Australian Government
Department of Defence
Defence Science and
Technology Organisation

Australian Defence Risk Management Framework: A Comparative Study

Svetoslav Gaidow and Seng Boey

Land Operations Division
Systems Sciences Laboratory

DSTO-GD-0427

ABSTRACT

In early 2002, the Secretary of Defence and the Chief of Defence Force endorsed a top-down, organisation-wide and systematic approach to risk management in Defence. As a result, the Australian Defence Risk Management Framework (DRMF) was established. This study is a quest for the credibility of DRMF. It provides a review of the DRMF and a comparative analysis in light of other national and international, defence and non-defence risk management publications and practices. Through this study the appropriateness of the approach and the acceptability of the DRMF are confirmed. The application of risk management in force and capability options development and analysis is identified as an area of future research.

Published by

DSTO Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR 013-345

Submitted: June 2004
Published: February 2005

Australian Defence Risk Management Framework: A Comparative Study

Executive Summary

In early 2002, the Secretary of Defence and the Chief of Defence Force endorsed a top-down, organisation-wide, systematic approach to risk management in Defence. As a result, the Australian Defence Risk Management Framework (DRMF) was established. The introduction of DRMF was preceded by a number of events at Commonwealth, corporate, public sector and departmental level. They included the public release of important risk management related publications and documents, and presentations given to professional audiences. DRMF built upon that information, and on the tradition in Defence of adopting risk management as an inherent part of the everyday way to do things. It also integrated the extant places and practices of recognised effective risk management.

The aim of this study is to reconfirm the approach adopted in the Australian Defence Organisation (ADO) and the appropriateness of granting DRMF the mandate to be implemented. This report provides a review of DRMF and a comparison with other national and international defence and non-defence risk management standards, policies and guidelines and 'best practices' from the countries of the American British Canadian and Australian Armies' Standardisation Program. The comparison is based on criteria, including compliance with an established risk management standard, ability to support the decision-making process, consistency in construction and terminology, and relative ease of application. This study establishes the credibility of the DRMF and its acceptability for use.

DRMF consists of a policy, an implementation plan, guidelines, and a support mechanism with corresponding funding, training and information system. There is an established specialised unit – Enterprise Risk Management to act as the focal point for any risk management activity throughout the ADO. Moreover, Enterprise Risk Management has to coordinate and support particularly the management effort associated with the enterprise, organisation-wide risks. Also DRMF is being incorporated and integrated within the existing departmental management framework. DRMF provides for and obligates all Defence personnel to implement risk management in any activity, thus creating the conditions for an entirely new risk management culture within the ADO. Furthermore, this recent approach is directed more to making better use of opportunities rather than to minimising losses or avoiding risk altogether, which has been the objective of the traditional approach.

DRMF creates the right environment for comprehensive and systematic application of risk management. Despite its diverse composition, the various elements share the same standard, terminology and procedures, and it is easy to use. DRMF reflects the rich experience accumulated in the area of risk management from this country and overseas. It provides the conditions for an improved decision-making process related to any activity and at any level in Defence.

This publication covers the pre-history of DRMF and the major events in the introduction of the framework up to June 2003. This includes in particular the relatively moderate contribution by DSTO to risk management in Defence. The study does not cover any developments after that, for example the publication of the Kinnaird review and the implementation of its recommendations, which may be the target of another investigation.

This investigation has been inspired by the introduction in early 2002 of the DRMF and the involvement of the authors in the S&T support for the Land Warfare Development Centre (LWDC) of the Australian Army. There is a significant potential for the application of risk management in the development of the Objective Force, currently undertaken by the Force Development Group in LWDC. Risk management can contribute as part of the Capability Options Development and Analysis System and directly as analytical support for decision-making. It can be used in capability options development to capture strengths and weaknesses in capabilities. Risk management can determine gaps in current capabilities by identifying areas of risk and uncertainty, and anticipate future capability requirements by seeking potential vulnerabilities and high pay off areas. Also, risk management may be applied to capability options analysis to evaluate capabilities. It can be used in the comparative analysis between options. Risk can be involved as an optimisation criterion for options, and as an assessment of current capability options.

Contents

List of Figures

List of Tables

Glossary

ABCA	America, Britain, Canada and Australia
ADO	Australian Defence Organisation
ALARP	as low as reasonably practicable
ANAO	Australian National Audit Office
APS	Australian Public Service
ARM	Army Risk Management
AS	Australian Standard
ATC	air traffic control
AVRM	aviation risk management
CA	Chief of Army
CDF	Chief of the Defence Force
CEI	Chief Executive's Instruction
CF	Canadian Forces
COA	course of action
CODAS	Capability Options Development and Analysis System
CRM	continuous risk management
CSIG	Corporate Services Infrastructure Group
CSLCM	Capability Systems Life Cycle Management
DAC	Defence Audit Committee
DC	Defence Committee
DERM	Defence Enterprise Risk Management
DGSP	Director General Strategic Planning
DI	Defence Instruction
DMASP	Directorate Materiel Acquisition and Support Program
DMO	Defence Materiel Organisation
DND	Department of National Defence
DoD	Department of Defence (USA)
DP&M	Defence Planning and Management
DPE	Defence Personnel Executive
DPPM	Defence Procurement Policy Manual
DRMF	(Australian) Defence Risk Management Framework
DRMIP	Defence Risk Management Implementation Plan
DRMP	Defence Risk Management Policy
DSA	Defence Security Agency
DSMA	Defence Safety Management Agency
DSMC	Defence Systems Management College
DSTO	Defence Science and Technology Organisation
ETA	event tree analysis
FMA	Financial Management and Accountability
FMEA	failure modes and effects analysis
FTA	fault tree analysis
HAZOP	hazard and operability study
HRA	human reliability assessment
HRM	human resource management
IEC	International Electrotechnical Commission
ISD	Information Systems Division
JTF	Joint Task Force
KPI	key performance indicator

LLAMP	Low Level Airspace Management Proposal
LWDC	Land Warfare Development Centre
METT-T	mission, enemy, terrain and weather, troops and support available, time (model)
MLO	Military Low Operations
MOD	Ministry of Defence
NAVSAFE	Navy Safety Management
NSW	New South Wales
NZ	New Zealand
OH&S	occupational health and safety
OME	ordnance, munitions and explosives
PHA	preliminary hazard analysis
PMO	project management office
QA	Quality Assurance
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy
RFP	Request for Proposal
RM:MSTTP	Risk Management: Multiservice Tactics, Techniques and Procedures
SAFETYMAN	Defence Safety Manual
SEC	Secretary
SWOT	strengths, weaknesses, opportunities and threats
TIB	Training Information Bulletin
UK	United Kingdom
US	United States (of America)
VCDS	Vice Chief of the Defence Staff

1. Introduction

This report covers the pre-history of the Australian Defence Risk Management Framework (DRMF) and the major events associated with its introduction up to June 2003. It does not cover any developments after that, which may be the target of another investigation.

1.1 Aim and Scope

The aim of this study is two-fold. First, to provide a review of the DRMF and its elements, and analytically compare it with other established national and international defence and non-defence risk management standards, policies and practices. Second, to apply the initial results to confirm the appropriateness of the recently adopted approach by Defence and the acceptability of the corresponding framework. This study is a quest for the credibility of the DRMF.

The review in this investigation is based on written materials, available in hard printed form or in electronic form on the Internet. Only a selected list of publications has been used due to the large number of options. Every effort has been made to include the most important contributions to the area of defence risk management.

1.2 Preview

This study begins with an overview of events leading to the introduction of the DRMF, followed by a review of some publications of Standards Australia on risk management and its applications. First the basic concepts and requirements are introduced. Then a detailed description follows of the risk management process with all its steps and additional activities. Specific features of risk management in the public sector, in outsourcing, and of technological systems are considered.

Chapter 4 deals with the risk management in the Australian Defence Organisation (ADO) before and after the introduction of the new approach. First comes the DRMF with its history and complete description of its elements. Second, examples of effective risk management implementations in Defence outside the Framework are presented.

Chapter 5 compares the Australian approach with the policies and practices in the defence organisations of the ABCA countries. A review of some major publications of the US DoD, the UK MOD, the Canadian DND, and of New Zealand is carried out. An analysis of the differences, terminological and/or conceptual is undertaken.

Chapter 6 discusses the DSTO contribution to risk management in Defence. All recent and current tasks in risk management are listed and some publications in the broader area of risk management are reviewed. DSTO is not identified as an active participant in the establishment of the Framework.

The Conclusion confirms the appropriateness of the approach and the Framework, and outlines some topics for future research.

2. Background

The introduction of the DRMF was preceded by a number of events at Commonwealth, corporate, public sector and departmental level. They include the public release of important publications and documents, and presentations given to professional audiences. Standards Australia published the second improved version of AS/NZS 4360:1999 *Risk Management* [49]. An evaluation of risk management in Defence was conducted during 1999 and 2000, resulting in an Inspector-General report [12]. Next, in 2000, the Commonwealth Government of Australia made public the White Paper: *Defence 2000 Our Future Defence Force* [8], while July 2001 saw the release of the *Defence Plan* [15]. Later, in November 2001, the Auditor-General for Australia, Pat Barrett, delivered his presentation [4] on recent developments in risk management in Canberra. And in October 2002, Ian McPhee – the Deputy Auditor-General talked about risk management and governance [41] at the National Institute for Governance.

The DRMF uses AS/NZS 4360:1999. This Standard provides generic guidance on the introduction and ongoing implementation of a risk management process, which enables organisations to identify and take opportunities, and avoid or mitigate losses. It may be applied to different activities or operations of any corporate, community or public sector organisation including the Department of Defence. AS/NZS 4360:1999 prescribes the development of a policy and support mechanism as the foundations of a framework. Moreover, it is the obligation of the executive to define, document, disseminate, apply, review and maintain the policy. Risk management can be applied at any level in any organisation, strategic or operational, tactical or project. There is no totally risk-free environment and all decisions involve risk management of some kind or another. Its effective application is especially essential in dealing with strategies, major policies or projects involving large amounts of resources.

The June 2000 published *Risk Management in Defence* [12] report by the Inspector-General targets the then current status of risk management in the ADO. The formal evaluation includes interviews with senior level stakeholders in Defence and is based on a comparative analysis of the approaches to risk management of external organisations. It focuses on "strategic, at and above Group" level risks as required by the Defence Executive. Risk management 'best practice' examples are considered. As a result the following key findings are established:

- "A comprehensive, structured, strategic risk management policy, framework and culture should be implemented using a top-down and incremental approach."
- "The AS/NZS 4360 and related Guidelines provide a very effective basis for a successful risk management framework."
- "A Portfolio risk management policy should be developed, agreed by the Defence Executive and promulgated by CDF and the Secretary."

- "A dedicated team should be established, … , to develop and implement these at the Portfolio level and to act as a focal point for risk management activity throughout the Portfolio."
- "The Corporate Plan should include a strategic risk assessment and all Group-level business plans should include a risk management plan to ensure some coherence and linkage among the various levels."
- "A risk management culture needs to be established by top level commitment, developing formal documentation and involving all staff in training, education or awareness of risk management."
- "A plethora of studies and reports provide adequate guidance on what arrangements should be in place to ensure effective and practical risk management practices, as well as how they might be put in place."
- "Different Groups had different perceptions of organisational risk drivers, and these reflected an inward focus. Current customer-provider arrangements, funding, pace of change, and uncertainty in Government direction were issues of concern across the Organisation."
- "Current management information systems are inadequate as a risk management/ business decision support tool."

The report also acknowledges the existence of extensive written documentation on risk management and, at the same time, the lack of any legislative requirement or Government initiative to implement a formal risk management approach across departments and agencies. Thus, one may conclude that, if implemented, the recommendations of the report would establish the Department of Defence as an example of a place with an effective organisation-wide risk management framework.

The Government's Defence White Paper [8] focuses on the fundamentals of the Australian strategic policy and the development of capabilities for the Defence of Australia over the next ten years, and naturally it does not focus on risk management. Moreover, its release significantly has preceded the adoption by Defence of a systematic, comprehensive, organisation-wide, top-down approach to risk management and the establishment of a support system. But the White Paper exhibits applications of elements of risk management in the process of decision making about Defence. The environment of uncertainty in which defence decisions must be made may serve as the context for strategic risk management. Risk identification may be used to determine military or non-military threats to this country. The White Paper applies risk analysis to emphasise the importance of both taking into account the likelihood of a particular threat and the impact of that threat, i.e. how serious it would be if it materialised. Risk assessment may provide the basis for evaluating the potential for major conflicts in our immediate neighbourhood, in Southeast Asia, or in the Asia Pacific region. Risk treatment may not eliminate strategic risks altogether and risk reduction has to follow "the most cost-effective ways". The White Paper states, that "even if the risk of an attack on Australia is low, the consequences would be so serious that it must be addressed". Therefore, one may conclude that risk management has played an important role in shaping this fundamental document for Defence and it is implicitly present in many of its key points.

The Defence Plan [15] continues the effort to establish a whole-of-Defence picture or a strategy map to guide the implementation of the Defence White Paper. Here, for the first time, at this high level, the introduction of a systemic approach to risk management and mitigation is formulated as task to be fulfilled by Defence in 2001-2002. It belongs to Strategic Theme 3, Promoting quality advice and decision making, from the six Defence Strategic Themes considered by the Defence Committee as strategy-focussing elements.

In his November 2001 presentation [4] entitled 'Some Recent Professional Initiatives and Issues in Risk Management', the Auditor-General for Australia acknowledges "the focus on risk management as part of sound corporate governance in recent years", but still there is a lot to be done. Risk management can help organisations be more entrepreneurial and proactive in addressing risk as an opportunity to improve their performance. However, there is significant pressure especially on the public service to be more risk averse in the present uncertain environment. The Presentation covers the CPA Australia Project, the Comcover Benchmarking Project and some Standards Australia projects.

- *Enterprise-Wide Risk Management – Best Practice Guide for the Public Sector* is the result of the CPA Australia Risk Management Project. The Guide provides guidance to organisations actively engaged in incorporating and integrating risk management within their existing management frameworks and processes. The integration of risk management into corporate and resource planning is a key challenge. Risk management may contribute positively as a decision support tool and in the identification and treatment of areas of concern. It may play an essential part in the effective management of stakeholders' objectives and expectations. Risk management has to be broadened to organisation-wide, operational and strategic level rather than be kept only at compliance level. The Guide recommends visible commitment and involvement by Chief Executive Officers and senior management, and the development of "dedicated risk management functions" and coordinators responsible for facilitating, promoting and supporting the implementation of risk management.
- The *Comcover Benchmarking Risk Management Program* has initially included only fund members, but later it has been extended to all Australian Government organisations: Commonwealth, State and Local. The Department of Defence has participated as well. The Program collects data related to ten Key Performance Indicators (KPI) using a questionnaire. It provides information on the results of the organisations' efforts to implement risk management. The KPIs are: integrated risk management approach; committed and led; positive and pro-active focus; process-driven; planned for continuous improvement; audited and documented; active communication; resourced; trained and educated; and value-based decisions. Every organisation receives a rating for each KPI and also an overall rating reflecting whether implementation has not yet started, or there is some progress but more is needed, or an established process is identified.
- The Presentation of the Auditor-General acknowledges some contributions of *Standards Australia* to the effort of implementing risk management. It mentions a number of projects involving several working parties. For example, one of them is to

outline the relationship between risk management, corporate governance and achieving better outcomes by organisations. The idea is to promote making better use of opportunities instead of simply avoiding risk.

The Presentation discusses the implementation of the 2000-2001 Commonwealth Risk Management Roll Out Plan. According to it, all Commonwealth Departments and Agencies would have a formal risk management plan prepared by March 2001, which would be followed by a Whole of Government Report by May 2001. The Report identifies some considerable achievements in several areas, that "a real start has been made", and recommends that the attention be concentrated on establishing an integrated strategic management approach, appropriate structures and adequate resources. The Presentation concludes with pinpointing the challenge of changing the organisation's culture to ensure risk management is applied to every activity at every level, thus having impact on the corporate goals and objectives.

The importance of risk management as a "component of disciplined management" in the public sector is further emphasised by the Deputy Auditor-General in his October 2002 paper 'Risk Management and Governance' [41]. It recognises the recent ideas of using risk management as a "vehicle for identifying positive business opportunities", rather than as a defensive strategy. Risk identification and treatment have to be contemplated well ahead of the traditional corporate and business-planning processes. There is also an upside to using risk management, i.e. improving organisational effectiveness and efficiency, and limiting the potential for shocks and adverse surprises. Moreover, the paper advocates the Enterprise Risk Management approach as improving the linkage of risk and opportunity, and giving a competitive edge to business risk management. This enterprise approach is supposed to align strategy, people, technology, knowledge and processes when an organisation assesses and treats uncertainties and hazards. A new framework is also needed to guide its implementation, especially in the public sector where there are strict requirements for accountability, probity and ethics.

The aforementioned documents and presentations identify the necessity for change in the Defence risk management approach and practices. They and the accumulated in-house experience have become the solid basis the Department of Defence needed to introduce a systematic and comprehensive risk management framework. Moreover, there has to be a radical change in the Defence risk culture. AS/NZS 4360:1999 and other Standards Australia publications provide the methodology and serve as a benchmark. A policy, a plan, guidelines and a support system have to form the risk management framework, which has to be incorporated and integrated within the departmental management framework. The Chief Executive Officers, meaning the Secretary and the Chief of Defence Force, have to endorse the change. The new approach has to consider Defence-wide risks as a first priority enterprise. The framework has to take into account the existing best practices in risk management, especially from the ABCA countries. The following sections describe an investigation to determine how the above idea has been materialised.

3. Standards Australia on Risk Management

According to a "Memorandum of Understanding between Standards Australia and the Commonwealth Government" since 1988, Standards Australia has been recognised as the top non-government, independent standards body in Australia. It represents Australia at the International Organisation for Standardisation and the International Electrotechnical Commission (IEC). One of its major activities is the development of technical and business standards. Whenever possible Standards Australia adopts overseas standards. It does not develop a new Australian standard if there is an acceptable international one.

3.1 Publications of Standards Australia

Standards Australia is a world leader in the area of risk management standardisation. The following are some of the most recent publications:

- AS/NZS 3931:1998 *Risk Analysis of Technological Systems – Application Guide*, Standards Australia, Homebush, NSW [48].
- AS/NZS 4360:1999 *Risk Management*, Standards Association of Australia, Strathfield, NSW [49].
- HB 141:1999 *Risk Financing Guidelines,* Standards Association of Australia, Strathfield, NSW.
- HB 142:1999 *A Basic Introduction to Managing Risk Using the Australian and New Zealand Risk Management Standard AS/NZS 4360:1999*, Standards Association of Australia, Strathfield, NSW [50].
- HB 143:1999 *Guidelines for Managing Risk in the Australian and New Zealand Public Sector*, Standards Association of Australia, Strathfield, NSW [51].
- HB 231:2000 *Information Risk Security Management Guidelines,* Standards Australia International, Sydney, NSW.
- HB 240:2000 *Guidelines for Managing Risk in Outsourcing Using the AS/NZS 4360 Process,* Standards Australia International, Sydney, NSW [52].
- HB 250:2000 *Organisational Experiences in Implementing Risk Management Practices,* Standards Australia International, Sydney, NSW [53].
- HB 228:2001 *Guidelines for Managing Risk in the Healthcare Sector,* Standards Australia International, Sydney, NSW.

The above publications cover the foundations of the risk management process and its applications in some specific industries. Appendix A of AS/NZS 4360:1999 provides a long list of other areas of application, including asset management, resource planning, disaster management, fraud detection and prevention, transport, and public relations. The publications may be used to establish a solid framework for risk management in the lifecycle of any activity or project, function or system, in any public, private or community organisation, including the Australian Defence Organisation (ADO).

3.2 Basic Requirements and Concepts

According to AS/NZS 4360:1999 risk management means "the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects". It helps organisations suffer fewer losses and improve their prospects. Risk management broadens horizons without causing exposure to unnecessary risks. Moreover, it enables the identification of opportunities as well as the reduction of losses.

Risk management stands for an approach directed at establishing the context, and identifying, assessing and treating risks while conducting continuous communication and review. The steps in the risk management process follow in a strict sequence, thus forming the basis for rigorous decision-making. As stated in HB 142:1999 [50], not applying risk management is equivalent to decision-making not based on solid facts and reasoning, including a careful consideration of all risks involved, i.e. to "risky management".

The process of risk management is an iterative one. With each 'repetition' of the cycle there may be changes in the risk criteria and hence a progressive improvement of the risk management process may be achieved. This may result in increasing the benefits from the application of the risk management approach. In general, the outcomes from the implementation of risk management may include more effective decisions, more effective allocation and use of resources, higher standard of customer service, more flexibility in meeting objectives, etc.

Risk management has to be an integral part of any management practice. It can be applied at any organisational level from strategic through operational, functional and tactical to project. Starting with the strategic aspect guarantees that the lower level aspects are accurately placed within the strategic context. The most benefit is obtained by employing risk management right from the beginning of an activity. But it may be applied to help the decision-making in specific situations or specific risk areas. Risk management may exhibit its relevance in times of major changes for an organisation as well as in everyday routine operations.

Risk management has to be an integral part of quality management. It has to be incorporated in the existing organisational structure at all levels. This will enable managers and staff to identify a wider range of options and strive for better outcomes. Risk management will facilitate greater responsibility and flexibility in the decision-making process. A structured risk management framework may also stimulate continuous improvement and innovative thinking.

Risk management has to be an essential part of corporate governance, i.e. direction, executive action, supervision and accountability. The tools and techniques of risk management give any manager at any level a systematic approach to managing risks within their corporate responsibilities. Risk management may also provide some protection in the case of adverse results. Corporate governance activities may be improved

by establishing links between risks, returns and resources, for example by applying risk management in the efficient allocation of resources.

To establish a risk management framework an organisation needs a policy, a support mechanism and an implementation program.

- A risk management policy declares the commitment and the objectives of the organisation regarding risk management. It is developed by the senior executives and is aligned with the organisation's goals, operational environment, nature of activities, and interests of stakeholders. It has to be endorsed for implementation at all levels of the organisation.
- Adequate resources and trained personnel have to be provided for the risk management activities, such as performance measurement, internal audit and review, data collection and knowledge dissemination.
- A risk management system has to be established and maintained, and its performance reported and reviewed. The status, responsibilities, authority and interrelationships of the risk management personnel have to be clearly defined and documented.
- An implementation program has to identify the steps to be undertaken in order to introduce a risk management framework within an organisation.

Appendix B of AS/NZS 4360:1999 provides generic guidelines for the development and implementation of a risk management program as a sequence of steps.

1. Step 1 considers the support of senior management. Risk awareness has to be developed and a broad view of risk management adopted at the highest echelons of the organisation. The Chief Executive Officer is to provide continuous support and another senior executive is to lead the effort.
2. Step 2 discusses the development of an organisational policy. It has to include the rationale for risk management and the policy objectives. It has to ensure the alignment of the organisation's strategic/corporate goals and the risk management goals. The policy has to clearly determine corporate and individual responsibilities, scope of application, review procedures, etc. It is endorsed by the organisation's executive(s) and implemented throughout the organisation.
3. Step 3 describes how the policy is to be communicated. Some of the means to ensure that risk management becomes an integral part of the general culture of the organisation are: raising risk awareness, organisation-wide dialogues/discussions, formal training and recognition of risk qualification levels, and assigning management responsibilities for the risk communication.
4. Step 4 considers risk management at organisational level. Managing risk has to be integrated within the planning and management processes at the organisational level. A risk management system has to be introduced and maintained as it is given in the implementation plan.
5. Step 5 discusses risk management at program, project and team level. The framework of organisational level has to be adjusted to these levels. Additional requirements, planning and management activities have to be taken into account.

6. Step 6 deals with monitoring and reviewing. Mechanisms for continuous monitoring and reviewing have to be developed and put in place. The implementation of the risk management policy is in this way guaranteed.

The jargon of risk management uses a number of terms on a regular basis, which are also part of any vocabulary. In order to avoid any potential ambiguity regarding the meaning of these terms a small number of definitions from Section 1.3 of AS/NZS 4360:1999 are quoted here. The wording and numbering is presented exactly as they appear in the standard. For the full list of definitions refer to the source.

Definition 1.3.1 Consequence
The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Definition 1.3.3 Event
An incident or situation, which occurs in a particular place during a particular interval of time.

Definition 1.3.7 Frequency
A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time.

Definition 1.3.8 Hazard
A source of potential harm or a situation with a potential to cause loss.

Definition 1.3.9 Likelihood
Used as a qualitative description of probability or frequency.

Definition 1.3.12 Organisation
A company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

Definition 1.3.13 Probability
The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.

Definition 1.3.15 Risk
The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

3.3 Risk Management Process

The AS/NZS 4360:1999 *Risk Management* provides generic guidance throughout all steps of the risk management process: establishing the context, risk identification, risk analysis, risk evaluation, and risk treatment, including monitoring and reviewing, communication and consultation, and documentation. Its detailed flow-chart is shown in Figure 1. This report follows very closely AS/NZS 4360:1999 in its brief description of the risk management process.

3.3.1 Establishing the Context

The risk management process takes place in the framework of organisation's strategic, organisational and risk management contexts.

- Establishing the strategic context means identifying the environment in which the organisation operates, its strengths, weaknesses, opportunities and threats. The financial, political, social, cultural, legal, public relations and physical aspects of the everyday business are very important to the organisation, its staff and its clients. This also includes the external and internal stakeholders, their objectives and risk perceptions. Risk management has to be aligned with the mission and strategic objectives of the organisation.
- Establishing the organisational context is based on the understanding of the organisation, its structure, its values, its policies, and its goals and strategies to achieve them. It also means making sure managers understand their role in the decision-making process with respect to risk acceptance criteria and risk treatment options.
- Establishing the risk management context means considering the scope and depth of the risk investigation. This determines whether the risk management process will be concerned with organisation-wide issues or will be limited to particular unit(s) or project(s) and their interactions. It is also recommended to consider the existence or non-existence of a current risk treatment process. The necessary steps (including studies, tools, resources) in the risk management process are to be identified within a balanced system of costs, benefits and opportunities.

This phase involves the development of criteria against which risk is to be evaluated. The criteria usually depend on the interests of the stakeholders and the objectives of the organisation. They may also reflect legal requirements. The nature of the criteria may be operational, technical, financial, social, environmental, legal, humanitarian, etc. Here the acceptable level for each risk has to be considered.

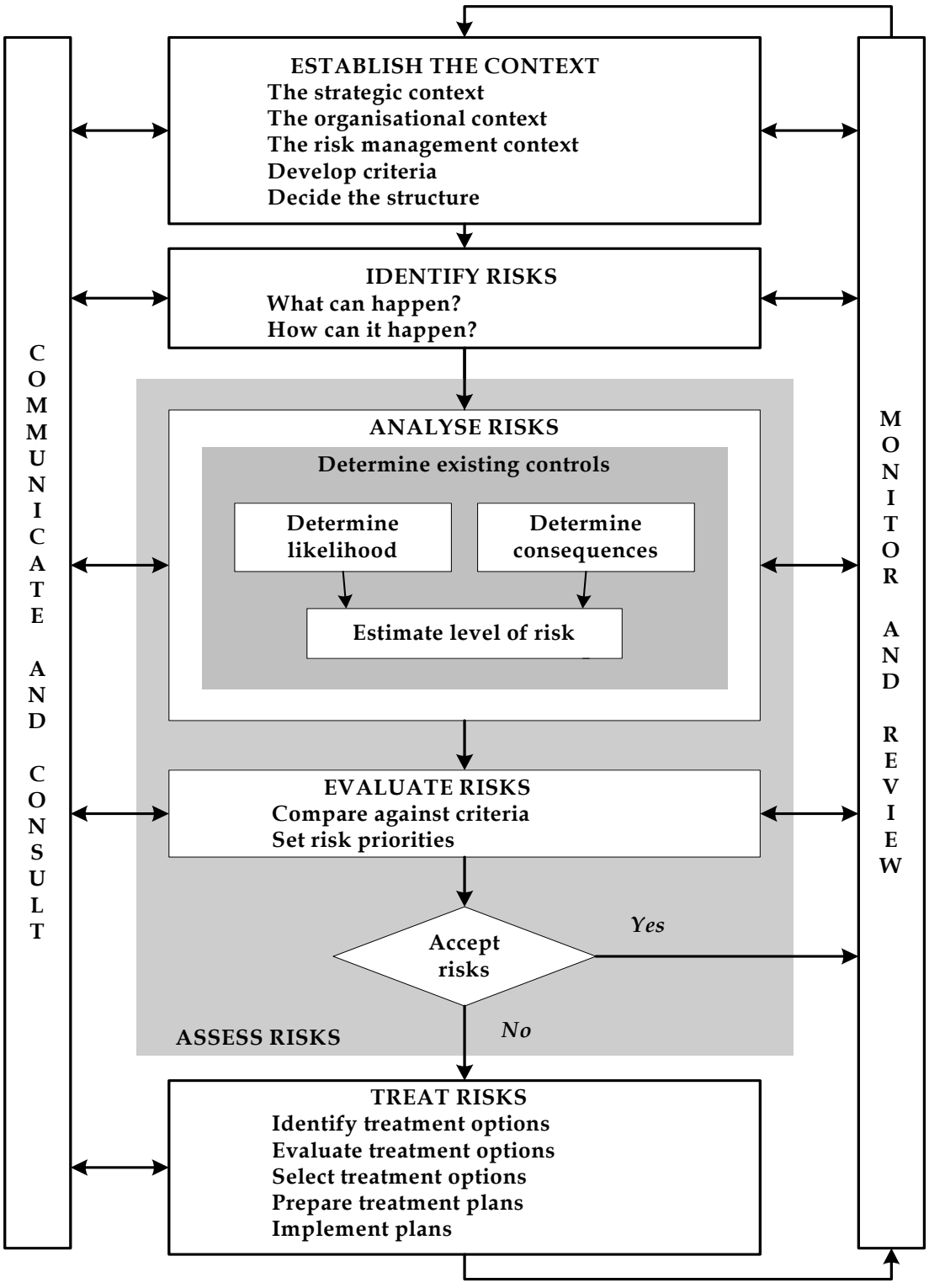

Figure 1: Risk Management Process (Adopted from AS/NZS 4360:1999 Risk Management)

At this stage the risk management structure is to be determined. The activity or project has to be subdivided into its components, thus providing a logical framework for comprehensive risk identification and assessment.

3.3.2 Risk Identification

At this step of the risk management process one has to apply a well-structured and systematic approach and try to identify all risks, which may potentially arise. Failure to do so may pose a major negative impact to one's activities. Moreover, any risk left unidentified is naturally not even included in the risk management plan. Risks beyond one's control are to be identified as well. HB 142:1999 [50] provides a long list of possible methods of identifying risks, for example interviews, audits, surveys, group discussions, brainstorming, scenario analysis, systems analysis, etc.

Risk identification is supposed to give answers to the following questions:

What can happen? How and why can it happen?

The "What can happen?" question aims at generating a comprehensive list of the sources of risk and the areas of risk impact. Such a list may be a long one, thus the necessity of a generic list. Appendix D2 from AS/NZS 4360:1999 provides a generic list of risk sources including commercial and legal relationships, economic circumstances, human behaviour, natural events, political circumstances, technological and technical issues, etc. Appendix D3 contains a generic list of possible areas of risk impact, for example asset and resource base, revenue and entitlements, personnel, costs, performance, community, schedule of activities, etc. The "How and why can it happen?" question aims at considering possible causes and scenarios provided in the list of sources of risk and the areas of impact.

3.3.3 Risk Analysis

At this step one considers the risk consequences (impact or magnitude of effect) and likelihood (measured by frequency or probability) of risk occurrence to combine them into the level of risk. The risk level is discussed within the context of existing or non-existing controls. Here the very low acceptable risks are separated from the major risks and excluded from further assessment.

Risk analysis is to avoid bias and hence is to be based on the best available sources of information and data management techniques. As examples of information sources AS/NZS 4360:1999 lists past records, published literature, market research, relevant individual and industry practice and experience, various models, and expert judgements. The techniques may include interviews, questionnaires, expert group discussions, computer modelling, statistical analysis, and decision-making tools.

There are three types of methods applicable in risk analysis (in order of complexity): qualitative, semi-quantitative, and quantitative. Usually one starts with the qualitative

analysis to get a rough approximation of the level of risk and then proceeds with a more accurate quantitative analysis.

- Qualitative analysis determines consequences and likelihood in verbal form based on descriptive scales. It is applied to determine level of risk where time and money do not justify a more detailed analysis. Its appropriateness is quite evident in risk situations with stakeholders of various backgrounds, interests and mathematical/statistical competency. Qualitative analysis is a more efficient tool when numerical data are inadequate for quantitative analysis. Appendix E of AS/NZS 4360:1999 gives examples of descriptive scales for likelihood and consequences and the resulting risk level matrix. They are reproduced in Table 1, Table 2, and Table 3. HB 142:1999 [50] provides further variations on the topic indicating how the tables can be tailored to suit one's needs. Unfortunately, they all lack some consistency in the scale descriptors and later some ambiguity in the risk level matrix emerges. There is, for example, a moderate likelihood, also a moderate consequence and even a moderate level of risk.

- Semi-quantitative analysis replaces the qualitative descriptive scales with number ranges. Here numbers do not correspond accurately to the level of likelihood and consequences. What counts is the consistency in the prioritisation approach. This type of analysis is supposed to go one degree of detail further but without achieving an entirely realistic assessment of risk levels. Numbers are used for comparison only and any calculations are meaningless.

- Quantitative analysis is applied when the likelihood and the consequences can be quantified. The quality of the numerical data and the sophistication of the methods used determine the accuracy of the analysis. Consequences are worded in terms of monetary, technical, or human criteria, while likelihood is presented as frequency or probability. Further they are combined to form the level of risk and the result depends essentially on the type of risk and the context. Appendix F of AS/NZS 4360:1999 provides examples of quantitative risk expressions, i.e. fatality risk, health risk, risk of financial loss or gain, etc.

In semi-quantitative and quantitative analysis likelihood is sometimes described as the combination of probability and frequency of exposure. Frequency of exposure measures the strength of association with the source of risk while the probability measures the chance of experiencing the consequences given the source of risk exists. One has to be careful if there is a strong relationship between frequency of exposure and probability.

Table 1: Qualitative Measures of Consequence or Impact (Adopted from AS/NZS 4360:1999 Risk Management and HB 142:1999 A Basic Introduction to Managing Risk)

Level	Descriptor	Detailed Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, on-site release immediately contained, medium financial loss
3	Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capacity, off-site release with no detrimental effects, high financial loss
5	Catastrophic	Death, toxic release off-site with detrimental effect, huge financial loss

or in the case of recognising and exploiting opportunities:

Level	Descriptor	Detailed description
1	Insignificant	Small benefit, low financial gain
2	Minor	Minor improvement to image, some financial gain
3	Moderate	Some enhancement to reputation, high financial gain
4	Major	Enhanced reputation, major financial gain
5	Catastrophic	Significantly enhanced reputation, huge financial gain

Table 2: Qualitative Measures of Likelihood (Adopted from AS/NZS 4360:1999, HB 142:1999 and HB 143:1999 Guidelines for Managing Risk)

Level	Descriptor	Detailed Description
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

Table 3: Qualitative Risk Analysis Matrix – Level of Risk (Adopted from AS/NZS 4360:1999 and HB 143:1999)

Likelihood	Consequences				
	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	High	High	Extreme	Extreme	Extreme
B (likely)	Medium	High	High	Extreme	Extreme
C (moderate)	Low	Medium	High	Extreme	Extreme
D (unlikely)	Low	Low	Medium	High	Extreme
E (rare)	Low	Low	Medium	High	High

3.3.4 Risk Evaluation

At this step of the risk management process the level of risk is compared with the pre-established risk criteria. Risk evaluation results in a ranked list of risks. Then, these risks are classified as acceptable or unacceptable. Acceptable risks are to be monitored and their acceptable status reviewed periodically. Unacceptable risks have to be prioritised by management for treatment. The risk evaluation has to consider the big picture including the stakeholders' objectives and risk tolerability, the degree of control over each risk, the cost, the benefits and potential opportunities.

The level of risk, produced at the risk analysis step, and the risk criteria, usually established at the context step, are to be considered on the same basis. For example, qualitative levels of risk are to be compared with qualitative criteria, and alternatively, quantitative levels with quantitative criteria.

An acceptable risk, which is not going to be treated, is not necessarily an insignificant risk. HB 142:1999 [50] lists reasons for accepting risks including unavailability of appropriate treatment within given resources, or unavailability of treatment altogether, or prohibitive insurance costs. Sometimes, advantages may far outweigh disadvantages making risk more justifiable.

The unacceptable risks are prioritised for action by management later on. They are to be included in the risk treatment plans of the organisation. Management is also to respond by allocating responsibilities in the risk treatment process with respect to the level of risk.

HB 142:1999 *A Basic Introduction to Managing Risk* provides a diagram introducing the "as low as reasonably practicable" (ALARP) principle. The original AS/NZS 4360:1999 does not even mention this descriptive risk evaluation tool. Here, the diagram is reproduced in Figure 2. The width of the V represents the level of risk. The area between the two levels, where costs and benefits are traded off in the risk evaluation process, indicates the ALARP region. Risks below the ALARP region are of negligible level, while risks above the ALARP region are intolerable.

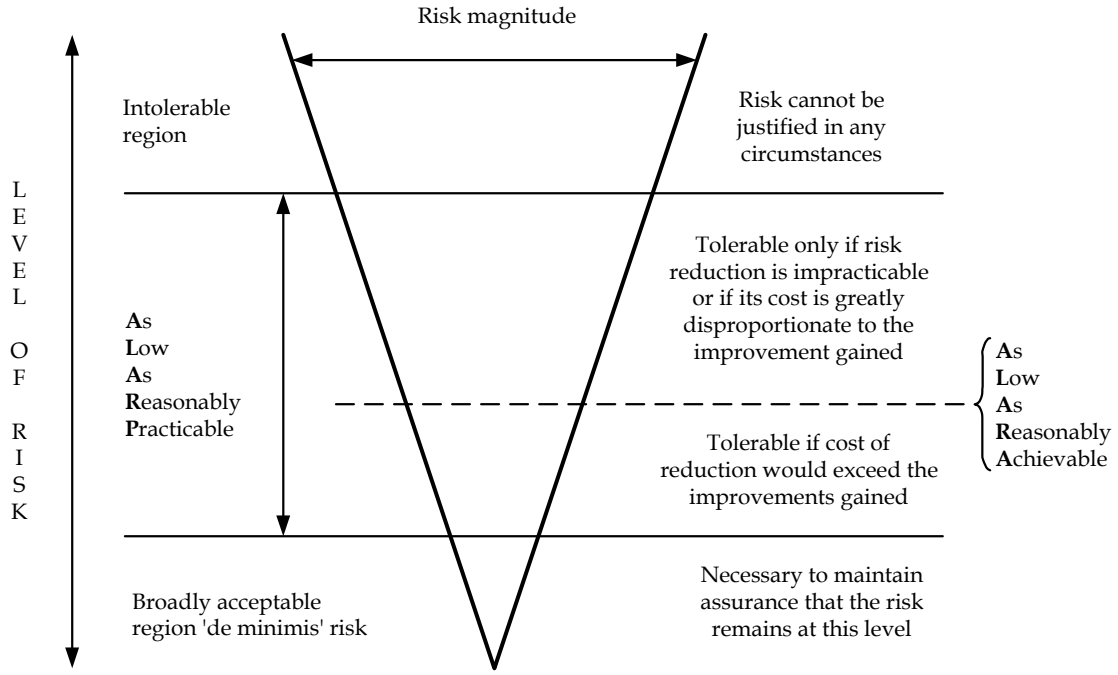

Figure 2: ALARP Principle (Adopted from HB 240:2000 Guidelines for Managing Risk in Outsourcing Using the AS/NZS 4360 Process)

3.3.5 Risk Treatment

This step of the risk management process starts with the accepting, monitoring and reviewing of risks of the lowest priority. For all other not acceptable risks one has to identify treatment options, assess these treatment options, prepare treatment plans, and implement them. A detailed flow-chart of the risk treatment process is shown in Figure 3. All activities have to meet the organisation's goals and objectives and be carried out within established funding limits. Moreover, the risk treatment resources should have been determined and established at the context step of the risk management process.

For the unacceptable and already prioritised risks various *treatment options have to be identified* and considered, including:

- Avoid risk by not proceeding with the risk-containing activity. If risk avoidance is inappropriately adopted due to a risk aversion attitude, it may cause an increase of the levels of other risks. Risk aversion may lead to bad decision making, delays in the risk treatment process, and ultimately failure to treat risk. Actually, risk avoidance means refusing to accept risk. Choosing a less risky alternative component within the activity, or choosing a different but more acceptable activity is not necessarily avoiding risk, it is rather a risk treatment aiming at reduction of likelihood or consequences.

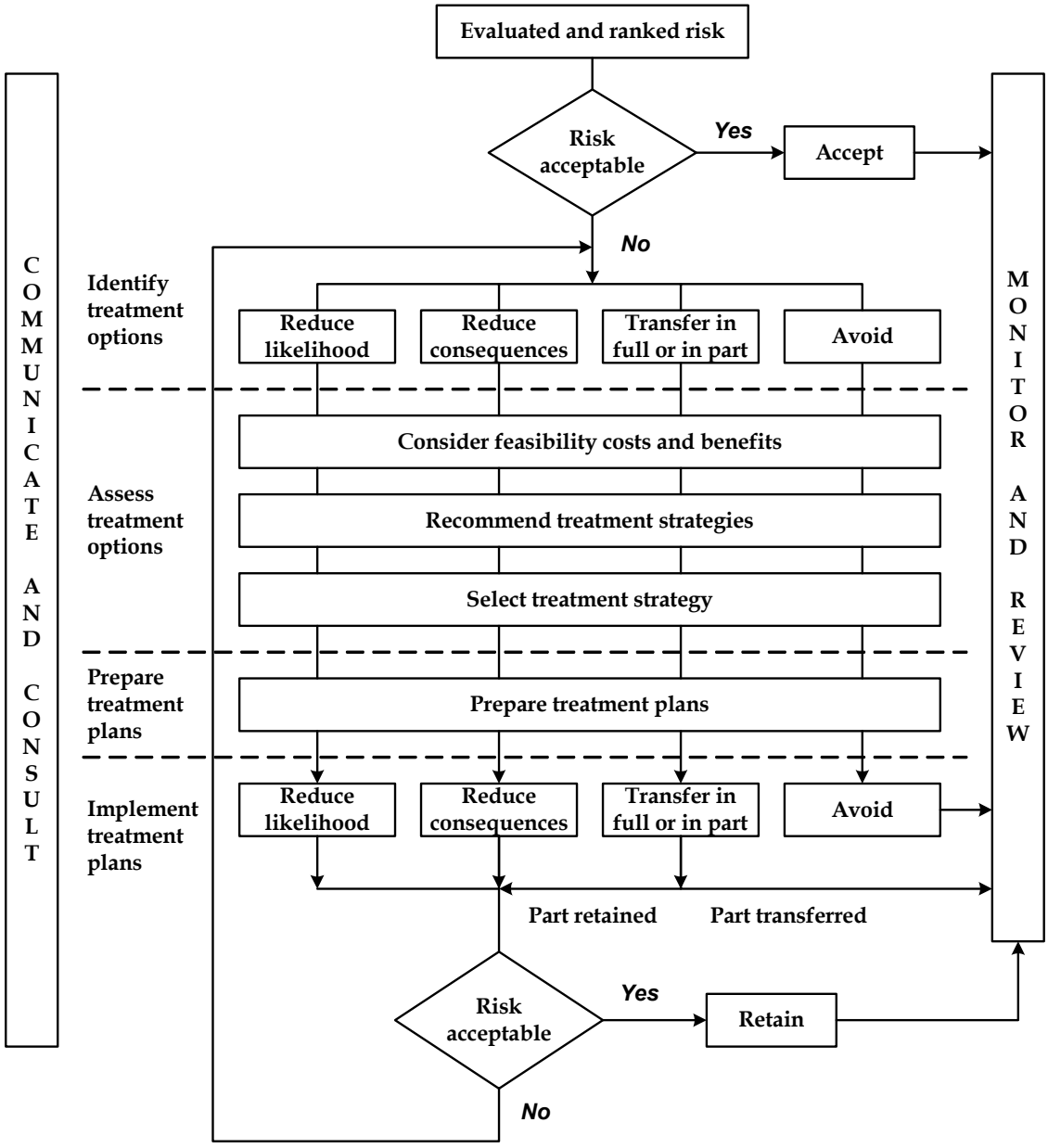

Figure 3: Risk Treatment Process (Adopted from AS/NZS 4360:1999 Risk Management)

- Reduce the likelihood of the occurrence or the consequences of risk, or both. Appendix G of AS/NZS 4360:1999 provides a list of actions to reduce the likelihood of risk occurrence and a list of procedures to reduce the consequences. As stated in the HB 142:1999 [50], there is a trade off between risk level and the cost of risk reduction to an acceptable level. A priori formulated risk criteria have to form the basis of this optimisation procedure while the specific circumstances and the established risk context will determine the most suitable criterion. Together, they will yield the solution to the risk reduction problem.

- Transfer risk in full or in part, means involving another organisation in bearing the risk as a whole or in sharing some part of the risk. In this way the original organisation will reduce the risk for itself but it may not cancel it altogether. The overall risk level to society may not decrease and the recipient organisation may not manage its new risk appropriately.
- Retain the risk, usually residual, after the completion of risk reduction or risk transfer procedures. Risk may be retained by default when it is not treated by the organisation.

Reduction of the likelihood of occurrence and reduction of the consequences are sometimes called risk control. As AS/NZS 4360:1999 states, risk control involves policies, standards, procedures, physical changes and their implementation to achieve the elimination or minimisation of adverse risks. Therefore, risk control is more than reduction of likelihood and consequences. For example, it also includes the analysis of new controls in view of the effectiveness of the existing ones.

To assess treatment options is to consider their feasibility, benefits and cost, to recommend treatment strategies, and to select a treatment strategy. Assessing risk treatment options is a process which has to be conducted with respect to the extent of risk level reduction, of the number of newly created opportunities, of the size of the additional benefits and with respect to the risk evaluation criteria including budget constraints. Usually a single risk treatment option cannot be the solution for a specific problem. A number of options have to be considered and applied together in combination. For example, reduction of risk likelihood, reduction of risk consequences, risk transfer, and risk retention, if applied simultaneously may provide a better solution.

When assessing risk treatment options one has to base the decision making on the balance between an option's cost implementation and benefits obtained from it. As a rule the cost has to be lower or at most commensurate with the benefits. Exceptions of this rule cover risks of rare likelihood with catastrophic (severe) consequences. Such risks have to be treated despite the potential or even real danger of being identified as unjustified in a financial context. Further on, if a high-level risk undertaking could be associated with a considerable number of new opportunities emerging from it, then the assessment would have to include risk treatment cost and the risk consequences rectification cost. These two costs have to be weighed against the impact of the aforementioned opportunities. In general, the ALARP principle has to form the basis of one's approach to dealing with the adverse risks.

Assessing risk treatment options may include implementation prioritising due to limited financial resources. Sometimes the cumulative cost of the options exceeds the budgeted one. Thus various Operations Research and other techniques have to be applied to strictly determine the priority order under which the risk treatment options will enter the treatment plan.

Prepared treatment plans show how the selected treatment strategies have to be implemented. They have to clearly delegate responsibilities, provide time schedules,

describe the expected treatment effects, secure adequate resourcing, determine performance measures, and establish a rigorous review process. Plans have to include performance criteria against which the implementation of the risk treatment options is to be tested. Treatment plans usually contain critical milestones needed in the implementation monitoring.

Implementing treatment plans requires the existence of a management system capable of identifying the techniques to be used, assigning the responsibilities and accountabilities to individual level, and monitoring the process against specified criteria.

3.3.6 Monitor and Review

Monitor and review is not just a step, but an ongoing process embedded in the risk management process. It deals with the performance of the risk management system and the potential changes affecting it according to the AS/NZS 4360:1999.

Risks change with time and circumstances. Hence the need to monitor them and their environments, the implementation of risk treatment plans, the system set up to control the risks and the established contexts and risk priorities.

Review is a continuous process and an integral part of the risk management plan. It makes sure the plan stays relevant and up-to-date. It introduces all changes in the risk management process. The inevitable regular repetition of the risk management cycle is based on the review process.

3.3.7 Communicate and Consult

Communicate and consult is also an integral part of the risk management process. It is ongoing and lasts as long as the whole risk management process.

Communication and consultation is an important process and involves a two-way information flow between all stakeholders. It is recommended to have a communication plan linking external and internal stakeholders from the very beginning and related to each step of the risk management process. Consultation has to be given priority rather than simply passing information from decision makers to the other participants in the process. Effective communication is vital in ensuring risk managers and all stakeholders understand the basis for decisions made and actions undertaken.

Risk perception among stakeholders differs due to differences in interests, needs, assumptions, concepts and backgrounds. Decisions regarding risk acceptability are usually made on the basis of risk perception. Stakeholders have a significant role in the decision-making process. Therefore, it is important to have all these perceptions, and everything flowing from them, identified and documented. The reasons for the differences have to be investigated and understood.

3.3.8 Documentation

Documentation has to be generated at each step of the risk management process. It will contain results, plans, reviews, assumptions, methods, data, etc. AS/NZS 4360:1999 prescribes appropriate documentation as required for the proper management of risk. Generally, documentation provides evidence of a systematic approach applied to the risk management process, helps the flow of communication, provides the basis for accountability and auditing, facilitates any monitor and/or review process, establishes a solid background for decision-making, helps develop archives and databases, etc. Appendix H in AS/NZS 4360:1999 contains guidance on the appropriate required documentation including examples.

The above brief description of the risk management process covers only the traditional view of dealing with events generating negative impacts, i.e. risks. Although AS/NZS 4360:1999 promotes also the application of risk management to dealing with events generating positive impacts, i.e. opportunities, it does not provide any explicit guidance. For example, treatment of opportunities may include specific recommendations on nurturing of opportunities to ensure they are realised.

3.4 Managing Risk in the Public Sector

The public sector and private sector share a common approach to risk management. But the need for public accountability and transparency results in some differences between them. There are issues which make the public sector risk context quite specific. This also includes inter-departmental issues. All employees are required to act in accordance with government regulations, public service values and ethics, and codes of conduct. The existence of the Ombudsman has a profound effect on the process of risk transfer. Risk management in the public sector must meet strict legal requirements. Federal, state and local governments have mostly provided risk financing to the public sector. However, some organisations go for more traditional, insurance-based, forms of risk financing or even for alternative ways of funding.

HB 143:1999 [51] provides guidelines for managing risk in the Australian and New Zealand public sector. It is based on AS/NZS 4360:1999 *Risk Management* [49]. Its contents are very similar to the contents of the more generic one HB 142:1999 [50]. This publication may serve as reference for elected representatives, appointed management boards, chief executive officers, line managers and general staff for developing risk management systems within their organisations. It also contains examples from the Australian and New Zealand public sectors.

3.5 Managing Risk in Outsourcing

Outsourcing is an arrangement where an external organisation takes on under contract the responsibility for supplying goods and/or services to an organisation, thus performing all

or part of that organisation's functions. This may include complete or partial transfer of staff and/or resources.

The outsourcing of non-core business and services has already become a norm rather than being an exception to the rule. Moreover, the share of ownership and operation of public facilities by the private sector has been rapidly growing. Now, many projects involve a multitude of participants with different objectives, work culture and risk management approaches. Globalisation and introduction of new technologies have significantly complicated the situation further. The risk environment has become really complex. Thus comes the need for robust and systematic risk management, which must be an integral part of the outsourcing process.

HB 240:2000 [52] provides guidelines for the implementation of AS/NZS 4360:1999 for managing risk in outsourcing. It stresses the specificity of the risk context when outsourcing and the challenges of applying the risk management approach and integrating it into the outsourcing process.

In general, outsourcing does not result in full transfer of governance, accountability and associated risks. In addition, new risks emerge due to the outsourcing process. Appendix A of HB 240:2000 [52] provides analysis of quite a few major risks when outsourcing. Some of them are summarised below.

- Outsourcing may adversely impact on the organisation's value chain, i.e. the linkages between activities that add value to the process of supplying a product/service, and hence enhancing the organisation's capabilities and giving it a competitive edge over its rivals. For example, the organisation may lose core personnel and/or support function skills, the ability to develop innovative concepts, the synergy among organisational structure, organisational culture and essential activities.
- Established traditions in the organisation may have a negative impact on the process of implementing an outsourcing strategy. Substantial changes in beliefs, routine and approaches may be required. Avoiding uncertainty and ambiguity may result in unnecessary conservatism. This may lead to attempts to manage the outsourced activity along familiar lines. On the other hand, the contractor will have a different work culture and/or different culture altogether and consequently different values, which will not fit into the initial value chain. Things may become even worse by introducing another sublevel of outsourcing.
- If information technology services are part of the outsourced activity, risk management has to include information security management. The risks involved are similar to any in-house information security risks. The difference is in their management, which may be beyond the control of the organisation. AS/NZS 444 Part 1 provides guidelines for treating information security risks when outsourcing. Risk management measures have to address access control, exchanges of information and software, network controls, software development. The organisation has to identify the potential harm which may be caused to it if information is accessed and corrupted and/or stolen.

- Intellectual property is an issue that may generate risks associated with outsourcing. Usually the use and development of intellectual property is the source of risk, for example failure to protect confidential information, copyright infringements especially with respect to third party owners, exploitation of intellectual property developed by a contractor either for another client or after the completion of the arrangement. The Appendix provides guidance on dealing with such risks using the outsourcing agreement.
- Occupational health and safety (OH&S) risks associated with outsourcing remain within the circle of management responsibilities of the organisation. These include risks to the personnel of the organisation and risks to the contractor's employees. The only exception is the case of performing the work on the contractor's site.
- Human resource management (HRM) planning is considered an essential risk treatment strategy in the process of outsourcing. For example, poor planning or not planning at all may result in implementation delays, industrial disputes, low moral, bad staff relations, and poor performance altogether. Appendix B: Tools, Tips and Traps of HB 240:2000 [52] provides a checklist for a HRM plan. Closely related is the problem of the organisation adopting the two alternative approaches to outsourcing, the clean break approach or the phased one. In the first case all related staff are deployed elsewhere or made redundant. In the second case, some of the related staff is considered for employment by the new provider before the actual outsourcing. The HB 240:2000 [52] discusses in detail their corresponding advantages and disadvantages.
- In outsourcing potential contractors may target experienced and skilled workers from the organisation thus creating the risk of loss of corporate knowledge. The impact will include loss of qualified employees, lower level of expertise, lesser management ability, and high costs for potential buy back. When outsourcing unique skills, organisations may run into even more delicate situations. The recruiting, training, development and promotion of employees of such particularly rare skills pose great problems if not addressed appropriately. Professional service providers may hire them and significantly reduce their own expenses.

The outsourcing process goes through three distinct phases: strategic analysis, transition/planning, and implementation. The strategic analysis phase determines whether the organisation is to outsource and if yes, what to outsource. The second phase develops the plans and strategies needed for the transition from in-house to outsourced projects. The third one includes the implementation of the above-mentioned plans and strategies. The risk management approach has to be applied at every phase of the outsourcing process. Figure 4 shows how the risk management process has to be systematically linked and embedded into the outsourcing process.

The strategic analysis phase is very important for establishing the future direction of the organisation. It has to confirm that the outsourcing activity is consistent with the organisation's vision and objectives. According to Part 2 of HB 240:2000 [52] the use of value chain analysis and organisational culture analysis is critical for understanding the strategic context. This may provide the basis for the application of SWOT analysis to

identifying organisation's limits. The second and the third phase underline the necessity of communication, interaction and cooperation within a continuous process of monitoring and reviewing. At each phase new risks may appear while old ones may change or even disappear. They may eventually influence the prospect of future outsourcing of the same activities.

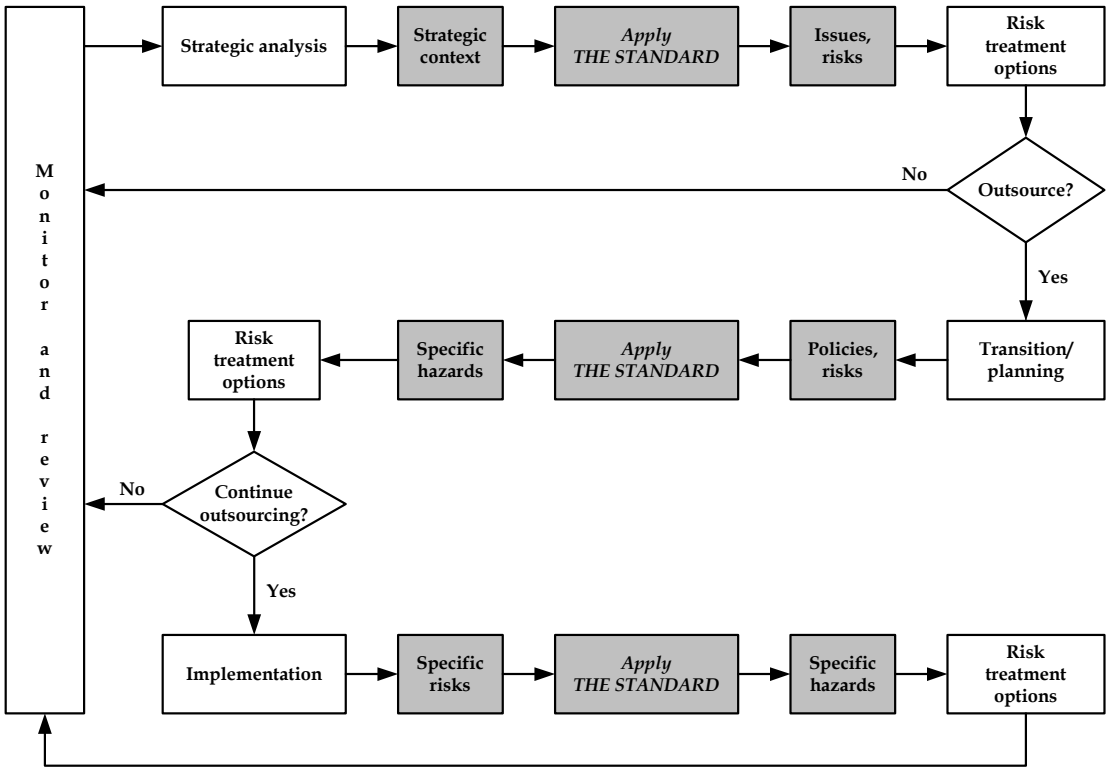

Figure 4: Integrated Process of Risk Management and Outsourcing (Adopted from HB 240:2000 Guidelines for Managing Risk in Outsourcing Using the AS/NZS 4360 Process)

Appendix C of HB 240:2000 contains two case studies with commentaries: "Contract management within Defence for the provision of contractor services"; and "Outsourcing experiences of the NSW State Government".

3.6 Risk Analysis of Technological Systems – Application Guide

AS/NZS 3911:1998 *Risk analysis of technological systems – Application guide* [48] is a copy of IEC 60300-3-9:1995 *Dependability management* Part 3: *Application Guide* Section 9: *Risk analysis of technological systems*, in accordance with Standards Australia's policy to adopt without changes an existing international standard, here the one on risk analysis. The objective has been to help the development of common methodology for technological risk analysis across industries and countries. In particular, it has to assist in adopting a common approach to the design, quality, reliability and safety of technological systems.

AS/NZS 3911:1998 provides guidance on selection and implementation of risk analysis techniques for technological systems. It has to ensure a considerable level of uniformity and consistency in the risk analysis planning, application, communication and decision-making. However, it introduces some principle differences between AS/NZS 4360:1999 (1995) and AS/NZS 3911:1998.

- AS/NZS 3911:1998 has a more limited scope. It does not cover the entire risk management process as described in AS/NZS 4360:1999. It concentrates only on the risk analysis part of the risk assessment step. This standard includes the risk analysis concepts, risk analysis process, and risk analysis methods. It deals with the negative "What can happen?" part of risk identification, i.e. "What can go wrong?" and then continues with risk assessment and some review and communication.
- The two standards exhibit some major differences in terminology, especially in the definition of risk. According to AS/NZS 3911:1998, risk is the "combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event", i.e. an "event which can cause harm". Here harm means physical injury or damage to health, property or the environment. However, according to AS/NZS 4360:1999, risk is the "chance of something happening that will have an impact upon objectives, and which is measured in terms of consequences and likelihood". Here risk relates as much to identification of opportunities as to loss or harm reduction.
- The two standards differ in the range of applications. AS/NZS 3911:1998 mainly concentrates on risk in technological systems. AS/NZS 4360:1999 considers risk inherent in any activity and risk management as part of any good management practice.

AS/NZS 3911:1998 provides guidance on selecting and implementing risk analysis techniques including: hazard and operability studies (HAZOP); failure modes and effects analysis (FMEA); fault tree analysis (FTA); event tree analysis (ETA); preliminary hazard analysis (PHA); human reliability assessment (HRA).

4. Risk Management in the Australian Defence Organisation

Managing risk has always been inherent to any type of activity in Defence. But now, more than ever, and in view of the recent events of global and local importance, the need for a coordinated and systematic approach to managing Defence's risks has emerged. Thus, in March 2002 a strategy was endorsed to introduce such an approach starting from the top with the Defence Committee (DC). As stated by the Secretary and the Chief of the Defence Force, the ADO is large and complex and without an organisation-wide perspective the actions and decisions of individuals or teams could compromise the ADO's ability to fulfil the mission of defending Australia and its interests. Furthermore, this top-down or

enterprise approach will make possible the link of risk management and performance at the highest levels of the ADO and will not be restricted simply to compliance and control. It has to be aligned with Defence's strategic objectives and corporate governance arrangements, and become part of the business decision-making, the planning and the reporting cycle. This approach has to provide the Government and the Parliament with the assurance that Defence has adopted a comprehensive approach to risk identification, assessment, treatment and monitoring. The introduction of a Defence Risk Management Framework is to help set a higher standard of risk management in Defence.

4.1 Defence Enterprise Risk Management

Enterprise Risk Management was set up first within the Strategic Business Management Branch of the Business Strategy Division within the Chief Finance Officer Group, but currently belongs to the Inspector General Group. Its creation was announced via a joint "Message from the Secretary and the Chief of the Defence Force". The objective of Enterprise Risk Management has been to ensure that a Defence-wide approach to risk management is established. Namely, "the Enterprise Risk Management Directorate guides development of risk management at all levels across Defence as part of Defence's corporate governance, business model and way of doing things." Particularly important has been the role of Enterprise Risk Management in developing the Defence Risk Management Policy (DRMP) [18], the Defence Risk Management Implementation Plan (DRMIP) [17], the Guidelines [23], and the DRMF al together.

The joint Message follows on findings of the Inspector General to consider the not so good track record of Defence in managing "strategic business risks". They are identified as the ones that "impact on, for example:

- Quality of the relationship with the Ministers;
- Effective achievement of the outputs;
- Allocation and use of resources;
- Standard of accountability;
- Quality of customer service;
- Morale of people;
- Level of creativity and innovation; and
- Quality of management decision making".

Enterprise Risk Management also looks after the Defence's membership in the Commonwealth insurance framework (Comcover). This is considered as an essential element of the Defence's pro-active risk management activities.

4.1.1 Defence Risk Management Chief Executive's Instruction

The Defence Risk Management Chief Executive's Instruction (CEI) [16] was issued as a part of *Chief Executive's Instructions, Edition 3* in July 2002. Its objective is to establish the framework of principles for the risk management activities in Defence. This CEI is based on the Financial Management and Accountability (FMA) Act 1997 section 52 and hence

any failure to comply with its provisions may be considered a breach of the FMA legislation, the Australian Public Service (APS) Code of Conduct, the Defence Force Discipline Act 1982, etc.

The Defence Risk Management CEI establishes the commitment of Defence to a comprehensive, coordinated and systematic approach to risk management. Furthermore, risk management is everyone's responsibility and will become a part of everyday management practices. All activities are to be consistent with the Australian/New Zealand Standard for Risk Management AS/NZS 4360:1999.

The Defence Risk Management CEI is linked to other relevant documents, e.g. the Defence Procurement Policy Manual [20], the CEI – Fraud Control in Defence and the DRMIP [17] in particular. The DERM website is also provided if the need for further advice on risk management arises. For details refer to section 3.1.5.

4.1.2 Defence Risk Management Policy

According to the Preamble of the DRMP [18], effective risk management is a key element in meeting the Government's expectations for the ADO. Risk is involved in all Defence activities and it is managed each day at different levels and in a wide variety of contexts.

The Policy clearly states the commitment of Defence to a comprehensive, coordinated and systematic approach to risk management. It has to be employed to anticipate uncertain events, exploit opportunities, and to respond appropriately to potential weaknesses. In particular, this means:

- Protection of Defence personnel;
- Use of resources for achievement of objectives under effective risk management;
- Reduction of the consequences of physical and other disasters and catastrophes;
- Asset management and environmental management;
- Defence's relationships with international and/or national, public and/or private organisations.

The DRMP formulates the policy objectives regarding risk management in Defence. Throughout the entire ADO, management of risk is everybody's responsibility and as such it will progressively become part of everyday activities in Defence. It will be an integral part of:

- Planning (identifying risks associated with key initiatives or activities leading to the results to be achieved);
- Decision making (prioritising and ranking risks associated with various options or alternative courses of action);
- Reporting (monitoring and communicating the treatment of identified and assessed risks); and
- Evaluation (reviewing the implementation of treatment plans, learning lessons from experience and improving action plans for the future).

The approach will distinguish among specialist risk categories in areas such as safety, fraud, information, and project management.

4.1.3 Defence Risk Management Implementation Plan 2002-2003

The Introduction of the DRMIP [17] declares the joint commitment of the Secretary and the Chief of the Defence Force to the formal management of risk throughout Defence. It states that their commitment is given effect via the Policy [18], and is supported by the Guidelines [23] and tools that lay the foundations of the DRMF. The Plan contains the DRMP in full. It quotes other relevant documents which should be taken into account.

The Plan [17] also recognises the existence of a number of areas of effective risk management. The Introduction contains a diagram describing how risks of all possible levels must be managed in Defence (see Figure 5). The DRMIP builds on the existing risk management environment by coordinating and standardising it into a single enterprise, i.e. top-down and Defence-wide, unified framework. Risk will be managed and reported at all levels of Defence via the Framework.

The DRMIP [17] establishes:

- The approach to managing risk;
- Risk governance and assurance arrangements;
- Responsibilities for managing and reporting risk;
- The education and training of risk managers and coordinators;
- The communication strategy;
- The effective measurement of risk management in Defence;
- The implementation of risk management over the next 2 to 3 years.

Defence's Approach to Risk Management?

The Plan uses the Australian/New Zealand Standard on risk management AS/NZS 4360: 1999 to define risk as "… the chance of something happening that will have an impact upon our results/objectives". Then it continues further by stating that risk "is inherent in everything Defence and its service providers do". Moreover, the "… failure to understand and to manage Defence's risks may result in potential adverse outcomes, including:

- Harming our people;
- Failed strategic business objectives;
- Financial loss;
- Organisational or political embarrassment;
- Operational disruption; and
- Legal liability.

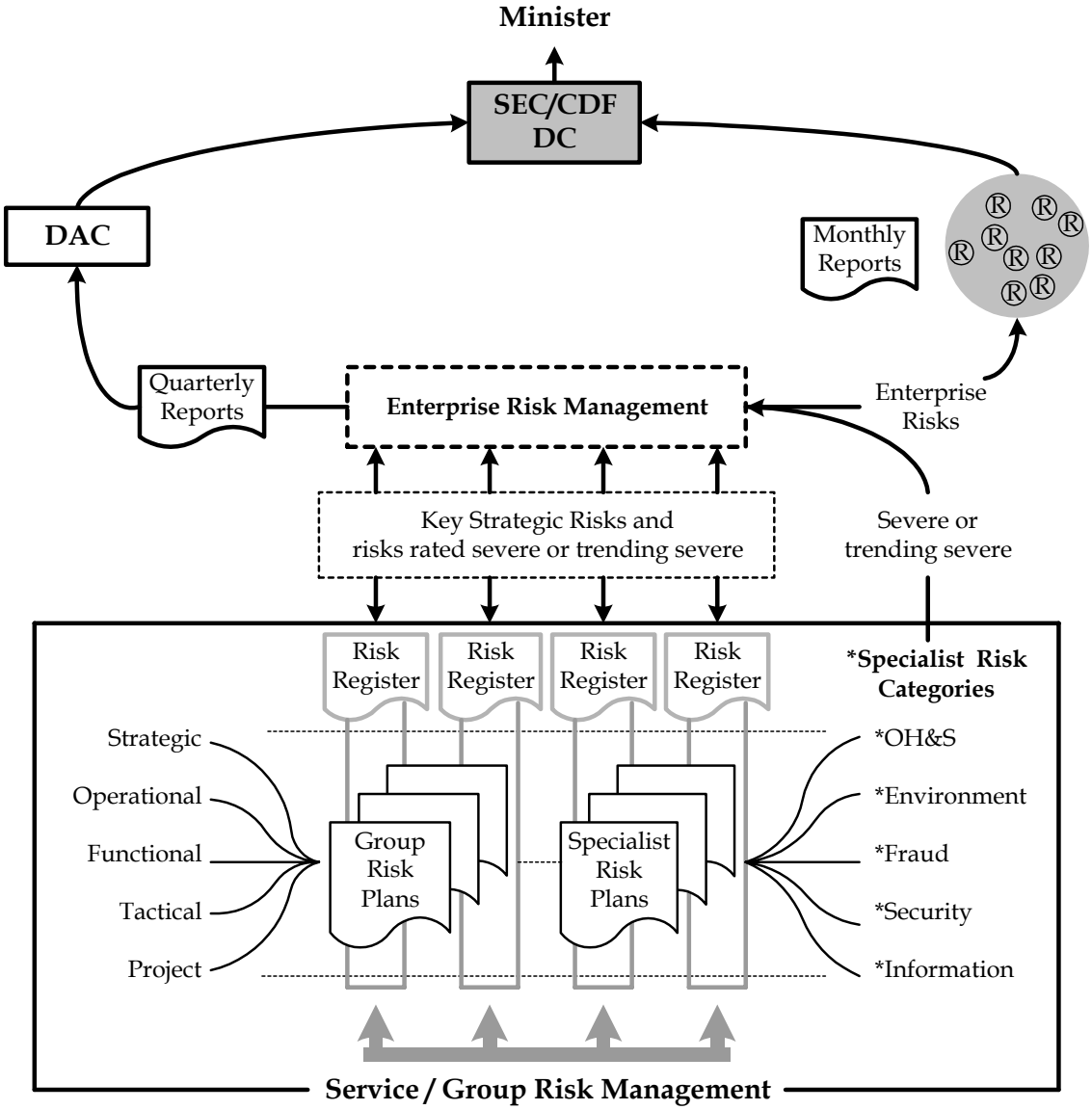

Figure 5: Managing Risk in Defence (Adopted from DRMIP [17])

Next, the Plan introduces the Australian/New Zealand Standard definition of risk management as: "…the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects". The risk management process is characterised as "… a systematic process to identify, assess, treat and monitor risk so that it is reduced and maintained within acceptable levels". Again the Plan has followed the Standard very closely.

Further the goals of Defence's enterprise-wide approach are determined. They "… are fourfold:

- To ensure that risk management becomes an intrinsic part of decision-making;
- To provide assurance that Defence's risk exposures have been identified and that processes and systems are in place to properly manage these risks;
- To ensure that risk management is integrated into Defence's business planning processes; and
- To establish processes and systems across Defence that will integrate and coordinate the various risk management measures already in place".

According to the Plan the benefits of a comprehensive risk management system throughout Defence are as follows:

- A management process providing better understanding of issues associated with an activity;
- A more effective reporting framework to better meet corporate governance requirements
- A greater openness and transparency in decision-making;
- Improved efficiency and effectiveness of Defence's activities;
- Fewer unacceptable outcomes and costly surprises; and
- Compliance with legal obligations.

From a broader perspective and more to the top end of Defence there will be some further management benefits, for example:

- Better communications with internal and external stakeholders;
- Improved accountability and performance measurement;
- Advanced decision-making at the strategic and operational level; and
- Development and implementation of business management strategies.

The above listed benefits can be characterised not only as contributions but as requirements as well.

The principles for managing risk in Defence reflect the best up-to-date practice in both the public and the private sectors. They include:

- Risk management rather than risk avoidance;
- Risk management corresponding to the authority to manage;
- Promotion of a risk management culture;
- External and internal stakeholders participate in risk management; and
- Decision-making is based on and supported by proper risk identification, assessment and treatment plans.

A Hierarchy of Defence Risks

The Plan identifies three levels of major risks in Defence: enterprise, strategic and operational. They are determined by the organisational levels necessary to manage the risks.

The *enterprise risks* have the potential to impact the ADO in its entirety. They recognise no established boundaries between Services, Groups, Divisions, etc. Such risks emerge due to the multitude of interdependencies among and within the various subsystems of Defence as a very large hierarchical organisation. Therefore, a single Service or Group cannot be responsible for managing a specific enterprise risk. The alternative could lead to difficulties in effort coordination and even loosing the holistic view of the problem. The Plan delegates the Secretary and the CDF the power to assign the risk management responsibility to *enterprise risk coordinators* with the DC as oversight.

The *strategic risks* are usually associated with the activities of a given Service or Group. They may adversely affect key deliverables and/or performance indicators that have been identified in its business plans. Further, the Plan considers "strategic risks that have been assessed as 'severe' or trending 'severe' when rated against the 'Enterprise Risk Management Matrix' and are to be raised to the DC…". Regrettably, the Plan neither defines 'severe', nor provides a link to the 'Enterprise Risk Management Matrix'. Moreover, the term 'severe' does not exist in the original AS/NZS 4369: 1999. One may assume that both originate from other risk management related publications, e.g. HB 142-1999 *A Basic Introduction to Managing Risk* [50], HB 143-1999 *Guidelines for Managing Risk* [51], and *Capability Systems Life Cycle Management Guide* [13], etc.

The *operational risks* emerge at a specific process level within a Service or Group. They are associated with systems active at sub-strategic level, i.e. at operational, functional, tactical or project. Operational risks usually arise at a lower organisational level: formation, unit, directorate, etc. When they are assessed as high or trending 'severe', they are to be reported to the next level of command and/or management. The procedure has to be specified in the corresponding Service/Group Risk Management Implementation Plan.

Risk Governance and Assurance

The Plan stipulates that the accountability in the Defence's governance framework requires risk management to be everyone's responsibility and that risk management has to be integrated into the framework. All enterprise and key strategic risks must be identified, assessed and assigned for treatment with respect to Defence's strategic objectives, both at Department and at Service/Group level. A chart of the top-end risk management structure in the ADO (see Figure 6) is provided.

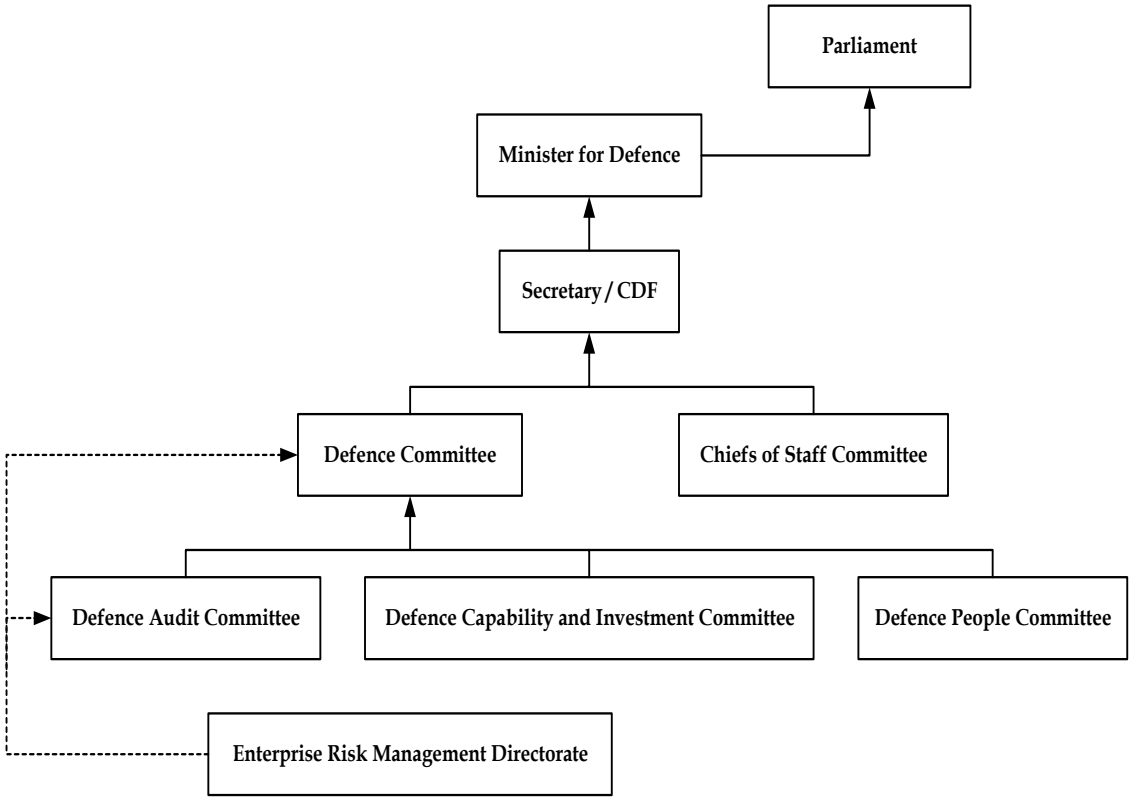

Figure 6: Defence Risk Governance and Assurance Structure (Adopted from DRMIP [17])

The Plan defines the roles and responsibilities of the highest levels in Defence for managing risks in the following way.

- The Secretary and the CDF share the joint overall responsibility to the Government via the Minister for Defence and the Parliament for establishing the Defence Risk Management Framework. This includes direction setting, control, accountability procedures, compliance with existing legal acts, etc.
- The DC serves as oversight of the application of the DRMP and the effective operation of the DRMF. Risk management has to be a standing item of DC's agenda. It reviews the Policy once a year, identifies and establishes the acceptable levels of enterprise risks in Defence, appoints the enterprise risk coordinators, assesses the effectiveness of the enterprise risk management strategies, periodically reviews the system of internal controls and supports the Secretary and CDF.
- The Chiefs of Staff Committee discusses single service, joint service and wider based risks in Defence. It serves as a platform for providing coordinated advice for consideration by the Secretary and the CDF.
- The Defence People Committee advises the Secretary and CDF, and DC on the range of planning and people initiatives. These personnel activities have to come with formal risk assessments attached.

- The Defence Capability and Investment Committee advises the Secretary and CDF, and DC on the levels of strategic, technical and financial risks accompanied by formal risk assessments, limits of acceptance and performance measures.
- The Defence Audit Committee advises the Secretary and CDF, and DC on existing risk management practices and potential improvement opportunities identified by audit and evaluation activities.
- The Enterprise Risk Management Directorate is to support the Secretary and CDF, and the DC in the management of enterprise risks and to assist the Service Chiefs and Group Executives with their key strategic risks.

According to the Plan there have to be appropriate sources of assurance incorporated within the Framework. There have to be formal audits to consider the adequacy and effectiveness of the risk management processes in Defence.

- The Inspector General (IG) is to provide to the Secretary and CDF an annual statement regarding the enterprise and the key strategic risks. The IG is the main source of independent internal audit advice.
- The DC may include other external and/or internal agencies in the assurance process.
- In general, the Australian National Audit Office (ANAO) considers risk management in its audit program. In 2002 the Auditor General is to conduct a specific study of risk management in the Commonwealth departments and agencies.

Risk Management – Making it Happen in Defence

Risk management in Defence relates not only to potential catastrophes and disasters. It covers also the circumstances where Defence may not meet the expectations of the Government due to under-performance. Hence an important question arises, namely, the question of how Defence is to improve its performance without exposure to unnecessary risks. Thus, risk management has to be integrated into all planning and performance management arrangements. It has to be an essential requirement for all members of Defence from the top end to the lowest ranks.

- The Service Chiefs and Group Executives are responsible for managing risks arising from their specific areas and from relationships with internal and external stakeholders. Each one is to establish a service/group implementation plan and a functional framework for risk management with explicit responsibilities delegated, and ensure integration at all levels of planning and reporting up to Defence Plan and Defence Management Financial Plan.
- The Defence Risk Management Leadership Reference Group is to consist of at least SES BAND 1/One Star (E) level representatives of the Services/Groups. Its members have to assist the risk management effort within their Service or Group and make sure it is consistent with the Framework. They are to advise Enterprise Risk Management about the progress of the risk management activities in their Service or Group.
- The Service/Group Risk Management Coordinators are accountable to their Service Chief/Group Executive for the regular updating of the Service/Group Risk

Management Implementation Plan, the reporting of operational/tactical risks assessed as high or tending severe, the maintaining of risk management information, the provision of methodological advice, etc.

- The Enterprise Risk Management Directorate is responsible for the leadership, development and implementation of the Defence Risk Management Framework. The Directorate is to coordinate risk analysis and reporting, and ensures that severe risks, trending severe risks and potential enterprise risks are reported to the DC.
- The specialist risk categories of security, fraud, information, environment information and OH&S have to be considered also for their enterprise, Defence-wide impact. Some of them (fraud and OH&S) are treated within established frameworks, while for others (information and security) the frameworks are still in the design and/or implementation stage. Specialist risks singled out as potential enterprise ones are to be assessed and reported through the Directorate to the DC.
- All Defence personnel have to apply best practice risk management in their area of responsibility in accordance with the corresponding Service/Risk Plan.

The above is hardly possible without the commitment of the Secretary and the CDF to equipping the people in Defence with risk management knowledge and skills. The Plan establishes a strategy, developed by Enterprise Risk Management, to guide and promote risk management education and training. It includes:

- Establishment of Guidelines for risk management in Defence and accompanying tools to assist the implementation of an effective risk management process;
- Promotion of risk management throughout Defence via awareness seminars and information fora;
- Integration of risk management into existing management training and development programs;
- Availability of appropriate training to Defence personnel directly involved in risk assessment and management. The Defence Materiel Organisation (DMO) and the Defence Safety Management Agency (DSMA) are specifically targeted.

Enterprise Risk Management is to cooperate with the Defence Personnel Executive (DPE) and the specialist risk areas in providing the necessary risk management knowledge and skills to personnel at all levels. According to the Plan, the DPE is developing a set of generic risk management competencies.

The Plan mentions a Defence Risk Management Communication Strategy. Over the short to medium term the aim of the Strategy is to "…promote and develop an understanding and acceptance at all levels of Defence of the need for, and the benefits associated with, effective risk management."

Enterprise Risk Management has prepared a multi-layered information package, which includes the Policy, the Plan, the Guidelines, etc. It allows commanders, managers, supervisors to 'pass down' relevant risk related information and tools to their

subordinates. Thus, risk management will complement and support the chain-of-command resulting in a cascading Defence risk management.

What's Next?

In conclusion the DRMIP summarises that the initial effort "has been directed towards building on the risk management arrangements that are already in place in some Services and Groups" and the identification of the enterprise and key strategic risks in Defence.

For the period 2002-2003 the emphasis was supposed to fall on the creation of Service/Group frameworks suitable to their requirements and in accordance with the Defence Enterprise Risk Management approach. An on-line risk information management system for use across Defence was to be introduced.

4.1.4 Defence Risk Management Guidelines

The Guidelines [23] are to support the implementation of the endorsed standard approach to risk management in Defence. They include templates and tools to be used across the entire ADO. The Guidelines have to help the creation of a risk management environment without ambiguity and differences in the terminology and the core procedures. A unified risk culture in Defence will be the ultimate criterion for the successful establishing of the Framework.

The Guidelines start with a chart of the risk management process following the AS/NZS 4360: 1999 and providing instructions for each of its steps: establish the context, identify risks, analyse risks, evaluate risks, and treat risks. The instructions are presented in the form of tables and may serve as an example of how one's own investigation has to be organised. Each one of them comprises of a list of tasks required to be accomplished, a description of the process to make it happen, an understanding/justification why one is to follow that specific process, and a documentation with outputs.

The Guidelines contain some optional support tools. The risk management plan outline provides guidance on the preparation of an organisation's plan and its key elements. The process of risk identification may be supported by using the following three forms: stakeholder analysis, identifying key risks, and management issue of concern. The risk register is used to record important descriptions of the risks, i.e. sources and impacts, assessments of risk levels, and treatment plans. This tool contains three, rather than two forms: Identifying & Analysing Risk Environment, Planned Risk Treatments (& Schedule), and Summary Risk Treatment Plan.

A number of supplements are added to the Guidelines. The first one presents a worked example on assessing and managing risk for a fictional team, where all steps of the process are illustrated in detail. The next supplement describes three potential areas of risk management concern, i.e. when focused on risks to actual outputs/deliverables, risks to unit's business capability/sustainability, or strategic management issues. The guide to

finding and analysing risk related information lists a number of methods to help look for all possible sources of information at each stage of the risk management process. It also quotes a variety of techniques applicable in risk identification and assessment, including process mapping, SWOT analysis, six-hat thinking, mind mapping, and fault tree analysis. The supplement on assessing the risk level provides guidance on how to determine the likelihood of the risk, how to determine the consequences of the risk, and how to combine them into the risk level (analysis) matrix. Here the Guidelines do not establish a unique and unambiguous terminology in describing the levels of the two factors (likelihood and consequences) and the combining matrix. They reflect the situation in the publications by Standards Australia. At least the Guidelines have not made it worse by providing just one example for each element of the risk analysis process. The next supplement presents the user with a checklist of the documentation to be maintained during the entire risk management process. Further, one can find a number of sources outside Defence offering risk advice, e.g. Standards Australia, Australian National Audit Office, UK National Audit Office, and Accounts Commission for Scotland. The last supplement lists areas and institutions in Defence that provide mainly specialist risk advice, including the Defence Safety Management Agency, the Defence Security Authority, and the Defence Materiel Organisation. The Enterprise Risk Management Directorate comes naturally at the end. Unfortunately, DSTO is not listed as a source of professional risk management advice.

4.1.5 Defence Enterprise Risk Management Website

Enterprise Risk Management has a website on the DEFWEB under the title of Defence Enterprise Risk Management (DERM) available at the time of writing at:

http://defweb.cbr.defence.gov.au/ig/ERM/ermintro2/

Its introductory page states the commitment of Defence to establish a comprehensive and systematic approach to risk management. It provides links to the Defence Risk Management CEI, the Defence Risk Management Policy, the Defence Risk Management Implementation Plan, the Guidelines, and related sites. A feedback option via comments and/or questions is also made available.

The DERM site contains a specific link to a page describing the enterprise risks as identified by the DC. They recognise no organisational and/or functional boundaries and cannot be managed by an individual Service/Group. These risks are the responsibility of the Secretary and the Chief of Defence Force. According to "The Risks" web page "the current areas covered by the enterprise risks are:

- Defence capability to respond adequately to our strategic environment and emerging threats;
- Effective management of our people, as a fundamental element of capability;
- Defence delivery of the major capital investment program (including equipment and facilities);
- Development and delivery of a Defence Information Environment appropriate to Defence's needs;

- Defence's ability to adjust its business processes in response to the changing environment;
- Senior Leadership support to the Minister and Sec/CDF in respect of their statutory responsibilities;
- Defence's planning assumptions reflecting our current and emerging strategic environment;
- Defence external stakeholders relationships; and
- Sourcing and managing of Defence finances".

4.1.6 Defence Enterprise Risk Management – Summary

The Australian Defence Organisation has introduced a coordinated and systematic approach to risk management in any Defence activity. The DRMF has come into existence based on the DRMP, the DRMIP, the Guidelines and the leadership efforts of Enterprise Risk Management. In essence ADO has adopted the approach described in the publications of Standards Australia and especially AS/NZS 4360:1999 *Risk Management*. Defence has followed strictly the generic guidelines for the introduction of a risk management framework in an organisation.

The DRMF via the Plan identifies the specific hierarchy of Defence risks: enterprise, strategic and operational. Special attention is devoted to the enterprise risks due to their ability to cross organisational and/or functional boundaries and inability to be managed by one service and/or group. In the top-down approach to risk management in Defence, the Secretary and CDF share jointly the responsibility for the enterprise risks, which is overseen and reviewed by the DC. Enterprise Risk Management has provided on its web site a list of the current enterprise risks in Defence.

An important part of DRMF is communicating the message of effective risk management to everyone in ADO. Enterprise Risk Management has established itself as the Defence-wide leader of the effort to make the Framework function. Its web site contains the most important documents and links to other helpful information sources. Moreover, the Defence Information Bulletin in its issue of December 2002 published a feature article [57] on DRMF under the title "Can an organisation the size of Defence minimise the hazards of its everyday business activities?" promoting risk management as a valuable element of the decision making process in Defence.

The DRMIP outlines also a strategy, developed by Enterprise Risk Management, regarding risk management education and training. It involves also the DPE in order to equip people in ADO with the necessary knowledge and skills. The bottom line is, risk management training has to be integrated into any management training and made available to people Defence-wide.

4.2 Non-DERM Publications and Documents

Risk management has always been applied to most activities in Defence. The three services and some major institutions within ADO have adopted risk management as an inherent part of their everyday ways to do things. For example, the DMO, the DSMA, the Defence Security Authority (DSA) and others have been recognised as places of effective risk management implementation. They have established risk management frameworks to suit their own needs and they have produced their own written documents, i.e. manuals, policies, rules, plans and guidelines.

4.2.1 Defence Procurement Policy Manual 3.0 (2002)

This is the third edition of the *Defence Procurement Policy Manual* (DPPM) [20]. It was released by DMO in 2002. The DPPM has to serve as the prime reference for all Defence personnel involved in procurement. This comprehensive up-to-date guide to procurement covers all aspects of the purchasing process including issues of risk management. Chapter 3.2 deals with the risk management in procurement, chapter 3.5 with the quality assurance in the management of risk, and annex 3A with the risk management matrix.

DPPM recommends that risk management be applied to all stages of the procurement cycle. It is an important part of public sector management and of corporate governance in general. Here, decision making also has to be conducted on the basis of transparency and accountability. The Commonwealth Procurement Guidelines and Best Practice Guidance formulates the policy and contains guidance on risk management in procurement, while AS/NZS 4360:1999 *Risk Management* serves as the standard.

Chapter 3.2 of DPPM considers some risk issues in procurement. As a general rule the risk management cost has to be commensurate with the gain. There is no need for a formal strategy in a simple procurement where the major risk is an unsuitable final product. Strictly following the requirements will be efficient risk management. In complex and strategic procurements there is a definite need for formal strategies since the risks may be significant. Sources of risk in procurement may include use of new technology, poorly defined specifications, procurement scale and timeframe. The consequences may be time delays in tendering and/or delivery, sky rocketing contract costs etc. Altogether procurement risks can be classified in three broad categories: technical, schedule and financial. In any case, risk management has to be an element of the procurement contract. There are certain tools that can protect organisations from risks generated by supplier's performance. They include indemnities, insurance and financial guarantees. The contracts may also contain dispute resolution mechanisms, quality assurance clauses, procedures for inspections, testing, etc. Comcover provides insurance cover for all Commonwealth departments and agencies including Defence. Thus contractors are required to take insurance as well. The Comcover Policy Manual deals with the range of Comcover's insurance policies. Further guidance regarding risk and insurance in strategic and complex procurement is available in the ASDEFCON (Strategic Materiel) and ASDEFCON (Complex Materiel) Templates and Handbooks.

Chapter 3.5 of DPPM provides Quality Assurance (QA) mechanisms used in Defence for risk reduction in procurement and making sure contractors meet their obligations with respect to quality. The Defence policy on QA strictly follows the Commonwealth one in its requirement of the application of risk management to QA. It prescribes the means of assuring quality to be linked to the level of risk in case of non-compliance. On the other hand, applying QA has to be part of the risk treatment process.

Annex 3A of DPPM contains an example of a generic risk management matrix, which can be used in any procurement. The table covers all stages of the procurement process:

- Developing a procurement method;
- Preparing the specifications;
- Requesting offers;
- Evaluating offers,

including the entire procurement process itself. The table identifies what can go wrong, what the consequences may be and how to deal with them at each stage. Any complicated procurement process requires a detailed risk assessment approach. It has to include a risk management plan for the purchaser and for the supplier.

4.2.2 Capability Systems Life Cycle Management Manual 2002

This is the first edition of the *Capability Systems Life Cycle Management* (CSCSM) *Manual*. Actually, it existed before as the CSLCM Guide 2001 [13] and even before that as the DI(G) on Capability Life Cycle Management. The CSLCM Manual 2002 serves as the prime source of reference for those with insufficient experience in capability management.

Annex D to Part 6 of the *Capability Systems Life Cycle Management Manual* 2002 describes risk management as an integral part of the capability life cycle management process. It quotes AS/NZS 4360: 1999 as its only reference. At the beginning a number of risk related definitions are given. Then the main elements of the risk management process, as shown in Figure 1, are introduced. Further, these elements (establish the context, identify risks, analyse risks, evaluate risks, treat risks, monitor and review, and communicate and consult) are discussed in more detail. The risk level matrix shown in Table 4 is one of the most unambiguous matrices existing in Defence publications where there is no overlapping of concepts. In the case of Major Capital Investment projects the key objectives identified as needing risk management are capability, cost and schedule. Thus, the appendix following Annex D to Part 6 contains the risk consequences expressed in terms of the risk impact on capability, cost and schedule.

Table 4: Risk Level Matrix (Adopted from Capability Systems Life Cycle Management Manual 2002)

LIKELIHOOD	CONSEQUENCE				
	1 Insignificant	**2 Minor**	**3 Significant**	**4 Major**	**5 Severe**
5 Almost Certain	Medium (c)	Medium (c)	High (b)	High (b)	Extreme (a)
4 Likely	Medium (c)	Medium (c)	Medium (c)	High (b)	Extreme (a)
3 Moderate	Low (d)	Medium (c)	Medium (c)	High (b)	High (b)
2 Unlikely	Low (d)	Low (d)	Medium (c)	Medium (c)	High (b)
1 Rare	Low (d)	Low (d)	Low (d)	Medium (c)	Medium (c)

Notes **(a)** **Extreme.** Immediate executive action required.
(b) **High.** Executive action required.
(c) **Medium.** Management responsibilities must be specified.
(d) **Low.** Manage using routine processes.

4.2.3 CA Directive – Army Risk Management

Chief of Army Directive No. 2/98 – Army Risk Management (ARM) [10] was issued in January 1998. It describes the ARM policy and implementation requirements for the application of risk management throughout Army. The ARM process is detailed in Annex A to the Directive and its eight appendices. The provisions of the ARM policy had to be incorporated as amendments to an updated future Manual of Occupational Health and Safety – Army 1996.

The Directive defines the ARM as "the process of identifying and assessing potential hazards to planned activities, and development of appropriate strategies to reduce the effect of identified hazards". ARM aims at reducing unnecessary risk impact on force preservation and task achievement. Although the Directive mentions the applicability of ARM to any Army activity, it concentrates on the role of risk management for improving safety management as the means for enhanced force preservation. Unfortunately, it does not discuss the identification of potential opportunities and how to make the most of them as an essential part of ARM.

The Directive states that risk management is the responsibility of all commanders. They have to incorporate it into the task or operations planning process, identify potential hazards, assess the levels of associated risks, adopt treatment measures, monitor and review the effectiveness of the process, and document the experience. These responsibilities mirror the steps of the generic risk management process described by

AS/NZS 4360:1995. The Directive stops short of regulating ARM as everyone's responsibility and as part of everyday management practices.

ARM preserves the generic nature of the process from the Standard. It is considered impractical to develop specific processes for the different environments across Army. Therefore, it has to be redeveloped and implemented as specific functional and/or organisational risk management procedures. The implementation of ARM generates tasks for the different levels of command. The Commander of Training Command – Army (COMD TC-A) has to design, develop and conduct the necessary training of personnel. COMD TC-A has to ensure ARM is incorporated into existing Army Doctrine and modifications are made to the Military Appreciation Process (MAP). Functional Commanders are to apply ARM at all levels of planning within their range of command. Formation and Unit Commanders have to use ARM to develop Risk Management Standard Operating Procedures (SOP) corresponding to the elements under command. Training activities have to include a risk management plan in their instructions, especially the collective ones.

Annex A provides a description of the ARM process. It is adopted from AS/NZS 4360:1995 and differs slightly from the more recent version of the Standard. ARM follows basically the same six-step process: task context analysis; risk identification; risk analysis; risk assessment and prioritising; risk control; and monitor and review. One can detect some minor differences in the terminology in comparison with the current one. More importantly, there is almost no difference in the interpretations of the concepts. It is essential to note only that the risk analysis step requires that each risk be considered with respect to its probability, exposure and consequence. Probability means likelihood that a hazard will lead to an incident. Exposure stands for frequency and duration of exposure to the hazard. Consequence is described in terms of the severity associated with personnel and/or asset loss, or mission failure. These three factors together determine the risk level.

The Directive introduces and discusses the concept of Hierarchy of Controls within Step 5, Risk Control. It offers an established order of preference and effectiveness of control measures, ranging from the most effective to the least. The Hierarchy of Controls, in decreasing order of effectiveness, is as follows:

- *Elimination* of risk is the preferred option and a permanent solution. It can be achieved by cancelling a task, prohibiting an activity, or stopping the exposure to a hazard. Unfortunately, risks in military operations cannot be totally eliminated in principle.
- *Isolation* of risk means separation of hazards from personnel by time and space. For example, restricting dangerous activities to specific designated zones within training areas is physical isolation of hazards.
- *Engineering* controls include modification of equipment to improve workplace safety, e.g. vehicle safety belts and machine guarding.
- *Procedural/Administrative* controls result in limiting the exposure of personnel to identified hazards. They are made effective via directives, safety instructions, training

instructions and orders. These controls may reduce time of exposure and number of personnel exposed, with Personal Protective Equipment (PPE) as the least effective.

Appendix 1 to Annex A to CA Directive 2/98 represents a flow chart of the risk management logic, which is very similar to the one in Figure 3. Appendix 2 contains definitions of concepts from the area of risk management. Appendix 3 provides verbal descriptor guides for the levels of probability, exposure, consequence and risk. Appendix 4 contains a Qualitative Risk Analysis Matrix, i.e. a risk level matrix based on exposure and consequence. The Quantitative Risk Analysis Matrix from Annex 5 provides the user with a numerical risk level score, which has to produce a more detailed prioritisation in comparison with the qualitative one. Appendix 6 contains the Risk Management Analysis Nomogram with notes on how to use it. As a worked example one may follow the completed Risk Management Work Sheet in Appendix 7. The final Appendix, 8, is a blank Risk Management Work Sheet. All appendices contain instructions on how it should be used.

4.2.4 TIB 83, Risk Management

The Training Information Bulletin (TIB) 83 *Risk Management* [11] was issued in April 1998. It contained the doctrine for risk management training and provided an interim measure before the full implementation of CA Directive No. 2/98 *Army Risk Management* [10]. TIB 83 had to be included in the updated doctrine on command, leadership and management. All training activities have to be conducted following the procedures described in TIB 83. It spells out how the application of risk management by everyone can contribute to force preservation. TIB 83 provides practical guidance to Army personnel and introduces a range of available risk management tools, including directives, instructions, orders, procedures, and use of expert advice and judgements. It also identifies the specific roles and responsibilities for applying the ARM process, namely policy making, activity planning, implementation and participation.

TIB 83 describes risk management as "an integral part of day-to-day management, a decision-making and problem-solving philosophy and a system integral to the Military Appreciation Process (MAP)". Risk management applies to any activity "relating to safety, use of property or equipment, political issues, public image, finance, project management, the environment, morale and legal issues". However, the focus of risk management within the Army is force preservation, which ultimately leads to maximisation of combat power. But achieving this objective may be hindered by a variety of risks based on policy, training, engineering, procedural and organisational issues. Hence, Army recognises the need for a systematic risk management approach, supported by an appropriate training process.

TIB 83 follows the logic and steps of the ARM process, as introduced by CA Directive No. 2/98. However, there are some additional elements to the nearly generic risk management process. For example, it can be applied at three levels: immediate, deliberate and detailed [11: Chapter 2, Annex B]. The immediate application involves a rapid appreciation process

usually without paper records, while the deliberate and detailed ones require more thorough and formal documented planning. Furthermore, there are important human dimensions of risk management related to risk perception. Individual, group and organisational risk perceptions emerge within a broad range of inter-related factors influencing the risk management process, details are given in Chapter 3.

Chapter 4 informs the practical application of risk management. The focus has to be on risk identification and risk treatment but complemented by considering risk benefits against risk costs. It is also essential to integrate risk management into all aspects of training. This will provide the solid foundation for implementing risk management into combat operations environments. At the end, Chapter 4 describes an operational case study as an example of risk management in action. The following two annexes deal with the application of risk management within the MAP. It appears that there is a logical correspondence between the steps of both processes. However, not all MAP steps have a direct risk management analogue.

4.2.5 ADF Aviation Risk Management – DI(G) OPS 40-2

This Defence Instruction (General) [14] was issued in July 2001. Its purpose is to provide the policy for the implementation of risk management applied to the Australian Defence Force (ADF) aviation operations. The policy is based on AS/NZS 4360:1999 and facilitates aviation risk management (AVRM) in a joint environment. AVRM offers a systematic, logical approach to identifying, assessing and treating risks to ADF aviation resources and missions. It supports operational decision making in order to enhance combat power and readiness while reducing the risk of loss and damage to personnel and equipment.

AVRM is an essential element of aviation operations management. In different conditions ranging from war to peace, commanders have to determine the acceptable level of risk by evaluating what it takes to achieve a mission against the nature of the risks involved. Three principles constitute the basis for a successful AVRM: avoid unnecessary risk; accept risk if benefits outweigh costs; and make risk related decisions at the appropriate level. Effective AVRM means also achieving the objectives while residual risks remain at acceptable levels. Despite the fact that military flying is considered more dangerous than civilian flying, it must not lead to accepting unnecessary risks in aviation operations.

The success of AVRM is based on an effective risk management culture throughout the ADF. It has to be integrated into the existing organisational and airworthiness framework. Risk management has to be employed at all levels of aviation operations management. Its application in planning and policy considerations makes it a part of the framework of orders and directives and ensures compliance. AVRM adds also to the Joint Appreciation Process. A fundamental feature of effectively applied AVRM is the capacity of commanders to make judgements and manage risks within their delegated authority limits.

Following strictly AS/NZS 4360:1999, the AVRM process exhibits the six steps of the generic risk management one. DI(G) OPS 40-2 only mentions a range of tools, techniques and procedures available to assist commanders in implementing the process, without providing a list of them or links to them. Annex A represents a glossary of the most important concepts and the source of each definition.

The instruction finishes with a list of related publications. It includes ABR 5147 – RAN Aviation Safety Manual where chapter 4 discusses briefly risk management, ABR 5150 – Naval Aviation Instructions, LWP-Aviation 1-3 – Army Aviation Mission Risk Management, and CA Directive 2/98 – Army Risk Management. A directive for RAAF Aviation Risk Management was referenced as still to be issued.

4.2.6 RAAF Aviation Risk Management – DI(AF) OPS 1-19

The Royal Australian Air Force Aviation Risk Management [19] is a new Defence Instruction (Air Force) Operational and was issued in November 2002. It identifies AVRM as the adaptation of AS/NZS 4360:1999 in the context of aviation operations as described by DI(G) OPS 40-2 [14]. It deals with the implementation of AVRM throughout the RAAF. AVRM has to be applied to the management of RAAF flying operations and flying activities, and even air traffic control (ATC) and air defence – ground environment (ADGE). This instruction does not cover risk management for aviation engineering design and maintenance, which are treated in several airworthiness manuals. In comparison with the previous one, DI(AF) OPS 1-19 provides in expanded form the philosophy, the principles and the process of AVRM including documentation (reports and risk register). The application of and the responsibilities in relation to aviation risk management are also described in more detail. For example, AVRM is to be used in:

- Tasks or flights;
- Operations, exercises and deployments;
- Development of operational concepts, doctrine and tactics;
- Introduction and operational evaluation of new equipment, procedures and organisational structures;
- Aviation command and operational airworthiness management;
- Amendments to systems, publications and procedures.

The section on responsibilities covers the AVRM personnel implementation issues, audit and review, training and general policy review. The instruction ends with a list of related publications similar to the one in DI(G) OPS 40-2 [14].

The four annexes attached to DI(AF) OPS 1-19 follow very closely AS/NZS 4360:1999 [49] within the specific RAAF context. Annex A contains the definitions and their sources for the major risk management concepts. Annex B describes in detail the aviation risk management process, which replicates the generic one from the Standard. Annex C, entitled Risk Analysis, actually presents the RAAF versions of the levels of risk, consequence and likelihood. They are expressed in the form of a set of qualitative

descriptions. The risk levels are extreme, very high, high, medium, and low. The likelihood is classified as likely, probable, possible, improbable, and rare. The consequences may be catastrophic, critical, major, moderate, and minor. Risk levels and consequences are described in terms indicating the significance of the adverse effects. They are further subclassified into dimensions of capability, safety, mission, and public image/morale. Here, the risk level matrix contains no repetitions of terms – the risk level may be medium, while the consequence may be moderate and the likelihood, possible. Annex D is a template for a risk management plan.

4.2.7 Defence Safety Publications

Defence Safety Manual (SAFETYMAN)

The first volumes of the first edition of the Defence Safety Manual [21] were published in 2002, and volume 3 was published in March 2004. SAFETYMAN reflects the commitment within the ADO that safe workplaces must be provided to all Defence personnel – uniformed, civilian, contractors and visitors. This manual has to be a comprehensive reference source for all matters related to safety. It incorporates and supersedes a number of existing documents, e.g. OHSMAN, DOHSMAN, Australian Army Manual of OH&S (3rd Ed.) and some DI(G) PERS. The Defence Safety Management Agency (DSMA) has the coordinating role for the production and continual improvement and applicability of SAFETYMAN. The Manual will consist of several volumes: General, Military, Defence Aviation Safety, and Group Specific.

Chapter 7 of Volume 1 (General) Part 1 (Occupational Health and Safety Management) deals with managing the safety risks within the ADO. It contains the policy of Defence on Safety Risk Management (SRM), which has been developed in consultation with Enterprise Risk Management. The SRM Policy provides guidance on the aim, procedures and responsibilities for safety risk management starting with the Secretary of Defence and CDF and cascading downwards to group executives, commanders, supervisors and employees. Chapter 7 also mentions the responsibility of DSMA for the development, review and update of a handbook "Guidelines for Managing Safety Risks" within the ADO. Chapter 7 of Volume 3 deals specifically with aviation risk management.

According to the SRM Policy, Safety Risk Management in Defence is consistent with the legal "duty of care" and is based on the AS/NZS 4360:1999.

NAVSAFE Manual – Navy Safety Management (ABR 6303)

This is the third edition of the NAVSAFE Manual [22] on Navy Safety Management. It was issued for use by the Royal Australian Navy (RAN) in early 2002. The Manual describes the safety framework adopted throughout the RAN and contains the Navy Safety Policy as a foreword. It identifies the Navy Certification, Safety and Acceptance Agency as responsible for the integrity and effectiveness of the safety management framework. The Policy states Navy's "duty of care" to all military and civilian employees, reservists,

cadets, visitors and contractors. It also commends the use of Operational Risk Management (ORM) as the means for establishing the balance between operations and safety.

The NAVSAFE system has to result in "lowering the risks of accidents and dangerous occurrences". It will be incorporated in the line management structure to secure its implementation according to Chapter 1 of the Manual. Annex A summarises the NAVSAFE principles and Annex B exhibits a flow chart of the system. The principal components of the NAVSAFE system are described in the subsequent chapters.

Chapter 5 deals with hazard and risk management within Navy's safety framework. The two major references are AS/NZS 4360:1999 *Risk Management* and AS/NZS 4804:1997 *Occupational Health and Safety Management Systems – General Guidelines on Principles, Systems and Supporting Techniques*. A brief description is provided of the risk management process and its elements. A point is made of the inconsistent application of up-to-date risk terminology and the adoption of AS/NZS 4360:1999 by NAVSAFE. Annex C and Annex D to Chapter 5 contain the necessary information to help avoid the confusions.

The RAN functions in a specific inherently dangerous environment not encountered by the other Services. ORM is a process of handling risk associated with military operations. It is based on principles used in higher risk level situations and procedures are streamlined and incorporated in an operational environment. The aim of ORM is to manage risk and not to eliminate it. Annex B to Chapter 5 provides specific guidance on risk control measures adopted by Navy, and called "Hierarchy of Controls"(See also Section 3.2.3). This is a structured process securing the most effective treatment possible in the circumstances. The Hierarchy of Controls starts with elimination, going through to substitution, engineering controls, administrative controls, and personal protective equipment (PPE) in decreasing order of effectiveness.

4.2.8 Other Defence Documents Related to Risk Management

DIS Business Rule 16 – Risk Management

Defence's Information Systems Division (ISD) belongs to the Corporate Services and Infrastructure Group (CSIG). The Division's BR 16 (at present under review) provides general guidance on risk management and its implementation to everyday business. It is dated October 1999 and uses the earlier version AS/NZS 4360:1995 and/or document(s) based on it. In essence it prescribes the adoption of risk management as part of any normal and routine activities, including projects and contracts. Annex A deals with the potential impact of internal and external risks, and the steps in the risk management process. A detailed description of each step is given in the form of a flow chart. Annex B provides a summary of approaches to the following categories: uncertainties and constraints; what can go wrong; potential consequences; and what to do. They are also classified with respect to the main activity fields: management; schedule; finance; technology; and contracts.

Work Instruction 2.1.3 Risk Analysis

WI 2.1.3 was issued in September 2002 and based on AS/NZS 4360:1999 and the Defence Risk Management Policy. It prescribes risk management to be integrated into the business planning process and a brief description of the procedure is given. The main tool of help is a template of the risk summary table, which comprises the risk level matrix, the bearer of responsibility and the treatment strategy.

Other documents

There are many other documents in Defence related to risk management. Some of them exist as hard copies, others in electronic form only. A list of these publications, without being exhaustive, includes:

- NASPO: SAFETY – Risk Management Philosophy
- Risk Analysis – Appendix 1 to CSP Practice Note 6
- MNC.G3.A – Manage the Risk Control System

4.2.9 Further Comments and Remarks

No military activities, operations and/or training are risk-free. Defence has the legal and moral obligation to prepare its personnel to operate and/or exercise within risk level limits that meet legal, military and social expectations. Risk management can be implemented in both individual and collective training environments. But the consequences of failing to apply it to collective training are rather more significant.

Nowadays military activities grow in complexity at a rapid rate and the increasing need for greater realism in training is an obvious trend. Hence, personnel must acquire the necessary skills in an atmosphere of elevated risk level, which leads to the need for an improved risk management framework in Defence.

An effective risk management framework must be based on a comprehensive, systematic and coordinated approach and on a culture recognising risk management as everyone's responsibility as a characteristic of the way of doing things. Recent activities in the ADO provide evidence that the process of adopting a unified Defence-wide approach to risk management has progressed significantly. Table 5 reflects the status quo and exhibits some minor differences.

The Guide on risk analysis for technological systems [48] is especially important since it provides the link with the international standard and because of its wide application in risk analysis of technological systems in Defence. The Chief of Army Directive 2/98 – Army Risk Management and TIB 83 Risk Management are based on the previous version of AS/NZS 4360 and is need of urgent overhaul. The other documents have already adopted the AS/NZS 4360:1999 standard in full.

Table 5: Comparison of Risk Management Processes in ADO

Step No.	AS/NZS 4360:1999 & DERM in detail	AS/NZS 3911:1998 Risk Analysis of Technological Systems & IEC 60300-3-9:1995	CA 2/98 Directive & AS/NZS 4360:1995	CSLCMM AVRM DPPM SAFETYMAN
1	**Establish context** (2.3.1) Strategic context Organisational context Risk management context	Scope definition	Task context analysis	Establish Context
2	**Identify risk** (2.3.2) What can happen? How and why can it happen?	Hazard identification What can go wrong? How likely is this to happen? What are the Consequences?	Risk Identifying	Identify Risk
3	**Assess risk** (2.3.3 & 2.3.4) Analyse risk Determine likelihood Determine consequences Estimate level of risk Evaluate risk Compare against criteria Set risk priorities Decide whether to accept risk	Risk estimation Frequency analysis Consequence analysis Risk calculations Risk evaluation Tolerability decisions	Risk Analysis Risk assessing and prioritising	Assess Risk
4	**Treat risk** (2.3.5) Identify treatment options Assess treatment options Prepare treatment plans Implement treatment plans	Analysis of options Risk reduction/control Decision making Implementation	Risk control	Treat Risk
5	**Monitor & review** (2.3.6) Monitor risk Review risk	Monitoring Verification and update	Monitor and review	Monitor and review
6	**Communicate & consult** (2.3.7) Communicate between stakeholders Consult all participants	Report		Communicate and consult
	Document Keep records at each step	Documentation		Document

5. Risk Management Approaches and Practices in the Other ABCA Countries

Australia has been a member of the American, British, Canadian and Australian Armies' Standardization Program (ABCA Program) since 1963. Although there are four countries officially in the ABCA Program, New Zealand has been an associate member through Australia since 1965. "The mission of the ABCA Program is to ensure that the ABCA Armies achieve levels of standardisation necessary for two or more ABCA Armies to operate effectively together within a coalition and in a joint environment … now and into the future." It has materialised in over 1000 documents known as Quadripartite Standardisation Agreements (QSTAG) and Quadripartite Advisory Publications (QAP). These documents have played an important role in the operations conducted by the Armies since the end of WWII during both conflicts and peacekeeping.

At the time of writing this report, QSTAG 1043 Edition 1, Individual Protective Equipment and Risk Management in an NBC Environment [46] has been the only publication related to risk management to be discovered in the databases of the ABCA Program. This Agreement dates back to the 11th meeting of the Quadripartite Working Group on NBCD held in the United Kingdom in April 1993. Although it recognises the importance of adopting a risk management philosophy for some activities in a nuclear, biological or chemical environment, it only identifies the factors leading to the introduction of individual protective equipment. However, QSTAG 1043/1 provides general recommendations on the implementation of risk management in the NBC environment.

The above comments naturally lead to the conclusion that a review of the risk management practices and publications in the ABCA Program has to proceed on an individual basis, country by country. The Australian contribution was discussed in Chapter 4.

5.1 US Department of Defense Publications on Risk Management

In 1996, in the US Department of Defense (US DoD), a Risk Management Working Group was established [47]. It included representatives from the Office of Secretary of Defense, the Military Services, and agencies involved in systems acquisition. The Group reviewed relevant US DoD Directives, how the Services managed risk, how industry applied risk management, and the status of education and training on risk management. The conclusions of the investigation include:

- Services have different approaches to risk management;
- There is no single comprehensive approach although each one has its strengths;
- A consolidation of the approaches may lead to a better risk management in the DoD.

At present some of the findings of the Group still hold, which naturally leads to a variety of policies, instructions, manuals and other publications. Some of these documents are reviewed in this Chapter.

5.1.1 DSMC Risk Management Guide

Risk Management: Concepts and Guidance [24] was published by Defense Systems Management College in 1989. It is an updated version of the 1983 DSMC publication *Risk Assessment Techniques*. This DSMC Guide expands the concept of risk management. It goes beyond management of technical risk and recognises also management of cost risk, schedule risk, programmatic risk and supportability risk. A holistic view on risk is adopted, so that risk is dealt with as a single entity consisting of the five aforementioned facets. But the Guide is limited only to risk management in the acquisition process. However, it makes the point that risk management is an essential part of project management altogether.

Chapters 1 and 2 provide an introduction to the Guide describing the history of risk management in the US Department of Defense, and discussing the need for risk management and the formal, systematic and disciplined manner of its application. Chapter 3 defines risk as "the probability of an undesirable event occurring and the significance of the consequence of the occurrence", i.e. the "severity of consequence if the event should occur". Further, the level of risk is introduced as a "subjective judgement concerning the combination of the first two". Here, the risk facets are considered and hence risks are classified, usually according to source of risk. Chapter 4 provides a description of the risk management process. It starts with a planning stage which sets out the requirements and continues with assessment, analysis and handling which in AS/NZS 4360:1999 terms correspond to risk identification and establishment of evaluation criteria, risk assessment (i.e. risk analysis and risk evaluation), and risk treatment. Chapter 5 discusses techniques applicable in the risk management process including expert interviews, lessons learned studies, network analysis, life cycle cost modelling, watch listing, and performance tracking. Chapter 6 summarises the information from all previous chapters in light of the implementation issues when executing the risk management program. Chapter 7 deals with the risk management problems when contracting. Risk management has to be an essential part of the Request for Proposal (RFP). The RFP has to include a risk management plan and a risk assessment report. Contracts have to include deliverables containing information related to risk. Chapter 8 discusses the future of risk management. It acknowledges the existence of the necessary body of knowledge, tools and required computing power. The need for a move towards a fundamental culture change with respect to risk is identified. It has to be based on standardised terminology, procedures and techniques. The results have to be presented in plain English, rather than mathematical statements and quantifying expert judgements.

The DSMC Guide has eight appendices. Appendix A provides an abbreviated list of the risk sources including technical, programmatic, and supportability ones. Appendix B reflects the status of the bibliography on risk management at the time of publication.

Appendix C contains excerpts on risk from the US DoD Acquisition Policy. A list of acronyms and a glossary form Appendix D. Appendix E serves as a short primer on probability theory. Appendix F discusses how to convert expert judgement into quantitative form, then describes the following techniques: diagrammatic, direct, betting, modified Churchman/Ackoff, and the Delphi approach. Appendix G treats some of the peculiarities that are part of software development, and points out the advantage of establishing a formal Software Quality Assurance Program. Appendix H is a subject index.

The DSMC Guide provides a solid basis for assessing and managing program risk. However, despite its availability and the existence of a number of US DoD directives, the risk management process has been inadequately implemented in some defence programs [6]. This article lists some common deficiencies observed in recent practices and discusses also in considerable detail how risk management has been applied in one DoD program. At the end, the conclusion emerges that the process must be embraced by senior leadership and conducted in an unbiased manner. Moreover, the deficiencies usually relate to cognitive issues including reliance on limited data, fitting ambiguous evidence into predispositions, disregarding information that conflicts with personal beliefs, etc. These issues are not confined to the defence area; they describe just a few of the challenges [37] facing society in general, when dealing for example with health, safety, or environmental risks. There are complex psychological, social, cultural, and political forces that dictate success and failure in risk management. On the other hand, risk management may be used in the specific area of systems engineering as applied to US DoD acquisition problems as described by [25].

5.1.2 Army Field Manual in Risk Management

Field Manual No. 100-14 (FM 100-14) *Risk Management* [9] was released by the US Department of the Army in April 1998. It applies to all US Army military and civilian personnel employed in the wide range of US Army operations. The manual explains the principles, procedures and responsibilities associated with the successful implementation of the risk management process. It has to be the basis for developing a framework to make risk management a routine part of planning, preparing, and executing operational missions and everyday tasks. Despite being primarily focused on operations, the Manual has to apply to all activities.

Initially risk management was used in the area of safety of personnel and other resources. The US Army introduced risk management into training, operations and acquisition in the late 1980s. Later, since the early 1990s it has had to be integrated into all US Army activities, and into each individual's behaviour both on and off duty. Thus, risk management has become an element of the decision-making process at all levels from commanders to soldiers and other staff. Also according to [44], risk management has to be an essential element of tactical decision-making.

Chapter 1 deals with the fundamentals of risk management described as basic concepts, background, principles, applicability and constraints. According to the Manual "risk

management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risks costs with mission benefits". Further, it identifies the proficiency in implementing risk management as critical to preserving combat power and resources. The data provided shows that the US Army has had more accidental casualties than casualties from enemy action during WWII, Korea, Vietnam, and Gulf wars. The principles of a risk management framework are:

- Integrating risk management into mission planning, preparation, and execution;
- Making risk decisions at the appropriate level in the chain of command; and
- Accepting no unnecessary risk.

Risk management may be applied to Army development, fielding and employment. Development includes force design, manpower allocation, training, combat, and materiel developments and battle laboratories. Fielding considerations deal with personnel assignments, sustainment and logistics, training, and base operations. Employment concerns relate to force protection and deployment, operations, and redeployment. Risk management may be restricted by legal constraints.

Chapter 2 describes in detail the risk management process. It starts with an overview of the five-step procedure: identify hazards, assess hazards to determine risks, develop controls and make risk decisions, implement controls, and supervise and evaluate. However, FM 100-40 Tactics is mentioned as providing insight into the context for the risk management application. Moreover, the correlation between the risk management steps and the military decision making tasks is discussed. Therefore, the US Army risk management process is very similar to the generic one from AS/NZS 4360:1999 despite some terminological differences. The Manual [9] also divides the risks into tactical and accident ones, where the former type is associated with presence of the enemy, while the latter includes the remaining risks even those related to friendly fire. The Appendix to FM 100-14 provides examples of risk management tools suitable for different decision-making levels. It also shows how risk management may be integrated into a mission-training plan. The chapter ends with the warning about the pitfalls of implementing the tools alone, and out of context.

Chapter 3 discusses the moral and ethical implications of risk management. It identifies essential responsibilities for all levels: commanders, leaders, soldiers, individuals, so that the process can be effectively integrated within the US Army. These are even more important when incorporating risk in training and operations. The Manual points out that the effectiveness of risk management is ultimately linked to combat readiness.

5.1.3 Risk Management: Multiservice Tactics, Techniques, Procedures

This publication [2] covers risk management as applicable to the US joint task force (JTF) and all service staffs. It was prepared by the Air Land Sea Application (ALSA) Center and released in February 2001 simultaneously as FM 3-100.12, NCRP 5-12.1C, NTTP 5-03.5 and AFTTP(I) 3-2.34. *Risk Management: Multiservice Tactics, Techniques and Procedures*

(RM:MSTTP) discusses the risk management process and its similarities and differences as implemented by each US Service. It has to serve as a multi-service reference on risk management and as a source document for developing joint and single-service manuals, regulations, instructions, etc. This publication targets specifically JTS headquarters staff.

RM:MSTTP contains the risk management multi-service tactics, techniques, and procedures used at tactical level in the planning and execution of joint operations. It introduces the fundamentals of risk management and applies to all force elements engaged in any force protection activity. This manual enables commanders and staffs to conduct effective risk management during planning, preparation, and execution of operations.

Chapter 1 describes risk management as "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 management is to help reduce the risk of threats to the force, where 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". Traditionally, each Service implements a relatively different risk management process. This manual provides a generic unified approach as the basis for managing risk from a common perspective. The process comprises the following phases:

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

Risk management has to be applied in sequence, because each phase is a building block for the next one. Moreover, all phases are important and require adequate time allocation to ensure maintaining balance in the process. Naturally, it is a continuous process and has to be implemented as a cycle. Effective risk management necessitates the full involvement of personnel actually exposed to the risks.

Chapter 2 describes the risk management process and how it may be applied to planning and execution of operations. It identifies pitfalls, types of controls, and feedback requirements. Instead of hazards or risks one discusses threats, always with the mission in focus, i.e. in the context of the big picture. Two common situation analysis models are provided. They are the mission, enemy, terrain and weather, troops and support available, time (METT-T) model and the man, machine, media, management, mission (5-M) model.

Chapter 3 explores the relationship between risk management and chain of command. It describes the necessity of leader involvement for the successful implementation of an effective risk management process; its integration into all aspects of the training and operational activities; and the responsibilities of commanders, leaders, staffs, and individuals. Reliable feedback is secured via constant review of the risk management process.

Appendix A contains some risk management tools including a risk management worksheet (Annex A), a force protection priority matrix (Annex B), a force protection tasks table (Annex C), a risk assessment matrix (Annex D), and a risk control options planning matrix (Annex E). Here, the risk severity categories, probability definitions and risk assessment levels contain no ambiguities. However, the normal terminological differences with DRMF are apparent. Appendix B deals with the force protection working group (FPWG), its role, composition and responsibilities. RM:MSTTP ends with lists of references, acronyms, terms and definitions.

5.1.4 Risk Management Guide for DoD Acquisition

The fifth edition of the *Risk Management Guide for DoD Acquisition* [26] was published by the US Defense Acquisition University in June 2002. It has to serve as a reference book for acquisition professionals and project management offices. This Guide may be used also as a classroom instruction aid. A more advanced treatment of the subject accompanied by numerous examples is presented in [5].

Chapter 1 states that any acquisition process has to be designed in a way to allow risks to be managed from conception to delivery. Risks are inherent to any project and they have to be identified and treated accordingly. Risk management has abandoned the view of risk as something to be avoided.

Chapter 2 deals with the concepts of risk and risk management:

- "Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints and has two components: (1) the probability/likelihood of failing to achieve a particular outcome, and (2) the consequences/impacts of failing to achieve that outcome."
- "Risk management is the act or practice of dealing with risk. It includes planning for risk, assessing (identifying and analysing) risk areas, developing risk-handling options, monitoring risks to determine how risks have changed, and documenting the overall risk management program."

The scope of the definition of risk reflects the relatively narrow acquisition project context. The steps in the risk management process roughly correspond to the ones from AS/NZS 4360:1999. The next sections provide a thorough description of the process with illustrations from the DoD acquisition area. The differences in terminology are apparent but not that significant. The characteristics of the acquisition risks are specified in this chapter as well.

Chapter 3 examines the relationship between risk management and the DoD acquisition process. It has to be an integral part of the overall management process. It has to be included in the Acquisition Plan at the earliest possible stage.

Chapter 4 treats risk management as viewed by program (project) management. It concentrates on practical issues, for example risk management design options, organisational structure, contractor risk management, reporting and information systems, and risk management training.

Chapter 5 provides up-to-date information on a number of techniques successfully used in the US DoD. Many of them may be used in sound management and systems engineering in general. Several tools may support a specific component of the risk management process, i.e. planning, assessing, handling, monitoring, and documenting. There is no tool to cover all facets of risk management. Moreover, the Guide recommends assessing a technique against the needs and the resources, and if necessary tailoring it accordingly. The following groups of techniques are listed:

- Risk planning technique;
- Risk assessment techniques including Product (WBS) Risk Assessment, Process Risk Assessment, Program Documentation Evaluation Risk Identification, Threat and Requirements Risk Assessment, Cost Risk Assessment, Quantified Schedule Risk Assessment, Expert Interviews, Analogy Comparison/Lessons Learned Studies
- Risk prioritisation technique including risk aggregation;
- Risk handling techniques including Risk Controls, Risk Avoidance, Risk Assumption, Risk Transfer;
- Risk monitoring techniques including Earned Value Management, Technical Performance Management, Integrated Planning and Scheduling, Watch List, Reports, Management Indicator System;
- Risk management information systems and documentation including Risk Information Form, Risk Assessment Report, Risk Handling Documentation, Risk Monitoring Documentation, Database Management System.

Risk management for software development is conducted essentially in the same way as for any project except it requires some specific methodologies. Three of them are described in the Guide: Software Risk Evaluation, Boehm's Software Risk Management Method, and Best Practices Initiative Risk Management Method.

The Guide includes five appendices that can serve as a source of reference, examples and backup material. Appendix A treats the key documents of DoD on risk management for acquisition. It contains verbatim extracts of sections from directives, instructions and manuals. Appendix B contains generic risk management plans with templates for the main activities as annexes. Appendix C is a list of acronyms. The next Appendix D describes the techniques used to convert qualitative estimates into quantitative probability distributions, i.e. techniques used to quantify expert judgement. Appendix E contains the bibliography.

5.2 British Ministry of Defence Publications on Risk Management

The British Standard (BS) 4778 defines risk management as "the process whereby decisions are made to accept a known risk and/or the implementation of actions to reduce the consequences or probability of occurrence". Although the concept is quite general, there is no hint to employing risk management to explore new options. Naturally, the usual areas of Defence application are safety and acquisition. This fact is reflected in the available publications on risk management. Some of them are summarised next.

5.2.1 Defence Standard on Safety Management for Defence Systems

The UK Ministry of Defence (UK MOD) published the second issue of the *Defence Standard 00-56* (Def Stan 00-56) *Safety Management Requirements for Defence Systems Part 1: Requirements* [42] and *Part 2: Guidance* [43] in December 1996. It supersedes Issue 1 from April 1991. The Standard claims to have taken into account international standards and supporting research and development. Part 1 deals with the requirements for safety management, including hazard analysis and safety assessment. Part 2 provides information and guidance on implementation of the requirements. Def Stan 00-56 has been designed also for use by contractors to meet their responsibilities for safety.

Part 1 of the Standard defines the safety program requirements for defence systems, including procedures, analysis techniques and verification activities. The aim is to minimise the potential for a system to be acquired for service without the necessary safety, although Def Stan 00-56 has to apply to the entire project lifecycle from initiation to disposal. Moreover, it does not cover project risk management, i.e. risks to cost and schedule. However, the Standard considers safety (risk) management as an integral part of any defence equipment procurement. Here likelihood is referred to as accident frequency and is classified as incredible, improbable, remote, occasional, probable and frequent. Consequence or impact is called accident severity and has four categories: negligible, marginal, critical and catastrophic. They result in a risk classification table with classes A, B, C, and D (intolerable, undesirable, to decreasing tolerable levels). Def Stan 00-56 introduces also the concept of safety integrity as an indicator of the required level (S1 to S4) of protection against systematic failure.

Part 2 of the Standard contains generic information and guidance applicable in accordance with the requirements from Part 1. The examples of methods and techniques provided are only for illustration purposes and no recommendation for particular suitability is implied. This part also deals in detail with the general principles of safety management and the associated documentation including plans and logs. A significant part of the Standard is devoted to system safety analysis. The study of hazards has to start with Preliminary Hazard Listing and Preliminary Hazard Analysis (techniques used: HAZOPS, FMECA, FTA) and leads to System Hazard Analysis. Functional analysis, zonal analysis, component failure analysis, operating and support hazard analysis, and occupational health hazard analysis may all be among the activities comprising the System Hazard Analysis. Here risk estimation if necessary is included in the investigation. Part 2 ends

with a proposed generic work program on project life cycle. There are annexes containing various support materials, e.g. checklists and tables.

5.2.2 Defence Acquisition Paper

The UK *Ministry of Defence Policy Paper No. 4* on Defence Acquisition [44] was published in December 2001. It builds on some recent programs including Public Private Partnerships, Smart Procurement, Smart Acquisition, and Prime Contracting. For the UK MOD the concept acquisition covers the whole process from establishing the requirement for new equipment, its procurement, through-life support, to disposal or decommissioning. It is based on a number of key principles:

- Acquiring against output-based specifications, rather than the traditional input-based approach;
- A whole-life approach to achieving value for money, rather than considering only initial purchase costs;
- Clarification of the respective roles of internal "customer" and "supplier" organisations; and
- Application of best practice from civil and private sectors.

Unfortunately, among these principles there is no explicit indication even for a potential role of risk management. It is common knowledge, that a broad range of uncertainties and corresponding risks influences the acquisition of new equipment, facility or service. Hence, any acquisition publication is bound to contain at least references to risk management, if not a section or a whole chapter.

However, one of the objectives of the Smart Acquisition Program is to acquire capabilities "progressively, at lower risk, and with the right balance between military effectiveness, time, and whole-life costs". Moreover, if requirements change during a project, the risks associated with them can be reduced via "Incremental Acquisition", i.e. an initially achieved baseline capability can be upgraded in a planned manner to incorporate changes in technology or lessons learned. Smart Acquisition also prescribes reduction of risk at the early stages before binding constraints on performance, cost and time are fixed.

Private Finance Initiative is considered a cornerstone of the Public Private Partnerships Program. It is supposed to create for the UK MOD the possibility of transferring risks to the private sector. When designing a contract, the associated risks have to be understood and well defined. Each area of risk has to be allocated to the party best able to manage it. By implementing a process called "due diligence", the finance providers have to test the assumptions behind the contractor's business plan and make sure the question of risk has been properly addressed.

5.2.3 Safety Management for Ordnance Munitions and Explosives

The Operating Procedures [45] of the Safety Management System for Ordnance, Munitions and Explosives (OME SMS OP) was issued in January 2002. It recommends the safety of an OME system to be considered throughout its entire life. Further, it also ties the level of effort and resources applied to the management of OME safety to the complexity of the system and the level of risk involved. Risk management is to be conducted according to Def Stan 00-56 [42, 43], which is based on the BS 4778.

It is UK MOD policy, that any risk related to an OME system is to be reduced to a level As Low As Reasonably Practicable (ALARP), or even totally eliminated through design. This requires a comprehensive risk management program. There are three activities in such a program according to OME SMS OP: hazard identification; risk assessment; and risk control. They are identified and scheduled in a Safety Program for the OME system, which has to be linked to the Safety Management Plan.

The Operating Procedures contain descriptions of different techniques employed during the risk management activities. The techniques for hazard identification include: preliminary hazards analysis; sub-systems hazards analysis; system hazards analysis; operating and support hazard analysis; and software hazard analysis. The risk assessment goes through three distinct phases:

- Accident Severity Categorization (Catastrophic, Critical, Marginal, Negligible)
- Accident Frequency Assessment (Frequent, Probable, Occasional, Remote, Improbable, Incredible)
- Risk Classification (Class A, B, C, and D).

Quantitative assessment may involve the use of Fault Tree Analysis, Event Tree Analysis and Reliability Analysis. Qualitative assessment may be based on expert judgement, research, evaluation of historical data, etc. A common table of both types of probabilities (verbal or numerical) is provided. Further, OME SMS OP links the risk control measures to the activities and stages of the life cycle of the system.

The Operating Procedures contain lots of templates and other generic documents for case reporting, auditing and reviewing.

5.2.4 Guide to Risk by the Scottish Accounts Commission

Shorten the Odds: A Guide to Understanding and Managing Risk [1] was issued by the Accounts Commission for Scotland in July 1999. It promotes the concept and good practices of effective risk management. The paper also outlines the roles and responsibilities of the major stakeholders in the process of developing and implementing an organisation-wide systematic risk management. A range of tools, techniques and templates included in the Guide support this approach.

Shorten the Odds provides generic guidance on the strategic and operational aspects of risk management. It goes beyond the traditional areas of insurance or health and safety. Yet it fails to quote BS 4778 as the major source of reference on risk management. However, the Guide describes risk management as "the process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them and/or responding to them. … It informs judgements about the appropriateness and effectiveness of policy options or service delivery methods. As such, it is integral to both strategic planning and operational management."

The risk management cycle comprises four stages: risk identification; risk analysis; risk control; and risk monitoring. There is no context establishing stage and risk analysis and risk control stand for risk assessment and risk treatment respectively. Further, hazards and associated risks are sub-divided into two categories: strategic and operational. Strategic risks may be political, economic, social, technological, legislative, environmental, etc. Operational risks may include professional, financial, legal, physical, and contractual. The Guide identifies the usual two criteria to be used to determine the scale (level) of risk associated with a specific hazard: the likelihood of the risk event occurring; and the severity of its consequences.

Effective risk management has to result in a variety of benefits to all parties involved. It may lead to improved strategic, operational, financial and customer management. But the delivery of effective risk management is to be based on a cyclical approach including strategy development, strategy implementation and strategy review. The development phase has to agree with the clearly identified Specific, Measurable, Agreed (or Action-oriented), Realistic, Timetabled (SMART) objectives.

The tools and techniques recommended by the Guide include group assessment, brainstorming, SWOT and PESTLE analysis, risk charting, risk checklists, site inspections, etc. Here SWOT stands for Strengths, Weaknesses, Opportunities and Threats, and PESTLE stands for Political, Economic, Social, Technological, Legislative and Environmental. The Guide also proposes maintaining information in a risk management portfolio with its six phases: gather risk experience information, identify current risks, assess likely frequency and consequences, identify control actions, implement actions, and monitor and review outcomes, comes very close to the six-step risk management procedure of AS/NZS 4360:1999.

5.3 Canadian Department of National Defence on Risk Management

Risk management is neither new to the Canadian Department of National Defence (DND), nor to the Canadian Forces (CF). An assessment by the Vice Chief of the Defence Staff (VCDS) posted on the web (D-NET) identifies the existence of a "relatively mature risk smart culture" in the management practices of the Defence institution in Canada. Risk management is classified as a constant factor "in the planning and execution of any modern defence practices". A continuous risk management process is the vehicle to taking

full advantage of the resources available, optimising the situation, making the most appropriate decisions possible and achieving the planned objectives.

The DND and CF have always applied the elements of a comprehensive risk management approach in their everyday activities. Identification and mitigation of risk in operations and even in the planning, support and generation of forces for operations have been of high priority. Activities not directly linked to military operations also have employed risk management. Moreover, there has been a significant improvement after the endorsement of a top-down methodology by Strategy 2020.

The Defence Management System (DMS) has to serve as the background for, and support the introduction and implementation of an integrated risk management framework in Defence. It has to be based on the existing "strong risk smart foundation" and function within the larger DND management framework. Although there is enough appeal in, and ground for the creation of a separate new framework, any expansion of the risk management capacity may be accommodated without adding unnecessary processes and institutions. However, improvements may be necessary at subordinate levels once the integrated strategic level is established.

5.3.1 Integrated Strategic Risk Management in Defence

Integrated Strategic Risk Management in Defence [27] was issued by the Director Strategic Planning Coordination of the Canadian DND and released by the VCDS in April 2001. This document is the first one to define corporate strategic risk and how it has to be managed in the DND. It is viewed as complimentary to the Integrated Risk Management Framework prepared by the Treasury Board, which acts in its role as the Management Board for the Government of Canada. The aim of this document is to describe and formalise the components of an integrated strategic risk management framework in the Canadian Defence.

The framework comprises four elements: developing the corporate risk profile; establishing an integrated risk management function; practicing integrated risk management; and ensuring continuous risk management learning. However, as already stated, the DND possesses considerable risk management experience, therefore the differences between any existing or emerging processes and the Treasury Board have to be considered. A description of the elements follows:

- **"Developing the risk profile at the corporate level** is intended to examine both threats and opportunities in the context of an organization's mandate, objectives and available resources." This element reflects the development of awareness of the range of risks in Defence and understanding of the risk management capacity and capability.
- "**Establishing an integrated risk management function** means setting up the corporate 'infrastructure' for risk management which is designed to enhance understanding and communication issues internally, to provide clear direction and senior management support." There will be no distinct risk management infrastructure

as recommended by the Treasury Board. However, operational and project risk management and integrated risk management at strategic level has to be conducted within the existing DMS.

- "**Practicing integrated risk management** builds on the results of an environmental scan and is supported by appropriate corporate infrastructure." The adoption of top-down management and decision-making on the basis of Strategy 2020 makes possible the realisation of this element. Moreover, the capability based planning framework with its tools and processes targeted at risk management can ensure an appropriate corporate infrastructure.
- "**Continuous risk management learning** is fundamental to more informed and proactive decision-making. It contributes to better risk management, strengthens organizational capacity and facilitates the integration of risk management into an organizational structure." DND will develop a comprehensive risk management learning environment based on exchanges, seminars, retreats, etc.

Further, the document considers the major elements of risk in the DND. Although they occur in other areas, they form a specific risk environment in which DND/CF operate. The elements may be listed in two categories according to the role the Department can play in the risk mitigation, namely: direct and decisive; and indirect and partial.

- Direct and decisive include: failure in operations; stewardship of defence resources; reliability of information systems, defence culture; and isolation from Canadians.
- Indirect and partial include: Government policy and direction; domestic environment; demographics; risk sharing in defence and security matters; and defence constituency.

Integrated risk management has to be incorporated within the DMS. Thus, a variety of DMS risk related elements are to become components of the risk management framework. A short list of these includes: Strategic Review, Military Assessment; Strategy 2020; Capability-Based Planning; Corporate Priority Setting; Defence Plan; Business Planning; Management Decisions. Naturally, DMS is not the only source of risk management practices. Processes associated with Ethics & Audit, Alliances, Integration, Checks & Balances, etc. may also reduce, mitigate or even prevent risk in Defence.

Annex A – Capability Based Planning deals with the mitigation of the two fundamental risks that DND/CF must treat in future planning. The first one reflects the inability of CF to accomplish the mission set for them by the Canadian Government including failure in operations or battle. The second one concerns the inability of DND/CF to deliver the required defence capability with the resources allocated.

Annex B – Project Risk Management describes the risk management support available to all project management offices (PMO) in the Canadian DND. It is offered by the Assistant Deputy Minister (Materiel) and the Directorate Materiel Acquisition and Support Program (DMASP). The sources of guidance within DMASP include: MA&S desktop; mentoring; workshops; training; standardised risk database (Risk Radar, version 1.1); and templates. The 1996 edition of 'Continuous Risk Management Guidebook' [29] published by the

Software Engineering Institute is adopted as the DND standard on Continuous Risk Management (CRM) within the PMOs. Here, the CRM process is viewed as the core of the risk management technology and includes the following phases: identify risk; analyse risk information; plan risk response; track risk indicators and actions; control risk response, and communicate risk information.

Annex C – Resource Management in DND/CF identifies the roles and responsibilities of the Vice Chief of Defence Staff (VCDS) as the senior resource manager and strategic planner and of the Assistant Deputy Minister (FinCS) as the senior financial officer of DND/CF. The specifics of risk management as related to their positions are discussed briefly.

Annex D – Legal Risk Management sets out a framework for legal risk management within DND/CF. It represents a proposal for the establishment of a comprehensive legal risk management process within the Canadian Defence. This process can be broken down into the following components: identifying issues and setting context; assessing key risk areas; measuring likelihood and impact; ranking risks; setting desired results; developing options; selecting a strategy; implementing the strategy; monitoring, evaluating and adjusting.

5.3.2 Risk Management Overview (DND - DP&M Web-Site)

Risk Management Overview [28] (February 2003 – last update used) is part of the Defence Planning and Management (DP&M) web site of the Canadian DND. DP&M is led by the Director General Strategic Planning (DGSP), who in turn reports to the Vice Chief of the Defence Staff (VCDS). The DP&M site is a "one-stop location for corporate-level Defence management information" including risk management.

The Risk Management Overview starts with the definition and purpose of risk management. The definition, which can be traced back to the Integrated Risk Management Framework in Defence and other publications, describes it as "the systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues". But the origin of this definition is the Treasury Board of Canada and its publications on risk. As far as the goal of risk management is concerned it "is to protect the Government of Canada and DND/CF by minimizing losses without overprotecting assets, balancing the costs of risk management with its benefits".

The Risk Management Overview provides two links as information sources. The first one leads to the above-discussed Integrated Strategic Risk Management in Defence. The second one connects to the Treasury Board of Canada Secretariat and two groups of documents. The Policies and Guidelines group contains 'Integrated Risk Management Framework', 'Policy on Active Monitoring' and 'Risk Management Policy'. The Publications group includes 'Annotated Bibliography for the Study on Best Practices in Risk Management, Private and Public Sectors Internationally', 'Best Practices in Risk

Management – Coordinated Conclusions from PMN and KPMG', 'Review of Canadian Best Practices in Risk Management', 'Risk, Innovation and Values – Examining the Tensions'.

The Risk Management Overview discusses the application of strategic risk management to business planning. Here, critical issues are identified, especially where there is a gap between assigned tasks and allocated resources, and the potential impact of the risks inherent in each of them. The basic risk management cycle includes the following phases: identification; assessment; response; monitoring/learning; and communication. It is imbedded in the business planning process, "depends heavily" on the type of business planning activities, and is managed through corresponding mechanisms. Further guidance on the application of risk management is provided via some additional documents:

- 'Steps in Risk Assessment' describes the procedure to be followed in managing risk in business planning. There are seven steps: understand the objective for risk management within the context of business planning; identify the risk issues with respect to the task assigned; determine the type of risk within the bigger management picture; evaluate the degree of risk using the Risk Management and Action Matrix; determine the ways and means to reduce risk including tolerance levels and action triggers; define the residual risk; and develop contingency plans to deal with the residual risk.
- Risk Management Definitions introduces the basic concepts in a formal way. "Risk is the probability that a decision or action will result in a negative or unwanted consequence, where the probability of each possible outcome is known or can be estimated." This concept is quite different from the Treasury Board one where "risk refers to the uncertainty that surrounds future events and outcomes; it is an expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives". Even more confusing is the definition of uncertainty as "the situation where the probability of each possible outcome cannot be estimated".
- The last attachment represents a risk assessment example in narrative form for each item. It relates to a decommissioning program.

5.4 Risk in Defence Equipment Selection in New Zealand

Discussion Paper 01/99 *A Review of Risk in Defence Equipment Selection* [40] provides some insight into the rationale driving defence equipment selection in New Zealand. It considers the risks inherent to the selection decision-making process and identifies corresponding moderation (treatment) options classifying even some opportunities as impractical. This paper discusses risk management options available in defence capability planning. It also investigates factors influencing the risk management process including risk likelihood estimation, risk penalties (consequences) and moderation costs. Moreover, risk moderation requires opportunities, associated timing, and methods. This publication stresses the "tacit linking of risk and capacity to moderate it".

The paper discusses a number of risks associated with military equipment, its acquisition and use. There are three tables listing risks, their consequences and corresponding treatment options. They reflect the three principal areas for risk moderation: policy; acquisition; and operational. Policy treatment options are associated with goal setting and equipment selection. In acquisition, the equipment decisions are implemented and details finalised. Any decision to get involved in military action/apply the equipment relates to the operational area and this is the time when some important potential risk moderation opportunities arise. However, with the life cycle moving from stage to stage, choices decrease in number and some consequences may be unavoidable, thus limiting the treatment options.

The paper considers some moderation approaches specific to the acquisition area. For example, FFBNW stands for Fitted For But Not With and implies that a major equipment is acquired with the capacity to have minor equipment installed on it at a later date. It may sound attractive but this option leads to some important drawbacks including higher cost, being time consuming, technical incompatibility, inability to meet an identified contingency, etc. Further examples of moderation approaches usually consider acquisition delay in part or as a whole. As a result of their application a number of the treatment options can be eliminated. The effect may be seen in the improved versions of the three aforementioned tables listing risks in acquisition.

Discussion Paper 01/99 also provides guidance on dealing with more technical points in the risk management process. It identifies the commonly used approaches to risk assessment, which does not always mean quantification. It can be relative ranking, verbal assessment, etc. Illustrative examples are given of the different types of assessments. Next, an analysis of the risk penalties (consequences) in acquisition, based on one of the previous tables, is undertaken. The possible causes and possible consequences for each penalty are investigated. Further, moderation opportunity costs are discussed in the context of planning and decision-making. Finally, risk reduction is considered by means of lowering the likelihood or the impact or by avoiding it altogether. The Paper considers two different types of undesirable events: conflict ones, and capability ones. Conflict events are linked to military presence, and capability events relate to situations where a capability is reduced to lower than adequate operational levels. Treatment strategies are formulated for all these risk situations.

5.5 Comparison of Concepts and Terminology

A risk management process is usually structured as a sequence of several basic steps or phases, usually 5 or 6. There are also additional ongoing procedures accompanying the process itself. They are mostly related to auditing, disseminating and documenting the results. The essential part of any risk management process is constant despite the existing terminological differences. Some of them do not mention the initial planning and/or context establishment although it is included implicitly as an important step. Table 6 summarises the ABCA experience in structuring a risk management process.

Table 6: Steps in a Risk Management Process

4360:1999 ADO DERM	Canadian DND	Scottish AC Shorten the Odds	UK MOD Def Stan 00-56	US DoD Acquisition	US Army US JTF
Establish the context	Setting context	Experience information	Safety requirements and plan	Risk planning	
Identify Risks	Identifying issues	Identify current risks	Hazard identification	Risk identifying	Identify hazards/ threats
Analyse Risks	Assessment Likelihood Impact	Assess likely frequency & consequence	Risk estimation	Risk analysis	Assess hazards to determine risks
Evaluate Risks	Ranking risks Setting results	Identify controls	Safety compliance assessments		Develop controls & make decisions
Treat Risks	Response	Implement controls	Corrective action	Risk handling	Implement controls
Monitor & review	Monitoring & learning	Monitor & review	Safety verification	Risk monitoring	Supervise & evaluate
Communicate & consult	Communi-cation	Gather information	Safety case construction		
Document Risk		Maintain risk portfolio	Hazard log	Document risk	

Table 7: Basic Concepts in Risk Management

CONCEPT	4360:1999 ADO,DERM	CANADA	UK	USA
Event	Incident or situation which occurs during a time interval	NA**	Significant happening in a system or its domain	Set of potential problems associated with uncertainty
Frequency	Measure of rate of occurrence of an event in a given time	NA**	NA**	NA**
Probability	Likelihood of event/outcome measured as desirables to totals ratio	Chance of occurrence	NA**	Number expressing the likelihood of occurrence of specific event
Likelihood	Qualitative description of probability or frequency	NA**	NA**	NA**

CONCEPT	4360:1999 ADO,DERM	CANADA	UK	USA
Hazard	Source of potential harm or situation with potential to cause loss	NA**	Situation or event which can cause harm or lead to an accident	Actual or potential condition leading to injury, loss, mission degradation
Consequence (Impact)	Outcome of event expressed quantitatively or qualitatively as gain, loss, injury or disadvantage	Impact like effect is a synonym for outcome (impact more direct than effect)*	NA**	NA**
Risk	Chance of something happening with impact upon objectives and measured as a combination of likelihood and consequences	Probability of decision/action resulting in a negative or unwanted consequence (expressed as likelihood and impact)	Chance that damage or adverse outcome occurring as a result of a particular hazard (combination of likelihood and severity)	Measure of potential inability to achieve objectives and has two components: probability and consequences

* Definition is unavailable in original publication [28], but link is provided to another source, i.e. the Canadian Defence Plan and its Lexicon, which is available at the time of writing at: http://www.vcds.force.gc.ca/DPOnline/Lexicon/Intro_e.asp.
** NA stands for not explicitly available in the form of definition in at least one of the reviewed publications of that category.

The differences may become very important at conceptual level. But despite the lack of definitions in some cases, and clear-cut definitions in others, the basic concepts exhibit an obvious similarity. Table 7 is provided in support of this observation.

The greatest variety in concepts is shown in the classification for likelihood of risk. The descriptors are strikingly different, as evidenced by Table 8.

The difference gap in terminology is not that wide in the case of consequence or impact levels. Table 9 summarises the most prevalent classifications. If necessary, they can include more than 5 descriptors.

Table 8: Likelihood Classification (Up to 5 levels)

4360:1999 ADO DERM	Canadian DND	Scottish AC Shorten the Odds	UK MOD Def Stan 00-56	US DoD Acquisition	US Army US JTF
Almost Certain	High	High	Frequent	Near certainty	Frequent
Likely			Probable	Highly likely	Likely
Moderate (Possible)	Medium	Medium	Occasional	Likely	Occasional
Unlikely	Low	Low	Remote	Unlikely	Seldom
Rare			Improbable	Remote	Unlikely

Table 9: Consequence/Impact Classification (Up to 5 levels)

4360:1999 ADO DERM	Canadian DND	Scottish AC Shorten the Odds	UK MOD Def Stan 00-56	US DoD Acquisition	US Army US JTF
Catastrophic (Severe)	High (Critical)	High	Catastrophic	Unacceptable	Catastrophic
Major			Critical	Acceptable No margin	Critical
Moderate (Significant)	Moderate (Material)	Medium	Marginal	Acceptable Reduced margin	Marginal
Minor	Low (Minor)	Low		Acceptable Some margin reduction	
Insignificant			Negligible	Minimal or no impact	Negligible

Risk is usually classified within 4, sometimes 3 levels. The common terms used are high, medium (moderate) and low. A more detailed classification may also include extreme, severe, very high, significant or trivial. The four risk levels adopted by the Canadian DND, which have been introduced by the Treasury Board of Canada, reflect the necessary level of management effort for risk treatment. In the UK MOD, Def Stan 00-56 describes the risk levels in tolerability terms and the need for review. Although each risk classification may be designed to suit the system or event under investigation, the existing multitude of descriptors (see Table 10) may prove to be a real difficulty in communicating and managing risk. This is a major problem, which the ABCA Standardisation Program has not even started to address.

Table 10: Risk Levels Classification

4360:1999 ADO DERM	Canadian DND & TB	Scottish AC Shorten the Odds	UK MOD Def Stan 00-56	US DoD Acquisition	US Army US JTF
Extreme (Severe)	Extensive management	High	Intolerable	High	Extremely high
(Very high) High	Considerable management		Undesirable		High
Medium (Moderate, significant)	Worthwhile management	Medium	Tolerable Major review	Moderate	Moderate
Low	Manage risk and monitor	Low	Tolerable Normal review	Low	Low
Trivial	Accept and monitor				

Most ABCA countries recognise three levels in their hierarchy of defence risks, namely enterprise (corporate), strategic and operational. The highest level is the enterprise, or corporate, or ultimate strategic, which has the potential to impact an entire defence organisation. Next comes the strategic risk corresponding to activities at service/group level, followed by the operational risk. Operational risks emerge at lower organisational levels and may include functional, tactical, project, team or individual risks in descending order of importance. Special risk categories, for example security, information, fraud, environment or OH&S, may emerge as potential enterprise risks despite being left out of the official hierarchy. However, enterprise risks are basically the focus, and the reason for the introduction of a systematic, integrated, top-down organisation-wide risk management effort. The result is usually the establishment of a comprehensive risk management framework.

All ABCA countries have in place a defence risk management framework or its essential subsystems, or are in the process of introducing it. As a principle, they are based on a risk management standard, with an endorsement policy and they follow an implementation plan. Supporting materials are made available and one or several web sites organised. The frameworks make use of government and/or non-government guidance and experience in their establishment and further development. Table 11 indicates how successful each defence organisation is in the introduction of an integrated risk management framework.

Australia has three columns in Table 11, in order to emphasise that AS/NZS 4360:1999 contains guidance on constructing a generic risk management framework, non-DERM reflects the risk management legacy at the time of writing this report and DERM describes the current changes occurring in Defence.

Table 11: Comparison of Risk Management Frameworks

CRITERIA	**AS/NZS** 4360: 1999	**Non-** DERM	DERM	CAN	UK	USA
Standard based	YES	YES	YES	YES	YES	Several
Endorsement policy	YES	Several	YES	YES	NO	Several
Implementation plan	YES	Several	YES	YES	NO	Several
Application guidelines	YES	Several	YES	YES	Several	Several
Website available	YES	Several	YES	YES	Several	Several
Government guidance	Partial	NO	NO	YES	YES	YES
Non-govern. guidance	YES	YES	YES	YES	YES	YES
Integrated framework	YES*	Partial	YES	YES	NO	Partial
Year started	N/A	N/A	2002	2001	N/A	N/A
Year adopted/issued	1999	N/A	2002	2002	N/A	N/A

* Available at a later time
N/A Not applicable

6. DSTO and Risk Management

This section aims to capture the current status of DSTO engagement in the recently adopted organisation-wide, top-down, systematic approach to risk management in Defence. Although DSTO has recognised achievements and considerable expertise in the area of risk management, it is not an active participant in the establishment of the Defence Risk Management Framework (DRMF). The DSTO potential to provide advice and support regarding the application of risk management methods and techniques is not acknowledged either by the DRMP, or the DRMIP, or the Guidelines. These statements are further evidenced by the review of DSTO activities.

6.1 DSTO Tasks in Risk Management

There are a relatively small number of current tasks in DSTO dedicated entirely to or partially dealing with risk management. Most of them investigate applications of risk analysis in the areas of reliability, safety, or security [30, 31, 32, 33 and 34]. There is hardly any task devoted to implementing risk management in military or non-military operations. Furthermore, most existing examples employ only the risk assessment stages, rather than the entire risk management process. Below one can find a review of some recent tasks in DSTO related to risk management. The brief summaries follow very closely the task plans and the corresponding progress or termination reports.

Air Traffic Management Risk Modelling (AIR 01/350) [30] is requested to review the draft Low Level Airspace Management Proposal (LLAMP) Military Low Operations

(MLO) risk model. This task has to support the timely delivery of the LLAMP model for military low level operations, and has to provide expert assessment of the risk evaluation methodology and identify deficiencies in the draft model. The outcomes have to ensure the internal and external consistency of the draft LLAMP model for military low level operations. The DSTO assistance with the LLAMP MLO risk model will significantly enable RAAF in its continued participation in national airs.

System Risk and Uncertainty Analysis Tools (LRR 01/353) [33] has to explore and identify appropriate risk and uncertainty analysis tools, techniques and methodologies in order to improve the understanding and assessment of risk and uncertainty. This work will enhance the decision-making process within the ADF.

Security Risk Modelling (STR 01/381) [34] is requested to develop defensible security risk metrics for Defence, initially in the Australian home based environment. Further studies might explore business continuity issues on the basis of the costs and benefits to the defence enterprise. This work will ensure the internal and external consistency of the security risk metrics for Defence and will assist the Security Policy Development Branch in its effort to maintain adequate security. Moreover, the task has high priority due to the urgent need of Defence to project a sense of taking reasonable measures to protect its assets, information, people and capabilities. Investment decisions regarding protective security are not only threat based and Defence has to safeguard its established corporate citizen image.

Probabilistic Risk Assessment of Aircraft (AIR 02/244) [31] is requested to develop the analytical tools and theory, and undertake analysis in the risk assessment of aircraft. It is directly linked to AIR 99/161, which involved developing methods and re-establishing the structural risk assessment methodology. This task is required to perform risk assessment of ADF aircraft such as currently underway on the F/A-18 and develop methods and understanding for performing this analysis. There are some difficulties of a probabilistic and numerical nature to be overcome. The investigation into remote risk likelihoods leads to dealing with tails of distributions and the necessity to extrapolate data to determine the probability of failure from remote flaws. Thus, questions regarding the accuracy and sufficiency of data in the region arise. This work will increase the capability of the RAAF to assess the risk of flying aircraft and may be applied to a number of different aircraft in the RAAF fleet.

6.2 DSTO Publications on Risk Management and Related Topics

The publications and articles by DSTO personnel related to risk management follow almost the same trend as DSTO tasks do. They cover only elements of the risk management process "relevant" to the areas of acquisition, personal safety, systems safety, reliability, and security. Not surprisingly, here again there are only a few research results dedicated to risk management in other areas of Defence. However, there are a couple of publications related to risk in general, e.g. [35] and [58]. A limited number of reports or articles are reviewed next.

System Modelling to Predict the Reliability, Maintainability and Supportability of RAN Platforms and Systems [55] serves two purposes: it provides an introduction to capability management and the capability management process; and it shows that systems modelling and simulation can be used to assist capability managers in their decision making. The paper describes the way to predict the future performance of maritime platforms and systems and is directed specifically at RAN Class Logistics Offices. The results are applied to a case study of the Minehunter Coastal auxiliary propulsion system as an illustrative example. Monte Carlo simulation of the system model is the main technique used. Risk management is involved as an element of the capability management process. It supports the decision-making, whether to change a capability or introduce a new one, by evaluating how operational requirements are met.

Literature Review on Aircraft Structural Risk and Reliability Analysis (DSTO-TR-1110) [54] discusses the current approaches and methodologies of interest in the area of aircraft structural integrity and fleet management. However, the present and future complex operational requirements determine the need for a more advanced tool or approach. The Structural Risk and Reliability Analysis (also Probabilistic Damage Tolerant Analysis) has emerged as the most appropriate one. It can identify the sources of variables affecting the fatigue life and fatigue strength of an airframe structure in terms of risk. It can be extended to provide additional information regarding inspection times, cost effectiveness and ongoing operation in the most economical manner. Extension programs can be established to allow aircraft to fly beyond their design life. Here, risk is defined as the chance or the probability of a failure event occurring within a population of details over a period of time. Later, instantaneous and cumulative risks are introduced depending on whether the time of exposure to risk is taken into account or not. The situation is even further complicated by the introduction of acceptable failure rate as a risk quantity. The review concludes that risk and reliability analysis is a powerful approach leading to a more efficient and effective utilisation of airframe structures and components. Even more important is the fact that it may facilitate the implementation of risk analysis and ultimately risk management regarding such expensive equipment.

Review of Risk and Reliability Methods for Aircraft Gas Turbine Engines (DSTO-TR-1306) [37] reflects the change away from a deterministic towards a stochastic approach in the design and analysis of aircraft gas turbine engines. The application of probabilistic methods for the analysis of component failure is a recent development for military aircraft. It leads to a greater appreciation of stochastic models and is based on the increased concern for airworthiness of aging aircraft. The report establishes the need for implementing risk and reliability methods in the management of military engine components. For example, the risk of continuing operation of an engine component beyond its safe life, as determined by the original equipment manufacturer, may generate significant problems in circumstances of high cost of component replacement or even component scarcity. Decision making at operational level requires risk estimates preferably in quantified form. Furthermore, risk assessment may help define inspection intervals. In this context, risk is the probability of failure within the service life of an

engine or a component, while reliability is the probability of not failing during service. The report contributes to the solution of the problem of assessing risk of flying an aircraft – an issue of concern to any military aircraft operator, including the ADF. It also formulates another question, namely the establishment of the acceptable flight failure limit, which may lead to the introduction of a rigorous risk management process in the future.

Without Logistics There Are No Operations! [56] discusses "some of the White Paper drivers that will impact the efficiency and effectiveness of Defence over the next 10 years". For example, cost-effectiveness in capability development and maintenance is identified by the White Paper as an objective of paramount importance given the current level of Defence funding. But any cost-effective solution will be based on two competing processes: maximising capability and minimising cost. Therefore, a balance between them is required and effective risk management is recommended as the foundation for achieving it. Naturally, many more tools and techniques will be needed to enable Defence to make informed decisions. Here DSTO has a unique role to play by providing expertise and independent advice in the area of capability management. This publication also describes a risk assessment decision tool based on artificial neural networks. The Real-Time Event Risk Assessment (RTERA) helps decision-makers use "real-time events during a mission to identify and prioritise risks in relation to the mission". The risks may be related to system failures, system degradation, and crew readiness and preparedness in the RAN.

A Preliminary Analysis of Direct Fire Guided Weapons for Project LAND 40-1 and Project 132 (DSTO-TR-1377) [7] presents the preliminary analysis preceding the potential acquisition of direct fire guided weapon systems by the Australian Army. The investigation starts with the choice of a broad capability option to best support future operations and the adequacy of the direct fire guided weapon systems. Then, a comparative analysis against stakeholder requirements determines a short list of options for further examination. The report also provides risk management as related to the maturity of the technology and the quality of the information available to the study. Risk assessment for the performance of the different options and recommendations for risk treatment are also included.

Land Command 2003 (For AIB 2003) Risk Analysis (U) (DSTO-CR-0238) [3] provides a review of the Force Rotation Model within Army's AIB 2003 Force Structure plan from a risk management perspective. This independent study has to investigate the factors and variables with the potential to influence the successful implementation of the Force Rotation Model. It has to highlight any flaws, hazards, or problems and suggest possible solutions within reasonable timeframes. The investigation follows the generic framework as outlined by AS/NZS 4360:1999. It is conducted in the context of the Land Command 2003 plan for the reorganisation of AIB 2003. The risk identification step produces a list of adverse events that may influence the Force Rotation Model, where each event is defined by the following three parameters: Fundamental Inputs to Capability (FIC); Force Rotation Model state / implementation phase; and source of risk. The first parameter includes all elements of the FIC structure adopted, plus two additional ones: joint – reflecting Defence

issues beyond Land Command; and political – reflecting domestic or international policy issues outside the ADO. The second parameter is associated with implementation and the operating phase of the Force Rotation Model and is either static, or non-deployed or deployed (dynamic). The third parameter characterises the events as presumably under the control of Land Command (internal) and those that are not (external). Objective estimates, due to lack of data, have been substituted by subjective ones based on the study team's degree of experience and belief. Further studies can utilise subject matter expertise and formal application of techniques like Analytic Hierarchy Process. The results of the risk analysis are described in verbal form in detail, accompanied by a summary as a table. A spreadsheet version of the results and visualisation charts of the risks enhance even further the findings of the investigation. Treatment options are discussed during the process of analysing the risks, but the major recommendations are concentrated in the Conclusions section of the study. A comprehensive risk treatment process has to be carried out as a follow up to finish the risk management process in its entirety.

7. Conclusion

This study provides a review of the Australian Defence Risk Management Framework and a comparison with other national and international defence and non-defence risk management standards, policies and guidelines. It seeks to establish the credibility of the DRMF and confirm the approach adopted in the Defence of this country. The ultimate goal of this investigation is to check the appropriateness of granting the DRMF the mandate to be implemented and its ability to work and produce results.

The study contains a literature review and a comparative analysis of selected major publications and 'best practices' from the countries of the ABCA Program. The analysis is based on criteria including, whether the DRMF complies with an established risk management standard, whether it supports decision-making, whether there is similarity in construction and terminology, and whether it may be applied with relative ease. Hence, the properties of the Framework may be viewed as qualitative measures of effectiveness, i.e. how well these properties satisfy the study criteria.

7.1 Summary of the Australian DRMF

The Australian DRMF consists of a policy, an implementation plan, guidelines using existing 'best practices', and a support mechanism with corresponding funding, training and information system. The Framework has emerged as the result of the recently adopted, integrated, systematic, top-down, organisation-wide (enterprise) approach endorsed by the Secretary and the Chief of Defence Force. The DRMF is based on the current standard AS/NZS 4360:1999 *Risk Management*.

There is an established specialised unit – Enterprise Risk Management, set up to act as the focal point for any risk management activity throughout ADO. Moreover, the section has to coordinate and support particularly the management effort associated with the Defence enterprise, organisation-wide risks. The DRMF has been established as "a structure composed of parts fitted and united together" and is being incorporated and integrated within the existing departmental management framework.

Indeed, the DRMF provides for and obligates all Defence personnel to implement risk management in any activity, thus creating the conditions for an entirely new risk management culture within the ADO. Furthermore, this recent approach is directed also at making better use of opportunities rather than minimising losses or avoiding risk altogether, which has been the objective of the traditional one. Thus a more entrepreneurial aspect of the approach is revealed.

The Guidelines of DRMF give hints as to what analytical tools are available, for example SWOT, Mind Maps, Fault Tree Analysis, and Critical Path Analysis. In principle, the Framework does not provide for many commonly used risk management techniques and the details about their applicability. Therefore the actual risk management methodology has been excluded from consideration in this study. They may be the subject of a separate review.

7.2 Properties of the Australian DRMF

The Framework has laid the foundations for making risk management an essential part of how things are done in Defence. It creates a solid unified basis for decision-making at all levels from the individual to the key strategic, and above all to the enterprise levels. Its elements are suitable for implementation by anyone in the ADO, in any sort of activity, be it analysis, training or acquisition. Any defence system, regardless of the complexity of its organisational structure, from soldiers and contractors to groups and services, can be a client of the DRMF and benefit from using it.

Risk management provides support in the decision-making process by exploring issues in an organised and structured way. It may bring clarity in current positions, uncover new insights and identify potential opportunities. One may discuss 'pros and cons' related to a specific course of action (COA) and compare advantages and disadvantages of different alternatives. Thus, the application of the risk management approach introduces a considerable level of objectivity in the decision-making process.

The Framework's elements are simple and easy to understand and implement. For example, the Guidelines contain numerous forms, templates, plans, worked examples, check lists, and other tools, which are there to help potential users. The available techniques contribute by and large to the easy understanding of the input-output relationships. Thus, the decision-maker can then have confidence in the end results of the risk management process.

The DRMF allows for a huge variety of different methods and techniques to be applied in the risk management process. As mentioned before, there are hardly any restrictions on the type of tool(s) to be used in a particular situation. This naturally leads to the availability of rich data of diverse origins, which may be used as input and/or output for a different purpose than that intended. The safeguards against it include the professional integrity, qualifications and experience of the stakeholders.

The Framework has been introduced and maintained and is to be further developed at a cost. Moreover, any gains achieved through risk management should be assessed against the expenses incurred and as a rule not exceeded by them. The integration of the DRMF within the departmental management system and the ability to perform cost-benefit analysis guarantees the proper balance between effectiveness and efficiency.

DRMF has the potential to produce good analyses, unbiased advice and recommendations by the attention devoted to the people factor. There have always been places of effective risk management in Defence. But a comprehensive training system has to be implemented to reflect the new realities of the recent approach, the documents endorsing it, and the support materials available on-line, etc. Risk management is considered as a combination of art and science. It is based on knowledge of the techniques and procedures in risk management and in a broader sense, of operations research and analysis.

According to the DRMF any risk management activity in Defence has to be carried out in the way indicated by the risk management flow-chart (see Figure 1). Any techniques and procedures to be used within the Framework must be consistent with the principles of logic and have a firm mathematical background, in particular probability theory. Thus, the condition of maintaining rigour in the Framework's functioning as required by the design of DRMF is fulfilled.

Here, the degree of agreement can be considered between the results of the DRMF and the results of other established frameworks, expert judgement, historical data or another body of knowledge, which stand as a substitute for reality. The comparison between the Australian DRMF and the similar frameworks in the ABCA Program countries, carried out in Chapter 4, has provided sufficient evidence of common background, terminology, elements, organisational structure, procedures and applications. The Framework reflects also the available 'best practices' in risk management from the public sector and the corporate world, from Australia and overseas. It incorporates the useful pre-DERM experience from the many places in Defence with traditions in risk management.

The Framework possesses an inner mechanism of self-development, continuous improvement, monitoring and review, i.e. of self-perfection. Ultimately it will result in the establishment of a new pro-active risk management culture in Defence. This way the conditions will be created for more relevant results as the premise for an improved decision-making process. However, the responsibility for the decision remains with the user/decision-maker.

All these properties lead to the conclusion that the Australian DRMF has created the right environment for comprehensive and systematic application of risk management. Despite its diverse composition, it shares one and the same standard, terminology, procedures and is easy to use. The DRMF reflects the rich experience accumulated in the area of risk management from this country and overseas. The Framework provides the conditions for an improved decision-making process related to any activity and at any level in Defence [57]. The Framework may be granted the mandate to work and produce results. It can serve as a powerful support system for decision-making in Defence. This study has thus provided evidence and established the appropriateness of the introduction of the Australian Defence Risk Management Framework.

7.3 Topics for Future Research

This investigation has been inspired mainly by the recent introduction of the Australian DRMF and the involvement of the authors in the S&T support for the Land Warfare Development Centre of the Australian Army. There is significant potential for the application of risk management in the development of the Objective Force, currently undertaken by the Force Development Group within LWDC. Risk management can contribute as part of the Capability Options Development and Analysis System and directly as analytical support to decision-making. In this area, uncertainty and fuzziness are inherent characteristics of any question raised. For an investigation one needs a systematic approach with a firm background. Risk management is one of the right approaches and the DRMF can provide the right environment. Hence the objective has emerged for confirming the appropriateness of the Defence approach and the Framework.

This study has established to a very satisfactory level the credibility of the Australian DRMF and its acceptability for use. Future analysis could use the DRMF to improve capabilities as follows. In principle, all steps of the risk management process can be applied to capability options development and analysis. It can be used in capability options development to capture strengths and weaknesses in capabilities. Risk management can determine gaps in current capabilities by identifying areas of risk and uncertainty, and anticipate future capability requirements by seeking potential vulnerabilities and high pay off areas. Also risk management can be applied to capability options analysis to evaluate capabilities. It can be used in the comparative analysis between capability options. Risk can be involved as an optimisation criterion for such options, and as an assessment of current capability options.

8. References

1. Accounts Commission for Scotland, 1999, *Shorten the Odds: A Guide to Understanding and Managing Risk*, Management Studies Unit, Accounts Commission for Scotland, Glasgow, UK. Available electronically at: http://www.audit-scotland.gov.uk/publications/pdf/00ms_01.pdf.

2. Air Land Sea Application Center, 2001, *Risk Management: Multiservice Tactics, Techniques, and Procedures*, ALSA Center, Langley Air Force Base, VA 23665-2785, USA. Available at the time of this writing in electronic form at: http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-100.12/fm3-100.12.htm.

3. Baker, S., Braithwaite, H., Janus, R., Nicholson, R., Philp, W., Richards, B., Shi, P., Stothard, C. and Sunde, J., 2002, *Land Command 2003 (For AIB 2003) Risk Analysis (U)*, DSTO-CR-0238.

4. Barrett, P., 2001, Some Recent Professional Initiatives and Issues in Risk Management, Presentation on 20 November 2001, Canberra, ACT. Available at the time of this writing in electronic form at: http://www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69B4A256B0D000230C4.

5. Conrow, E. H., 2000, *Effective Risk Management: Some Keys to Success*, American Institute of Aeronautics and Astronautics, Reston, VA 20191-4344, USA.

6. Conrow, E. H. and Fredrickson, M. A., 1996, Some Considerations for Implementing Risk Management in Defense Programs: A Faithfully Followed, Structured Risk Management Process is Critical to Maximizing Program Success, *Program Manager: the Defense Systems Management College Newsletter*, Vol. XXV, No. 1, January-February, 6-11.

7. Davis, P.J. and Curtis, N.J., 2002, A Preliminary Analysis of Direct Fire Guided Weapons for Project LAND 40-1 and Project 132, DSTO-TR-1377.

8. *Defence 2000: Our Future Defence Force*, 2000, Commonwealth of Australia. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/whitepaper/white_paper.htm.

9. Department of Army, USA, 1998, *Field Manual No. 100-14 (FM 100-14) Risk Management*, Headquarters, Department of Army, Washington, DC, USA. Available at the time of this writing in electronic form at: http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/100-14/default.htm.

10. Department of Defence, Australia, 1998, Chief of Army Directive No. 2/98 – Army Risk Management. Hard copy available at the time of this writing from the Office the Chief of Army only.

11. Department of Defence, Australia, 1998, TIB 83. Risk Management, Training Command – Army, Australian Army. Accessed on 24 March 2004 at: http://adel.defence.gov.au:8087/doctrine/t083/t083-front…..

12. Department of Defence, Australia, 2000, *Risk Management in Defence*, Inspector General Program Evaluation Assessment Report, June 2000, p.6-5. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/ig/PER/perdocs/RiskManagement.pdf

13. Department of Defence, Australia, 2001, *Capability Systems Life Cycle Management Guide 2001*, Department of Defence, Canberra, ACT. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/home/documents/departmental/manuals/cslcm.htm.

14. Department of Defence, Australia, 2001, Defence instruction (General) Operations 40-2 ADF Aviation Risk Management. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/home/documents/DATA/ADFPUBS/DIG/go40_02.pdf.

15. Department of Defence, Australia, 2001, *2002-03 Defence Plan*.

16. Department of Defence, Australia, 2002, Defence Risk Management CEI (Chief Executive Instruction). Available at the time of this writing in electronic form at: http://intranet.defence.gov.au/hive/cei/49/6859_1.html, and
http://intranet.defence.gov.au/cei/49/8335_1.html.

17. Department of Defence, Australia, 2002, Defence Risk Management Implementation Plan 2002-2003, DERM. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/cfo/derm2/plan.pdf.

18. Department of Defence, Australia, 2002, Defence Risk Management Policy, DERM. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/cfo/derm2/policy.pdf.

19. Department of Defence, Australia, 2002, Defence Instruction (Air Force) Operations 1-19 RAAF Aviation Risk Management. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/home/documents/DATA/RAAFPUBS/DIAF/RO01_19.PDF.

20. Department of Defence, Australia, 2002, *Defence Procurement Policy Manual, Version 3.0,* Department of Defence, Canberra, ACT. Also available at the time of this writing in electronic form at: http://stagedao.cbr.defence.gov.au/magd/CPO/publications/DPPM/Dppm.htm.

21. Department of Defence, Australia, 2002, *Defence Safety Manual.* Available at the time of this writing in electronic form at: http://dsma.dcb.defence.gov.au/main/ohslibrary/safetyman/index.htm.

22. Department of Defence, Australia, 2002, *NAVSAFE Manual – Navy Safety Management*. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/navysyscom/navsafe/Documents/ABR6303.pdf.

23. Department of Defence, Australia, 2002, Guidelines to Managing Risk in Defence, DERM. Available at the time of this writing in electronic form at: http://defweb.cbr.defence.gov.au/cfo/derm2/guide/menu.htm.

24. Department of Defense, USA – DSMC, 1989, *Risk Management: Concepts and Guidance*, Defense Systems Management College, Ft. Belvoir, VA 22060-5426, USA.

25. Department of Defense, USA – SMC, 2000, *Systems Engineering Fundamentals (Chapter 15)*, Defense Acquisition University Press, Ft. Belvoir, VA 22060-5565, USA. Also available at the time of this writing in electronic form at: http://www.dau.mil/pubs/gdbks/sys_eng_fund.asp.

26. Department of Defense, USA – DAU, 2002, *Risk Management Guide for DoD Acquisition (5th Ed),* Defense Acquisition University Press, Ft. Belvoir, VA 22060-5565, USA. Also available at the time of this writing in electronic form at: http://www.dau.mil/pubs/gdbks/risk_management.asp.

27. Department of National Defence, Canada, 2001, Integrated Strategic Risk Management in Defence, Strategic Planning Coordination, Vice Chief of Defence Staff (VCDS), Canada. Available at the time of this writing in electronic form at: http://www.vcds.dnd.ca/dgsp/cosstrat/isrm/doc_e.asp.

28. Department of National Defence, Canada, 2003, Risk Management Overview, website: http://www.vcds.dnd.ca/dgsp/pubs/dp_m/risk-man_e.asp.

29. Dorofee, A. J., Walker, J. A., Alberts, C. J., Higuera, R. P., Murphy, R. L. and Williams, R. C., 1996, *Continuous Risk Management Guidebook*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.

30. DSTO Task AIR 01/350 Air Traffic Management Risk Modelling – A. Ibrahim (Task Manager).

31. DSTO Task AIR 02/244 Probabilistic Risk Assessment of Aircraft – P. D. White (Task Manager).

32. DSTO Task IND SRM/DSTO Financial Risk Management and Advice.

33. DSTO Task LRR 01/353 System Risk and Uncertainty Analysis Tools – A. Ibrahim (Task Manager).

34. DSTO Task STR 01/381 Security Risk Modelling – A. Ibrahim (Task Manager).

35. Ford, J., 1999, *Risk Sensitive Filtering and Parameter Estimation,* DSTO-TR-0764.

36. Hughes, W. P., 1997, *Military Modeling for Decision Making,* 3rd Edition, MORS.

37. Kappas, J., 2002, *Review of Risk and Reliability Methods for Aircraft Gas Turbine Engines*, DSTO-TR-1306.

38. Kunreuther, H. and Slovic, P., 1996, *Challenges in Risk Assessment and Risk Management*, Annals of American Academy of Political and Social Science, Volume 545, Sage Periodicals Press, Thousand Oaks, USA.

39. Markow, P, 2000, Risk Management in Tactical Decision Making, *Flightfax: Report of Army Aircraft Accidents*, Vol. 28, No. 1, November, 2-3.

40. McMillan, B., 1999, *A Review of Risk in Defence Equipment Selection,* Discussion Paper 01/99, Centre for Strategic Studies, Victoria University of Wellington, NZ. Available at the time of this writing in electronic form at: http://www.vuw.ac.nz/css/docs/discussion_papers/Risk.html.

41. McPhee, I., 2002, Risk Management and Governance, Presentation on 16 October 2002, National Institute for Governance, Canberra, ACT. Available at the time of this writing in electronic form at: http://www.anao.gov.au/WebSite.nsf/Publications/7BCEC0251ECF4420CA256C540003EAD0.

42. Ministry of Defence, UK, 1996, *Defence Standard 00-56 (PART1)/Issue2 Safety Management Requirements for Defence Systems, Part 1: Requirements.* Available at the time of this writing in electronic form at: http://www.dstan.mod.uk/data/00/056/01000200.pdf.

43. Ministry of Defence, UK, 1996, *Defence Standard 00-56 (PART2)/Issue2 Safety Management Requirements for Defence Systems, Part 2: Guidance.* Available at the time of this writing in electronic form at: http://www.dstan.mod.uk/data/00/056/02000200.pdf.

44. Ministry of Defence, UK, 2001, *Ministry of Defence Policy Paper No.4 Defence Acquisition*, London, UK. Available at the time of this writing in electronic form at: http://www.mod.uk/linked_files/def_acquisition.pdf.

45. Ministry of Defence, UK, 2002, Ordnance, Munitions and Explosives (OME) Safety Management System (SMS): Operating Procedures (OPs). Available at the time of this writing in electronic form at: http://www.mod.uk/linked_files/dosg_smsop151.pdf.

46. QSTAG 1043 Ed 1 (1998) Individual Protective Equipment and Risk Management in a NBC Environment. Available at the time of this writing in electronic form at: http://www.odusa-or.army.mil/qwg-aor/reports/qaps-qstags.htm.

47. Schaeffer, M. D., 1998, Risk Management in the Department of Defense: Identifying Risks to be Taken and Risks to be Avoided, *Program Manager*: the Defense Systems Management College Newsletter, Vol. XXVII, No. 2, March-April, 48-52.

48. Standards Australia, 1998, *AS/NZS 3931:1998 Risk Analysis of Technological Systems – Application Guide*, Standards Australia, Homebush, NSW.

49. Standards Australia, 1999, *AS/NZS 4360:1999 Risk Management*, Standards Association of Australia, Strathfield, NSW.

50. Standards Australia, 1999, *HB 142:1999 A Basic Introduction to Managing Risk Using the Australian and New Zealand Risk Management Standard AS/NZS 4360:1999*, Standards Association of Australia, Strathfield, NSW.

51. Standards Australia, 1999, *HB 143:1999 Guidelines for Managing Risk in the Australian and New Zealand Public Sector*, Standards Association of Australia, Strathfield, NSW.

52. Standards Australia, 2000, *HB 240:2000 Guidelines for Managing Risk in Outsourcing Using the AS/NZS 4360 Process,* Standards Australia International, Sydney, NSW.

53. Standards Australia, 2000, *HB 250:2000 Organisational Experiences in Implementing Risk Management Practices,* Standards Australia International, Sydney, NSW.

54. Tong, Y. C., 2001, *Literature Review on Aircraft Structural Risk and Reliability Analysis*, DSTO-TR-1110.

55. Tyndall, M. and Whitehouse, T., 2000, *System Modelling to Predict the Reliability, Maintainability and Supportability of RAN Platforms and Systems*. DSTO, Defence Operations Analysis Symposium, Melbourne, 16-17 March 2000.

56. Tyndall, M., Whitehouse, T., Turner, B., and Woolley, A., 2001, *Without Logistics There Are No Operations!* DSTO, Defence Operations Analysis Symposium, Canberra, 4-5 June 2001.

57. Underwood, A., 2002, Risk Management. Evaluating the Decision Making Process in Defence. Can an Organisation the Size of Defence Minimise the Hazards of Its Everyday Business Activities?, *Defence Information Bulletin,* December 2002, 24-25.

58. White, A. and Parker, R. P., 1999, Cost Benefit Analysis Concepts for Insensitive Munitions Policy Implementation, DSTO-GD-0230.

DISTRIBUTION LIST

Australian Defence Risk Management Framework: A Comparative Study

Svetoslav Gaidow and Seng Boey

AUSTRALIA

DEFENCE ORGANISATION

		No. of copies
Task Sponsor	**COMD LWDC**	1
Director Defence Safety Management Agency, Defence Personnel Executive		1

S&T Program

Chief Defence Scientist FAS Science Policy AS Science Corporate Management Director General Science Policy Development	shared copy
Counsellor Defence Science, London	Doc Data Sheet
Counsellor Defence Science, Washington	Doc Data Sheet
Scientific Adviser to MRDC, Thailand	Doc Data Sheet
Scientific Adviser Joint	1
Navy Scientific Adviser	Doc Data Sht & Dist List
Scientific Adviser - Army	1
Air Force Scientific Adviser	Doc Data Sht & Dist List
Scientific Adviser to the DMO	Doc Data Sht & Dist List

Systems Sciences Laboratory

Chief of Land Operations Division	Doc Data Sht & Dist List
Research Leader Operations Research	1
Head TFM (Paul Gaertner)	1
Task Manager (Richard Egudo)	1
Author:	
Svetoslav Gaidow	1
Chief of Air Operations Division	1
Seng Boey	1
Chief of Maritime Operations Division	1

DSTO Library and Archives

Library Edinburgh	1 + Doc Data sheet
Library Fishermans Bend	Doc Data Sheet

Defence Archives 1

Capability Development Group

Director Capability Systems Division 1
Director General Maritime Development 1
Director General Land Development 1
Director General Capability and Plans 1
Assistant Secretary Investment Analysis 1
Director Capability Plans and Programming 1
Director Trials 1

Chief Information Officer Group

Deputy CIO Doc Data Sheet
Director General Information Policy and Plans Doc Data Sheet
AS Information Strategies and Futures Doc Data Sheet
AS Information Architecture and Management Doc Data Sheet
Director General Australian Defence Simulation Office Doc Data Sheet
Director General Information Services Doc Data Sheet

Strategy Group

Director General Military Strategy Doc Data Sheet
Director General Preparedness Doc Data Sheet
Assistant Secretary Strategic Policy Doc Data Sheet
Assistant Secretary Governance and Counter-Proliferation Doc Data Sheet

Navy

Director General Navy Capability, Performance and Plans, Navy Headquarters Doc Data Sheet
Director General Navy Strategic Policy and Futures, Navy Headquarters Doc Data Sheet
Maritime Operational Analysis Centre, Building 89/90 Garden Island Sydney NSW
Deputy Director (Operations)
Deputy Director (Analysis) shared Doc Data Sht & Dist List

Army

Director Doctrine and Simulation Group, LWDC, Puckapunyal 1
Director Force Development Group, LWDC, Puckapunyal 1
ABCA National Standardisation Officer, Land Warfare Development Sector, Puckapunyal e-mailed Doc Data Sheet
SO (Science) - Land Headquarters (LHQ), Victoria Barracks NSW Doc Data & Exec Summ
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD Doc Data Sheet

Air Force

SO (Science) - Headquarters Air Combat Group, RAAF Base, Williamtown NSW 2314 Doc Data Sht & Exec Summ

Joint Operations Command

Director General Joint Operations	Doc Data Sheet
Chief of Staff Headquarters Joint Operations Command	Doc Data Sheet
Commandant ADF Warfare Centre	Doc Data Sheet
Director General Strategic Logistics	Doc Data Sheet

Intelligence and Security Group

DGSTA Defence Intelligence Organisation	1
Manager, Information Centre, Defence Intelligence Organisation	email pdf
Assistant Secretary Corporate, Defence Imagery and Geospatial Organisation	Doc Data Sheet
Director Enterprise Risk Management, Inspector General Group	1

Defence Materiel Organisation

Deputy CEO	Doc Data Sheet
Head Aerospace Systems Division	Doc Data Sheet
Head Maritime Systems Division	Doc Data Sheet
Chief Joint Logistics Command	Doc Data Sheet

Defence Libraries

Library Manager, DLS-Canberra	Doc Data Sheet
Library Manager, DLS - Sydney West	Doc Data Sheet

OTHER ORGANISATIONS

National Library of Australia	1
NASA (Canberra)	1
Library of New South Wales	1
State Library of South Australia	1

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy	
Library	1
Head of Aerospace and Mechanical Engineering	1
Head of Information Technology and Electrical Engineering	1
Hargrave Library, Monash University	Doc Data Sheet
Librarian, Flinders University	1

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center	email pdf
United Kingdom - Dstl Knowledge Services	email pdf
Canada - Defence Research Directorate R&D Knowledge & Information Management (DRDKIM)	1

NZ Defence Information Centre	1

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service	1
Engineering Societies Library, US	1
Materials Information, Cambridge Scientific Abstracts, US	1
Documents Librarian, The Center for Research Libraries, US	1

SPARES			5
Number of copies:	**Printed**	**44**	
	PDF	**3**	
	Total		**47**

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Australian Defence Risk Management Framework: A Comparative Study

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Svetoslav Gaidow and Seng Boey

5. CORPORATE AUTHOR

Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-GD-0427	AR 013-345	General Document	February 2005

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
2004/1040979	ARM 02/079 ARM 02/080	COMD LWDC	87	58

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0427.pdf

14. RELEASE AUTHORITY

Chief, Land Operations Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Risk management
Risk assessment
Standardization

19. ABSTRACT

In early 2002, the Secretary of Defence and the Chief of Defence Force endorsed a top-down, organisation-wide and systematic approach to risk management in Defence. As a result, the Australian Defence Risk Management Framework (DRMF) was established. This study is a quest for the credibility of DRMF. It provides a review of the DRMF and a comparative analysis in light of other national and international, defence and non-defence risk management publications and practices. Through this study the appropriateness of the approach and the acceptability of the DRMF are confirmed. The application of risk management in force and capability options development and analysis is identified as an area of future research.