RISK MANAGEMENT

> "It is my experience, that bold decisions give the best promise of success. But one must differentiate strategical and tactical boldness and a military gamble. A bold operation is one in which success is not a certainty but which in case of failure leaves one with sufficient forces in hand to cope with whatever situation may arise. A gamble, on the other hand, is an operation which can lead either to victory or to complete destruction of one's force. Situations can arise where even a gamble may be justified--as, for instance, when in the normal course of events defeat is merely a matter of time, when the gaining of time is therefore pointless and the only chance lies in an operation of great risk.
>
> Field Marshall Erwin Rommel[1]

INTRODUCTION

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.

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.

BACKGROUND

Risk Management is an effective process for maintaining readiness in peacetime and achieving success in combat without infringing upon the prerogatives of the

commander. Historically, the greater percentage of losses during combat operations was due to mishaps. Unnecessary losses either in battle or during training are detrimental to operational capability. It provides a means to help define risk and control it where possible, thereby assisting the commander in choosing the best course of action and seizing the opportunities which lead to victory.

Risk management is integrated into the military decision-making process. When assessing the risk of hazards in operations, the commander and staff must look at two kinds of risk, tactical risk and accident risk. Tactical risk is risk associated with hazards that exist due to the presence of the enemy on the battlefield. The consequences of tactical risk take two forms. The first is if the enemy takes action in an area where the commander has accepted risk. For example, an enemy attack where the friendly commander is conducting economy of force operations in order to mass the effects of combat power elsewhere. The second is one of lost opportunity, viz, the commander takes risk in moving forces across restricted terrain to gain the advantage of surprise, but is unable to mass the effects of combat power because the unit is unable to rapidly traverse the terrain. The commander alone determines how and where he is willing to take tactical risk. Accident risk includes all operational risk considerations other than tactical risk, and can include activities associated with hazards concerning friendly personnel, equipment readiness, and environmental conditions. Accident hazards exist regardless of enemy action, even in the absence of an enemy force. Examples of accident hazards include personnel that are not adequately trained to conduct certain kinds of operations, equipment that is not fully operational, and environmental conditions that make operations more dangerous, such as limited visibility and extreme cold weather. Accident risk is managed by both the commander and the staff. Staff members are constantly looking for accident hazards associated with their areas of expertise, and they recommend controls to reduce risk. Tactical risk and accident risk may be diametrically opposite. The commander may accept a high level of accident risk in order to reduce tactical risk. For example, during the seizure of the Remagen Bridge in Europe during WW II, the benefit of seizing an intact bridge over the Rhine outweighed the extremely high risk of sending soldiers across a bridge rigged for demolitions. Both types of risks are managed by the commander with assistance from his staff. Risk decisions are the sole responsibility of the commander. The same risk-management process is used to assess and evaluate both tactical and accident risks. Risk management must become a pattern of thinking—identify and assess the hazard, develop controls to reduce the risk, decide if the benefit from the operation justifies the risk, and then implement controls and supervise.

Key Aspects of Risk Management

First reckon, then risk.

- Field Marshal Helmet Von Moltke.

Risk management assists the commander or leader by:-

- Enhancing operational mission accomplishment.
- Supporting well-informed decision making to implement a Cause of Action (COA).
- Providing assessment tools to support operations.
- Enhancing decision-making skills based on a reasoned and repeatable process.
- Providing improved confidence in unit capabilities. Adequate risk analysis provides a clearer picture of unit readiness.
- Preserving and protecting personnel, combat weapon systems, and related support equipment while avoiding unnecessary risk.
- Providing an adaptive process for continuous feedback through the planning, preparation, and execution phases of military operations.
- Identifying feasible and effective control measures where specific standards do not exist.

However, Risk Management does not—

- Replace sound tactical decision making.
- Inhibit the commander's and leader's flexibility, initiative, or accountability.
- Remove risk altogether, or support a zero defect mindset.
- Sanction or justify violating the law.
- Remove the necessity for rehearsals, tactics, techniques, and procedures.

Principles of Risk Management

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

(a) Accept No Unnecessary Risk.
(b) Make Risk Decisions at the Appropriate Level.
(c) Accept Risk When Benefits Outweigh the Cost.
(d) Anticipate and Manage Risk by Planning.

Risk Management Process Overview

> Sizing up opponents to determine victory, assessing dangers and distances is the proper course of action for military leaders.
>
> - Sun Tzu, The Art of War.

Risk is characterized by both the probability and severity of a potential loss that may result from hazards due to the presence of an enemy, adversary, or some other hazardous condition. Perception of risk varies from person to person. What is risky or dangerous to one person may not be to another. Perception influences leaders' decisions.

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.

This five-step process is integrated into the decision-making process is shown in Figure 1.

Decision Making Process	**Risk Management Steps**				
	Step 1 Identify Hazards	**Step 2** Assess Hazards	**Step 3** Develop Controls/Make Risk Decision	**Step 4** Implement Controls	**Step 5** Supervise and Evaluate
Mission Receipt	**X**				
Begin Planning	**X**	**X**			
Arrange for Reconnaissance	**X**	**X**	**X**		
Complete the Plan	**X**	**X**	**X**		
Issue the Order		**X**	**X**	**X**	
Supervise					**X**
Each "X" represents when each of the five risk management steps would apply to different phases of the decision-making process					

Figure 1. Risk Management Steps Correlated With The Decision-Making Process

STEP 1. IDENTIFY HAZARDS

A hazard is an actual or potential condition where the following can occur due to exposure to the hazard:-

- ❖ Injury, illness, or death of personnel.
- ❖ Damage to or loss of equipment and property.
- ❖ Mission degradation.

Hazards are sources of danger or risks due to enemy or adversary presence and other conditions not due to enemy or adversary capabilities. Hazards are found in all operational environments.

Terrain and Weather. In addition to those due to the enemy or adversaries, the most obvious hazards to military operations are due to terrain and weather. Terrain and weather affect the type of hazard encountered. When the enemy uses terrain to his advantage, the risk is clearly tactical.

Terrain. The terrain analysis includes both map and on-the ground reconnaissance to identify how well unit capabilities and mission demands can be accommodated by the terrain. The five main military aspects of terrain are :-

- Observation and fields of fire.
- Camouflage and concealment.
- Obstacles.
- Key terrain features.
- Avenues of approach.

Weather. Weather works hand-in-hand with terrain to create hazards. To identify weather hazards, soldiers must assess the impact on operating systems. Mistakes include not

considering the—

- Adverse effects of heat and cold hazards on the performance of Soldiers.
- Effects of climate and weather on maintenance of vehicles and equipment before beginning an operation.
- Hazardous effects of weather on the five military aspects of terrain.

STEP 2. ASSESS HAZARDS

Step 2 completes the risk assessment. Risk is the chance of hazard or bad consequences. This step examines each hazard in terms of probability and severity to determine the risk level of one or more hazardous incidents that can result from exposure to the hazard. This step is conducted during four steps of the decision-making process—begin planning, arrange for reconnaissance, make reconnaissance, and complete the plan. This step is also conducted after controls are developed.

Substep A. Leaders and staffs assess each hazard in relation to the probability of a hazardous incident. The probability levels estimated for each hazard may be based on the mission, COAs being developed and analyzed, or frequency of a similar event.

Figure 2 provides a summary of the four degrees of probability. The letters in parentheses following each degree (A through D) provide a symbol for depicting probability. For example, the letter A represents a likely probability.

DEGREE OF PROBABILITY	DESCRIPTION
Likely (A)	Likely to occur immediately or within a short period of time. Expected to occur frequently to an individual item of person or continuously to a fleet inventory or group.
Probably (B)	Probably will occur in time. Expected to occur several times to an individual item or person or frequently to a fleet, inventory, or group.
May (C)	May occur in time. Can reasonably be expected to occur some time to an individual item or person or several times to a fleet, inventory, or group.
Unlikely (D)	Unlikely to occur.

Figure 2. Hazard Probability

Substep B. Substep B addresses the severity of each hazard. It is expressed in terms of—

- Degree of injury or illness.
- Loss of or damage to equipment or property.
- Environmental damage.
- Other mission-impairing factors such as lost combat power.

The degree of severity estimated for each hazard may be based on knowledge of the results of similar past events. Figure 3 provides a summary of the four degrees of hazard severity. Hazard severity categories are assigned Roman numerals to depict each degree of severity (I through IV) in descending order. For example, Category I represents the highest degree of severity and Category IV represents the lowest degree of severity.

CATEGORY	DEGREE OF SEVERITY
Category I	The hazard may cause death, loss of facility/asset or result in grave damage to national interests.
Category II	The hazard may cause severe injury, illness, property damage to national or service interests, or degradation to efficient use of assets.
Category III	The hazard may cause minor injury, illness, property damage, damage to national, service or command interests or degradation to efficient use of assets.
Category IV	The hazard presents a minimal threat to personnel safety or health,

	property, national, service or command interests, or efficient use of assets.

Figure 3. Hazard Severity

Substep C. In this substep leaders and staffs expand what they understand about probable hazardous incidents into estimates of levels of risk for each identified hazard and an estimate of the overall risk for the operation. Estimating risk follows from examining the outcomes of Substeps A and B; that is, both the probability and severity of hazardous incidents. This substep is more art than science. Much depends on the use of historical lessons learned, intuitive analysis, experience, and judgment. Uncertainty can arise in the assessment of both the probability and severity of a hazardous incident. Uncertainty results from unknowns about a situation; from incomplete, inaccurate, undependable, or contradictory information; and from unforeseen circumstances. Therefore, assessment of risk requires good judgment.

Figure 4 is a standardized matrix that can be used to assist in this process. Leaders and staffs enter the estimated degree of severity and probability for each hazard in Substeps A and B from the severity row and probability column, respectively. The point where the severity row and probability column intersect defines the level of risk, and is known as the Risk Assessment Code. (RAC).

Risk Assessment Matrix					
		PROBABILITY			
SEVERITY	**CATEGORY**	**A**	**B**	**C**	**D**
	I	**1**	**1**	**2**	**3**
	II	**1**	**2**	**3**	**4**
	III	**2**	**3**	**4**	**5**
	IV	**3**	**4**	**5**	**5**

Figure 4. Risk Assessment Matrix

The RAC combines the elements of hazard probability and hazard severity, and is expressed as a single Arabic number that corresponds to varying levels of risk, as shown in Figure 5.

For example, if the hazard severity is estimated at category II and the hazard probability is estimated at probably (B), the risk assessment code is serious (2).

Risk Assessment Code (RAC)	
Number	**Corresponding Level of Risk**
1	Critical
2	Serious
3	Moderate

4	Minor
5	Negligible

Figure 5. Risk Assessment Code (RAC)

STEP 3. DEVELOP CONTROLS AND MAKE RISK DECISIONS

Step 3 is accomplished in two substeps: develop controls and make risk decisions. This is done during arrange for reconnaissance, make reconnaissance, and complete the plan steps of the decision-making process. After assessing each hazard, leaders develop one or more controls that either eliminate the hazard or reduce the risk (probability and/or severity) of a hazardous incident. When developing controls, they consider the reason for the hazard not just the hazard itself.

Types of Controls. Controls can take many forms, but they fall into three basic categories—educational controls, physical controls, and avoidance.

- **Educational controls**. These controls are based on the knowledge and skills of the unit 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, guards, or signs to warn individuals and units that a hazard exists. Additionally, special controller or oversight personnel responsible for locating specific hazards fall into this category.
- **Avoidance**. These controls are applied when leaders take positive action to prevent contact with an identified hazard.

Criteria for Controls. To be effective, each control developed must meet the following criteria:-

Suitability. It must remove the hazard or mitigate (reduce) the residual risk to an

acceptable level.

Feasibility. The unit must have the capability to implement the control.

Acceptability. The benefit gained by implementing the control must justify the cost in resources and time. The assessment of acceptability is largely subjective. Figure 6 gives criteria for determining acceptability of controls for each identified hazard.

Support	Availability of adequate personnel, equipment, supplies, and facilities necessary to implement suitable controls.
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 competent enough to implement a control.
Individual	Individual Marines are sufficiently self-disciplined to implement a control.

Figure 6. Criteria for Determining Acceptability of Controls

Examples of Controls. Examples of controls include:-

- Engineering or designing to eliminate or control hazards.
- Selecting a course of action that avoids identified hazards.
- Limiting the number of people and the amount of time they are exposed to hazards, consistent with mission requirements.
- Selecting personnel with appropriate mental, emotional, and physical capabilities.
- Providing protective clothing, equipment, and safety and security devices.
- Providing such services as adequate sanitation facilities and water purification capabilities.
- Providing warning signs and signals.
- Scheduling vehicle and aircraft silhouette drills.
- Planning training, including rehearsals, battle drills, and so forth.
- Programming communications links for key civilian organizations.
- Establishing battlefield controls such as areas of operations and boundaries,
- direct fire control measures, fire support coordination measures, rules of engagement, airspace control measures, bridge classification, traffic control, and so forth.
- Developing terrorist attack warning systems and response plans.

STEP 4. IMPLEMENT CONTROLS

> Leaders must supervise the execution of their orders. The more untrained the roops, the more detailed this supervision must be.
>
> Infantry in Battle, 1939

Leaders and staffs ensure that controls are integrated into Standard Operating Procedures (SOP), written and verbal orders, mission briefings, and staff estimates. The critical check for this step, with oversight, is to ensure that controls are converted into clear, simple execution orders understood at all levels. Implementing controls includes coordination and communication with:-

- ✓ Appropriate superior, adjacent, and subordinate units and those executing the mission.
- ✓ Civilian agencies that are part of the force.

Leaders must explain how supervisors will implement controls. Examples of control implementation include:-

- Conducting vehicle and aircraft silhouette drills.
- Conducting rehearsals, battle drills, and so forth.
- Conducting intensive threat and friendly vehicle identification refresher training for all antiarmour and air defense weapons crews.
- Conducting orientation for replacement personnel.
- Installing and maintaining communications links for key civilian organizations.
- Operating in convoys of four vehicles minimum.
- Carrying weapons and wearing flak jackets and helmets when outside secure compounds.

STEP 5. SUPERVISE AND EVALUATE

During mission preparation and execution, leaders must ensure that their subordinates understand how to execute risk controls. Leaders continuously assess risks during the conduct of operations, especially during long-term missions .Leaders maintain situational awareness. They guard against complacency to ensure that risk control standards are not relaxed or violated. To gain insight into areas needing improvement, leaders must continuously evaluate their units' effectiveness in managing mission risks.

IMPLEMENTATION

> The higher up the chain of command, the greater is the need for boldness to be supported by a reflective mind, so that boldness does not degenerate into purposeless bursts of blind passion Command becomes progressively less a matter of personal sacrifice and increasingly concerned for the safety of others and for the common purpose.
>
> - Col Von Clausewitz, On War

Leaders should not expect that all missions would be accomplished with zero defects—free from errors, flaws, or less-than-perfect performance. Demanding such rigid standards leads to over supervision and paralysis; it produces timid leaders, afraid to make tough decisions in crisis and unwilling to take risks necessary for success in military operations. A zero defects mindset creates conditions that will lead inevitably, in the larger sense, to failure in battle and higher casualties. Leaders are morally bound to support a subordinate's decision to accept risks that are within his commander's intent and guidance, as he understands it. Furthermore, risk management does not justify taking actions to facilitate an unethical or immoral action.

Avoiding the zero-risk mindset requires the exercise of positive leadership. The commander's approach to managing risk should be through empowering leaders by pushing risk decisions as far down the chain of command as feasible within the next higher commander's guidance.

Commanders are responsible and accountable for their own actions and those of units under their charge. Commanders must weigh the repercussions of casualties, damage to the environment, and loss of equipment. They must also consider the level of public reaction to loss against national, strategic, operational, or tactical objectives. Commanders are also responsible for keeping soldiers from falling into complacency.

A risk is the accepted result of an informed decision; a gamble is an uninformed bet or guess on a hopeful outcome. Leaders and soldiers must clearly understand the difference. Command is often exercised in conditions of uncertainty and ambiguity, where violence, danger, fear, and friction abound, and under the ever-present time constraints driven by operation tempo. Risk decisions are frequently required and dependent on the immediate

situation. Judgment is required; a formula, rule, or checklist, by itself, is not appropriate under such circumstances.

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. Nothing is worth the cost of a life as the result of taking unnecessary risk. If an action will result in an unacceptable risk, measures should be taken to mitigate it.

Figure 7 shows that the risk management process continues throughout a mission as well as from mission to mission. It is integral to the military decision-making process. Its application requires good judgment and intuitive analysis borne of confidence, experience, and situational awareness.

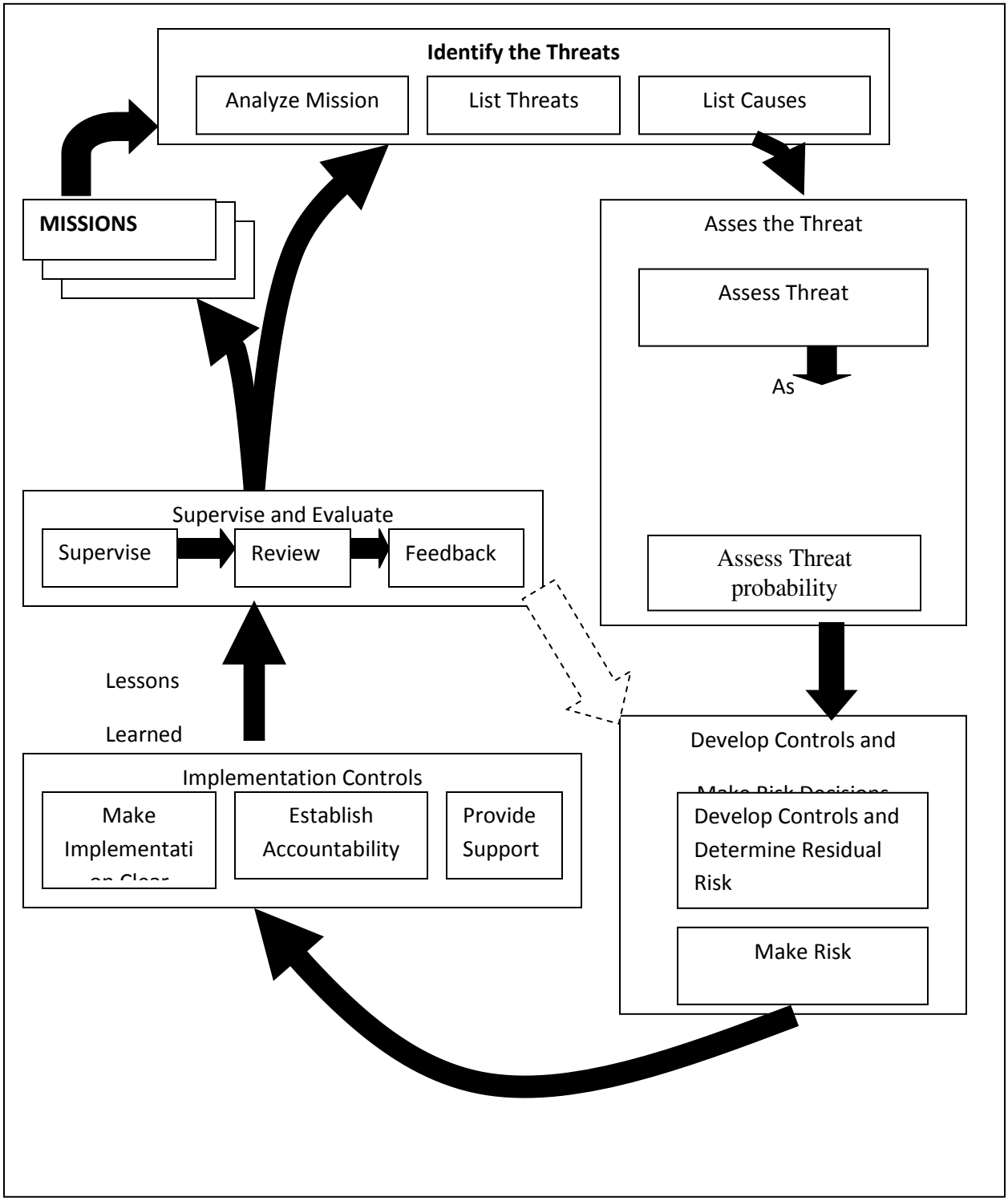

Figure 7. Continuous Application of Risk Management

CONCLUSION

Take calculated risks. That is quite different from being rash.

- General George S Patton, Jr.

Operations in Armed Forces are demanding and complex. Many of these operations are inherently dangerous, including tough, realistic training. The Risk Management process allows commanders and individuals to make informed, conscious decisions to manage and accept risks. Risk Management should not be limited to any one service. It must be a joint process standardized across service lines and inculcated in the planning and execution of every military operation.

Risk Management in a relatively new concept being adapted by the modern armed forces of the world specially United States Military. In April 1996 then vice chief of US Naval operations testified before congress after a series of F-14 aircraft crashes, " We have directed that Operational Risk Management be a key factor in the planning and execution of all aviation training and operations".

In the US Armed forces the subject of Risk Management has been taken very seriously and has been included in their doctrine publications. US Army has a Fild Manual, equivalent to our GS Pamphlet, FM 100-14 Risk Management. The subject has also been dealt in Chapter 4 of Field Manual FM 101-5, Command and Staff Decision Process. US Marine Corps has issued OPNAV Instructions 3500-39A on Operational Risk Management (ORM). In addition US Marine Corps Institute has published ORM,1-0 on Operational Risk Management. Multi Service Tactics, Techniques and Procedures on Risk Management has been published by Air Land Sea Application Centre.

The September 2001 terror attacks caused billion of dollars is losses and led to the expenditure of additional billions of dollars to enhance security against possible future attacks. There is a potential mismatch between resources and needs. Recently RAND Corporation, the leading Think Tank in USA has collaborated with Risk Management Solutions (RMS), the world's leading provider of product and services for catastrophic risk management on how to manage terrorism risk.

The most suitable institute to undertake study on Risk Management in Indian Scenario is College of Defence Management, Secunderabad. Unfortunately nothing substantial has been done on the subject by them. It will be most appropriate if this elite joint service training establishment takes up the subject with the importance it deserves and comes up with a viable joint service doctrine on Risk Management.

BIBLIOGRAPHY

1. B.H. Liddell Hart, from the Rommel Papers. Harcourt Brace & Co., NY 1964,

2. US Army Field Manual FM 100-14 ,Risk Management.

3. US Marine Corps Institute Publication, ORM, 1-0.

4. Lt Cdr Stephen W. Beckvonpeccoz, Operational Risk Management, Increasing Mission Effectiveness Through Improved Planning and Execution of Joint Operations, Naval War College,Newport, RI.

5. Air Land Sea Application Center Publication Risk Management, available at

www.adtdl.army.mil

6. United States Marine Corps OPNAV INSTRUCTION 3500.39A Operational Risk Management (ORM).

7. Department of the Navy, Chief of Naval Operations, Cold, NS 11, OPNAVINST 3500.XX, Operational Risk Management.

8. US Field Manual FM 101- 5. Command and Staff Decision Process.

Published in Defence Management, September 2004 issue.