risk that is extremely simple to control. Figure 2-2 depicts the necessary actions.

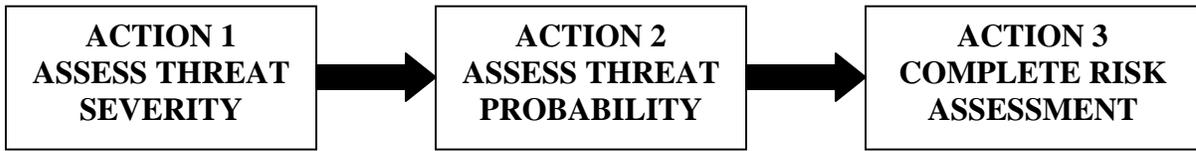


Figure 2-2. Assess the Threat

(1) **Action 1—Assess Threat Severity.** Determine the severity of the threat in terms of its potential impact on the mission, exposed personnel, and exposed equipment. Severity categories are defined to provide a qualitative measure of the worst credible outcome resulting from external influence, such as combat or terrorist action, personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system and subsystem, or component failure or malfunction.

(2) **Action 2—Assess Threat Probability.** Determine the probability that the threat will cause a negative event of the severity assessed in Action 1. Probability may be determined through experienced-based estimates or derived from research, analysis, and evaluation of historical data from similar missions and systems. The typical event sequence is much more complicated than a single line of erect dominos; tipping the first domino, threat, triggers a clearly predictable reaction. Supporting rationale for assigning a probability should be documented for future reference. Generally accepted definition for probability may be found in section 103.

(3) **Action 3—Complete Risk Assessment.** Combine severity and probability estimates to form a risk assessment for each threat. When combining the probability of occurrence with severity, a matrix may be used to assist in identifying the level of risk. A sample matrix is in section 107. Existing databases and/or a panel of personnel experienced with the mission and threats can also be used to help complete the risk assessment.

(4) **Output of Risk Assessment.** The outcome of the risk assessment process is a prioritized list of threats. The highest priority threat is the most serious one to the mission; the last is the least serious risk of any consequence.

16 May 2006

(5) **Risk Assessment Pitfalls.** The following are some pitfalls that should be avoided during the assessment:

(a) Over optimism: "It can't happen to us. We're already doing it." This pitfall results from not being totally honest and not looking for root causes of the threats.

(b) Misrepresentation: Individual perspectives may distort data. This can be deliberate or unconscious.

(c) Alarmism: "The sky is falling" approach, or "worst case" estimates are used regardless of their possibility.

(d) Indiscrimination: All data is given equal weight.

(e) Prejudice: Subjectivity and/or hidden agendas are used instead of facts.

(f) Inaccuracy: Bad or misunderstood data nullify accurate risk assessment.

(g) Enumeration: It is difficult to assign a numerical value to human behavior.

1. Numbers may oversimplify real life situations.

2. It may be difficult to get enough applicable data; this could force inaccurate estimates.

3. Numbers often take the place of reasoned judgment.

4. Risk can be unrealistically traded off against benefit by relying solely on numbers.

c. **Develop Controls and Make Risk Decisions.** Figure 2-3 depicts the necessary actions.

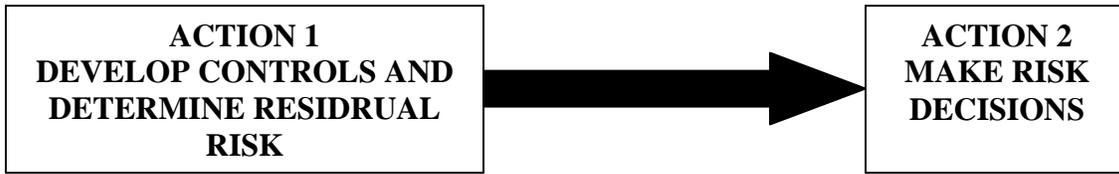


Figure 2-3. Develop Controls and Make Risk Decisions

(1) **Action 1–Develop Controls.** After assessing each threat, leaders should develop one or more controls that either eliminate the threat or reduce the risk probability and/or severity) of threats. For each threat identified, develop one or more control options that either avoid the threat or reduce its risk to a level that meets the commander’s risk guidance. Examples of criteria for establishing effective controls are listed in Table 2-1

Table 2-1 Criteria for Effective Controls	
CONTROL CRITERIS	REMARKS
Suitability	Control removes the threat or mitigates (reduces) the residual risk to an acceptable level.
Feasibility	Unit has the capability to implement the control.
Acceptability	Benefit gained by implementing the control justifies the cost in resources and time.
Explicitness	Clearly specifies who, what, where, when, why, and how each control is to be used.
Support	Adequate personnel, equipment, supplies, and facilities necessary to implement a suitable control is available.
Standards	Guidance and procedures for implementing a control are clear, practical, and specific.
Training	Knowledge and skills are adequate to implement controls.
Leadership	Leaders are ready, willing and able to enforce standards required to implement a control.
Individual	Individual personnel are sufficiently self-disciplined to implement a control

16 May 2006

(2) Some types of controls are as follows:

(a) Engineering controls. These controls use engineering methods to reduce risks, such as developing new technologies or design features, selecting better materials, identifying suitable substitute materials or equipment, or adapting new technologies to existing systems. Examples of engineering controls that have been employed in the past include development of aircraft stealth technology, integrating global positioning system data into cruise missiles, and development of night vision devices.

(b) Administrative controls. These controls involve administrative actions, such as establishing written policies, programs, instructions, and SOPs, or limiting the exposure to a threat either by reducing the number of personnel/assets or length of time they are exposed.

(c) Educational controls. These controls are based on the knowledge and skills of the units and individuals. Effective control is implemented through individual and collective training that ensures performance to standard.

(d) Physical controls. These controls may take the form of barriers and guards or signs to warn individuals and units that a threat exists. Use of personal protective equipment, fences around high power high frequency antennas, and special controller or oversight personnel responsible for locating specific threats fall into this category.

(e) Operational controls. These controls involve operational actions such as pace of operations, battlefield controls (areas of operations and boundaries, direct fire control measures, fire support coordinating measures), rules of engagement, airspace control measures, map exercises, and rehearsals.

(f) A control should avoid/reduce the risk of a threat by accomplishing one or more of the following:

1. Avoiding the risk. This often requires canceling or delaying the task, mission, or operation and is, therefore, an option rarely exercised because of mission importance. However, it may be possible to avoid

16 May 2006

specific risks: risks associated with a night operation may be avoided by planning the operation for daytime; thunderstorm or surface-to-air-missile risks can be avoided by changing the flight route.

2. Delay a COA. If there is no time deadline or other operational benefit to speedy accomplishment of a task, it may be possible to reduce the risk by delaying the task. Over time, the situation may change and the risk may be eliminated, or additional risk control options may become available (resources become available, new technology becomes available, etc.) reducing the overall risk. For example, a mission can be postponed until more favorable weather reduces the risk to the force.

3. Transferring the risk. Transferring a mission, or some portion of that mission, to another unit, may reduce risk or platform that is better positioned, more survivable, or more expendable. Transference decreases the probability or severity of the risk to the total force. For example, the decision to fly an unmanned aerial vehicle into a high-risk environment instead of risking a manned aircraft is risk transference.

4. Assigning redundant capabilities. To ensure the success of critical missions to compensate for potential losses assign redundant capabilities. For example, tasking a unit to deploy two aircraft to attack a single high value target increases the probability of mission success.

(g) **Determine Residual Risk.** Once the leader develops and accepts controls, he or she determines the residual risk associated with each threat and the overall residual risk for the mission. Residual risk is the risk remaining after controls have been identified, selected, and implemented for the threat. As controls for threats are identified and selected, the threats are reassessed, and the level of risk is revised. This process is repeated until the level of residual risk is acceptable to the commander or leader or cannot be further reduced. Overall residual risk of a mission must be determined when more than one threat is identified. The residual risk for each of these threats may have a different level, depending on the assessed probability and severity of the hazardous incident. Overall residual mission risk should be determined based on the threat having the greatest residual

16 May 2006

risk. Determining overall mission risk by averaging the risks of all threats is not valid. If one threat has high residual risk, the overall residual risk of the mission is high, no matter how many moderate or low risk threats are present.

(3) **Action 2—Make Risk Decisions.** A key element of the risk decision is determining if the risk is justified. The leader should compare and balance the risk against the mission's potential gain. The leader alone decides if controls are sufficient and acceptable and whether to accept the resulting residual risk. If the leader determines the risk level is too high, he or she directs the development of additional or alternate controls, or modifies, changes, or rejects the COA. Leaders can use the risk assessment matrix or other tools, in conjunction with their commanders' guidance, to communicate how much risk they are willing to allow subordinate leaders to accept.

d. **Implement Controls.** Once the risk control decision is made, assets must be made available to implement the specific controls. Part of implementing controls is informing the personnel in the system of the risk management process results and subsequent decisions. Figure 2-4 depicts the actions necessary to complete this step. Careful documentation of each step in the risk management process facilitates risk communication and the rational processes behind risk management decisions

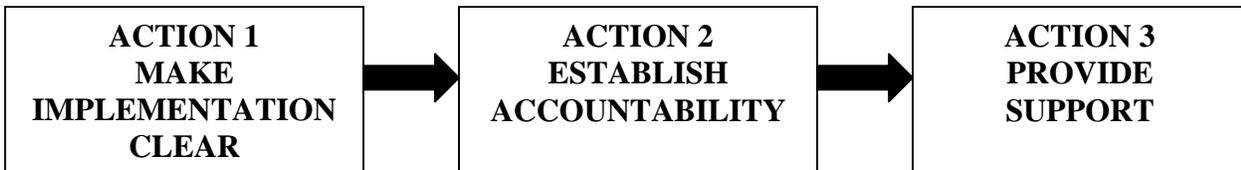


Figure 2-4. Implementing Controls

(1) **Action 1—Make Implementation Clear.** To make the implementation directive clear, consider using examples, providing pictures or charts, including job aids, etc. Provide a roadmap for implementation, a vision of the end state, and description of successful implementation. The control should be presented so the intended audience will receive it positively. This can best be achieved by designing in user ownership.

16 May 2006

(2) Action 2—Establish Accountability.

Accountability is important to effective risk management. The accountable person is the one who makes the decision (approves the control measures); therefore, the right person (appropriate level) must make the decision. Clear assignment of responsibility for implementation of the risk control is required.

(3) Action 3—Provide Support. To be successful, the command must support the risk controls. This support requires—

(a) Providing the personnel and resources necessary to implement the control measures.

(b) Designing in sustainability from the beginning.

(c) Employing the control with a feedback mechanism that will provide information on whether the control is achieving the intended purpose.

c. **Supervise and Review.** Supervise and review involves determining the effectiveness of risk controls throughout the operation. There are three aspects: monitoring the effectiveness of risk controls; determining the need for further assessment of either all, or a portion of, the operation due to an unanticipated change; and capturing lessons learned, both positive and negative. Figure 2-5 depicts the necessary actions.



Figure 2-5. Supervise and Review

(1) Action 1—Supervise. Monitor the operation to ensure—

(a) Controls are implemented correctly, effective, and remain in place.

(b) Changes requiring further risk management are identified.

16 May 2006

(c) Action is taken to correct ineffective risk controls and reinitiate the risk management process in response to new threats.

(d) Risks and controls are reevaluated any time the personnel, equipment, or mission tasks change, or new operations are anticipated in an environment not covered in the initial risk management analysis. Successful mission performance is achieved by shifting the cost versus benefit balance more in favor of benefit through controlling risks. By using risk management whenever anything changes, we consistently control risks identified before an operation and those that develop during the operation. Addressing the risks before they get in the way of mission accomplishment saves resources and enhances mission performance.

(2) **Action 2-Review.** The risk management process review must be systematic. After controls are applied, a review must be accomplished to see if the risks and the mission are in balance. To determine if appropriate risk management controls have been applied, compare METT-T or the 5-M model from the earlier steps to the present risk management assessment.

(a) To accomplish an effective review, commanders identify whether the actual cost is in line with expectations. The commander needs to determine what affect the risk control had on mission performance. It is difficult to evaluate the risk control by itself; therefore, the focus should be on the aspect of mission performance the control measure was designed to improve.

(b) Measurements are necessary to ensure accurate evaluations of how effectively controls eliminated threats or reduced risks. After Action Reports (AAR), surveys, and in-progress reviews provide great starting places for measurements.

(3) **Action 3-Feedback.** A review by itself is not enough; a mission feedback system should be established to ensure that the corrective or preventative action taken was effective and that any newly discovered threats identified during the mission were analyzed and corrective action taken.

16 May 2006

(a) When a decision is made to accept risk factors, cost versus benefit information, involved in the decision should be recorded; proper documentation allows for review of the risk decision process. Then, when a negative consequence occurs, the decision process can be reviewed to determine where errors in the process may have occurred.

(b) Risk analysis will not always be perfect the first time. When errors occur in an analysis, use feedback such as briefings, lessons learned, benchmarking, or database reports to identify and correct those errors. This feedback will help determine if the previous forecasts were accurate, contained errors, or were completely incorrect.

203. Integration of Risk Management

Tables 2-2 and 2-3 integrate the risk management process into each phase of the deliberate and crisis action Joint Operation Planning and Execution System (JOPES). The annotations of the Joint Task Force (JTF) and Major Subordinate Element (MSE) in the matrix identify the level of command primarily responsible for risk management execution during each particular phase of planning. The risk management process should be considered throughout the planning process by each level of command.

Table 2-2 Risk Management Execution (Risk Management in Deliberate Planning)					
Deliberate Planning	Identify Threats	Assess Threats	Develop Controls Make Risk Decisions	Implement Controls	Supervise And Review
PHASE I Initiation	JTF				
PHASE II Concept Development	JTF	JTF			
PHASE III Plan Development	MSE	MSE	JTF MSE		
PHASE IV Plan Review			JTF		
PHASE V Supporting Plans	MSE	MSE	MSE	JTF MSE	
EXECUTION	JTF MSE	JTF MSE	JTF MSE	JTF MSE	JTF MSE

16 May 2006

Table 2-3 Risk Management Execution (Risk Management in Crisis Action Planning)					
Crisis Action Planning	Identify Threats	Assess Threats	Develop Controls Make Risk Decisions	Implement Controls	Supervise and review
PHASE I Situation Development	JTF	JTF			
PHASE II Crisis Assessment	JTF	JTF	JTF		
PHASE III COA Development	JTF MSE	JTF MSE	JTF MSE		
PHASE IV COA Selection			JTF MSE	JTF	
PHASE V Execution Planning			JTF MSE	JTF MSE	
PHASE VI Execution	MSE	MSE	MSE	JTS MSE	JTS MSE

204. Analysis Models

a. **The METT-T Model.** The METT-T model can be used for conducting a situation analysis by breaking it into five general areas: (a) the mission itself, (b) the enemy, (c) terrain/weather, (d) troops and support available, and (e) time available.

(1) **Mission.** Leaders first analyze the assigned mission. They look at the type of mission to be accomplished and consider possible subsequent missions. Certain kinds of operations are inherently more dangerous than others. For example, a deliberate frontal attack is more likely to expose a unit to losses than would a defense from prepared positions. Identifying missions that routinely present greater risk is imperative. Leaders also look for threats associated with complexity of the plan (such as a scheme of maneuver that is difficult to understand or too complex for accurate communications down to the lowest level) or the impact of operating under a fragmentary order.

(2) **Enemy.** Commanders look for enemy capabilities that pose significant threats to the operation. For example, "What can the enemy do to defeat my operation?"

16 May 2006

(a) Common shortfalls that can create threats during operations include failure to-

1. Assess potential advantages to the enemy provided by the battlefield environment.
2. Fully assess the enemy's capabilities.
3. Understand enemy capabilities and friendly vulnerabilities to those capabilities.
4. Accurately determine the enemy's probable COA's.
5. Plan and coordinate active ground and aerial reconnaissance activities.
6. Disseminate intelligence about the enemy to lower echelons.
7. Identify terrorist threats and capabilities.

(b) Intelligence plays a critical part in identifying threats associated with the presence of an enemy or an adversary. Intelligence preparation of the battle space is a dynamic staff process that continually integrates new information and intelligence that ultimately becomes input to the commander's risk assessment process. Intelligence assists in identifying threats during operations by-

1. Identifying opportunities and constraints the battlefield environment offers to enemy and friendly forces.
2. Thoroughly portraying enemy capabilities and vulnerabilities.
3. Collecting information on populations, governments, and infrastructures.

(3) **Terrain and Weather.** Terrain and weather pose great potential threats to military operations. The unit must be familiar with both the terrain and its associated environment for a mission to succeed. Basic issues include availability of reliable weather forecasts, how long the

16 May 2006

unit has operated in the environment and climate, and whether the terrain has been crossed before.

(a) Terrain. The main military aspects of terrain are observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach; these may be used to identify and assess threats impacting friendly forces. Terrain analysis includes both map and visual reconnaissance to identify how well the terrain can accommodate unit capabilities and mission demands.

1. Observation and fields of fire.

Threats associated with observation and fields of fire usually involve when the enemy will be able to engage a friendly unit and when the friendly unit's weapon capabilities allow it to engage the enemy effectively.

2. Cover and concealment. Threats

associated with cover and concealment are created either by failure to use cover and concealment or by the enemy's use of cover and concealment to protect his assets from observation and fire.

3. Obstacles. Threats associated with

obstacles may be caused by natural conditions (such as rivers or swamps) or man-made conditions (such as minefields or built-up areas).

4. Key terrain. Threats associated with

key terrain result when the enemy controls that terrain or denies its use to the friendly forces.

5. Avenues of approach. Threats associated

with avenues of approach include conditions in which an avenue of approach impedes deployment of friendly combat power or conditions that support deployment of enemy combat power.

(b) Weather. To identify weather threats, leaders and unit personnel must assess the impact on operating systems. Threats may arise from-

1. Lack of understanding of reliability

and accuracy of weather forecasting.

16 May 2006

2. Effects of climate and weather on personnel and equipment operation and maintenance.

3. Effects of weather on mobility.

(4) **Troops and Support Available.** Leaders analyze the capabilities of available friendly troops. Associated threats impact both individual personnel and the unit. Key considerations are level of training, manning levels, the condition and maintenance of equipment, morale, availability of supplies and services, and the physical and emotional health of personnel. All personnel must be vigilant to the fact that threats in these areas can adversely affect a mission. Even when all tactical considerations point to success, mission failure can be caused by-

(a) Threats to physical and emotional health. The health threat depends on a complex set of environmental and operational factors that combine to produce "disease non-battle injuries" as well as combat injuries. Care of troops requires long-range projection of logistical and medical needs with close monitoring of mission changes that could impact troop support.

(b) Threats to task organization or units participating in an operation. Threats include poor communication; unfamiliarity with higher headquarters SOPs, and insufficient combat power to accomplish the mission. How long units have worked together under a particular command relationship should be considered when identifying threats.

(c) Threats associated with long-term missions. Long-term missions include peacekeeping, or insurgency/counterinsurgency operations. Threats associated with these missions include the turmoil of personnel turnover, lack of continuity of leadership, inexperience, and lack of knowledge of the situation and the unit's operating procedures. Long-term missions can also lead to complacency; units conditioned to routine ways of accomplishing the mission fail to see warnings evident in the operational environment. An especially insidious threat is the atrophy of critical-skills that results from not performing mission-essential task list related missions.

16 May 2006

(5) **Time Available.** The threat is insufficient time to plan, prepare, and execute operations. Planning time is always at a premium. Leaders routinely apply the one-third/ two-thirds rule (providing two thirds of time available to subordinates for planning) to ensure their subordinate units are given maximum time to plan. Failure to accomplish a mission on time can result in shortages of time for subordinate and adjacent units to accomplish their missions.

b. **5-M Model.** The 5-M model provides an alternative framework for conducting mission analysis by examining the impacts and inter-relationships between the composite elements of Man, Machine, Media, Management, and Mission. The amount of overlap or interaction between the individual components is a characteristic of each mission and evolves as the mission develops.

(1) **Man.** This is the area of greatest variability and thus possesses the majority of risks. Some considerations and potential threats are listed in Table 2-4.

Table 2-4 Consideration and Potential Threats Analyzed (Man Element, 5-M Model)	
Considerations	Potential Threats
Selection	Wrong person psychologically/physically, not proficient in assigned task, no procedural guidance.
Performance	Lack of awareness, false perceptions, over-tasking, distraction, channelized attention, stress, peer pressure, over/lack of confidence, poor insight, poor adaptive skills, pressure/workload, fatigue.
Personal Factors	Expectations, lack of job satisfaction, poor values, families/friends, command/control, poor discipline, (internal and external), perceived pressure (over tasking) and poor communication skills.

(2) **Machine.** Used as intended, limitations interface with man. Some considerations and potential threats are listed in Table 2-5.

16 May 2006

Table 2-5 Considerations and Potential Threats Analyzed (Machine Element, 5-M Model)	
Consideration	Potential Threats
Design	Engineering reliability and performance, ergonomics
Maintenance	Availability of time, tools, and parts, ease of access
Logistics	Supply, upkeep, and repair
Technical Data	Clear, accurate, useable, and available

(3) **Media.** This includes external, largely environmental forces. Some considerations and potential threats are listed in Table 2-6.

Table 2-6 Considerations and Potential Threats Analyzed (Media Element, 5-M Model)	
Considerations	Potential Threats
Climatic	Ceiling, visibility, temperature, humidity, wind, and precipitation
Operational	Terrain, wildlife, vegetation, man-made obstructions, daylight, maritime environment, and darkness
Hygienic	Ventilation/air quality, noise/vibration, dust, and contaminants
Traffic ability	Pavement, gravel, dirt, ice, mud, dust, snow, sand, hills, and curves

(4) **Management.** Directs the process by defining standards, procedures, and controls. While management provides procedures and rules to govern interactions, it cannot completely control the system elements. For example, weather is not under management control and individual decisions affect off-duty personnel much more than management policies. Some considerations and examples are listed in Table 2-7.

Table 2-7 Management Tools and Examples Analyzed (Management Element, 5-M Model)	
Considerations	Examples
Standards	Doctrine statements, applicable criteria, and policy directives
Procedures	Checklists, SOPs, work cards, and multi-command manuals
Controls	Crew rest, altitude/airspeed/speed limits, restrictions, training rules/limitations, rules of engagement (ROE), lawful orders

(5) **Mission.** The desired outcome. Objectives: Big picture understood, well defined, obtainable. The results of the interactions of the other 4-Ms (Man, Media, Machine, and Management).