National Defence　Défense Nationale

B-GJ-005-502/FP-000

Joint Doctrine Manual

RISK MANAGEMENT FOR CF OPERATIONS

Change 1

(ENGLISH)

Issued on Authority of the Chief of Defence Staff

Custodian: Joint Doctrine Branch

November 2007

Canada

LIST OF EFFECTIVE PAGES

Insert latest changed pages, dispose of superseded pages in accordance with applicable orders.

Dates of issue for original and changed pages are:

Original	0	2002	Change	3	
Change	1	Nov 07	Change	4	
Change	2		Change	5	

Zero in Change No. Column indicates an original page. Total number of pages in this publication is 44 consisting of the following:

Page No.	Change No.
Title	1
A	1
i/ii	1
iii/iv	1
1-1 to 1-2	1
2-1 to 2-4	1
3-1 to 3-10	1
4-1 to 4-8	1
A-1 to A-2	1
B-1 to B-2	1
C-1 to C-2	1
G-1 to G-4	1
LA-1 to LA-2	1
REF-1 to REF-2	0

Contact Officer: CFEC Joint Doctrine Branch

PREFACE

1. Some measure of risk occurs in almost every aspect of everyday life. Due to the nature of military operations, the identification and mitigation of risk takes on added importance. In military operations the failure to manage risk can lead to the loss of resources, lives and ultimately catastrophic mission failure. There is a need for operational planners to have a simple, easy to use template to examine risk so they speak from a commonly understood base.

2. The purpose of this manual is to provide a decision process that will aid planners in identifying, analyzing, evaluating and controlling all types of risk. Its key aim is to ensure that significant risks are identified and that appropriate action is taken to minimize these risks balanced against operational objectives.

3. A multitude of risk analysis techniques exist today. Some are best suited to financial evaluation while others are key tools in project management. Similarly, some risk analysis techniques, particularly in engineering design, involve an enormous amount of calculations. In broad terms, many, because of their complexity, are ill suited to operational planning. The process described in this manual has been limited to ensure that the key aspects of risk analysis are considered without overburdening the planner. The techniques described in this manual mirror the United States services' techniques in order to promote interoperability.

4. Risk communication, the communication on risk issues between stakeholders, is not dealt with as a separate issue in this manual even though it is a normal risk management process. As risk management in this manual is described in the context of the CF Operational Planning Process it was determined that interaction in the planning process covered the risk communication requirements.

5. In risk management processes the causes of risk are widely referred to as either hazards or threats. They are synonymous. For the purposes of this manual the term "threat" will be used.

6. This manual is intended to guide risk management in operational planning in the Canadian Forces. It represents the idealized process. Units and formations will tailor it use to their specific needs with their standing operations procedures. As doctrine, this manual is authoritative but the processes require judgement in application.

7. The processes in this manual and in B-GJ-005-500/FP-000, CF Operational Planning Process, are synchronized and need to be used in conjunction with each other.

FOREWORD

1. The manual outlines the risk management procedures to be applied in the Canadian Forces Operational Planning Process (OPP). This process is designed for use by the following:

   a. Commanders and their staffs at the strategic and operational levels (e.g. The Strategic Joint Staff (SJS) and the Operational Commands);

   b. task forces established for routine and contingency operations, as well as all formations and agencies supporting such operations; and

   c. command and staff colleges and other teaching institutions within the framework for officer professional development.

2. This manual is presented in two main sections - an introduction to the basics of risk management and then a discussion of its application to the CF OPP. The first section, chapters 1 and 2, is the background of risk management. The second section, chapters 3 and 4, detail the specific application of the techniques to operational planning.

3. This manual is to be used in conjunction with the *CF Operational Planning Process Manual*, B-GJ-005-500/FP-000 and other manuals. It is subordinate to the CF OPP manual. The risk management process described in this manual closely mirrors those used by the individual services in the United States. This manual is modelled on the United States Air, Land, Sea Application Center's manual: *Risk Management, February 2001.*

4. Comments and recommendations for changes should be forward to the custodian: CFEC Joint Doctrine Branch.

5. The Chief of Force Development is the ratification authority for this doctrine.

TABLE OF CONTENTS

List of Effective Pages .... B
Preface i
Foreward ii
Table of Contents iii

CHAPTER 1 — RISK MANAGEMENT FOR CF OPERATIONS 1-1

101. Introduction 1-1
102. Aim of Risk Management 1-1
103. Risk Management - General 1-1
104. Risk Management Definitions 1-2

CHAPTER 2 — FUNDAMENTALS OF RISK MANAGEMENT 2-1

201. Key Aspects of Risk Management 2-1
202. Principles of Risk Management 2-1
203. Risk Management and the Planning Environment 2-2
204. Risk Management Process Overview 2-2
205. Risk Management Process Application Guidelines 2-2
206. Relationship of Force Protection to Risk Management 2-3

CHAPTER 3 — RISK MANAGEMENT – APPLICATION TO OPERATIONS 3-1

SECTION I - THE RISK MANAGEMENT PROCESS 3-1

301. General 3-1
302. Phase I - Identify Threats 3-1
303. Phase II - Assess Threats 3-1
304. Phase II - Develop Controls and Make Risk Decisions 3-2
305. Phase IV - Implement Controls 3-4
306. Phase V - Supervise and Review 3-5

SECTION II - APPLICATION TO THE CF OPERATIONAL PLANNING PROCESS 3-6

307. Integration of Risk Management 3-6
308. Stage I – Initiation 3-6
309. Stage II – Orientation 3-7
310. Stage III – COA Development 3-9
311. Stage IV – Plan Development 3-10
312. Stage V – Plan Review 3-10

CHAPTER 4 — STAFF FUNCTIONS AND RESPONSIBILITIES 4-1

401. Background 4-1
402. Responsibilities 4-1

403. Integration into Training and Operations 4-6
404. Review of the Risk Management Process 4-7
ANNEX A — RISK ASSESSMENT TOOLS A-1
ANNEX B — RISK MANAGEMENT WORKSHEET B-1
ANNEX C — RISK SCORE MATRIX C-1
GLOSSARY G-1
LIST OF ABBREVIATIONS LA-1
REFERENCES REF-1

LIST OF FIGURES

Figure 2-1 Continuous Application of Risk Management 2-4

LIST OF TABLES

Table 1-1 Risk Management Terms 1-2
Table 3-1 Criteria for Effective Controls 3-3
Table 3-2 Risk Management in CF Operations 3-6
Table 4-1 Risk Management Responsibilities 4-6

CHAPTER 1

RISK MANAGEMENT FOR CF OPERATIONS

101. INTRODUCTION

1. Some measure of risk is inherent in all military operations. By its very nature, the application of force will place individuals and resources in harm's way. Many mechanisms already exist to assist in the control and mitigation of risk. They include doctrine, standard operating procedures (SOPs), drills and technical design standards. A clear process of risk management is required in military planning to ensure that threats are fully considered, appropriate measures taken to minimize their effects and that risk decisions are fully understood. Risk management assists in developing the proper balance between means and ways to achieve the desired end-state.

2. There are broad categories of risk that apply to military planning:

a. **Operational Risk**. Operational risk is concerned with threats that exist due to the specific conditions that exist that may impact the successful conduct of a campaign. Operational risk is associated with friendly operations within a theatre (fire, manoeuvre, sustainment), civilian activities, equipment readiness, force protection and operational security. These threats may also arise from situations such as difficulties achieving interoperability of forces within a coalition or the instability of local governments and institutions;

b. **Tactical Risk**. Tactical risk is concerned with threats that exist because of the presence of either an enemy or a party to a conflict capable of violent acts. It applies to all levels of war and across the spectrum of conflict; and

c. **Accident Risk**. Accident risk comprises all risk considerations other than operational and tactical. It includes the inherent threats associated with military operations within any theatre of operations. These risks include, but are not limited to road traffic accidents, general safety issues, fires, disease or other health issues and environmental conditions.

3. **Mission Failure**. Any plan, operation or task could fail. For instance, at the strategic level an inappropriate assignment of resources could retard the delivery of core projects or critical capabilities. At the operational level, a deployment constrained by lack of strategic lift could result in a poorly timed entry into theatre that puts a task force at an immediate disadvantage. Mission failure is an outcome that must be averted by properly addressing risks throughout the planning process.

4. In recent conflict, military forces have been exposed to a wide variety of hazards including occupational health, medical, climatic and many others. In modern conflict, tactical risk remains a key consideration but operational and accident risk play major roles in successfully deploying forces to diverse environments and adequately supporting them to accomplish their mission. Therefore, consideration of all risk categories is essential to proper planning. These measures equally apply in training.

102. AIM OF RISK MANAGEMENT

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

103. RISK MANAGEMENT - GENERAL

1. Risk management is a process that assists decision makers in determining how to reduce or offset risk and to make informed decisions that weigh risks against mission benefits. It is a methodology that assists in the identification of the optimum course of action (COA) and ensures that the implications of the residual risks are understood. Risk management, a commander's responsibility, must be fully integrated into the planning, preparation, and execution of operations. Risk management consists of risk assessment (threat identification and

assessment) and risk mitigation (develop controls, make decisions, implement controls, and supervise and review). For the purposes of this document, the following definition will be used. A “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. An event occurs when a threat happens. Risk is an expression of a possible loss or negative mission impact stated in terms of probability and severity of an event.

2. Risk management is useful in generating, training, deploying, and employing any task force. Generating a force concerns organizational design, resource allocation, training requirements and sustainment issues. Deploying and employing the joint force highlights force protection concerns and the need to balance risk against resource constraints.

3. Military operations are inherently complex, dynamic, dangerous and involve the acceptance of risk. The level of risk is often related to potential gain, so leaders must be able to weigh the estimated cost properly against the desired ends for each operation. The commander's judgment balances the requirement for mission success with the inherent risks. 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. The Canadian Forces Operational Planning Process (OPP) is a methodology that is already designed to identify and manage risk to a certain degree by examining each situation and enabling the commander to choose a course of action that is most likely to produce mission success. When risk management is integrated into OPP, the process ensures that all risks are adequately examined, measures are put in place to mitigate them to an acceptable level and residual risks are fully understood.

104. RISK MANAGEMENT DEFINITIONS

1. Key risk management definitions are detailed below.

RISK MANAGEMENT TERMS			
Threat	Any real or potential condition that can cause injury, illness or death of personnel or damage to, or loss of, equipment, property or lead to mission degradation	**Controls**	Actions taken to mitigate risks normally by reducing their probability or severity.
Risk	Chance of injury or loss expressed in terms of probability and severity.	**Risk Assessment**	The identification and assessment of threats (first two phases of the risk-management process).
Event	When a threat occurs.	**Residual Risk**	The level of risk remaining after all risk controls have been identified and applied.
Exposure	The frequency and length of time subjected to a threat.		
Probability	The likelihood that an event will occur.	**Risk Decision**	The decision to accept or not accept the risk(s) associated with an action; made by the commander or individual responsible for performing that action.
Severity	The expected consequence of an event in terms of degree of injury, property damage, or other mission-impinging factors (loss of combat power, adverse publicity, etc.) that could occur.		

Table 1-1 Risk Management Terms

CHAPTER 2

FUNDAMENTALS OF RISK MANAGEMENT

201. KEY ASPECTS OF RISK MANAGEMENT

1. Risk management assists the commander by:

a. enhancing operational mission accomplishment;

b. supporting well-informed decision-making to select and implement a COA;

c. providing assessment tools to support operations;

d. enhancing decision-making skills based on a reasoned and repeatable process;

e. providing improved confidence in the task force's capabilities in that adequate risk analysis provides a clearer picture of the task force's readiness;

f. preserving and protecting personnel, combat weapon systems, and related support equipment while avoiding unnecessary risk;

g. providing an adaptive process for continuous feedback through the planning, preparation, and execution phases of military operations; and

h. identifying feasible and effective control measures where specific standards do not exist.

2. Risk management does not:

a. replace sound operational decision-making;

b. inhibit the commander's flexibility, initiative, or accountability;

c. remove risk altogether, or support a zero defect mindset;

d. sanction or justify violating applicable laws; or

e. remove the necessity for rehearsals, tactics, techniques and procedures.

202. PRINCIPLES OF RISK MANAGEMENT

1. The basic principles of risk management process are outlined below.

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 the 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 responsible for executing the mission or task determines that the 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 commander'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.

203. Risk Management and the Planning Environment

1. The risk management process equally applies in both planning environments: crisis action and deliberate. Time is the basic factor that determines the level of effort to be devoted to risk management procedures.

a. **Crisis Action.** In crisis action planning risk management is an “on-the-run” mental or verbal review of the situation using an abbreviated version of the basic risk management process. Decisions are made in a time-compressed situation. This methodology is used during the execution phase of training or operations as well as in planning and execution during time critical responses.

b. **Deliberate.** In deliberate planning the complete process of risk management is applied, as time is not critical. It primarily uses experience and brainstorming to identify threats and develop controls. It is most effective when done in a group. The complete application of the process normally is conducted when planning upcoming operations, reviewing SOPs, maintenance, training, and developing damage control or disaster response plans.

204. RISK MANAGEMENT PROCESS OVERVIEW

1. The risk management process involves the two key activities - risk assessment and risk mitigation.

a. **Risk Assessment**. Risk assessment includes the threat identification and threat assessment phases of the risk management process. In threat identification, individuals identify the threats that may be encountered in executing a mission. In threat assessment, they determine the anticipated 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. **Risk Mitigation.** Risk mitigation includes the development of controls, making risk decisions, implementing controls, and supervising and reviewing the implementation of the controls. These phases of the risk management process are the essential follow-through actions to manage risk effectively. Commanders weigh risk against benefits and take appropriate actions to eliminate unnecessary risk. During planning, preparation and execution, the commander communicates his acceptable risks to subordinates and continuously assesses risks to the overall mission. Finally, leaders and individuals evaluate the effectiveness of controls and capture lessons learned.

205. RISK MANAGEMENT PROCESS APPLICATION GUIDELINES

1. This section provides general guidelines to get the maximum benefit from this process.

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 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 procedures, the time must be allocated to ensure the total cycle can be completed. 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 2-1 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.

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 controls to ensure these controls support the mission.

206. RELATIONSHIP OF FORCE PROTECTION TO RISK MANAGEMENT

1. The commander has the dilemma of weighing mission requirements and force protection measures. A primary tool for reconciling these items is by assessing and balancing risk and thus forming a direct relationship between force protection and risk management. Force protection must be integrated in the planning of all phases of an operation: warning, preparation, deployment, employment and redeployment. As depicted in figure 2-1 below, risk management in each phase compliments the development of force protection measures and alert postures.

a. In the warning and preparation phase, risk assessment and mitigation is carried out to properly generate the force and to train safely;

b. In the deployment and employment phases, updated risk assessments and implemented controls ensure force protection measures are correlated with the threat; and

c. In the redeployment phase, updated assessments and adjusted controls aid the safe re-constitution of the force and the mitigation of health issues.

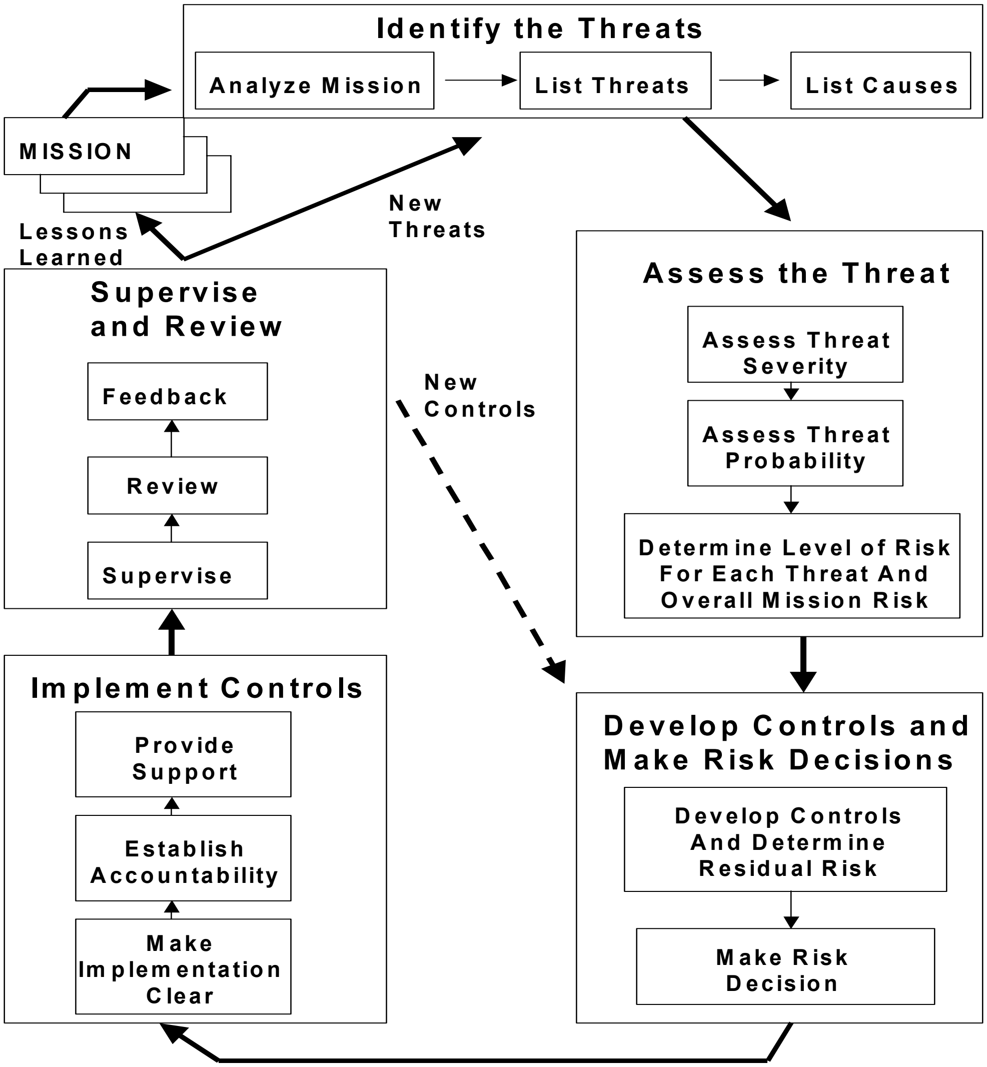

Figure 2-1 Continuous Application of Risk Management

CHAPTER 3

RISK MANAGEMENT – APPLICATION TO OPERATIONS

SECTION I - THE RISK MANAGEMENT PROCESS

301. GENERAL

1. This chapter discusses the risk management process and how it can be applied in the operational planning process (OPP). Though not specifically described here it is equally relevant to training.

302. PHASE I - IDENTIFY THREATS

1. A threat is a source of danger - any opposing force, condition, source or circumstance with the potential to have a negative impact on the accomplishment of the mission or that will 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 multiplying effect on the impact of the total risk management process. The steps outlined below highlight the actions necessary to identify threats associated with any operation or mission.

2. **Step 1 - Analyze Mission**. The mission is analysed 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; and

d. breaking the operation down into "bite-size" chunks.

3. **Step 2 - List Threats**. Threats (and factors that could generate threats) are identified based on the mission and associated vulnerabilities. The output of this step is a summary 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 centres of gravity for any critical vulnerability. Threats may be tracked on paper or in a computer spreadsheet/database system in order to organize ideas and serve as a record of the analysis for future use.

4. **Step 3 - List Causes**. Make a list of the causes associated with each threat identified in Step 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.

303. PHASE II - ASSESS THREATS

1. Each threat is assessed for probability of occurrence and severity. *Probability* is the estimate of the likelihood that a threat will occur (an event) and cause an impact on the mission. Some threats occur 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, for example, something that is not a significant risk but that is extremely simple to control.

2. **Step 4 - 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 Annex A provide guidance for a wide variety of missions and systems.

3. **Step 5 - Assess Threat Probability**. Determine the probability that the threat will occur causing an event of the severity assessed in Step 4. 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 a complicated process with unclear and complex triggers. Supporting rationale for assigning a probability should be documented for future reference. Generally accepted definitions for probability may be found at Annex A.

4. **Step 6 - 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 Annex A. Existing databases and/or a panel of personnel experienced with the mission and threats can also be used to help complete the risk assessment.

5. **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.

6. **Risk Assessment Pitfalls**. The following pitfalls 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 nullifies accurate risk assessment; and

g. Enumeration: It is difficult to assign a numerical value to human behaviour.

(1) Numbers may oversimplify real life situations ;

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

(3) Numbers often take the place of reasoned judgment; and

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

304. PHASE II - DEVELOP CONTROLS AND MAKE RISK DECISIONS

1. **Step 7 - Develop Controls**. After each threat is assessed then one or more controls are developed that either eliminate the threat or reduce the risk associated with it. Controls are used to reduce risk levels in line with the commander's risk guidance. Examples of criteria for establishing effective controls are listed in the table 3-1.

Criteria for Effective Controls	
Control Criteria	**Remarks**
Suitability	Control removes the threat or mitigates (reduces) the residual risk to an acceptable level.
Feasibility	Force/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 are 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.

Table 3-1 Criteria for Effective Controls

a. Some types of controls are:

(1) **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 the development of fire control mechanisms for armoured vehicles, the integration of global positioning system data into command and control suites and the fielding of night vision devices.

(2) **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.

(3) **Educational and Training Controls**. These controls are based on the knowledge and skills of the forces, units and individuals. Effective control is implemented through individual, collective and joint training that ensures performance to standard.

(4) **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.

(5) **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 mitigate the risk of a threat by one or more techniques.

(1) **Avoidance**. Ultimately, risk avoidance may require cancelling the task, mission or operation; however, this option is rarely exercised because of mission importance. Risk can be avoided by choosing a different COA, by training to overcome an inadequacy, inoculating against disease or by using different methods. For instance, it may be possible to avoid the specific risks associated with a night operation by re-scheduling for daytime. Thunderstorm or surface-to-air-missile risks can be avoided by changing the flight route.

(2) **Delay**. 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 favourable weather reduces the risk to the force.

(3) **Transference**. 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.

(4) **Redundancy**. To ensure the success of critical mission's redundant capabilities may be assigned to compensate for potential losses. 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 controls are developed and accepted, the residual risk associated with each threat and the overall residual risk for the mission is determined. Residual risk is the risk remaining after controls have been identified, selected and implemented for the each threat. Typically, controls are applied until the level of residual risk matches the commander's guidance or cannot be further reduced. The residual risk can vary for each threat depending on the final assessed probability and severity. Overall residual mission risk is 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. **Step 8 - Make Risk Decisions**. A key element of the risk decision is determining if the risk is justified. The balance between the risk and the mission's potential gain must be compared. The commander alone decides if controls are sufficient and acceptable and whether to accept the resulting residual risk. If considered too high, the development of additional or alternate controls will be directed, or the COA may be modified, changed or rejected. The risk assessment matrix found in Annex A or some comparable tool, in conjunction with their commanders' guidance, can be used by commanders to communicate how much risk they are willing accept.

305. PHASE IV - IMPLEMENT CONTROLS

1. 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. Careful documentation of each step in the risk management process facilitates risk communication and the rational processes behind risk management decisions.

2. **Step 9 - Make Implementation Clear**. To make the implementation directive clear, consider using examples, providing pictures or charts, etc. Provide a roadmap for implementation, a vision of the end state, and description of successful implementation. The control should be presented so the intended audience will receive it positively. This can best be achieved by designing user ownership into the control.

3. **Step 10 - 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.

4. **Step 11 - Provide Support**. To be successful, the commander must support the risk controls by:

a. providing the personnel and resources necessary to implement the control measures;

b. designing in sustainability from the beginning; and

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

306. PHASE V - SUPERVISE AND REVIEW

1. 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 all or a portion of the operation due to an unanticipated change; and capturing lessons learned, both positive and negative.

2. **Step 12 - Supervise**. Monitor the operation to ensure that:

a. controls are implemented correctly, effectively, 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; and

d. risks and controls are re-evaluated 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.

3. Successful mission performance is achieved by shifting the cost versus benefit balance more in favour of benefit through controlling risks. By using risk management whenever anything changes risks identified before an operation and those that develop during it are consistently controlled. Addressing the risks before they get in the way of mission accomplishment saves resources and enhances mission performance.

4. **Step 13 - 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 the preliminary assessments to the present risk management assessment.

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

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

5. **Step 14 - 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 are analyzed and corrective action taken.

a. When a decision is made to accept risk, factors (i.e. 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 if or where errors in the process may have occurred.

b. Risk analysis will seldom be perfect the first time. When errors occur in an analysis, use feedback (such as briefings, lessons learned, benchmarking or database reports) to identify and correct those errors. This feedback will help determine if the previous forecasts were accurate, contained errors, or were completely incorrect.

SECTION II - APPLICATION TO THE CF OPERATIONAL PLANNING PROCESS

307. INTEGRATION OF RISK MANAGEMENT

1. The risk management process must be considered in each phase of deliberate and crisis action planning as indicated in table 3-2 below. The matrix identifies the key risk management activities that must be performed in the planning step.

Risk Management in CF Operational Planning						
		Identify Threats	**Assess Threats**	**Develop Controls Make Risk Decisions**	**Implement Controls**	**Supervise And Review**
C F O P P	**Stage I Initiation**	**X**				
	Stage II Orientation	**X**	**X**			
	Stage III COA Development	**X**	**X**	**X**		
	Stage IV Plan Development			**X**	**X**	
	Stage V Plan Review					**X**
Rehearsals					**X**	**X**
Employment and Assessment					**X**	**X**

Table 3-2 Risk Management in CF Operations

2. Risk management in operational planning must be balanced against the time available to plan. The goal is to perform the least amount of risk assessment necessary to clearly identify the critical threats and permit courses of action (COAs) to be compared and risk acceptance decisions to be made. Excessive risk assessment may contribute little to the further clarification of the COAs and may impede the tempo of planning. For complete details on the CF OPP see B-GJ-005-500/FP-000, *CF Operational Planning Process*.

308. STAGE I – INITIATION

1. During the initiation stage the commander and his staff perform an assessment of the higher headquarters' order/plan. An initial review of the threats that could be encountered is also conducted. This evaluation examines whether there will be appropriate time to prepare for the mission, conditions of the forces available, availability of strategic lift (if required) and other factors.

2. The commander and staff look at the type of mission to be accomplished and consider possible subsequent missions. Certain kinds of operations are inherently more dangerous than others are. For example, a deliberate frontal attack is more likely to expose a force to losses than would a defence from prepared positions. Identifying missions that routinely present greater risk is imperative. Threats may also be associated with the complexity of the plan (such as a scheme of manoeuvre that is difficult to understand or too complex for accurate communications down to the lowest level) or the impact of operating in a very fluid environment.

309. STAGE II – ORIENTATION

1. When conducting mission analysis the higher headquarters' plan/order may specify a number of threats. When determining assigned, and implied tasks there may be tasks beyond a task force's capabilities - they become "mission" threats. The higher commander may specify the operational, tactical and accident risk he is willing to accept. Intelligence preparation of the battlefield (IPB) should identify many threats including enemy, terrain and weather. The process of IPB is directed by the formation of the commander's priority intelligence requirements (PIRs), which are formulated as questions pertaining to threat actualities (weather and terrain), capabilities (doctrine and order of battle (ORBAT)) and intentions. The following paragraphs outline some of the considerations necessary in the orientation stage.

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:

(1) fully assess the enemy's capabilities including weapons of mass destruction and CBRN;

(2) understand enemy capabilities and friendly vulnerabilities to those capabilities;

(3) assess potential advantages to the enemy provided by the battlespace environment;

(4) asses the effect that the support or lack of support of the local population will have on the enemy;

(5) plan and coordinate active ground and aerial reconnaissance activities;

(6) disseminate intelligence about the enemy to lower echelons; and

(7) identify terrorist threats and capabilities.

b. Intelligence plays a critical part in identifying threats associated with the presence of an enemy or an adversary. Intelligence preparation of the 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:

(1) identifying opportunities and constraints the battlespace environment offers to enemy and friendly forces;

(2) thoroughly portraying enemy capabilities and vulnerabilities; and

(3) collecting information on populations, governments, infrastructures, issues and trends.

3. **Terrain and Weather**. Terrain and weather pose great threats to military operations. The task force must be familiar with both the terrain and its associated environment to enhance the likelihood of mission success. 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 task force capabilities and mission demands.

(1) **Observation and Fields of Fire**. Threats associated with observation and fields of fire usually take place when the enemy will be able to engage a friendly element and when the friendly element's weapon capabilities allow it to engage the enemy effectively. It also includes their observation capabilities: visual and throughout the electro-magnetic spectrum.

(2) **Cover and Concealment**. Threats associated with cover and concealment are created either by failure to use cover and concealment or by the enemy's use of cover and concealment to protect his assets from observation and fire.

(3) **Obstacles**. Threats associated with obstacles may be caused by natural conditions (such as rivers or swamps) or man-made conditions (such as minefields or built up areas).

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

(5) **Avenues of Approach**. Threats associated with avenues of approach include conditions in which an avenue of approach impedes deployment of friendly combat power or conditions that support deployment of enemy combat power.

b. **Weather**. To identify weather threats, its impact on operating systems must be assessed. Threats may arise from:

(1) lack of understanding of reliability and accuracy of weather forecasting;

(2) effects of climate and weather on personnel and equipment operation and maintenance; and

(3) effects of weather on mobility.

4. **Troops and Support Available**. The capabilities of available friendly and or coalition troops must be analyzed. Associated threats impact both individual personnel and the units. Key considerations are level of training, manning levels, national caveats and rules of engagement, the condition and maintenance of equipment, morale, availability of supplies and services and the physical and emotional health of personnel. Even when all tactical considerations point to success, a mission could be compromised by threats due to:

a. **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 have impact on troop support;

b. **Task Organization or Units Participating in an Operation**. Threats include poor communication, unfamiliarity with higher headquarters SOPS, interoperability issues with joint or combined forces, 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; and

c. **Long-term Missions**. Long-term missions include such things as peace support operations, sanction enforcement or any extended mission within a particular theatre of 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.

5. **Time Available**. The threat is that insufficient time is available 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 planning on time can result in shortages of time for subordinate and adjacent units to accomplish their missions.

6. **Civilian Considerations**. 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 non-governmental organizations (NGOs), and the handling of refugees and non-combatants.

7. **Other Elements of National/Alliance Power**. The impact of military actions on the diplomatic, informational, and economic aspects of national power must be considered and assessed and the converse is true. Military operations that do not consider risks they may pose to operations or programs that other governmental departments are undertaking within a theatre of operations may be detrimental to the overall success of an operation or a campaign. Military activities may produce collateral damage to infrastructure that is acceptable from a mission accomplishment perspective but this damage my adversely impact the economic stability or political situation within the region. Conversely, economic sanctions or uneven aid distribution in certain areas may adversely effect military operations or regional security buy increasing local support for insurgent forces.

8. To complete the risk assessment, each staff officer identifies threats in his functional area that are not adequately controlled and that are likely to cause the loss of combat power.

9. In nominating information requirements (IRs) for selection by the commander as his critical information requirements (CCIRs), the staff should consider tactical and accident threats that have been determined to be not adequately controlled. During the process of selecting the course of action, controls will be developed for most of these threats, and they will drop from the IR list.

10. When conducting the mission analysis brief, a list of threats that are not adequately controlled, each with its level of risk, should be presented. A risk management worksheet, see Annex B, could be used to collect these threats into a single list for presentation.

11. The commander's planning guidance will address risk. It includes where and how much risk he will accept concerning tactical and accident risk. It also includes general or specific control measures to reduce the risk of threats. The commander's risk guidance should be included in the warning order.

310. STAGE III – COURSE OF ACTION DEVELOPMENT

1. During COA development the commander and staff continue to identify threats and begin to develop controls options to reduce their risk. Risk should be considered when applying the COA viability requirements of feasibility and acceptability. In terms of feasibility, the task force must have the type, amount, capability and condition of personnel and equipment necessary to minimize the operational, tactical and accidental risk. To be acceptable, the tactical or operational advantage gained must justify the potential cost in resources and casualties.

2. The scheme of manoeuvre will include a statement of where the commander will accept tactical risk. Planners develop control measures to minimize the risk of fratricide. COA statements and sketches will cover any significant tactical or accident risks and where they will occur for the force as a whole. Sketches will include boundaries, obstacle control measures and fire, support coordination measures. Proposed control measures will be discussed during the COA briefing.

3. **COA Validation**. During COA validation additional threats and control measures may be identified.

4. **War Gaming**. War gaming is an analysis method that can be used to identify unforeseen problems and the strengths and weaknesses of each COA. Each COA must be analyzed for feasibility and acceptability in terms of residual risk: the risk remaining once recommended control measures are implemented. The COA's overall level of risk matches that of the highest residual risk once all feasible control measures have been applied.

5. **COA Comparison**. The residual risk findings are distributed to the staff. The staff may modify controls or identify new ones to reduce risk further. Risk is tracked both with the risk management worksheets (Annex B) and with the COA risk score matrix (Annex C). The COAs' level of risk can be compared directly using the risk score matrices if the threats are similar. If not approved weight factors may be used to conduct a comparison. This scoring identifies the differences between COAs regarding residual risk to soldiers, equipment and mission accomplishment. This information is included in the commander's decision brief.

6. **COA Selection**. The commander selects a preferred COA. He then decides what level of residual risk he will accept and approves the control measures. He must obtain the higher commander's approval to accept risk that might imperil that commander's intent or is not consistent with his risk guidance.

311. STAGE IV – PLAN DEVELOPMENT

1. The staff implements the control measures approved by the commander by coordinating them and integrating them into the appropriate planning products. The development of branches and sequels reflects the need to develop measures to respond to risk in the employment phase.

2. This is the culmination of the planning phase, the key time to identify threats and develop controls to reduce their risk. Tactical threats will have been identified but typically not all of them will be clear in the planning stage of an operation. As the employment phase nears and then commences tactical threats will clarify. This means that risk management of tactical threats actually increases as the operation transitions from the planning to the employment phase. As knowledge of the tactical threat increases, relevant controls are implemented to counter them.

312. STAGE V – PLAN REVIEW

1. When a plan is reviewed it must be determined if the risk management process was applied correctly. The CF Lessons Learned Process will evaluate the application of risk management.

CHAPTER 4

STAFF FUNCTIONS AND RESPONSIBILITIES

401. BACKGROUND

1. Commanders and their staff integrate risk management by embedding the risk management process into operations, culture, organization, systems and individual behaviours.

2. Successful risk management is supported by the chain of command. Commanders should not expect every mission to be accomplished without errors and problems - a zero defect mentality. Commanders need to support subordinates' decisions to accept risks that are within their understanding of the commander's intent and guidance. Demanding rigid standards, such as zero defects, leads to over-supervision and paralysis. This produces timid leaders who are afraid to make tough decisions in crisis and who are unwilling to take the necessary risks for success in military operations. A zero defects mindset creates conditions that will stifle initiative at all levels. On a high tempo battlefield or operation this could lead to failure and higher casualties.

3. Commanders must understand that things may go wrong in an operation, even with the certain knowledge that they and their subordinates have anticipated the threats and have done all within their power to prevent unnecessary incidents. When incidents occur, leaders step forward and accept the responsibility along with their subordinates.

402. RESPONSIBILITIES

1. With the assistance of their subordinates and staffs, commanders manage risks. As summarized in Table 4-1, minimizing risk is the responsibility of everyone in the chain of command - from the highest commander, to subordinate commanders, to each individual service member. Managing risk is critical for all operations, whether for training or operations - commanders must issue clear risk guidance. However, **risk management does not justify taking actions that are unethical, immoral or illegal**.

2. 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 both:

a. identified during planning, preparation, and execution of operations; and

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.

3. Sometimes commanders are not properly advised in situations where the assumption of risk may imperil their units, adjacent units or other governmental organization operations in the area or affect the intent of their higher commander. This is most often attributed to:

a. risk denial syndrome - commanders 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;

c. subordinates failure to fully understand the higher commander's guidance;

d. failure to adequately understand a complex battlespace; and/or

e. 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.

4. **The Commander's Responsibilities**

a. 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 behaviour. 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 favourable for risk management integration by:

(1) demonstrating consistent and sustained risk management behaviour through leading by example - habitually doing risk management and actively participating throughout the risk management process;

(2) providing clear guidance where to accept risk or what risks to accept;

(3) obtaining and providing to subordinates the necessary assets to control risk;

(4) knowing their own limitations, their leaders' and service members' limitations, and their unit's capabilities;

(5) preventing a zero-defects mindset from creeping into their command's culture;

(6) allowing subordinates to make mistakes and learn from them;

(7) demonstrating full confidence in subordinates' mastery of their trade and their ability to execute a chosen COA;

(8) keeping subordinates informed and consulting with subordinate leaders before making a decision, if feasible;

(9) listening to subordinates;

(10) establishing clear, feasible risk management policies and goals;

(11) conducting detailed planning within time constraints; assessing each mission and task in terms of its risk; continuously re-assessing risk as the mission and conditions change and experience is gained;

(12) making informed risk decisions; establishing and clearly communicating risk guidance;

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

(14) examining how subordinates manage risk and how service members protect themselves;

(15) supervising and evaluating the unit's execution of risk controls during the mission;

(16) advising the chain of command on risks and risk-reduction measures and providing subordinates with feedback on their performance and ways to improve;

(17) assessing the effectiveness of their unit's risk management program; and

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

b. 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.

c. 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.

d. 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.

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

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

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

(a) If, during mission execution, the subordinate determines the risk is too great, the development of additional or alternate controls is directed, or the COA is modified or changed; then the next higher commander is notified of this action. Note that requiring subordinates to report to the higher commander whenever a risk decision point is reached during mission execution can result in paralysis and should be kept to a minimum.

(b) The objective of managing risk is not to remove all risk, but is 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, a commander will take measures to mitigate it. If the risk cannot be mitigated to an acceptable level, a commander will 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.

5. The Staff’s Responsibilities

a. The Chief of Staff (COS) will normally 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). The COS coordinates development of risk controls with emphasis on de-conflicting controls that affect multiple functional areas and adjacent units. The staff officer helps the commander eliminate unnecessary risks by:

(1) analyzing his functional area and applying risk management during the operational planning process;

(2) identifying both constraints and restraints in the higher commander's risk guidance;

(3) including threats and their risks in the mission analysis briefing;

(4) including a risk assessment for the commander's planning guidance;

(5) considering the risk assessment while developing COAs;

(6) including risks and recommending ways to reduce their impact in the staff planning;

(7) implementing risk controls by coordinating and integrating them into the appropriate paragraphs and graphics of the operation order (OP O) and into products such as SOPs and operation plans (campaign plans, OPLANs, CONPLAN);

(8) establishing clear and practical procedures and standards;

(9) determining the effectiveness of risk controls and continuously assessing their suitability, feasibility, supportability, clarity, and acceptability;

(10) supervising, evaluating, and assessing the integration of risk management during an operation;

(11) continuously identifying threats, assessing initial and residual risks for each threat, and recommending control measures to reduce the risk; and

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

b. Staffs focus on threats and their risks across the spectrum of protecting the force. These staffs

(1) identify friendly vulnerabilities during current operations and implement controls to mitigate risk; and

(2) implement commander's intent on acceptance of risk in current operations.

c. The following list identifies some of the risk management responsibilities of the primary joint staff directorates:

(1) J-1 (Personnel):

(a) estimates time delay risks on personnel deployment flow;

(b) with J2 input, determines casualty risks for each COA;

(c) estimates casualty and replacement flow risks on future operations;

(d) ensures controls for personnel-related activities are conducted to diminish operations security vulnerabilities and support military deception initiatives; and

(e) estimates risks of employed local civilian labour in coordination with the J-4 (logistics), J-2 (intelligence) and the legal officer;

(2) J-2 (Intelligence):

(a) monitors and report threats that counter the effectiveness of friendly combat identification/counter-fratricide measures;

(b) develops current regional threat assessments;

(c) develops terrain and climate assessment; and

(d) determines risk of loss of low-density intelligence collection assets;

(3) J-3 (Operations):

(a) develops risk assessment for the commander's estimate;

(b) performs as staff proponent for combat identification/counter-fratricide measures;

(c) develops policy, procedures and assign responsibility for combat identification/counter-fratricide measures;

(d) reports and investigate reports of fratricides;

(e) develops risk assessment of military and political aspects of draft ROE and supplemental ROE;

(e) develops risk assessment of combined or joint interoperability aspects of the operation; and

(g) determines criticality and vulnerability of bases in the Joint Rear Area to prioritize controls and levels of response;

(4) J-4 (Logistics):

(a) assesses the risk of critical supply levels not meeting required number of days of supply;

(b) determines petroleum, oils, and lubricants storage site vulnerabilities and controls; and

(c) determines munitions storage site vulnerabilities and safety requirements;

(5) J-5 (Plans):

(a) integrates functional directorate risk management controls and combat identification/counter-fratricide measures into deliberate planning products; and

(b) identifies friendly manoeuvre and firepower vulnerabilities during mission analysis, war gaming and plan controls to mitigate risk;

(6) J-6 (Communications): is responsible for assessing risk to geospatial information and services systems and developing controls to counter threats;

(7) J-9 (CIMIC) is responsible for assessing the risk to and from local civilian governments and agencies, NGOs, the local population, and the local infrastructure and advising on the development of controls, policies or programs to mitigate the risk;

(8) J-3/5 (IO/PA). The lack, or inadequate application, of the information operations and public affairs functions in CF Ops could lead to adverse perceptions, on the part of national or international audiences thereby affect the Commander’s ability to attain a planned end-state. The J-3/5 (PA) staff will assess, develop and implement controls for risk associated with:

(a) the provision and dissemination of information (OPSEC vs public’s right to know);

(b) inaccurate messaging of public policy;

(c) possible conflicts between information operations (in particular psychological operations) and public messaging;

(d) differing internal and external messaging for public affairs and information operations; and

(e) effects of differing national, international and local public opinion over the mission;

(9) Special staff offices: Risk management should be addressed by various special staff offices including:

(a) J4 HSS for health and non-battle injury, return to duty policy, preventative medicine;

(b) J5 Legal for Canadian and international law, law of armed conflict, and host nation (HN) law;

(c) J8 Fin to ensure commanders are aware of the financial implications of decisions by providing timely and accurate analysis and advice on incremental costs, funding sources and requisite approval authorities associated with each COA;

(d) Special advisors from other national government department (DFAIT, CIDA); and

(e) The Safety officer

RISK MANAGEMENT RESPONSIBILITIES	
Commander	Provide Risk Guidance
	Select Control Options
	Make Risk Decision for COA
	Enforce and Evaluate Controls
Chief of Staff	Supervise Risk Management and Integration Across Entire Staff
	Ensure Threats and Controls are Integrated into Plans and Orders
	Ensure Staff Monitors Controls During Execution
Staff Officers (Functional Areas)	Identify Threats Most Likely to Result in the Loss of Combat Power
	Develop Control Options that Address Causes of Threats
	Integrate Threats and Selected Controls into Functional Area Paragraphs, Graphics, and Annexes of OP O and plans and Then Monitor Implementation During Execution

Table 4-1 Risk Management Responsibilities

6. **The Individual’s Responsibilities**

a. An individual's level of expertise and maturity influences their risk management proficiency. Managing risk can be subjective where it is based on an individual’s 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:

(1) overestimating their ability to respond to, or recover from, a hazardous incident - they become overconfident; and/or

(2) underestimating the level of risk posed by a threat.

b. It is imperative that individuals understand and execute controls directed by leaders and staffs. Individuals should be aware of and fully understand the situation and maintain self-discipline when they perform their duties. They should:

(1) understand and apply risk management;

(2) execute controls directed by their leaders (i.e. perform to standards);

(3) carry risk management over into all activities both on and off duty; and

(5) look out for others.

c. Every individual has the authority to halt something that is inherently unsafe.

403. INTEGRATION INTO TRAINING AND OPERATIONS

1. Integrating risk management into training and operations delivers three key benefits. It:

a. contributes to mission success;

b. preserves life and well-being of everyone involved (military members, civilian partners and local populations); and

c. conserves equipment, facilities, environmental resources and combat power.

2. Risk management is planned up front, not treated as an afterthought. Leaders and managers of materiel acquisition, base operations, and industrial operations must 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.

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

a. the complexity of mission development and associated changing interrelationships with other national and local government agencies;

b. the inclusion of civilian contractors, such as logistics civilian augmentation programs, as part of the force; and

c. the presence of the media, NGOs, and local populations. These diverse elements need to be considered in the risk management process.

4. A key consideration relevant to managing risk in complex operational environments is to understand 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.

5. 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. 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 training goals to ensure that they are supported by realistic risk management.

404. REVIEW OF THE RISK MANAGEMENT PROCESS

1. 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:

a. whether effective risk management is embedded into planning and preparing for operations;

b. how well subordinate leaders and service members understand risk management; and

c. whether effective risk management is being used in the execution phase of operations. Leaders assess the effectiveness of their units by reviewing how well threats are identified and risk controls are developed and implemented:

(1) in oral and written OP O, plans and SOPs;

(2) in communications to the lowest level of the chain of command;

(3) in short-, near- and long-term training plans;

(4) into all activities, on and off duty;

(5) in force protection programs; and

(6) in AARs and captured in lessons learned.

2. 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 reduction of risk and hazardous incidents.

This Page Intentionally Blank

ANNEX A - RISK ASSESSMENT TOOLS

1. **Risk Assessment Matrix.** The Risk Assessment Matrix combines severity and probability estimates to form a guide to 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

Table A-1 Risk Assessment Matrix

2. **Risk Definitions**

a. **E - Extremely High Risk**: If these threats occur during the mission, it will most likely fail with severe consequences to personnel and equipment or operational objective(s). The ability to accomplish the mission will be lost.

b. **H – High Risk**: If these threats occur during the mission a significant degradation of capability in terms of achieving the required operational objective(s), the inability to accomplish all parts of the mission, or the inability to complete the mission to standard will occur.

c. **M – Moderate Risk**: If these threats occur during mission the expected degradation of mission capability in terms of achieving the required operational objective(s), accomplishing all parts of the mission, or completing the mission to standard will occur. An unlikely probability of catastrophic loss exists.

d. **L – Low Risk:** Expected losses or effects have little or no impact on accomplishing the mission.

3. **Severity Categories.** The following table outlines severity categories:

Risk Severity Categories	
Category	**Definition**
CATASTROPHIC (I)	Loss of ability to accomplish the mission or mission failure. Death or permanent disability. Loss of political support or coalition effectiveness. 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. Damage to political support or coalition effectiveness. 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 impact on political support of coalition effectiveness. 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. No adverse affect on political support or

Risk Severity Categories	
Category	**Definition**
	coalition effectiveness. First aid or minor medical treatment. Slight equipment or system damage, but fully functional and serviceable. Little or no property or environmental damage.

4. **Probability Categories**. The following table outlines probability categories for the risk assessment matrix:

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 B - RISK MANAGEMENT WORKSHEET

1. Mission/Task:		COA #			2. DTG	
3. Date Prepared:			4. Prepared By: ______________________________ Rank/ Last Name / Position			
5.Threat	6. Initial Level of Risk	7. Controls	8. Residual Level of Risk	9. How to Implement	10. How to Supervise	11. Controls Effective ?
ENEMY						
TERRAIN						
TROOPS						
EQUIPMENT						
TIME						
CIVILIAN CONCERNS						
NATIONAL POWER/ALLIANCE CONCERNS						
12. Overall Risk Level After Controls are Implemented (Circle One) LOW MODERATE HIGH EXTREMELY HIGH			13. Risk Decision Authority ______________________________ Rank / Last Name / Position			

Note: modify to reflect risk factors for the operation being evaluated.

This Page Intentionally Blank

ANNEX C - RISK SCORE MATRIX

COA # ___________________

Preliminary Risk Score Matrix						
COA #		**Probability**				
Severity		**Frequent** **A**	**Likely** **B**	**Occasional** **C**	**Seldom** **D**	**Unlikely** **E**
Catastrophic	**I**					
Critical	**II**					
Marginal	**III**					
Negligible	**IV**					

Residual Risk Score Matrix						
COA #		**Probability**				
Severity		**Frequent** **A**	**Likely** **B**	**Occasional** **C**	**Seldom** **D**	**Unlikely** **E**
Catastrophic	**I**					
Critical	**II**					
Marginal	**III**					
Negligible	**IV**					

Working from the Risk Management Worksheet for the COA concerned the number of threats at each particular risk level is tabulated. This forms the preliminary risk score matrix. Once controls are applied the residual risk score is tabulated. COAs can be compared directly by their residual risk score matrix depending on the similarity of the threats.

EXAMPLE

Preliminary Risk Score Matrix						
COA # 2		**Probability**				
Severity		**Frequent** **A**	**Likely** **B**	**Occasional** **C**	**Seldom** **D**	**Unlikely** **E**
Catastrophic	**I**	**1**	**2**	**3**		
Critical	**II**	**1**		**2**		
Marginal	**III**	**3**	**4**	**1**		
Negligible	**IV**	**4**				

Residual Risk Score Matrix						
COA # 2		**Probability**				
Severity		**Frequent** **A**	**Likely** **B**	**Occasional** **C**	**Seldom** **D**	**Unlikely** **E**
Catastrophic	**I**					
Critical	**II**	**1**	**1**			
Marginal	**III**	**2**	**1**	**3**		
Negligible	**IV**	**4**	**2**	**4**		

In the preliminary risk score matrix the scoring indicates that there are “3” threats in quadrant IIIA, “2” rated in IB and so on. Controls are imposed to eliminate the priority risks: those most likely to occur and with the most severe consequences. Once the controls are imposed the risk is re-evaluated to determine its new level. The goal is to have residual risk at the minimum level possible.

GLOSSARY

Acceptable Risk

The level of risk that decision-makers have perceived as sustainable, and are willing to bear, in pursuit of their goals.

Cause

Something that produces an effect, result or consequence. The person, event or condition responsible for an action or result.

Sample Threats and Causes

NOTE: A threat at one echelon may be a cause at another echelon.

Threats	Causes
Operating Equipment	Operator error- Mechanical failure
Weather	Dark clothing- Limited visibility
Enemy Forces	Enemy Actions
Friendly Forces	Unclear control measures
Live Fire	Cook off – live weapons training
Terrain	Vehicle Rollover
Change	New hazards & reduced effectiveness of controls

A cause is more specific than a threat. A method of clarifying if something is a threat or a cause is to ask the question, “Is this specific enough to help identify a corrective control?” If the answer is ‘no’ it is a threat, if the answer is ‘yes’ it is a cause. It is important to identify threats and causes properly because there may be several causes associated with one threat. If the more specific causes are not identified, necessary controls may be omitted resulting in the threat not being eliminated or its risk inadequately mitigated.

Controls

Actions taken to mitigate risks, normally by reducing their probability or severity.

Event

A risk that occurs.

Real Risk

The actual risk resulting from a threat whether a commander or his staff have properly identified it or not.

Residual Risk

The portion of risk that remains after safeguards (or controls) have been selected and implemented.

Risk

Chance of injury or loss expressed in terms of probability and severity.

Risk Assessment

The process of identifying and assessing threats. Phase 1 and 2 of the risk management process constitute risk assessment.

Risk Communication

Any two-way communication between stakeholders about the existence, nature, form, severity and acceptability of risk.

Risk Management

Risk management is a decision- making tool used by people at all levels to increase operational effectiveness by anticipating threats and reducing the potential for loss, thereby increasing the probability of a successful mission.

Risk Mitigation

Once risks have been identified, the steps taken to reduce and control risks and ensure that the controls are effective, phases 3 to 5 of the risk management process.

Risk Perception

The significance assigned to risk by stakeholders. This perception is derived from the stakeholder’s expressed needs, issues and concerns.

Severity

Expected consequence of an event in terms of degree of injury, illness, property damage or other mission-impairing factor.

Stakeholder

Individuals, groups or organizations that have an interest or share in an undertaking or relationship and its outcome - they may be affected by it, impact or influence it, and in some way be accountable for it.

Threat

A condition with the potential to cause illness, injury, death, property damage or mission degradation.

LIST OF ABBREVIATIONS

The following abbreviations are used in this publication.

AAR	After Action Report
C2	Command and Control
CAP	Crisis Action Planning
CBRN	Chemical, Biological, Radiological and Nuclear
CCIR	Commander’s Critical Information Requirement
CF	Canadian Forces
CIDA	Canadian International Development Agency
CIMIC	Civilian-military cooperation
COA	Course of Action
COP	Contingency Operations Plan
COS	Chief of Staff
DND	Department of National Defence
DFAIT	Department Foreign Affairs and International Trade
FPWG	Force Protection Working Group
HNS	Host Nation Support
Impl O	Implementation order
IO	Information Operations
IPB	Intelligence Preparation of the Battlefield
IR	Information Requirement
LOAC	Law of armed conflict
NGO	Non-Governmental Organization
Op O	Operations order
OPLAN	Operations Plan
OPSEC	Operations Security
OPP	Operational Planning Process
ORBAT	Order of Battle
PA	Public Affairs
PIR	Priority Intelligence Requirements
SJS	Strategic Joint Staff
SOP	Standard Operating Procedure
TF	Task Force
TFC	Task Force Commander
TFHQ	Task Force Headquarters
Wng O	Warning Order

This Page Intentionally Blank

REFERENCES

OFFICIAL PUBLICATION/DOCUMENTS

Government of Canada

Treasury Board, Integrated Risk Management Framework

Dept of National Defence, VCDS, DSPC, Integrated Strategic Risk Management in Defence.

B-GJ-005-500/FP-000, *CF Operational Planning Process*

United States

Air Land Sea Application Center, Risk Management, February 2001

Marine Corp. Operational Risk Management.

US Coast Guard, Risk-based Decision-making Guidelines, Vol 1-4.

US Army

> Center for Army Lesson Learned, No. 95-9, Risk Management for Brigades and Battalions, June 1995.
>
> Center for Army Lesson Learned, No. 99-5, Risk Management for Brigades and Battalions: Task Force XXI, Update, April 1999.
>
> Operation Support Hope: Risk Management Leader's Guide.
>
> FM 100-14, Risk Management, 23 April 1998

Australia

Australian Army, Training Information Bulletin Number 83: Risk Management, 1998.

OTHER DOCUMENTS

Beckvonpeccoz, LCdr S.W., Operational Risk Management: Increasing Mission Effectiveness Through Improved Planning and Execution of Joint Operations, Naval War College Paper, 27 Feb 1997.

Canadian Standards Association, CSA-Q850-97, Risk Management Guidelines for Decision Makers.

Latrash, LCdr F., Risk Management: An Integral Part of Operational Planning, Naval War College Paper, 5 Feb 1999.

Vertzberger, Yaacov, Risk Taking and Decisionmaking: Foreign Military Intervention Decisions, Stanford: Stanford UP, 1998.

Wininger, LCol Wally, Risk and National Defense Strategy, USAWC Strategic Research Project, 14 Feb 2001.

This Page Intentionally Blank