ARMY, MARINE CORPS, NAVY, AIR FORCE



RISK MANAGEMENT

FM 3-100.12
MCRP 5-12.1C
NTTP 5-03.5
AFTTP(I) 3-2.34

AIR LAND SEA APPLICATION CENTER

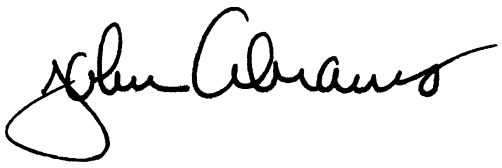
FEBRUARY 2001

DISTRIBUTION RESTRICTION:
Approved for public release;
distribution is unrestricted

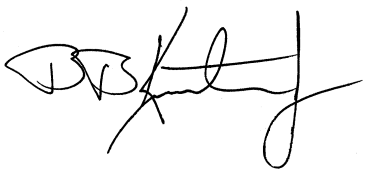
MULTISERVICE TACTICS, TECHNIQUES, AND PROCEDURES

FOREWORD

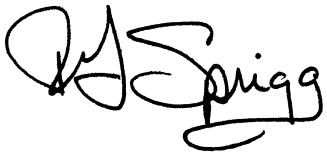
This publication has been prepared under our direction for use by our respective commands and other commands as appropriate.



JOHN N. ABRAMS
General, USA
Commander
Training and Doctrine Command



BRUCE B. KNUTSON, JR.
Lieutenant General, USMC
Commanding General
Marine Corps Combat
Development Command



ROBERT G. SPRIGG
Rear Admiral, USN
Commander
Navy Warfare Development Command



LANCE L. SMITH
Major General, USAF
Commander
Headquarters Air Force Doctrine Center

This publication is available on the General Dennis J. Reimer Training and Doctrine Digital Library at www.adtdl.army.mil

PREFACE

1. Scope

This publication describes risk management functions and responsibilities applicable to the joint task force (JTF) and service staffs. It applies risk management planning procedures to the military decision making process and employs the Joint Operation Planning and Execution System (JOPES) for the operation planning team.

2. Purpose

This publication provides a consolidated multiservice reference addressing risk management background, principles, and application procedures. To facilitate multiservice interoperability, this publication identifies and explains the risk management process and its differences and similarities as it is applied by each service.

3. Applicability

The audience for this publication includes combatant command, JTF, and functional and service component staffs. The target staff level is the JTF headquarters staff. This publication serves as a source document for developing service and joint manuals, publications, and curricula, and may be used as a stand-alone document.

4. Implementation Plan

Participating service command offices of primary responsibility will review this publication, validate the information, and reference and incorporate it in service and command manuals, regulations, instructions, and curricula as follows:

Army. The Army will incorporate this publication in U.S. Army training and doctrinal publications as directed by the Commander, U.S. Army Training and Doctrine Command (TRADOC). Distribution is in accordance with DA Form 12-99-R.

Marine Corps. The Marine Corps will incorporate the procedures in this publication in U.S. Marine Corps (USMC) training and doctrinal publications as directed by the Commanding General, U.S. Marine Corps Combat Development Command (MCCDC). Distribution is in accordance with Marine Corps Publication Distribution System (MCPDS).

Navy. The Navy will incorporate these procedures in U.S. Navy (USN) training and doctrinal publications as directed by the Commander, Navy Warfare Development Command (NWDC). Distribution is in accordance with Military Standard Requisitioning and Issue Procedures (MILSTRIP) Desk Guide and Navy Standing Operating Procedures (NAVSOP) Publication 409.

Air Force. The Air Force will validate and incorporate appropriate procedures in accordance with applicable governing directives. Distribution is in accordance with Air Force Instruction 33-360, Volume 1.

5. User Information

a. The TRADOC-MCCDC-NWDC-Headquarters (HQ) Air Force Doctrine Center (AFDC) and Air Land Sea Application (ALSA) Center developed this publication with the joint participation of the approving service commands. ALSA will review and update this publication as necessary.

b. This publication reflects current joint and service doctrine, command and control organizations, facilities, personnel, responsibilities, and procedures. Changes in service

protocol, appropriately reflected in joint and service publications, will be incorporated in revisions of this document.

c. We encourage recommended changes for improving this publication. Key your comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendations directly to—

Army

Commander
U.S. Army Training and Doctrine Command
ATTN: ATDO-A
Fort Monroe, VA 23651-5000
DSN 680-3153 COMM (757) 788-3153

Marine Corps

Commanding General
U.S. Marine Corps Combat Development Command
ATTN: C42 (Director)
3300 Russell Road
Quantico, VA 22134-5001
DSN 278-6234 COMM (703) 784-6234

Navy

Commander
Navy Warfare Development Command
ATTN: N5
686 Cushing Road
Newport, RI 02841-1207
DSN 948-4201 COMM (401) 841-4201

Air Force

HQ Air Force Doctrine Center
ATTN: DJ
216 Sweeney Boulevard Suite 109
Langley Air Force Base, VA 23665-2722
DSN 574-8091 COMM (757) 764-8091
E-mail Address: afdc.dj@langley.af.mil

ALSA

ALSA Center
ATTN: Director
114 Andrews Street
Langley Air Force Base, VA 23665-2785
DSN 575-0902 COMM (757) 225-0902
E-mail: alsa.director@langley.af.mil

FM 3-100.12 — **U.S. Army Training and Doctrine Command, Fort Monroe, Virginia**

MCRP 5-12.1C — **Marine Corps Combat Development Command, Quantico, Virginia**

NTTP 5-03.5 — **Navy Warfare Development Command, Newport, Rhode Island**

AFTTP(I) 3-2.34 — **Headquarters Air Force Doctrine Center, Maxwell Air Force Base, Alabama**

15 February 2001

RISK MANAGEMENT
Multiservice Tactics, Techniques, and Procedures for Risk Management
TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY ..... **v**

Chapter I RISK MANAGEMENT FUNDAMENTALS **I-1**
1. Background **I-1**
2. Risk Management Goal **I-1**
3. Key Aspects of Risk Management **I-1**
4. Principles of Risk Management **I-2**
5. Levels of Risk Management **I-3**
6. Risk Management Process Overview **I-3**
7. Risk Management Process Application Guidelines **I-3**
8. Relationship of Force Protection to Risk Management **I-5**

Chapter II RISK MANAGEMENT PROCESS AND OPERATIONAL CONSIDERATIONS **II-1**
1. Background **II-1**
2. Application of Risk Management **II-1**
3. Integration of Risk Management **II-7**
4. Analysis Models **II-8**

Chapter III STAFF FUNCTIONS AND RESPONSIBILITIES **III-1**
1. Background **III-1**
2. Responsibilities **III-1**

Distribution Restriction: Approved for public release. Distribution is unlimited

3. Integration into Training and Operations **III-6**
4. Review of the Risk Management Process **III-6**

Appendix A Risk Management Tools **A-1**

Appendix B Force Protection Working Group **B-1**

References **References-1**

Glossary **Glossary-1**

Index **Index-1**

Figures

I-1. Continuous Application of Risk Management **I-4**
II-1. Identify the Threats **II-1**
II-2. Assess the Threat **II-2**
II-3. Develop Controls and Make Risk Decisions **II-3**
II-4. Implement Controls **II-5**
II-5. Supervise and Review **II-6**
A-A-1. Sample Completed Risk Management Worksheet **A-A-1**
A-B-1. Sample Force Protection Priority Matrix **A-B-1**
A-D-1. Risk Assessment Matrix **A-D-1**
A-E-1. Sample Risk Control Options Planning Matrix **A-E-1**
B-1. Potential Sources for the FPWG **B-1**
B-2. Example FPWG Meeting Agenda **B-2**
B-3. Sample Risk Considerations Matrix **B-5**

Tables

II-1. Criteria for Effective Controls **II-3**
II-2. Risk Management Execution (Risk Management in Deliberate Planning) **II-7**
II-3. Risk Management Execution (Risk Management in Crisis Action Planning) **II-8**
II-4. Considerations and Potential Threats Analyzed (Man Element, 5-M Model) **II-11**
II-5. Considerations and Potential Threats Analyzed (Machine Element, 5-M Model) **II-11**
II-6. Considerations and Potential Threats Analyzed (Media Element, 5-M Model) **II-12**
II-7. Management Tools and Examples Analyzed (Management Element, 5-M Model) **II-12**
A-C-1. Sample Force Protection Tasks, Conditions, Desired Effects, and Activities **A-C-1**
A-D-1. Risk Severity Categories **A-D-2**
A-D-2. Probability Definitions **A-D-3**
A-E-1. Examples of Risk Control Options **A-E-2**

EXECUTIVE SUMMARY

Risk Management

This publication—

- **Provides multiservice tactics, techniques, and procedures for tactical level risk management in the planning and execution of operations in a joint environment.**
- **Provides a basic risk management process that may be used by all services.**
- **Applies to all elements of a force that assists in planning and conducting force protection.**
- **Provides risk management tools for commanders and staffs to use to manage risk during planning, preparation, and execution of joint operations.**

Chapter I
Risk Management Fundamentals

Chapter I introduces risk management as a process to assist decision makers in reducing or offsetting risks. It identifies the goal, key aspects, and principle concepts of the process; provides general guidelines for applying the process; and gives an overview of the process:

- Identifying threats.
- Assessing threats to determine risks.
- Developing controls and making risk decisions.
- Implementing controls.
- Supervising and reviewing.

Chapter II
Operational Considerations and Implementation

Chapter II describes the actions involved in applying the risk management process; identifies pitfalls, types of controls, and feedback requirements; and integrates the risk management process into the planning process. This chapter describes how common situation analysis tools support the risk management process.

Chapter III
Staff Functions and Responsibilities

Chapter III ties the risk management process to the chain of command and the staff directorates, and describes how leader involvement at all levels is necessary for the process to be effective. This chapter also describes the integration of the risk management process into all aspects of operations and training and illustrates how constant review of the process leads to improvement in the process.

PROGRAM PARTICIPANTS

The following commands and agencies participated in the development of this publication:

Army

HQ TRADOC (ATDO-A) & (ATBO-SO), Ingalls Rd Bldg 133 Room 7, Ft. Monroe, VA 23651-5000

Combined Arms Center (CAC), Combined Arms Doctrine Directorate (CADD), Ft Leavenworth, KS

OG-D, BCTP, Ft Leavenworth, KS

CDR, XVIII Airborne Corps, Ft Bragg, NC

Army Safety Center, Training Division, Ft Rucker, AL

USAREUR, DCSPER, Unit 29351, APO AE, 09063

Marine Corps

Marine Corps Combat Development Command, Joint Doctrine Branch (C427) 3300 Russell Rd, 3rd Floor Suite 318A, Quantico, VA 22134-5021

Marine Corps Combat Development Command, MSTP (C54) 2076 South Street, Quantico, VA 22134-5021

Commandant of the Marine Corps (Code SD), 2 Navy Annex, Room, 3317, Washington, DC 20380-1775

Navy

OPNAV, N09K, 2000 Navy Pentagon 5E816, Washington, DC 20305-2000

Commander, Navy Warfare Development Command/N5, 686 Cushing Rd, Newport, RI 02841-1207

Commander, Naval Safety Center, 375 A Street, Norfolk, VA 23511-4399

COMPHIBGRU TWO, NAB Little Creek, Norfolk, VA 23521

Air Force

HQ Air Force Doctrine Center, 155 N Twining Street, Maxwell Air Force Base, AL 36112

AFDC Detachment 1, 216 Sweeny Bvld. Ste 109, Langley Air Force Base, VA 23665

HQ USAF/SE, 9700 G Ave SE, Kirkland Air Force Base, NM 87117-5670

Chapter I
RISK MANAGEMENT FUNDAMENTALS

1. Background

Risk management is a process that assists decision makers in reducing or offsetting risk (by systematically identifying, assessing, and controlling risk arising from operational factors) and making decisions that weigh risks against mission benefits. Risk is an expression of a possible loss or negative mission impact stated in terms of probability and severity. The risk management process provides leaders and individuals a method to assist in identifying the optimum course of action (COA). Risk management must be fully integrated into planning, preparation, and execution. Commanders are responsible for the application of risk management in all military operations. Risk management facilitates the mitigation of the risks of threats to the force. For the purposes of this document, threat is defined as a source of danger—any opposing force, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability.

a. Each of the services uses similar but slightly different processes. This publication provides a single process to enable warfighters from different services to manage risk from a common perspective.

b. Risk management is useful in developing, deploying, and employing the joint force. Development concerns force design, manpower allocation, training development, and combat material developments. Deploying and employing the joint force generates concerns in force protection and balancing risk against resource constraints.

c. Military operations are inherently complex, dynamic, dangerous and, by nature, involve the acceptance of risk. Because risk is often related to gain, leaders weigh risk against the benefits to be gained from an operation. The commander's judgment balances the requirement for mission success with the inherent risks of military operations. Leaders have always practiced risk management in military decision making; however, the approach to risk management and degree of success vary widely depending on the leader's level of training and experience.

d. Since the Korean conflict, United States forces have suffered more losses from non-combat causes than from enemy action. Key factors contributing to those losses include—

(1) Rapidly changing operational environment.

(2) Fast-paced, high operations tempo and high personnel tempo.

(3) Equipment failure, support failure, and effects of the physical environment.

(4) Human factors.

2. Risk Management Goal

The fundamental goal of risk management is to enhance operational capabilities and mission accomplishment, with minimal acceptable loss.

3. Key Aspects of Risk Management

a. Risk management assists the commander or leader by—

(1) Enhancing operational mission accomplishment.

(2) Supporting well-informed decision making to implement a COA.

(3) Providing assessment tools to support operations.

(4) Enhancing decision-making skills based on a reasoned and repeatable process.

(5) Providing improved confidence in unit capabilities. Adequate risk analysis provides a clearer picture of unit readiness.

(6) Preserving and protecting personnel, combat weapon systems, and related support equipment while avoiding unnecessary risk.

(7) Providing an adaptive process for continuous feedback through the planning, preparation, and execution phases of military operations.

(8) Identifying feasible and effective control measures where specific standards do not exist.

b. Risk Management does not—

(1) Replace sound tactical decision making.

(2) Inhibit the commander's and leader's flexibility, initiative, or accountability.

(3) Remove risk altogether, or support a zero defect mindset.

(4) Sanction or justify violating the law.

(5) Remove the necessity for rehearsals, tactics, techniques, and procedures.

4. Principles of Risk Management

The basic principles that provide a framework for implementing the risk management process include—

a. **Accept No Unnecessary Risk.** An unnecessary risk is any risk that, if taken, will not contribute meaningfully to mission accomplishment or will needlessly endanger lives or resources. No one intentionally accepts unnecessary risks. The most logical choices for accomplishing a mission are those that meet all mission requirements while exposing personnel and resources to the lowest acceptable risk. All military operations and off-duty activities involve some risk. The risk management process identifies threats that might otherwise go unidentified and provides tools to reduce or offset risk. The corollary to this axiom is "accept necessary risk" required to successfully complete the mission or task.

b. **Make Risk Decisions at the Appropriate Level.** Anyone can make a risk decision; however, the appropriate level for risk decisions is the one that can make decisions to eliminate or minimize the threat, implement controls to reduce the risk, or accept the risk. Commanders at all levels must ensure that subordinates know how much risk they can accept and when to elevate the decision to a higher level. Ensuring that risk decisions are made at the appropriate level will establish clear accountability. The risk management process must include those accountable for the mission. After the commander, leader, or individual responsible for executing the mission or task determines that controls available to them will not reduce risk to an acceptable level, they must elevate decisions to the next level in the chain of command.

c. **Accept Risk When Benefits Outweigh the Cost.** The process of weighing risks against opportunities and benefits helps to maximize mission success. Balancing costs and benefits is a subjective process and must remain a leader's decision.

d. **Anticipate and Manage Risk by Planning.** Integrate risk management into planning at all levels. Commanders must dedicate time and resources to apply risk management effectively in the planning process, where risks can be more readily assessed and managed. Integrating risk management into planning as early as possible provides leaders the greatest opportunity to make well-informed decisions and implement effective risk controls. During execution phases of operations, the risk management process must be

applied to address previously unidentified risks while continuing to evaluate the effectiveness of existing risk control measures and modify them as required.

5. Levels of Risk Management

The risk management process has two levels of application: crisis action and deliberate. Time is the basic factor that contributes to the selection of the level of application used.

a. **Crisis Action.** Crisis action risk management is an "on-the-run" mental or verbal review of the situation using the basic risk management process. The crisis action process of risk management is employed to consider risk while making decisions in a time-compressed situation. This level of risk management is used during the execution phase of training or operations as well as in planning and execution during crisis responses. It is particularly helpful for choosing the appropriate COA when an unplanned event occurs.

b. **Deliberate.** Deliberate risk management is the application of the complete process when time is not critical. It primarily uses experience and brainstorming to identify threats and develop controls and is, therefore, most effective when done in a group. Examples of deliberate applications include planning upcoming operations, reviewing standing operating procedures (SOP), maintenance, training, and developing damage control or disaster response plans.

6. Risk Management Process Overview

The risk management process involves the following:

- Identifying threats.
- Assessing threats to determine risks.
- Developing controls and making risk decisions.
- Implementing controls.
- Supervising and reviewing.

a. **Threat Identification and Threat Assessment.** These elements comprise the risk assessment portion of risk management. In threat identification, individuals identify the threats that may be encountered in executing a mission. In threat assessment, they determine the direct impact of each threat on the operation. Risk assessment provides enhanced awareness and understanding of the situation. This awareness builds confidence and allows timely, efficient, and effective protective measures.

b. **Develop Controls, Make Decisions, Implement Controls, Supervise, and Review.** These remaining elements of the risk management process are the essential follow-through actions of managing risk effectively. Leaders weigh risk against benefits and take appropriate actions to eliminate unnecessary risk. During planning, preparation, and execution, the commander should communicate his acceptable risks to subordinates and continuously assess risks to the overall mission. Finally, leaders and individuals evaluate the effectiveness of controls and capture lessons learned.

7. Risk Management Process Application Guidelines

This section provides general guidelines for applying the risk management process. To get maximum benefit from this tool—

a. **Apply the Process in Sequence.** Each element is a building block for the next one. For example, if threat identification is interrupted to focus control on a particular threat, other more important threats may be overlooked and the risk management process may be distorted. Until threat identification is complete, it is not possible to prioritize risk control efforts properly.

b. **Maintain Balance in the Process.** All parts of the process are important. If only an hour is available to apply the risk management process, the time must be allocated to ensure the total process can be completed. Spending fifty minutes of the hour on threat identification may not leave enough time to apply the other parts of the process effectively. The result would be suboptimal risk management. Of course, it is simplistic to rigidly insist that each of the parts is allocated ten minutes. The objective is to assess the time and resources available for risk management activities and allocate them to the actions in a manner most likely to produce the best overall result.

c. **Apply the Process as a Cycle**. See Figure I-1 below. Notice that "supervise and review" feeds back into the beginning of the process. When "supervise and review" identifies additional threats or determines that controls are ineffective, the entire risk management process should be repeated.

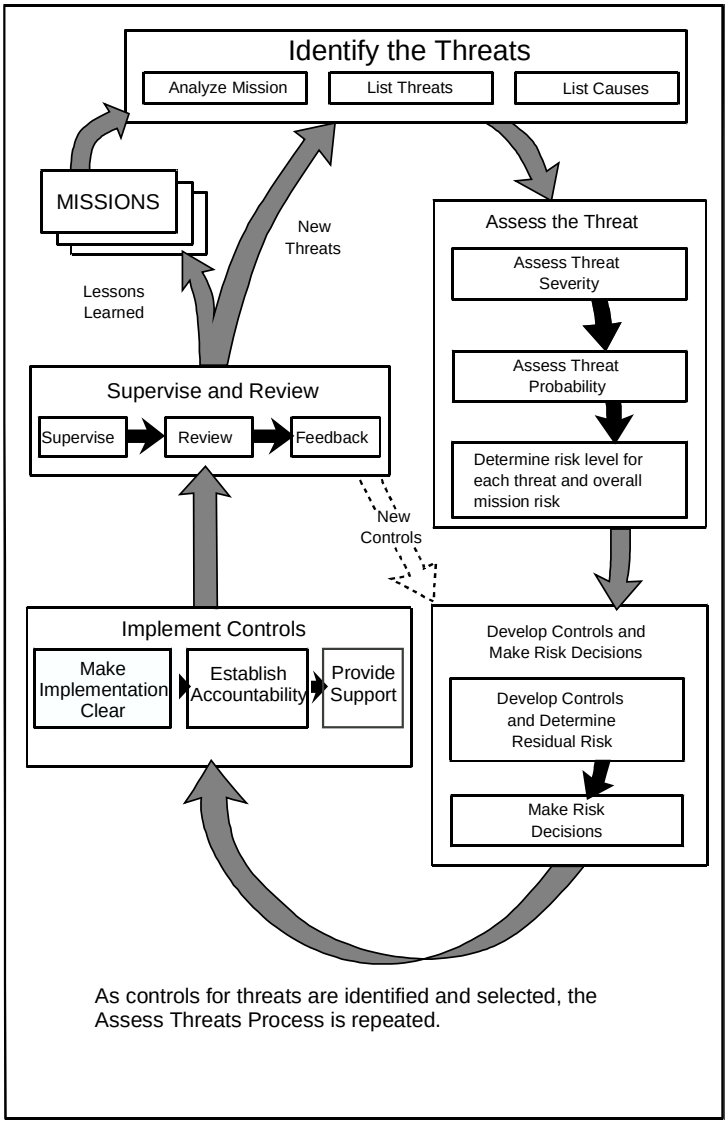


Figure I-1. Continuous Application of Risk Management

d. **Involve People Fully.** The only way to ensure the risk management process is effective is to involve the people actually exposed to the risks. Periodically revalidate risk management procedures to ensure those procedures support the mission.

8. Relationship of Force Protection to Risk Management

The commander has the dilemma of weighing mission requirements and force protection measures. One of his primary tools for weighing mission and protection is reconciled by assessing and balancing risk. This process forms a direct relationship between force protection and risk management. In the force protection process, we consider three elements: planning, operations, and sustainment. Risk management enables the force protection process by using risk assessment and controls in each element. The relationship between force protection and risk management is evident in the following:

a. In planning, we conduct risk assessment and develop controls.

b. In operations, we update risk assessment and implement controls.

c. In sustainment, we continue to update assessments and adjust controls.

Chapter II
RISK MANAGEMENT PROCESS AND OPERATIONAL CONSIDERATIONS

1. Background

This chapter discusses the risk management process and how it may be applied in the planning and execution phases of all operations. This chapter also provides two situational analysis models. These models are the mission, enemy, terrain and weather, troops and support available, time (METT-T) model and the man, machine, media, management, mission (5-M) model.

2. 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 II-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.

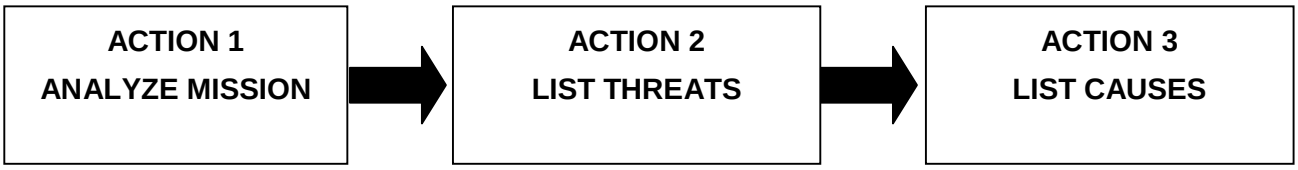


Figure II-1. Identify the Threats

(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.

(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 vulnerabilities. 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 II-2 depicts the necessary actions.

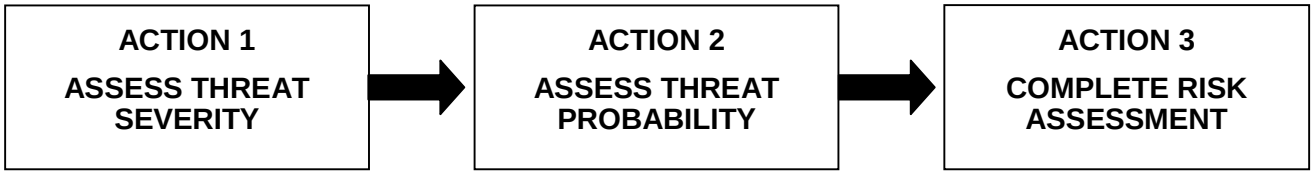


Figure II-2. Assess the Threat

(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, subsystem, or component failure or malfunction). Severity categories listed in Appendix A, Annex D, provide guidance for a wide variety of missions and systems.

(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 definitions for probability may be found at Appendix A, Annex D.

(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 Appendix A, Annex D. 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.

(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.

- Numbers may oversimplify real life situations.
- It may be difficult to get enough applicable data; this could force inaccurate estimates.
- Numbers often take the place of reasoned judgment.
- Risk can be unrealistically traded off against benefit by relying solely on numbers.

c. **Develop Controls and Make Risk Decisions.** These actions are listed as separate and distinct parts of the overall process by the U.S. Air Force (USAF), but will be dealt with under this overall heading for the purpose of this publication. Figure II-3 depicts the necessary actions.

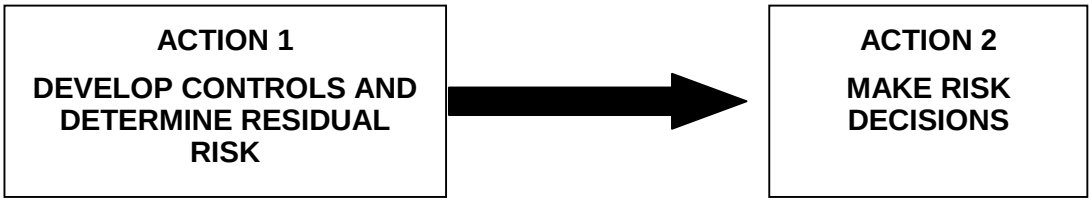


Figure II-3. Develop Controls and Make Risk Decisions

(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 II-1.

Table II-1
Criteria for Effective Controls

CONTROL CRITERIA	***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 a control.
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.

(a) Some types of controls are as follows:

- **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.

- **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.

- **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.

- **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.

- **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.

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

- **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 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.

- **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.

- **Transferring the risk.** Risk may be reduced by transferring a mission, or some portion of that mission, to another unit 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.

- **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.

(c) **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 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.

(2) **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 found in Appendix A, 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 II-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.

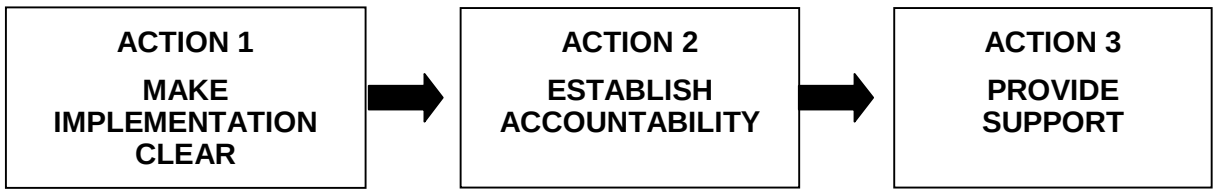


Figure II-4. Implement Controls

(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 it will be received positively by the intended audience. This can best be achieved by designing in user ownership.

(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.

e. **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 II-5 depicts the necessary actions.



Figure II-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.

(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 effect 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.

(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, cross-tell reports, 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.

3. Integration of Risk Management

Tables II-2 and II-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 II-2
Risk Management Execution
(Risk Management in Deliberate Planning)

Deliberate Planning	***Identify Threats***	***Assess Threats***	***Develop Controls Make Risk Decision***	***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**

Table II-3 Risk Management Execution (Risk Management in Crisis Action Planning)					
CRISIS ACTION PLANNING	***Identify Threats***	***Assess Threats***	***Develop Controls Make Risk Decision***	***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**	**JTF MSE**	**JTF MSE**

4. 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: (1) the mission itself, (2) the enemy, (3) terrain/weather, (4) troops and support available, and (5) time available.

Note. The U.S. Army uses mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC), adding civil considerations as a sixth area of analysis.

(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?"

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

- Assess potential advantages to the enemy provided by the battlefield environment.
- Fully assess the enemy's capabilities.
- Understand enemy capabilities and friendly vulnerabilities to those capabilities.

- Accurately determine the enemy's probable COAs.
- Plan and coordinate active ground and aerial reconnaissance activities.
- Disseminate intelligence about the enemy to lower echelons.
- 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 battlespace 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—

- Identifying opportunities and constraints the battlefield environment offers to enemy and friendly forces.
- Thoroughly portraying enemy capabilities and vulnerabilities.
- 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 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.

- *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.
- *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.
- *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).
- *Key terrain.* Threats associated with key terrain result when the enemy controls that terrain or denies its use to the friendly forces.
- *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—

- Lack of understanding of reliability and accuracy of weather forecasting.
- Effects of climate and weather on personnel and equipment operation and maintenance.
- 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.

(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. **U.S. Army Situation Analysis.** While Joint, Marine Corps, Air Force, and Navy doctrine use METT-T for situation analysis, the Army uses METT-TC. The "C" in METT-TC is civil considerations—how the attitudes and activities of the civilian leaders, populations, and organizations within an area of operations will influence the conduct of military operations. Threats associated with civil considerations include, but are not limited to, collateral damage, changing political and social attitudes, civilian unrest, the influence of the press on public opinion, conflicting goals and objectives of private voluntary organizations (PVOs) and nongovernmental organizations (NGOs), and the handling of refugees, noncombatants, and protesters.

c. **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 II-4.

Table II-4
Considerations 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 II-5.

Table II-5
Considerations and Potential Threats Analyzed
(Machine Element, 5-M Model)

Considerations	***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 II-6.

Table II-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**
Trafficability	**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 II-7.

Table II-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).

Chapter III
STAFF FUNCTIONS AND RESPONSIBILITIES

1. Background

The unit commander, staff, leaders, and individual members integrate risk management by embedding the risk management process into unit operations, culture, organization, systems, and individual behaviors.

a. Successful risk management is underwritten by the chain of command. Leaders do not expect all missions to be accomplished with zero defects. Leaders need to support subordinates' decisions to accept risks that are within the leaders' understanding of the commander's intent and guidance. Demanding rigid standards, such as zero defects, leads to over-supervision and paralysis, producing timid leaders afraid to make tough decisions in crisis, and unwilling to take risks necessary for successful military operations. A zero-defects mindset creates conditions that will inevitably lead to failure and higher casualties in battle.

b. Leaders anticipate things may go wrong, even with the certain knowledge that subordinates do all within their power to prevent incidents. When incidents occur, leaders step forward and accept the responsibility along with their subordinates. Furthermore, risk management does not justify taking actions to facilitate an unethical, immoral, or illegal action.

2. Responsibilities

a. **Commanders.** With the assistance of their leaders and staffs, commanders manage risks. Minimizing risk is the responsibility of everyone in the chain of command, from the highest commander, through his subordinate leaders, to each individual service member. Managing risk is critical for all operations, whether for training or operations; commanders should issue clear risk guidance.

(1) Military plans should make risk management a priority. It is an inherent part of every mission and a basic responsibility of commanders. Leaders and service members at all levels are responsible and accountable for managing risks by ensuring that threats and associated risks are—

(a) Identified during planning, preparation, and execution of operations.

(b) Controlled during preparation and execution of operations. Service members are responsible for executing risk controls to standards. They continuously assess variable threats such as fatigue, equipment serviceability, and the environment. They make risk decisions consistent with the higher commander's guidance.

(2) Sometimes commanders are not properly advised in situations where the assumption of risk may affect or imperil their units, the intent of their higher commander, or the operations of an adjacent unit. This is most often attributed to—

(a) Risk denial syndrome—leaders do not want to know of the risk.

(b) Staff members who believe that the risk decision is part of their jobs and do not want to bother the commander or section leader.

(c) Subordinates failure to fully understand the higher commander's guidance.

(d) Complacency—outright failure to recognize a threat or the level of risk involved, or overconfidence in one's abilities or the unit's capabilities to avoid or recover from a hazardous incident.

(e) Use of a standardized risk assessment tool, such as a risk assessment matrix, that is not tailored to the unit's mission or adapted to the factors of METT-T/5-M and may put missions in the routine low-risk category.

b. **Commanders/Leaders.**

(1) The commander directs the organization and sets priorities and the command climate (values, attitudes, and beliefs). Successful preservation of combat power requires embedding risk management into unit behavior. This requires commitment, creative leadership, innovative planning, and careful management. It also requires the chain of command's demonstrated support of the risk management process. Commanders establish a command climate favorable for risk management integration by—

(a) Demonstrating consistent and sustained risk management behavior through leading by example—habitually doing risk management—and actively participating throughout the risk management process.

(b) Providing clear guidance where to accept risk or what risk to accept.

(c) Obtaining and providing to subordinates the necessary assets to control risk.

(d) Knowing their own limitations, their leaders' and service members' limitations, and their unit's capabilities.

(e) Preventing a zero-defects mindset from creeping into their command's culture.

(f) Allowing subordinates to make mistakes and learn from them.

(g) Demonstrating full confidence in subordinates' mastery of their trade and their ability to execute a chosen COA.

(h) Keeping subordinates informed and consulting with subordinate leaders before making a decision, if feasible.

(i) Listening to subordinates.

(j) Establishing clear, feasible risk management policies and goals.

(k) Conducting detailed planning within time constraints; assessing each mission and task in terms of its risk; continuously reassessing risk as the mission and conditions change and experience is gained.

(l) Making informed risk decisions; establishing and clearly communicating risk guidance.

(m)Training on the risk management process. Ensuring subordinates understand who, what, where, when, how, and why of managing risk, and how the risk management process applies to their circumstances and assigned responsibilities.

(n) Examining how subordinates manage risk and how service members protect themselves.

(o) Supervising and evaluating the unit's execution of risk controls during the mission.

(p) Advising the chain of command on risks and risk-reduction measures and providing subordinates with feedback on their performance and ways to improve.

(q) Assessing the effectiveness of their unit's risk management program.

(r) Capturing and disseminating lessons learned to ensure they are continued from mission to mission so that others may benefit from the experience.

(2) Commanders weigh the repercussions of casualties, damage to the environment, impact on civilians, and loss of equipment. They also consider the public reaction to loss against national, strategic, operational, or tactical objectives. Commanders are also responsible for keeping subordinates from becoming complacent. An acceptable risk is the result of an informed decision. A gamble is an uninformed bet or guess on a hopeful outcome. Leaders and service members need to clearly understand the difference.

(3) Risk decisions are frequently required by, and dependent on, the immediate situation. Judgment is required; a formula, rule, or checklist, by itself, is not appropriate under such circumstances. An effective commander's approach to managing risk is to empower leaders by pushing risk decisions as far down the chain of command as feasible within the next higher commander's guidance. Subordinates consider threats outside their assigned responsibilities that impact the mission. The result is coordination and communication—laterally and up and down the chain of command.

(4) Risk management is a two-way street. It is important that those involved in mission preparation and execution are fully aware of the amount of command involvement and actions necessary to control or remove threats.

(a) The higher commander's guidance specifies the degree of acceptable damage or risk to subordinate units during the current operation.

(b) Subordinates ensure they understand and implement their commander's intent and guidance.

- If, during the planning process, residual risk exceeds that which the higher commander is willing to accept, the subordinate informs his commander. He requests the resources necessary to mitigate the risk.

- If, during mission execution, the subordinate determines the risk is too great, he directs the development of additional or alternate controls or modifies or changes the COA; then he notifies the next higher commander of his decision. Requiring subordinates to report to the higher commander when a risk decision point is reached during mission execution can result in paralysis.

(5) The objective of managing risk is not to remove all risk, but to eliminate unnecessary risk. Commanders conduct tough, realistic training, knowing that they may put lives and property at risk in the course of military operations. If an action will result in an unacceptable risk, take measures to mitigate it. If the risk cannot be mitigated to an acceptable level, do not execute the action. Circumstances may occur during mission execution when a decision to stop and defer execution of the operation should be made to avoid taking unwarranted risk. Such a situation will generally occur at the tactical level. For example, circumstances may determine if a trade-off between maintaining the momentum of the attack and risking fratricide or serious accidents is justified.

c. **Staffs.**

(1) The chief of staff or executive officer may be assigned responsibility for supervising integration of risk management across the staff. As a means of assessing and monitoring threats, commanders may establish a force protection working group (FPWG), which is covered in detail in Appendix B. He coordinates development of risk controls with emphasis on deconflicting controls that affect multiple functional areas and adjacent units. The staff officer helps the commander eliminate unnecessary risks by—

(a) Analyzing his functional area and applying risk management during the military decision-making process.

(b) Identifying both constraints and restraints in the higher commander's risk guidance.

(c) Including threats and their risks in the mission analysis briefing.

(d) Including a risk assessment for the commander's estimate.

(e) Considering the risk assessment in the operations estimate.

(f) Including risks and recommending ways to reduce their impact in the staff estimate.

(g) Implementing risk controls by coordinating and integrating them into the appropriate paragraphs and graphics of the operation order (OPORD) and into products such as SOPs and operation plans (OPLANs).

(h) Establishing procedures and standards that are clear and practical.

(i) Determining the effectiveness of risk controls and continuously assessing their suitability, feasibility, supportability, clarity, and acceptability.

(j) Supervising, evaluating, and assessing the integration of risk management during an operation.

(k) Continuously identifying threats, assessing initial and residual risks for each threat, and recommending control measures to reduce the risk.

(l) Identifying and assessing threats associated with complacency, especially during extended operations, and recommending appropriate actions to the commander.

(2) Staffs focus on threats and their risks across the spectrum of protecting the force. These staffs—

(a) Identify friendly vulnerabilities during current operations and implement controls to mitigate risk.

(b) Implement commander's intent on acceptance of risk in current operations.

(3) The following list identifies some of the risk management responsibilities of the primary JTF directorates:

(a) J-1 (Personnel):

- Estimate time delay risks on personnel deployment flow.
- Determine casualty risks for each COA.
- Estimate casualty and replacement flow risks on future operations.
- Ensure controls for personnel-related activities are conducted to diminish operations security vulnerabilities and support military deception initiatives.
- Estimate risks of employed local civilian labor in coordination with the J-4 (logistics), J-2 (intelligence), and legal officer.

(b) J-2:

- Monitor and report threats that counter the effectiveness of friendly combat identification/counter-fratricide measures.
- Develop current regional threat assessments.
- Determine risk of loss of low-density intelligence collection assets.

(c) J-3 (Operations):

- Develop risk assessment for the commander's estimate.

- Perform as staff proponent for combat identification/counter-fratricide measures. Develop policy, procedures and assign responsibility for combat identification/counter-fratricide measures.

- Report and investigate reports of fratricides.

- Develop risk assessment of military and political aspects of draft ROE and supplemental ROE.

- Determine criticality and vulnerability of bases in the Joint Rear Area to prioritize controls and levels of response.

(d) J-4:

- Make recommendations to the JTF commander on the combat identification/counter-fratricide technology acquisition and procurement strategies.

- Assess the risk of critical supply levels not meeting required number of days of supply days.

- Determine petroleum, oils, and lubricants storage site vulnerabilities and controls.

- Determine munitions storage site vulnerabilities and safety requirements.

(e) J-5 (Plans):

- Integrate functional directorate risk management controls and combat identification/counter-fratricide measures into deliberate planning products.

- Identify friendly maneuver and firepower vulnerabilities during mission analysis, wargaming and plan controls to mitigate risk.

(f) J-6 (Communications): Responsible for assessing risk to geospatial information and services systems and developing controls to counter threats.

(g) Special staff offices: Risk management should be addressed in the various special staff offices, including—

- Surgeon (health and nonbattle injury, return to duty policy, preventative medicine).

- Legal officer (Uniform Code of Military Justice, law of armed conflict, and host nation (HN) law).

- Public affairs officer (media coverage, public opinion, etc.).

- Safety officer.

d. **Individuals.**

(1) An individual's level of expertise and maturity influences risk management proficiency. Managing risk is subjective because its basis is individual judgment. Inexperienced service members are routinely charged with executing risk controls and risk reduction measures. Their limited experience can significantly increase the level of risk they are willing to accept. Their sense of indestructibility, motivation (esprit de corps), and willingness to achieve the mission at any cost can lead to failure to consider risks. Due to inexperience or complacency, they may become susceptible to—

(a) Overestimating their ability to respond to, or recover from, a hazardous incident—they become overconfident.

(b) Underestimating the level of risk posed by a threat. It is imperative that individuals understand and execute controls directed by leaders and staffs.

(2) Individuals should be aware of, and fully understand, the situation, and maintain self-discipline when they perform their duties. They should—

(a) Understand and apply risk management.

(b) Execute controls directed by their leaders, that is, perform to standards.

(c) Carry risk management over into all activities—both on and off duty.

(d) Look out for others—anyone has authority to halt something that is inherently unsafe.

3. Integration into Training and Operations

a. Integrating risk management into training and operations—

(1) Preserves the lives and well-being of everyone.

(2) Conserves equipment, facilities, environmental resources, and combat power.

b. Risk management is planned up front, not treated as an afterthought. Leaders and managers of materiel acquisition, base operations, and industrial operations budget risk control costs up front at the level of expected payback over the duration of the activity, or the life cycle of materiel/weapons system.

c. When integrating risk management into sustained operations, leaders consider increases in turbulence, personnel turnover, critical skill atrophy, and mission development. Leaders continuously assess—

(1) The complexity of mission development and associated changing interrelationships with other agencies.

(2) The inclusion of civilian contractors, such as logistics civilian augmentation programs, as part of the force.

(3) The presence of the media, NGOs, and PVOs. These diverse elements need to be integrated into the risk management process.

d. A key consideration relevant to managing risk in complex operational environments is understanding the culture of the indigenous population or society and its way of doing business. Leaders consider the impact of interference with the indigenous population's way of life and local customs. Such interference could risk damage to relationships and increase the potential for introducing instability into the local society. Leaders do not, however, intentionally allow these considerations to endanger their force or its mission.

e. Leaders and service members systematically provide observations and assessments of the unit's risk management performance for the training management cycle and SOPs. They should have the skills, knowledge, and attitude to manage risks inherent in all operations effectively. Effective training helps service members become proficient. It qualifies them technically and tactically, and as leaders, to accomplish the mission without unnecessary risk.

f. Unit leaders and their staffs continually assess and evaluate the integration of risk management into short-, near-, and long-term training plans. They continually review Joint Mission Essential Task Lists to ensure that training is supported by realistic risk management objectives. The services consider past experiences to avoid repeating mistakes.

4. Review of the Risk Management Process

a. Reviewing the risk management process determines a unit's current level of proficiency in implementing the process. How well risk is managed affects readiness. Leaders need to know the current status and effectiveness of their unit's risk management

program. Reviewing the unit's effectiveness in managing risk permits the unit to gain insight into areas for improvement and obtain feedback on subordinates' understanding and application of risk guidance. The objective is to determine how—

(1) Effectively risk management is embedded into planning and preparing for operations.

(2) Well subordinate leaders and service members understand risk management.

(3) Effectively risk management is used to execute operations. Leaders assess the effectiveness of their units by reviewing how well threats are identified and risk controls are—

(a) Specified in oral and written OPORDs, OPLANs, and SOPs.

(b) Communicated to lowest level of chain of command.

(c) Included in short-, near-, and long-term training plans.

(d) Implemented into all activities, on and off duty.

(e) Embedded into force protection programs.

(f) Included in AARs and captured in lessons learned.

b. Risk management cannot be seen as a competitive program whereby a unit or leader is judged or compared in a competitive sense. Focus is strictly on both reduction of risk and hazardous incidents.

Appendix A
Risk Management Tools

Commanders, leaders, and staffs use risk management tools to facilitate the risk management process—identification of threats and development of controls. The tables and matrices in this appendix are samples of tools that commanders, leaders and staffs may use when integrating the risk management process. It is impractical to create detailed procedures to ensure the "right" tools are used for each activity and every contingency. However, choosing the best tools is important when planning a potentially hazardous operation. Most tools in this appendix can be used in a variety of creative ways; the user selects the appropriate tool, or combination of tools, and the extent of effort to expend on each. Since there are no right or wrong selections, the user must rely on his knowledge and experience to make the right choice for each situation.

Annex A: Risk Management Worksheet

Annex B: Force Protection Priority Matrix

Annex C: Force Protection Tasks, Conditions, Desired Effects and Activities

Annex D: Risk Assessment Matrix

Annex E: Sample Risk Control Option Planning Matrix

Annex A
Risk Management Worksheet

The risk management worksheet provides a starting point to track the process of threats and risks logically. It can be used to document risk management steps taken during planning, preparation, and execution.

Mission				**Date Worksheet Prepared**			
Identify Threats			**Assess Threats**	**Develop Risk Controls and Make Risk Decisions**		**Implement Controls**	**Supervise**
Phases	**Threats**	**Causes**	**Initial RAC**	**Develop Controls**	**Residual RAC**	**How to Implement**	**How to Supervise**
Initial entry	Protesters	Religious belief	Medium	Personnel awareness, cantonment area	Low	Training Civil Affairs, perimeter fencing	First line supervisors
Initial entry	Diseases	Water airborne	High	Immunize field sanitation	Low	Predeployment actions, training	Component commanders
Lodgment expansion	Pilferage	Local economy	High	Increase security force	Medium	Augment force	J-3/4
Lodgment expansion	Air Defense Artillery Battery (-)	Deny airfield	High	Direct action	Medium	Airfield takedown 1st Ranger Battalion	J-3
				Accept Risks Yes/No Comm with Higher/Yes No			
Legend: RAC—Risk Assessment Code							

Figure A-A-1. Sample Completed Risk Management Worksheet

Annex B
Force Protection Priority Matrix

This matrix prioritizes force protection tasks and operating systems used for protection in each task. It reverses the normal targeting methodology and focuses the Joint Planing Group on what it needs to protect for each specific task.

	Force Protection Task 1: Maintain flank security		***Force Protection Task 2: Maintain security of vital areas***	
Priority	***Operational Operating System***	***Protected Capability***	***Operational Operating System***	***Protected Capability***
1	Maneuver	3d Marine Division (PD) 101st Airborne Division (Air Assault) (PD)	Logistics	CSSA (PN) JLOTS Site (PN)
2	Logistics		Command and Control	MEB Command Post (PN) TACC (PN) Ground Mobile Force Site (PS)
3	Fires		Fires	Airbase A (PN) Airbase B (PN)
4	Intelligence	UAV FOB	Intelligence	
5	Command and Control		Maneuver	
6	Force Protection		Force Protection	Tactical Combat Force (PD)

Key:

PD—Prevent Destruction
PN—Prevent Neutralization
PS—Prevent Suppression

Legend:

CSSA—combat service support area
FOB—forward operating base
JLOTS—joint logistics over the shore
MEB—Marine Expeditionary Brigade
TACC—Tactical Air Command Center
UAV—unmanned aerial vehicle

Figure A-B-1. Sample Force Protection Priority Matrix

Annex C
Force Protection Tasks, Conditions, Desired Effects, and Activities

Troop-to-task analysis may reveal deficiencies that require risk assessment and subsequent adjustments. The following table is a sample analysis that draws out the logical consequences of a force protection task. It can also be rendered as a decision tree. During COA development, each member of the joint planning group needs to be able to justify the tasking of resources to support force protection tasks.

Table A-C-1.
Sample Force Protection Tasks, Conditions, Desired Effects, and Activities

Force Protection Task • Maintain security of vital areas • Minimize losses
Force Protection Condition • GMF remains fully operational during H-hour to H+24 • Rapid evacuation of casualties
Force Protection Desired Effect • GMF site safe from local attack and from effects of weapons of mass destruction • Air MEDEVAC less than 20 minutes • Surface MEDEVAC to regimental aid stations only
Force Protection Activities • Local security in place • TCF prepared to respond to level III threat • TBMD coverage includes GMF site • Task MAW to dedicate/configure 2 CH-46 for air MEDEVAC during H+10 – H+ 24 • Ensure adequacy of Class VIII prior to H + 10
Legend: GMF—Ground Mobile Force MAW—Marine Air Wing MEDEVAC—medical evacuation TBMD—theater ballistic missile defense TCF—Tactical Combat Force

Annex D
Risk Assessment Matrix

The Risk Assessment Matrix combines severity and probability estimates to form a risk assessment for each threat. Use the Risk Assessment Matrix to evaluate the acceptability of a risk, and the level at which the decision on acceptability will be made. The matrix may also be used to prioritize resources, to resolve risks, or to standardize threat notification or response actions. Severity, probability, and risk assessment should be recorded to serve as a record of the analysis for future use.

Risk Assessment Matrix						
		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	**I**	**E**	**E**	**H**	**H**	**M**
Critical	**II**	**E**	**H**	**H**	**M**	**L**
Marginal	**III**	**H**	**M**	**M**	**L**	**L**
Negligible	**IV**	**M**	**L**	**L**	**L**	**L**

Figure A-D-1. Risk Assessment Matrix

1. Risk Definitions

a. **E - Extremely High Risk**: Loss of ability to accomplish the mission if threats occur during mission. A frequent or likely probability of catastrophic loss (IA or IB) or frequent probability of critical loss (IIA) exists.

b. **H – High Risk**: Significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if threats occur during the mission. Occasional to seldom probability of catastrophic loss (IC or ID) exists. A likely to occasional probability exists of a critical loss (IIB or IIC) occurring. Frequent probability of marginal losses (IIIA) exists.

c. **M – Moderate Risk**: Expected degraded mission capabilities in terms of the required mission standard will have a reduced mission capability if threats occur during mission. An unlikely probability of catastrophic loss (IE) exists. The probability of a critical loss is seldom (IID). Marginal losses occur with a likely or occasional probability (IIIB or IIIC). A frequent probability of negligible (IVA) losses exists.

d. **L – Low Risk:** Expected losses have little or no impact on accomplishing the mission. The probability of critical loss is unlikely (IIE), while that of marginal loss is seldom (IIID) or unlikely (IIIE). The probability of a negligible loss is likely or less (IVB through (IVE).

2. Severity Categories

The following table outlines severity categories:

Table A-D-1
Risk Severity Categories

Category	*Definition*
CATASTROPHIC (I)	Loss of ability to accomplish the mission or mission failure. Death or permanent disability. Loss of major or mission-critical system or equipment. Major property (facility) damage. Severe environmental damage. Mission-critical security failure. Unacceptable collateral damage.
CRITICAL (II)	Significantly degraded mission capability, unit readiness, or personal disability. Extensive damage to equipment or systems. Significant damage to property or the environment. Security failure. Significant collateral damage.
MARGINAL (III)	Degraded mission capability or unit readiness. Minor damage to equipment or systems, property, or the environment. Injury or illness of personnel.
NEGLIGIBLE (IV)	Little or no adverse impact on mission capability. First aid or minor medical treatment. Slight equipment or system damage, but fully functional and serviceable. Little or no property or environmental damage.

3. Probability Categories

The following table outlines probability categories for the risk assessment matrix:

Table A-D-2 Probability Definitions	
Element Exposed	***Definition***
FREQUENT (A) Occurs very often, continuously experienced	
Single item	Occurs very often in service life. Expected to occur several times over duration of a specific mission or operation.
Fleet or inventory of items	Occurs continuously during a specific mission or operation, or over a service life.
Individual	Occurs very often. Expected to occur several times during mission or operation.
All personnel exposed	Occurs continuously during a specific mission or operation.
LIKELY (B) Occurs several times	
Single item	Occurs several times in service life. Expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs at a high rate, but experienced intermittently (regular intervals, generally often).
Individual	Occurs several times. Expected to occur during a specific mission or operation.
All personnel exposed	Occurs at a high rate, but experienced intermittently.
OCCASIONAL (C) Occurs sporadically	
Single item	Occurs some time in service life. May occur about as often as not during a specific mission or operation.
Fleet or inventory of items	Occurs several times in service life.
Individual	Occurs over a period of time. May occur during a specific mission or operation, but not often.
All personnel exposed	Occurs sporadically (irregularly, sparsely, or sometimes).
SELDOM (D) Remotely possible; could occur at some time	
Single item	Occurs in service life, but only remotely possible. Not expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs as isolated incidents. Possible to occur some time in service life, but rarely. Usually does not occur.
Individual	Occurs as isolated incident. Remotely possible, but not expected to occur during a specific mission or operation.
All personnel exposed	Occurs rarely within exposed population as isolated incidents.
UNLIKELY (E) Can assume will not occur, but not impossible	
Single item	Occurrence not impossible, but can assume will almost never occur in service life. Can assume will not occur during a specific mission or operation.
Fleet or inventory of items	Occurs very rarely (almost never or improbable). Incidents may occur over service life.
Individual	Occurrence not impossible, but may assume will not occur during a specific mission or operation.
All personnel exposed	Occurs very rarely, but not impossible.

Annex E
Sample Risk Control Options Planning Matrix

This matrix combines risk control options and responsible personnel that appear suitable and practical with potential options. Many of these options may be applied at more than one level. For example, the training option may be applied to operators, supervisors, senior leaders, or staff personnel.

OPTIONS	*OPERATOR*	*LEADER*	*STAFF*	*COMMANDER*
ENGINEER				
Limit energy	X	X	X	
Substitute safer form				X
Prevent release		X	X	
Rechannel/separate in time/space			X	
Provide special maintenance of controls		X	X	X
EDUCATIONAL				
Core tasks (especially critical tasks)			X	X
Leader tasks			X	X
Emergency/contingency tasks			X	
Rehearsals	X	X		X
Briefings		X	X	
ADMINISTRATIVE				
Facilities/equipment	X	X		
Number of people or items		X	X	
Mental criteria		X		X
Emotional criteria		X		X
Physical criteria		X		X
Experience		X		
Emergency medical care	X		X	
PHYSICAL				
Barrier between	X	X		
On human or object	X	X		
Raise threshold (harden)		X		
Time		X		X
Signs/color coding		X	X	
Audio/visual alarms			X	
OPERATIONAL				
Sequence of events		X	X	X
Timing (within tasks, between tasks)	X	X	X	
Simplify tasks	X	X		
Backout options			X	X
Contingency capabilities			X	X
Emergency damage control procedures		X	X	
Backups/redundant capabilities			X	X
Mission capabilities	X			

Figure A-E-1. Sample Risk Control Options Planning Matrix

Table A-E-1
Examples of Risk Control Options

Option	Example
	ENGINEER
Limit energy	Small amount of explosives, reduce speeds
Substitute safer form	Use air power, precision guided munitions
Prevent release	Containment, double/triple containment
Separate	Barriers, distance, boundaries
Provide special maintenance of controls	Special procedures, environmental filters
	EDUCATIONAL
Core Tasks (especially critical tasks)	Define critical minimum abilities, train
Leader tasks	Define essential leader tasks and standards, train
Emergency contingency tasks	Define, assign, train, verify ability
Rehearsals	Validate processes, validate skills, verify interfaces
Briefings	Refresher warnings, demonstrate threats, refresh training
	ADMINISTRATIVE
Mental criteria	Essential skills and proficiency
Emotional criteria	Essential stability and maturity
Physical criteria	Essential strength, motor skills, endurance, size
Experience	Demonstrated performance abilities
Number of people or items	Only expose essential personnel and items
Emergency medical care	Medical facilities, personnel, medical evacuation
Personnel	Replace injured personnel, reinforce units, reallocate
Facilities/equipment	Restore key elements to service
	PHYSICAL
Barrier	Between revetments, walls, distance, ammunition storage facility
On human or object	Personal protective equipment, energy absorbing materials
Raise threshold (harden)	Acclimatization, reinforcement, physical conditioning
Time	Minimize exposure and number of iterations/rehearsals
Signs/color coding	Warning signs, instruction signs, traffic signs
Audio/visual	Identification of friendly forces, chemical/biological attack warning
	OPERATIONAL
Sequence of events (flow)	Put tough tasks first before fatigue, do not schedule several tough tasks in a row
Timing (within tasks, between tasks)	Allow sufficient time to perform, practice, and time between tasks
Simplify tasks	Provide job aids, reduce steps, provide tools
Reduce task loads	Set weight limits, spread task among many
Backout options	Establish points where process reversal is possible when threat is detected
Contingency capabilities	Combat search and rescue, rescue equipment, helicopter rescue, tactical combat force
Emergency damage control procedures	Emergency responses for anticipated contingencies, coordinating agencies
Backups/redundant capabilities	Alternate ways to continue the mission if primaries are lost
Mission capabilities	Restore ability to perform the mission

Appendix B
Force Protection Working Group

1. Purpose

The purpose of the force protection working group (FPWG) is to review threats, identify vulnerabilities, recommend counter-measures, determine force protection levels, assess in place measures, review tasks to components, monitor corrective actions, and direct special studies (force protection assessment teams). The primary responsibility is to monitor and assess the risk and threats to forces in the joint operations area and implement risk controls to maintain the protection of the force. Each command and control node, rear, intermediate support base, or FOB, should have a FPWG.

2. Group Composition

The composition will vary based on the threats and forces available. Suggested potential sources to provide representatives to the FPWG are listed in Figure B-1.

Chief of Staff	Senior Enlisted Representative	Army Forces
Personnel	Public Affairs	Marine Forces
Intelligence	Surgeon	Air Force Forces
Operations	Nuclear, Biological, and Chemical	Navy Forces
Logistics	Chaplain	Special Operations Forces
Plans	Staff Weather Officer	Security Forces
Communications	Safety	Judge Advocate General
Engineer	Political Advisor	
Aviation	Host Nation Support Representative	
BOTTOM LINE: Composition is Mission Dependent		

Figure B-1. Potential Sources for the FPWG

3. Procedures

The group may meet daily, weekly, or on-call in the vicinity of the Joint Operations Center to use the risk management process.

4. Agenda

The officer in charge of the command and control node or a designated representative should chair the meetings. The chairperson for the FPWG is not necessarily designated by duty position, but based on the ability of the person to fulfill the duties of force protection officer. A recommended agenda for conducting FPWG meetings follows:

a. Start with updates from—

(1) J2 Representative: intelligence update with focus on changes to the situation that may lead to additional threats for the force.

(2) Counterintelligence (CI) representative: follows the J2, clarifies and provides details of current risks based on his field reports.

(3) J3 Representative: overview of current operations and force protection measures currently in place.

b. Next, update new or evolving threats. This is an open discussion by functional area. For example, the surgeon would focus on medical health of command, the veterinary on new or changing food sources, etc. Steady state activities are raised during this phase of the meeting. All members consider emerging trends and determine if new vulnerabilities within their area of responsibility require the focus of the task force or if they are just isolated incidents. Each member comes to the meeting with documented concerns and recommendations.

c. When new threats are identified, the FPWG will discuss measures to reduce the threat. For example, Threat identified: current route from billeting area to the Joint Operations Center is dangerous and not acceptable at night. Control: CI team will contact the country team, identify alternate routes, and drive and assess the routes. At the next FPWG meeting a decision will be made to change route.

d. Once controls are decided upon (above example, CI to conduct a reconnaissance of a new route), that information is captured by the J3 representative and placed, as a directive for action, in the next fragmentary order.

e. Following identification and development of controls for new threats, the group will review current measures in effect against known threats and determine the requirement for any changes or adjustments. Figure B-2 is an example FPWG agenda.

Event	***Input***
Threat Situation Review	J2
Current Force Protection Levels	J3
Current Operations	J3
Results of Previous Meeting	Components, J3
Threat Identification	FPWG
Vulnerability Identification	FPWG
Identify Controls	FPWG
Recommend Force Protection Level	FPWG
Recommend Taskings	FPWG
Summary	J3
Confirm Next Meeting	J3

Figure B-2. Example FPWG Meeting Agenda

5. Assessment Teams

To maintain visibility of threats, the FPWG may designate assessment teams to monitor the situation continuously. These teams may be tailored to review specific threats (such as preventive medicine and surgeon for medical, CI and Provost Marshal/Security Officer/Chief Security Forces for perimeter security). These teams may be assigned and operate at all operating bases throughout the joint operations area.

a. The assessment teams mission includes—

(1) Identify and assess threats and vulnerabilities.

(2) Recommend controls.

(3) Report through FPWG to Commander of the JTF.

(4) Gather information.

b. Assessment teams may use the following checklist:

(1) Threat.

(a) What is the terrorist threat/capability?

(b) What is the in-country leave and pass policy?

(c) Are there any areas service members should avoid due to criminal or terrorist threats?

(d) What is the pre-disposition of the local populace to Americans (is it safe for service members to mix with public)?

(e) Could operations be affected by civil disturbances protesting U.S. policy?

(f) What criminal threats are likely to threaten operations (are there any threats of pilferage affecting sustainment operations)?

(g) What is the relationship of local population with host nation (HN) authorities (is there any threat of civil unrest that could affect operations)?

(h) Are there other threats such as para-military organizations or hostile intelligence that may target operations?

(2) Facilities.

(a) What facilities will the task force occupy?

- Tent city vs. hard site?
- Location—urban or rural?

(b) What is the status of—

- Perimeters?
- Barriers?
- Lighting?
- Motor pool facilities?

(c) Will the node collocate with HN or friendly forces?

(d) Is secure storage available for arms, ammunition, and explosives and classified, high dollar, and sensitive items?

(e) Are there high-speed avenues of approach?

(f) What checkpoints and barriers are necessary to control compound access?

(3) Where will mission-essential vulnerable areas be established for arms, ammunition, and explosives storage; sensitive item storage; pilferable high dollar value item storage; fuel storage etc.?

(a) What is their proximity to the perimeter?

(b) What is their vulnerability to attack or observation?

(4) Will the task force operate any sustainment operations facilities at air, sea, or rail ports?

(5) Joint Operations.

(a) If the task force occupies facilities with HN or friendly forces, who has command and control for force protection?

(b) Who must the task force coordinate with concerning force protection, HN, friendly forces?

(c) What are capabilities of friendly forces, HN armed forces, HN police forces, and HN security forces?

(d) How are in-place friendly forces approaching force protection?

(e) What historical problems have in-place friendly forces had concerning criminal activity (such as pilferage, assaults, terrorist threat, civil disturbance, and hostile intelligence)?

(f) What threats do they perceive as possible?

(g) What operations security measures are in effect?

(h) What movement security measures are in effect?

6. FPWG Products

Based on the FPWG meeting, there are three suggested deliverables.

a. First—an update to the Force Protection Matrix. This should be briefed to the JTF commander and placed on the SECRET Internet Protocol Router Network for the staff and components. Figure B-3 is an example of the risk considerations matrix.

b. Second—Fragmentary Order directing execution of the new FPWG measures.

c. Third — risk assessment for the current phase of the operation.

d. Force protection assessment—continuous process throughout the conduct of the operation.

Event: JTF FOB establishment location /component: FOB				
Operational Operating System	**Threat**	**Vulnerability**	**Countermeasure**	**Action**
Movement/ Maneuver	Local faction	Troop movement Route to hotel	Minimize Standard route/ Alternate routes	Adjust battle rhythm All drivers with alternate route maps
	Aircraft	Crossing flight lines	Do not cross	
Intelligence	Accident	Civil rights	Know embassy numbers	Accident card USAF security patrols post speed limit
	Speeding flight line	Pedestrians	Slow speed (15 mph)	LNOs brief forces
Fires	Loitering	Theft/bad press	Minimum presence in hotel	Place of duty or room
Sustainment	Fire Threats	Personnel and equipment	Know route, exiting and alert procedure	Fire break around FARP
	No help/assist	Personnel stranded	Blood chits	Order 500 chits
Command and Control	Personnel accountability/ location	Unsafe location/ Unknown location	Frequent reporting, improve communication	Command emphasis Distribute cell phones
Protection	Heat	Injury	Water discipline	Monitor WGBT
	Disease-malaria	Health	Buddy check	Take pills
			Field sanitation	Clean latrines
	Dogs	Injury/health	Caution	Stay clear
Legend: FARP—forward arming and refueling point LNO—liaison officer mph—miles per hour USAF—U.S. Air Force WGBT—wet globe bulb temperature				
Notes. Any changes made by the FPWG are highlighted. An additional column labeled "Assessment" can show how the countermeasures are working				

Figure B-3. Sample Risk Considerations Matrix

REFERENCES

National

Presidential Decision Directive 39, *U.S. Policy on Counterterrorism*, 21 June 1995

Department of Defense

DODI 6055.1, *DOD Safety and Occupational Health (SOH) Program,* 19 August 1998

Joint

CJCSM 3500.03, *Joint Training Manual for the Armed Forces of the United States*, 1 June 1996

CJCSM 3500.04, *Universal Joint Task List*, 1 November 1999

CJCSM 3500.05, *Joint Task Force Headquarters Master Training Guide,* 15 April 1997

JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 September 2000

JP 3-0, *Doctrine for Joint Operations,* 1 February 1995

JP 3-10, *Joint Doctrine for Rear Area Operations*, 28 May 1996

JP 3-11, *Joint Doctrine for Operations in Nuclear, Biological, and Chemical (NBC) Environments,* 11 July 2000

JP 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W),* 7 February 1996

JP 3-54, *Joint Doctrine for Operations Security*, 24 January 1997

JP 3-58, *Joint Doctrine for Military Deception*, 31 May 1996

JP 4-0, *Doctrine for Logistics Support of Joint Operations*, 6 April 2000

JP 5.00.1, *Joint Tactics, Techniques, and Procedures for Joint Campaign Planning (Draft*)

JP 5-00.2, *Joint Task Force (JTF) Planning Guidance and Procedures*, 13 January 1999

Air Force

AFDD 2-4.1, *Force Protection*, 29 October 1999

AFPD 90-9, *Operational Risk Management*, 1 April 2000

AFI 90-901, *Operational Risk Management,* 1 April 2000

AFPAM 90-902, *Operational Risk Management Guidelines and Tools,* 14 December 2000

Army

FM 3-0 (FM 100-5), *Operations*, 14 June 1993

FM 3-07 (FM 100-20), *Military Operations in Low Intensity Conflicts,* 5 December 1990

FM 3-07.3 (FM 100-23), *Peace Operations*, 30 December 1994

FM 3-58 (FM 90-2), *Battlefield Deception,* 3 October 1988

FM 6-22 (FM 22-100), *Army Leadership,* 31 August 1999

FM 3-21.10 (FM 7-10), *The Infantry Rifle Company*, 31 October 2000

FM 7-10 (FM 25-101), *Battle Focused Training,* 30 September 1990

Coast Guard

COMMANDANT INSTRUCTION 3500.3 *Operational Risk Management (Draft*)

Marine Corps

Marine Corps Order 3500.27, *Operational Risk Managemen*t, 3 April 1997
ALMAR 210/97, *Operational Risk Management,* 15 July 1997
MCDP-1, *Warfighting,* June 1997
MCDP 1-2, *Campaigning,* August 1997
MCWP 3-22, *Antiair Warfare,* 23 June 2000
MCWP 5-1, *Marine Corps Planning Process,* January 2000

Navy

OPNAVINST 3500.38, *Universal Naval Task List,* 30 September 1996
OPNAVINST 3500.39, *Operational Risk Management*, 3 April 1997

Glossary

PART I—ABBREVIATIONS AND ACRONYMS

5-M	man, machine, media, management, mission
	A
AAR	After Action Report
AFB	Air Force Base
AFDC	Air Force Doctrine Center
AFTTP	Air Force Tactics, Techniques, and Procedures
AL	Alabama
ALSA	Air Land Sea Application
APO	Army Post Overseas
	C
CAC	Combined Arms Center
CADD	Combined Arms Doctrine Development Center
Cdr	commander
CI	counterintelligence
COA	course of action
CSSA	combat service support area
	D
DC	District of Columbia
DCSPER	Deputy Chief of Staff for Personnel
DSN	Defense Switched Network
	E
etc	etcetera
	F
FARP	forward arming and refueling point
FM	field manual
FOB	forward operating base
FPWG	force protection working group
	G
GMF	ground mobile force

H

HN	host nation
HQ	headquarters

J

J-1	Manpower and Personnel Directorate of a joint staff
J-2	Intelligence Directorate of a joint staff
J-3	Operations Directorate of a joint staff
J-4	Logistics Directorate of a joint staff
J-5	Plans Directorate of a joint staff
J-6	Command, Control, Communications, and Computer Systems Directorate of a joint staff
JLOTS	joint logistics over-the-shore
JOPES	Joint Operation Planning and Execution System
JP	joint publication
JTF	joint task force

K

KS	Kansas

L

LNO	liaison officer

M

MAW	Marine air wing
MCCDC	Marine Corps Combat Development Command
MCPDS	Marine Corps Publication Distribution System
MCRP	Marine Corps Reference Publication
MEDEVAC	medical evacuation
METT-T	mission, enemy, terrain and weather, troops and support available, time available
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, civil considerations (Army)
MILSTRIP	Military Standard Requisitioning and Issue Procedures
MSE	major subordinate element
MSTP	Marine Air Ground Task Force Training Program

N

NAVSOP	Navy Standing Operating Procedure
NC	North Carolina
NWDC	Navy Warfare Development Command
NGO	nongovernmental organization
NM	New Mexico

O

OPLAN	operation plan
OPORD	operation order

P

PD	prevent destruction
PN	prevent neutralization
PS	prevent suppression
PVO	private voluntary organization

R

RAC	risk assessment code
RI	Rhode Island
ROE	rules of engagement

S

SOP	standing operating procedure

T

TACC	Tactical Air Command Center
TBMD	theater ballistic missile defense
TCF	tactical combat force
TRADOC	United States Army Training and Doctrine Command

U

UAV	unmanned aerial vehicle
USAF	United States Air Force
USAREUR	United States Army, Europe
USMC	United States Marine Corps
USN	United States Navy

PART II—TERMS AND DEFINITIONS

acceptable risk. The portion of identified risk that is allowed to persist without further controls

assessment. 1. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity.

2. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 1-02)

controls. Actions taken to eliminate threats or reduce their risk. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

exposure. The frequency and length of time subjected to a hazard (FM 3-100.12/100-14).

extremely high risk. Risk that could result in loss of ability to accomplish the mission if threats occur during mission. A frequent or likely probability of catastrophic loss (IA or IB) or frequent probability of critical loss (IIA) exists. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication**.**

high risk. Risk that could result in significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if threats occur during the mission. Occasional to seldom probability of catastrophic loss (IC or ID) exits. A likely to occasional probability exists of a critical loss (IIB or IIC) occurring. Frequent probability of marginal losses (IIIA) exists. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

identified risk. A risk determined by applying severity and probability analysis to an identified threat.

inherently dangerous. An activity or task containing a danger to life or limb that is a permanent and inseparable element of the activity. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

low risk. Risk that could result in expected losses having little or no impact on accomplishing the mission. The probability of critical loss is unlikely (IIE), while that of marginal loss is seldom (IIID) or unlikely (IIIE). The probability of a negligible loss is likely or less (IVB through IVE). This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

moderate risk. Risk that could result in degraded mission capabilities in terms of the required mission standard will have a reduced mission capability if threats occur during mission. An unlikely probability of catastrophic loss (IE) exists. The probability of a critical loss is seldom (IID). Marginal losses occur with a likely or occasional probability (IIIB or IIIC). A frequent probability of negligible (IVA) losses exists. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

operational protection. The conservation of the forces' fighting potential so that it can be applied at the decisive time and place. This activity includes actions taken to counter the enemy's forces by making friendly forces (including operational formations, personnel, etc.), systems, and operational facilities difficult to locate, strike, and destroy. (CJCSM 3500.04)

probability. The likelihood that a hazardous incident will occur.

frequent (A): Occurs very often, continuously experienced.

likely (B): Occurs several times

occasional (C): Occurs sporadically

seldom (D): Remotely possible; could occur at some time

unlikely (E): Can assume will not occur, but not impossible.

This term and its definitions are applicable only in the context of this publication and should not be referenced outside this publication.

residual risk. The level of risk remaining after controls have been identified and selected for threats that may result in loss of combat power. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

risk. 1. Probability and severity of loss linked to threats.

2. See degree of risk. See also risk management. (JP 1-02)

risk assessment. Identification and assessment of threats; an identified threat is assessed to determine the risk (both the probability of occurrence and resulting severity) of a hazardous incident due to the presence of the threat. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

risk decision. The decision to accept or not accept the risks associated with an action; made by the commander, leader, or individual responsible for performing that action. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

risk management. A process by which decision makers reduce or offset risk. Also called RM. (JP 1-02) The systematic process of identifying, assessing, and controlling risks arising from operational factors and making decisions that weigh risks against mission benefits.

severity. The intensity of the expected consequence of an event in terms of degree of injury, property damage, or other mission-impairing factors (loss of combat power and so on) that could occur.

catastrophic (I): Loss of ability to accomplish the mission or mission failure. Death or permanent total disability. Loss of major or mission critical system or equipment. Major property (facility) damage. Severe environmental damage. Unacceptable collateral damage. Mission-critical security damage.

critical (II): Significantly degraded mission capability or unit readiness. Permanent partial disability. Extensive (major) damage to equipment or systems. Significant damage to property or the environment. Security failure. Significant collateral damage.

marginal (III): Degraded mission capability or unit readiness. Minor damage to equipment or systems, property, or the environment.

negligible (IV): Little or no adverse impact on mission capability. Slight equipment or system damage, but fully functional and serviceable. Little or no property or environmental damage.

This term and its definitions are applicable only in the context of this publication and should not be referenced outside this publication.

threat. A source of danger; any opposing force, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability. This term and its definition are applicable only in the context of this publication and should not be referenced outside this publication.

total risk. The sum of identified risk and unidentified risk. It is accepted by the appropriate decision-maker because further efforts at risk control are not justified by the perceived gain.

unacceptable risk. The risk that cannot be tolerated and must be eliminated or controlled.

unidentified risk. The risk that has not been identified. It is unknown or immeasurable.

Index

A

acceptability, II-3, III-4, A-D-1

acceptable loss, I-1

acceptable risk, I-2, I-3, II-3, II-5, III-3, A-D-1, Glossary-4

accountability, I-2, II-5, III-1, B-5

administrative controls, II-4, A-E-1, A-E-2

alarmism, II-2

application of risk management, i, I-1, I-3, I-4, II-1

assessment, I-1, I-3, I-5, II-2, II-3, II-5, II-6, II-8, II-9, III-2, III-4, III-5, III-6, A-1, A-A-1, A-C-1, A-D-1, A-D-2, B-1, B-2, B-3, B-4, B-5, Glossary-3, Glossary-4, Glossary-5

- complete, II-2
- matrix, A-D-1
- output, II-2
- pitfalls, v, II-2
- teams, B-1

assigning redundant capabilities, II-5, A-E-1, A-E-2

avenues of approach, II-9, B-3

avoiding the risk, I-2, II-3, II-4, III-3

C

catastrophic, A-D-1, A-D-2, Glossary-4, Glossary-5

chain of command, v, I-2, III-1, III-2, III-3, III-7

civil consideration, II-8, II-10, III-3, III-4, III-6, A-A-1, B-3, B-4, B-5, Glossary-2

climate, II-9, III-2

commander, i, v, vi, I-1, I-2, I-3, I-5, II-3, II-5, II-6, II-8, II-9, III-1, III-2, III-3, III-4, III-5, A-1, A-A-1, A-E-1, B-3, B-4, Glossary-1, Glossary-5

complacency, II-10, III-1, III-4, III-5

complete risk assessment, II-2

controls, risk, v, I-2, I-3, I-4, I-5, II-1, II-3, II-4, II-5, II-6, II-7, II-8, II-9, II-12, III-1, III-2, III-3, III-4, III-5, III-6, III-7, A-1, A-A-1, A-E-1, A-E-2, B-1, B-2, Glossary-4, Glossary-5

- administrative, II-4, A-E-1, A-E-2
- avoiding risk, I-2, II-3, II-4, III-3
- delay COA, II-4
- develop, v, I-3, I-5, II-3, II-4, II-5, II-7, II-8, III-3, III-5, A-1, A-A-1, B-2
- educational, II-4, A-E-1, A-E-2
- engineering, II-4, A-E-1, A-E-2
- implement, v, I-3, I-5, II-3, II-4, II-5, II-6, II-7, II-8, III-4, A-A-1, B-1
- operational, II-4, A-E-1, A-E-2
- options, II-3, II-4, A-1, A-E-1, A-E-2
- physical, II-4, A-E-1, A-E-2
- planning matrix, A-E-1

redundant capabilities, II-4, A-E-1, A-E-2
residual risk, II-3, II-5, III-3, III-4, A-A-1, Glossary-5
support, v, II-3, II-6, III-2, III-4
transferring risk, II-4
course of action (COA), I-1, I-3, I-4, II-3, II-4, II-5, II-8, II-9, III-2, III-3, III-4, A-C-1, Glossary-1
cover and concealment, II-9
crisis action, I-3, II-7, II-8
critical, I-3, II-1, II-4, II-9, II-10, III-1, III-5, III-6, A-D-1, A-D-2, A-E-1, A-E-2, Glossary-4, Glossary-5

D

decisions, i, v, I-1, I-2, I-3, II-3, II-5, II-6, II-7, II-8, II-12, III-1 III-2, III-3, A-A-1, A-C-1, A-D-1, B-2, Glossary-5, Glossary-6
delay, II-4, III-4
deliberate, I-3, II-2, II-7, II-8, III-5
develop controls, v, I-3, I-5, II-3, II-5, II-7, II-8, III-3, III-5, A-1, A-A-1, B-2

E

enemy, I-1, II-1, II-8, II-9, Glossary-2, Glossary-4
engineering, II-4, II-11, A-E-1, A-E-2, B-1
exposure, II-4, A-E-2

F

feasibility, I-2, II-3, III-2, III-3, III-4
feedback, v, I-2, II-6, II-7, III-2, III-7
force protection, v, I-1, I-5, III-3, III-7, A-1, A-B-1, A-C-1, B-1,B-2, B-4, Glossary-1
activities, A-C-1
agenda, B-1, B-2, B-3
assessment team, B-1, B-2
checklist, B-3
composition, B-1
conditions, A-1, A-C-1
effects, A-1, A-C-1
facilities, B-3, B-4
priority matrix, A-1, A-B-1
procedures, B-1
products, B-4
tasks, A-1, A-B-1, A-C-1
force protection working group (FPWG), III-3, B-1, B-2, B-3, B-4, B-5, Glossary-1
forward area refueling point (FARP), B-5, Glossary-1

H

high risk, II-5, A-A-1, A-D-1, Glossary-4

host nation (HN), III-5, B-1, B-3, B-4, Glossary-1

hygienic, II-12

I

identify, i, v, I-1, I-2, I-3, I-4, II-1, II-2, II-3, II-4, II-5, II-6, II-7, II-8, II-9, II-10, III-1, III-3, III-4, III-5, III-7, A-1, A-A-1, A-B-1, A-E-2, B-1, B-2, Glossary-4, Glossary-5, Glossary-6

impact, mission, probability and severity, I-1, I-3, II-1, II-2, II-8, II-9, II-10, III-3, III-4, III-6, A-D-2, Glossary-4, Glossary-5

implementation, i, v, I-1, I-2, I-3, I-5, II-3, II-4, II-5, II-6, II-7, II-8, III-3, III-4, III-6, III-7, A-A-1, B-1

J

Joint Operation Planning and Execution System (JOPES), i, II-7, Glossary-2

joint task force (JTF) i, II-7, II-8, III-4, III-5, B-3, B-4, B-5, Glossary-2

K

key aspects, v, I-1, II-6, II-9, III-5

L

logistics, II-10, II-11, III-4, III-6, A-B-1, B-1, Glossary-2

loss, I-1,II-2,II-4, II-8, III-3, III-4, A-C-1, A-D-1, A-D-2, Glossary-4, Glossary-5

low risk, I-2, II-5, III-2, A-A-1, A-D-1, Glossary-4

M

machine, II-1, II-10, II-11, II-12, Glossary- 1

maintenance, I-3, II-9, II-10, II-11, A-E-1, A-E-2

major subordinate element (MSE), II-7, II-8, Glossary-2

man, machine, media, management, mission (5-M) model, II-1, II-6, II-10, II-11, II-12, III-2, Glossary-1

managing, I-3, III-1, III-2, III-3, III-5, III-6, III-7

marginal, A-D-1, A-D-2, Glossary-4, Glossary-5

media, II-1, II-10, II-12, III-5, III-6, Glossary-1

METT-T (mission, enemy, terrain and weather, troops and support available, time available), II-1, II-6, II-8, II-10, III-2, Glossary-2

METT-TC (mission, enemy, terrain and weather, troops and support available, time available, civil considerations [Army]) II-8, II-10, Glossary-2

moderate risk, II-5, A-D-1, Glossary-4

N

negligible, A-D-1, A-D-2, Glossary-4, Glossary-5

O

objective, I-4, II-10, II-12, III-3, III-6, III-7

observation, II-9, III-6, B-3
operational, v, I-1, II-1, II-4, II-10, II-12, III-3, III-6, A-B-1, A-C-1, A-E-1, A-E-2, B-5, Glossary-4, Glossary-5
operation order (OPORD), III-4, III-7, Glossary-3
operation plan (OPLAN), III-4, III-7, Glossary-3
operations, military, v, I-1, I-2, I-3, I-5, II-1, II-4, II-6, II-8, II-9, II-10, III-1, III-3, III-4, III-6, III-7, A-1, A-D-3, B-1, B-2, B-3, B-4, Glossary-2

P

performance, II-4, II-6, II-11, III-2, III-6, A-E-2
personal, II-1, II-4, II-11, A-D-2, A-E-2
physical, I-1, II-4, II-10, II-11, A-E-1, A-E-2
probability, I-1, II-1, II-2, II-3, II-4, II-5, A-D-1, A-D-2, A-D-3, Glossary-4, Glossary-5,
  category, A-D-2
  definitions, A-D-3
procedures, i, v, I-2, I-3, I-5, II-3, II-10, II-12, III-4, III-5, A-1, A-E-1, A-E-2, B-1, B-5, Glossary-1, Glossary-2, Glossary-3
process, i, v, I-1, I-2, I-3, I-4, I-5, II-1, II-2, II-3, II-5, II-6, II-7, II-9, II-12, III-1, III-2, III-3, III-6, A-1, A-A-1, A-E-2, B-1, B-4, Glossary-5

R

residual risks, II-3, II-5, III-3, III-4, A-A-1, Glossary-5,
responsibilities, i, v, II-5, III-1, III-2, III-3, III-4, III-5, B-1, B-2
  commander, III-1, III-2, III-3
  leaders, III-1, III-2
  individual, III-5
  staff, III-3
risk, i, v, I-1,1-2, I-3, I-4, I-5, II-1, II-2, II-3, II-4, II-5, II-6, II-7, II-8, II-9, II-11, III-1, III-2, III-3, III-4, III-5, III-6, III-7, A-1, A-A-1, A-C-1, A-D-1, A-D-2, A-E-1, A-E-2, B-1, B-4, B-5, Glossary-3, Glossary-4, Glossary-5, Glossary-6
  assessment, II-2, III-4, A-C-1, A-D-1, A-D-2
  probability categories, A-D-2
  probility definitions, A-D-3
  severity categories, II-2, A-D-2
  unacceptable, III-3, Glossary-6
  unnecessary, I-2, I-3, III-3, III-6
risk management, i, v, I-1, I-2, I-3, I-4, I-5, II-1, II-5, II-6, II-7, II-8, II-10, II-12, III-1, III-2, III-3, III-4, III-5, III-6, III-7, A-1, A-A-1, B-1, Glossary-5
  application guidelines, I-3, III-7
  application, i, I-1, I-3, II-1
  assessment, I-1, II-6, III-6
  crisis action, I-3, II-7, II-8
  cycle, I-4
  decisions, II-5

deliberate, I-3, II-7
execution, II-7, II-8
feedback, v, I-2, II-6, II-7, III-2, III-7
framework for implementing, I-2
fundamentals, v, I-1
goal, v, I-1
implement, I-2, III-6
integration, v, II-7, III-2, III-3, III-4, III-6
key aspects, v, I-1
levels, I-3
objective, III-3, III-6, III-7
principles, i, v, I-2
process, i, v, I-1, I-2, I-3, I-4, I-5, II-1, II-5, II-6, II-7, III-1, III-2, III-6, A-1, B-1, Glossary-5
review, v, I-3, I-4, II-1, II-6, II-7, II-8, III-6, III-7
sequence, I-3
supervise, I-3, I-4, II-6, II-7, II-8, A-A-1
training, III-2, III-6
use, I-1, I-3
worksheet, A-1, A-A-1
risk management fundamentals, v, I-1
risk management goal, v, I-1, II-10, III-2

S

services, v, I-1, II-10, III-5, III-6
situational analysis, II-1
supervise and review, I-3, I-4, II-6, II-7, II-8, A-A-1

T

threat, v, I-1, I-2, I-3, I-4, II-1, II-2, II-3, II-4, II-5, II-6, II-7, II-8, II-9, II-10, II-11, II-12, III-1, III-3, III-4, III-5, III-7, A-1, A-A-1, A-C-1, A-D-1, A-E-2, B-1, B-2, B-3, B-4, B-5, Glossary-4, Glossary-5, Glossary-6
assessment, I-3, III-4
causes, II-1, II-2, A-A-1
checklist, B-3
identification, v, I-2, I-3, I-4, II-1, II-3, II-5, II-7, II-8, II-9, II-10, III-4, A-1, A-A-1, B-2, Glossary-4, Glossary-5
probability, II-1, II-2, II-3, A-D-1, Glossary-5
severity, II-1, II-2, II-3, Glossary-4, Glossary-5

U

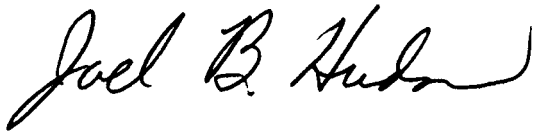
unacceptable risk , III-3, Glossary-6
unnecessary risk, I-2, I-3, III-3, III-6

FM 3-100.12
MCRP 5-12.1C
NTTP 5-03.5
AFTTP(I) 3-2.34
15 February 2001

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0106101

DISTRIBUTION:
Active Army, Army National Guard, and U.S. Army Reserve: **To be distribute in accordance with the initial distribution number 115840 requirements for FM 3-100.12.**

By Order of the Secretary of the Air Force:

LANCE L. SMITH
Major General, USAF
Commander
Headquarters Air Force Doctrine Center

Air Force Distribution: F

MARINE CORPS: PCN 14400009300