Enterprise Risk Management

The Way Ahead for DRDC within the DND Enterprise

R.G. Dickinson
Dr. B.W. Taylor
DRDC CORA

DRDC CORA TR 2010-035
March 2010

Defence R&D Canada
Centre for Operational Research & Analysis

Strategic Planning Operational Research Team

National Defence Défense nationale

Canada

Enterprise Risk Management

The Way Ahead for DRDC within the DND Enterprise

R.G. Dickinson
Dr. B.W. Taylor
DRDC CORA

Defence R&D Canada – CORA

Technical Report
DRDC CORA TR 2010-035
March 2010

Principal Author

Original signed by R.G. Dickinson

R.G. Dickinson

Office of the Chief Scientist, Special Projects

Approved by

Original Signed by Charles Morrisey

C.C. Morrisey

Acting Section Head Joint & Common OR

Approved for release by

Original signed by D. Haslip

D. Haslip

Acting DRDC CORA Chief Scientist

DRDC Enterprise 09 Task 3.4 Report

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

Enterprise Risk Management (ERM) is the process of managing risk from an organization-wide perspective, in order to achieve an organization's overall corporate objectives. This is often a high-level view of the general process of Integrated Risk Management (IRM) which brings a systematic and deliberate approach to the management of risk, integrated throughout the management culture at all levels. This paper examines the nature of ERM in order to make recommendations on the way ahead on ERM for DRDC within the DND enterprise. It explores ERM both from the perspective of DRDC's understanding and application internally, but also from the perspective of DRDC's possible contributions to the research and development of ERM tools and practice within DND. This paper describes: the general ERM process; the importance of a supportive ERM culture; the results of a DRDC management workshop on ERM; the practice of ERM within peer organisations; and suggestions for possible research areas in ERM. Two partial case studies demonstrate the application of enterprise risk management to high-level objectives, first to enterprise risk management itself and then to the science and technology program within DND.

Résumé

La gestion du risque d'entreprise (GRE) est le processus de gestion du risque d'une perspective organisationnelle, en vue d'atteindre les objectifs généraux d'une organisation. Il s'agit souvent d'une perspective de haut niveau du processus général de la gestion intégrée du risque (GIR), qui apporte une approche systématique et délibérée à la gestion du risque, intégrée dans l'ensemble de la culture de gestion à tous les niveaux. Dans le présent document, on examine la nature de la GRE afin de faire des recommandations sur la voie à suivre en ce qui concerne la GRE pour RDDC au sein du MDN. On explore la GRE de la perspective de la compréhension et de l'application interne de RDDC, mais aussi du point de vue des contributions possibles de RDDC à la recherche et au développement d'outils et de pratiques de GRE au sein du MDN. Le document décrit ce qui suit : le processus général de la GRE; l'importance d'une culture de GRE positive; les résultats d'un atelier de RDDC sur la GRE pour les gestionnaires; la pratique de la GRE au sein d'organismes pairs; et des suggestions de domaines de recherche possibles en GRE. Deux études de cas partielles démontrent l'application de la gestion du risque d'entreprise à des objectifs de haut niveau, d'abord à la GRE comme telle, puis au programme de science et de technologie au sein du MDN.

This page intentionally left blank.

Executive summary

Enterprise Risk Management

R.G. Dickinson, B. Taylor; DRDC CORA TR 2010-035; Defence R&D Canada – CORA; March 2010.

This paper examines the nature of enterprise risk management in order to make recommendations for the way ahead in this area for DRDC within the DND enterprise.

Integrated risk management (IRM) is a continuous, proactive and systematic process to understand, manage and communicate *risk* from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives. (TBS definition)

Enterprise risk management (ERM) is often used synonymously with IRM, but it is also used to mean risk management at the enterprise level.

TBS is working with Departments to develop guidance on IRM. DND and DRDC are involved in this exercise of importing world-wide best practice and standards into general, adaptable guidance for Departments and Agencies.

> Recommendation: DRDC should continue to be involved in this Inter-Departmental work, as well as providing support for continuing development of process and tools in the future. DRDC should support DND in its adaptation of these general guidelines for its purposes.

Risk management (RM), IRM and ERM consist of five basic activities: Risk Identification, Risk Assessment, Risk Response, Monitoring, and Documentation. Any process supporting ERM will have these activities, although there are numerous variations and models of the ERM process built on these. The forthcoming ISO 31000 RM standard sets this within a context of communication and consultation.

ERM processes can vary with level and risk factor. At the enterprise level there are a wide variety of risk factors. The nature of uncertainty and the language to describe risk can vary significantly between risk factors, causing problems in communication and misunderstandings.

> Recommendation: Conduct research into the understandings of risk, the nature of uncertainty and the use of risk language in different disciplines and with respect to different risk factors relevant to DND.

Creating a culture attuned to risk is the greatest challenge to broad acceptance of ERM. Within DRDC the understanding and practice of RM or ERM is variable. Individual Managers may intuitively understand and practice risk management, but there is a lack of deliberate, explicit and consistent use of RM in strategic thinking, planning, programs, and projects of DRDC.

Recommendation: Engage internal and/or external experts with experience in ERM over a period of years to work with DRDC managers to create a culture attuned to risk management.

Recommendation: Expedition 11 should include activity to develop ERM support to DND and to further identify and modify DRDC planning, program, and project processes to explicitly include RM.

DRDC would like to not only prepare itself to support DND in its practice of risk management, but DRDC would also like to embrace risk management within its own management practices and so provide examples to the rest of DND of successful risk management.

Current practice in ERM and RM generally is variable within DND at all levels. At the highest, enterprise level ERM can clarify objectives, delineate associated risks with their impacts and identify well-posed questions for further analysis. Conducting ERM at the enterprise level allows for a holistic rather than piecemeal approach to meeting DND objectives and dealing with their associated risks. Questions which then cascade down from the enterprise level will lead to more robust answers across the broad risk space of DND. ERM at the enterprise level is thus critical.

A proper understanding of risk management should not only prepare government to deal with risk, but also help it to focus efforts on the critical risks and tools to manage such risk. ERM/IRM is not a new silo but an activity which must be integrated across all levels and areas of the Department to be most effective. Nevertheless some dedicated analyst support should be made available to specifically support the enterprise level.

Recommendation: DRDC should assist DND in enterprise level risk management. It should dedicate sufficient resources, at least a small analytic team, to spearhead this effort and support DND staff. This team would focus on direct support to DND ERM (with associated formulation of enterprise level strategy and plans), interact with the most senior levels of DND, support its processes and methods, and draw on expertise across DRDC as required.

RM is not a new activity, and DRDC has a good basis on which to build. A large part of DRDC activity already supports IRM or ERM in some way - especially in risk identification, assessment and response. DRDC does not support IRM consistently at all levels because a framework of the type envisaged in ISO 31000 has not been implemented. IRM is thus far ad hoc in its implementation within DND. DRDC could practice and so demonstrate to DND a more deliberate approach to ERM within DRDC.

Recommendation: DRDC should find a focal point for its support to risk management within DND, and not seek to provide support everywhere. DRDC should focus its initial efforts to support ERM in the area of its strengths – risk identification and assessment – and seek to engage senior decision makers by that route.

Recommendation: To define Expedition 11, DRDC RDEC should engage external support to work with them in an ERM approach which serves to simplify and focus the strategy to achieve S&T objectives within the DND enterprise.

Research in ERM has several different thrusts, with impact in short-, mid- and long-term. Fundamental research into the nature of uncertainty and the perception and measurement of risk would potentially improve RM and ERM in the long-term. Research into complex systems, systems dynamics and the like can also support ERM in the mid- to long-term. Applied research into the application of ERM to the strategic planning processes of DND is essential and must interact with capability planning and performance management processes in the short- to mid-term. Incorporating ERM into whole-life cycle of a technology concept from idea to insertion can begin at any time with likely benefits at all stages. Specific constrained complex systems or defence areas, such as urban warfare, may benefit by the incorporation of ERM methods as part of the operational context.

At the enterprise level assessing and responding to risk across a wide range of different kinds of risk factors is a huge challenge. There is a need to research the human aspects of the process – risk perception, risk estimation, risk attitude and risk language – across these different risk factors. In addition there is a need to do research into multi-factor risk, especially consistent and rigorous "aggregated" enterprise level risk assessment and response across these different risk factors. This is *not* a matter of "rolling up" the risks from lower levels. This must be kept simple in practice, even if its fundamentals are profound.

> Recommendation: DRDC should undertake a mix of fundamental and applied research in ERM, short-, mid- and long-term as it applies to DND risk factors. At the enterprise level key aspects of this research will involve both human aspects of risk and multi-factor risk assessment. This work aligns with research capability development in complex systems.

Risks are often defined in terms of both likelihood and impact. Both of which must be considered as distributions reflecting a range of possibilities within a 'space' rather than as prescriptive single point cases. Doing so avoids "point scenario trap" where possibilities are too narrowly or specifically defined with resulting lack of robustness. This avoids optimizing on narrow parameters to determine "best" solutions, and leads to solutions which are more robust across a range of likely alternatives.

Two partial case studies in this paper illustrate the ERM process: applying ERM for introducing ERM, and applying ERM in a focused manner to the S&T Program (PAA) for developing an ERM supported strategy.

Implementation of ERM, i.e. at the enterprise level, must engage senior managers. They must speak to their risk concerns in their language, and lower levels supporting them must come to understand and communicate in this language.

This page intentionally left blank.

Sommaire

Enterprise Risk Management

R.G. Dickinson, B. Taylor; DRDC CORA TR 2010-035; R & D pour la défense Canada – CORA; Mars 2010.

Dans le présent document, on examine la nature de la gestion du risque d'entreprise afin de faire des recommandations sur la voie à suivre à cet égard pour RDDC au sein du MDN.

La gestion intégrée du risque (GIR) est un processus systématique, proactif et continu pour comprendre, gérer et communiquer le *risque* du point de vue de l'ensemble de l'organisation. Il s'agit de prendre des décisions stratégiques qui contribuent à la réalisation des objectifs globaux de toute l'organisation (définition du SCT).

L'expression gestion du risque d'entreprise (GRE) est souvent employée comme synonyme de GIR, mais elle désigne également la gestion du risque au niveau de l'entreprise.

Le SCT collabore avec les ministères en vue d'élaborer des directives relatives à la GIR. Le MDN et RDDC participent à cet exercice d'importation de pratiques exemplaires et de normes internationales dans l'optique d'élaborer des directives générales applicables aux ministères et organismes.

> Recommandation : RDDC devrait continuer de participer à ces travaux interministériels, en plus de fournir du soutien pour assurer l'élaboration continue du processus et des outils à l'avenir. RDDC devrait aider le MDN à adapter ces directives générales à ses objectifs.

La gestion du risque (GR), la GIR et la GRE comportent cinq activités principales : identification du risque, évaluation du risque, réponse au risque, surveillance et documentation. Les processus qui appuient la GRE comportent tous ces activités, mais une foule de variantes et de modèles du processus de GRE découlent de ces activités. La norme à venir ISO 31000 sur la GR établit cette réalité dans un contexte de communication et de consultation.

Les processus de la GRE peuvent varier en fonction du niveau et du facteur de risque. Au niveau de l'entreprise, il y a un large éventail de facteurs de risque. La nature de l'incertitude et la terminologie employée pour décrire le risque peuvent varier considérablement d'un facteur de risque à l'autre, entraînant des problèmes de communication et des malentendus.

> Recommandation : Faire une recherche sur les connaissances sur le risque, la nature de l'incertitude et l'emploi du vocabulaire du risque dans différentes disciplines et à l'égard de différents facteurs de risque se rapportant au MDN.

La création d'une culture arrimée au risque est la plus grande difficulté liée à l'acceptation généralisée de la GRE. Dans le cadre de RDDC, les connaissances et les pratiques relatives à la GR ou à la GRE sont variables. Chaque gestionnaire peut comprendre et exercer la gestion du

risque intuitivement, mais l'utilisation délibérée, explicite et constante de la GR dans la réflexion stratégique, la planification, les programmes et les projets de RDDC est insuffisante.

> Recommandation : Faire appel à des experts internes et/ou externes ayant acquis plusieurs années d'expérience en GRE pour travailler avec les gestionnaires de RDDC en vue de créer une culture arrimée à la gestion du risque.

> Recommandation : Expédition 2011 devrait intégrer des activités visant à obtenir du soutien en GRE pour le MDN, ainsi qu'à préciser et à modifier les processus de planification, de programme et de projet de RDDC pour inclure explicitement la GR.

RDDC aimerait non seulement se préparer à aider le MDN à exercer sa fonction de gestion du risque, mais aussi intégrer la gestion du risque à ses propres pratiques de gestion, et donc fournir au reste du MDN des exemples de gestion du risque réussie.

En général, la pratique actuelle de la GRE et de la GR est variable au sein du MDN à tous les niveaux. Au niveau le plus élevé de l'entreprise, la GRE peut clarifier les objectifs, délimiter les risques associés en fonction de leurs conséquences et cerner des questions pertinentes en vue d'une analyse future. En réalisant la GRE au niveau de l'entreprise, on peut adopter une approche intégrée plutôt que fragmentée en vue d'atteindre les objectifs du MDN et de composer avec les risques connexes. Les questions qui découlent ensuite du niveau de l'entreprise entraîneront des réponses plus solides dans le large spectre du risque du MDN. La GRE au niveau de l'entreprise est donc essentielle.

Grâce à une connaissance adéquate de la gestion du risque, le gouvernement devrait non seulement être en mesure de composer avec le risque, mais aussi pouvoir axer ses efforts sur les risques importants et les outils permettant de gérer ce genre de risque. La GRE/GIR n'est pas un nouveau domaine, mais plutôt une activité qui doit être intégrée à tous les niveaux et secteurs du Ministère pour en assurer l'efficacité optimale. Néanmoins, une certaine part de soutien assuré par des analystes spécialisés devrait être offert pour soutenir spécialement le niveau de l'entreprise.

> Recommandation : RDDC devrait aider le MDN à réaliser la gestion du risque au niveau de l'entreprise. Elle devrait prévoir des ressources suffisantes, à tout le moins une petite équipe d'analyse, pour mener cette initiative et pour appuyer le personnel du MDN. Cette équipe se concentrerait sur le soutien direct de la GRE du MDN (y compris la formulation connexe d'une stratégie et de plans au niveau de l'entreprise), interagirait avec les niveaux supérieurs du MDN, soutiendrait ses processus et ses méthodes et s'appuierait au besoin sur l'expertise présente à l'échelle de RDDC.

La GR n'est pas une nouvelle activité, et RDDC peut s'appuyer sur une base solide. Une large part des activités de RDDC soutiennent déjà la GIR ou la GRE d'une manière ou d'une autre, surtout en ce qui concerne l'identification du risque, l'évaluation du risque et la réponse au risque. Le soutien de la GIR de RDDC n'est pas constant à tous les niveaux, vu l'absence d'un cadre du type envisagé dans la norme ISO 31000. La mise en œuvre de la GIR au sein du MDN a été

ponctuelle à ce jour. RDDC pourrait adopter, et donc démontrer au MDN, une approche plus délibérée de la GRE au sein de l'agence.

> Recommandation : RDDC devrait trouver un centre d'intérêt pour son soutien de la gestion du risque au sein du MDN et ne pas chercher à fournir du soutien partout. RDDC devrait cibler ses efforts initiaux pour appuyer la GRE dans la sphère de ses points forts (identification et évaluation du risque) et chercher à orienter des décideurs expérimentés dans cette voie.

> Recommandation : Pour définir Expédition 2011, le CERD de RDDC devrait faire appel à du soutien externe pour collaborer à une approche de la GRE visant à simplifier et à cibler la stratégie pour atteindre les objectifs de S et T au sein du MDN.

La recherche à l'égard de la GRE comporte plusieurs objectifs différents, associés à des conséquences à court terme, à moyen terme et à long terme. La recherche fondamentale en ce qui concerne la nature de l'incertitude et la perception et la mesure du risque pourrait améliorer la GR et la GRE à long terme. La recherche relative aux systèmes complexes, à la dynamique des systèmes et ainsi de suite peut également soutenir la GRE à moyen et à long terme. La recherche appliquée sur l'utilisation de la GRE pour les processus de planification stratégique du MDN est essentielle et doit interagir avec les processus de planification de la capacité et de gestion du rendement à court et à moyen terme. L'intégration de la GRE à la totalité du cycle de vie d'un concept de technologie, c'est-à-dire de l'idée à la mise en œuvre, peut commencer en tout temps et les avantages peuvent surgir à toutes les étapes. Les systèmes complexes contraints spécifiques ou les zones de défense, comme le combat en zone urbaine, peuvent être avantagés par l'intégration des méthodes de GRE dans le contexte opérationnel.

Au niveau de l'entreprise, le processus d'évaluation du risque et de réponse au risque compte tenu du large éventail des différents types de facteurs de risque est extrêmement difficile. Il faut faire des recherches sur les aspects humains du processus (perception du risque, estimation du risque, attitude face au risque et vocabulaire du risque) dans l'ensemble de ces différents facteurs de risque. Il faut également faire des recherches sur le risque multifactoriel, en particulier une évaluation du risque et une réponse au risque constantes et rigoureuses de façon agrégée au niveau de l'entreprise pour l'ensemble de ces facteurs de risque. Il ne s'agit *pas* de cumuler les risques des niveaux inférieurs. Cet exercice doit demeurer simple en pratique, même si son fondement est complexe.

> Recommandation : RDDC devrait entreprendre une combinaison de recherche fondamentale et appliquée en GRE à court, à moyen et à long terme, conformément aux facteurs de risque du MDN. Au niveau de l'entreprise, les aspects clés de cette recherche comprendront les aspects humains du risque et l'évaluation multifactorielle du risque. Ces travaux sont conformes à l'élaboration de la capacité de recherche des systèmes complexes.

Les risques sont souvent définis par rapport à la probabilité et aux conséquences. Ces deux aspects doivent être considérés comme des distributions désignant un éventail de possibilités dans un « espace », plutôt que des cas ponctuels normatifs. Ainsi, on évite le « piège du scénario ponctuel », où les possibilités sont trop étroitement ou précisément définies, ce qui donne lieu à

une rigueur insuffisante. Par conséquent, on évite l'optimisation de paramètres étroits pour déterminer les « meilleures » solutions et on obtient des solutions qui sont plus fiables par rapport à un large éventail de solutions de rechange probables.

Deux études de cas partielles dans le présent document illustrent le processus de GRE : mise en pratique de la GRE pour introduire la GRE, et application ciblée de la GRE au programme de S et T (AAP) en vue d'élaborer une stratégie appuyée par la GRE.

Pour mettre en œuvre la GRE, c.-à-d. au niveau de l'entreprise, il faut faire intervenir les cadres supérieurs. Ces derniers doivent parler de leurs préoccupations à l'égard du risque dans leurs mots, et les effectifs des échelons inférieurs qui les appuient doivent en venir à comprendre et à communiquer dans ces mêmes mots.

Table of contents

List of figures

Acknowledgements

The authors wish to acknowledge Diana Del Bel Belluz, President of Risk Wise Inc., for her thorough expert review of, and helpful comments on, the penultimate draft of this paper.

This page intentionally left blank.

1 Introduction

Government has mandated Departments to manage risks in an integrated manner. The management of risk is meant to be deliberate and integrated throughout the management culture at all levels.

> ***Integrated Risk Management*** is a continuous, proactive and systematic process to understand, manage and communicate *risk* from an organization-wide perspective. It is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives. (TBS)

This TBS definition of integrated risk management (IRM) is essentially similar to definitions for enterprise risk management (ERM). If there is any difference it is that enterprise risk management can connote a high-level strategic enterprise perspective and focus rather than the broad risk management activity integrated at all levels. ERM can thus mean risk management at the enterprise level. With this view, ERM can be achieved through IRM. Although they are not synonymous, the terms will be used somewhat interchangeably in this paper, with ERM used on occasion to emphasize the high-level strategic view.[1] The management of risk at the enterprise level brings challenges that go beyond the usual and normal practice of risk management.

This paper examines those challenges which are peculiar to enterprise risk management for DRDC as part of the DND enterprise. DRDC would like to not only prepare itself to support DND in its practice of risk management, but DRDC would also like to embrace risk management within its own management practices and so provide examples to the rest of DND of successful risk management.

This work then is undertaken as part of DRDC's change program, Expedition 09. The intent is to advise management both on how it can better provide full service to DND in the area of risk management and on how it can better inculcate risk management within its own management practices and research initiatives.

It is not the intention here to provide a full discussion of ERM. Enough of the nature and process of ERM will be sketched to point out areas in which DRDC can improve its own management of risk, develop tools or capability for risk or showcase the use of risk management techniques to DND.

Similarly this paper assumes a level of knowledge of risk; it does not spend time on definitions and basic concepts. The reader should keep in mind, then, that risk includes both likelihood and consequence, and that risk can have positive and negative associations.

[1] IRM is a term used and defined by TBS. ERM is a term used widely with numerous variations in its definition. It is not reasonable or necessary to agree to one definition of ERM. It is enough to note the strategic view and corporate emphasis in ERM. There are also grey areas between Operational Risk Management (ORM) and ERM as discussed in the chapter by Del Bel Belluz referred to in the Bibliography.

Risk management is an important topic, especially so at a time where there is increased uncertainty in the planning environment. In such a large, diverse and inherently uncertain environment as defence, enterprise risk management is a potentially vital tool. However, Government bureaucracy is by nature risk averse and abundant regulations attempt to minimize the impact of any risk. An improper understanding of risk management has created processes which unduly focus on low probability occurrences of little consequence. Regulations aimed at risks with major consequences broadly applied simply stifle or slow down all initiatives. Thus a proper understanding of risk management should not only prepare government to deal with risk, but also help it to focus efforts on the critical risks and tools to manage such risk.

The paper will first describe in broad terms what is involved in an enterprise risk management framework and process. Second, the most crucial element of implementing ERM, the organizational culture, is discussed. Third, the practice of ERM is described within various contexts including DRDC, DND, OGDs, and Defence Allies within peer organisations and in other environments to produce an informed view as to what risk means to DND. Fourth, possible research areas in ERM are enumerated. Fifth, to illustrate at least the initial stages of risk management while at the same time giving concrete illustration, two case studies will be looked at: Enterprise Risk Management itself and the S&T Program (PAA) within DND. The paper finishes with some general concluding discussion. Throughout the paper recommendations will be made. The basic conclusions and recommendations are summarized in the Executive Summary.

2 Enterprise Risk Management Overview

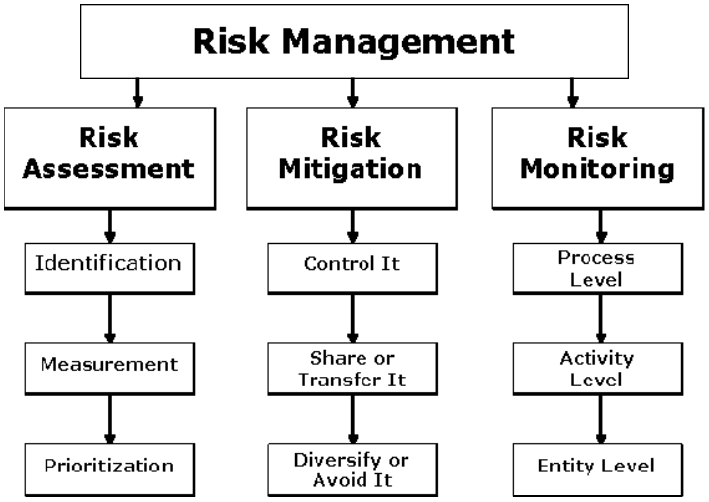
An overview of ERM will recognize that the primordial activity is to establish objectives and context for the organization. Within these objectives and context there will be a process of risk management, which will involve continual communication and consultation. Since ERM is about making strategic decisions that contribute to the achievement of an organization's overall corporate objectives, clear objectives and understanding of the broad context in which those objectives are to be achieved is the necessary starting point.

There are numerous variations on the process of risk management depending on a variety of factors including level, the external and internal environment and so on. Nevertheless, risk management generally consists of five main activities, typically described in words like the following:

- Risk Identification: Identify the risks that threaten or enhance the achievement of objectives and expected results in the immediate or more distant future; risk identification also includes Environmental Scanning and Scenario Analysis.
- Risk Assessment: Assess the probability (likelihood) and impact of the risk occurring and order risks according to significance.
- Risk Response: Find cost-effective options and define strategies to prevent or reduce the probability or impact of the risk.
- Monitoring: Monitor the functioning and effectiveness of risk responses and any changes to the management concerns or tolerances of risks. Communicate findings and decisions.
- Documentation: Document the risk management process to record the rigor of the process and to enable discovery and sharing of lessons learned.

These five activities provide a structure for examining how DRDC should focus its research and support in ERM.

Figure 1 below shows an alternate way of describing the process of risk management, using slightly different terms and ordering, but covering essentially the same activities. Minor variations of this kind are typical of descriptions of RM and ERM.

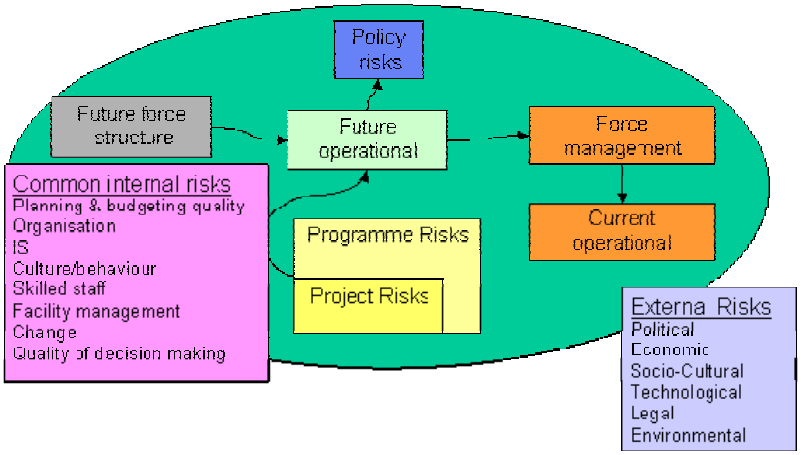


Source: Business Risk Assessment. 1998 – The Institute of Internal Auditors

Figure 1: A Risk Management Model

The high-level enterprise view and practice of risk management has several features which make it more challenging than risk management at the project level. At the enterprise level there are a variety of strategic factors, both external and internal to the organization. Figure 2 below illustrates factors which must be considered in enterprise risk management: external factors – political, economic, socio-cultural, technological, legal, environmental and so on; and internal factors related to these such as finances, people, infrastructure, as well as the structure and functions of the organization – culture, planning processes, support facilities, and so on. Not only are these various factors usually based on quite different disciplines, speaking different "languages" and concerned about disparate realities and contexts, but those concerned with them also have different attitudes and approaches to risk management. These differences are a significant challenge in the assessment, understanding and communication of risk at the enterprise level.

The various risk factors at the enterprise level add both complications and complexity to the management of enterprise risk. Risk means different things to different people and organisations. Effective risk management requires a shared risk lexicon and an understanding of the language used to express risks, with constant communication to clarify meaning. Effective risk management also requires understanding of who manages which kind of risks, the attitude and approach to risk in different areas, and the process to transfer risk "ownership" to appropriate authority. Enterprise risk management can be significantly complicated by the possible synergistic nature of various factors. Furthermore, the scope and complexity of enterprise risk management means not all risks will be recognized and prepared for.



Source: Risk in Capability Management, Taylor, B., Jobson, N., Yue, Y., DSTL/WP25188, June 2007

Figure 2 : Risk Factors

Recommendation: DRDC should conduct research into the different understandings of risk and use of risk language in different disciplines and with respect to different risk factors. This would cover a wide span of disciplines and factors: from social sciences and political science to systems engineering and mathematics; from political and socio-cultural factors to technological and financial factors. The ISO 31000 terminology would be the natural starting point. The application focus of this work should, of course, align with the concerns of the DND enterprise.

3 The Culture of Enterprise Risk Management

At the January 2009 Conference Board of Canada Conference on ERM, practitioners and experts in the field created a quick list of 30 key issues to be addressed in ERM. Half of these issues were in the area of organizational culture and leadership. A culture and leadership fully supporting and engaged in ERM is a precondition of success. Meeting this precondition may well be at least half the battle in inculcating enterprise risk management in government.

A risk management culture is nothing new in Government. In many instances there is reason to be careful about risk for the public good: health care, food inspection, security, and the like all require careful attention to and management of risks. The cynical, however, would say that government pays too much attention to risk, and is severely handicapped by risk aversion. Nevertheless, the Auditor General will undoubtedly continue to uncover instances where risk has not been managed well.

The challenge within Government, as in many other sectors, is appropriate risk assessment and management. Often government appears to act in ignorance of good risk management practices and applies risk management tools such as regulation and rules that do not address the key consequences of risk. Undue effort is spent on managing risk of low probability occurrences of little consequence.

The challenge within Government is also to view risk management in its broadest terms where risk can have positive as well as negative results. One of the speakers at the CB ERM Conference stressed the need to use different terminology because of the negative connotations with the word "risk". This is a key part of the culture of risk management.

The participants in the CB ERM Conference identified key aspects, especially including aspects of openness and tolerance about risk which will be hard to instil in Government, perhaps especially DND. There is an in-bred aversion to failure. Management is rewarded on successful initiatives and not rewarded for taking chances and innovation leading to greater value creation (due to risk aversion).

The CB ERM Conference participants argued the need for an open and transparent culture of risk management where bad news is not hidden and uncertainty is tolerated. Organisational effectiveness and learning could be significantly improved by requiring an "oops report" – a record of errors with no associated blame or shame. Individual RM learning opportunities should be experienced through staff development. A culture of candour is necessary so that different views are expressed and discussed in natural and healthy engagement, avoiding group-think.

The CB ERM Conference participants recognized the need for strong leadership not just to instil the culture of risk management but to effectively and clearly communicate the policies and decisions on which the risk is to be managed. Senior Leadership must set policy, and create and nurture a network of risk champions. Senior management must reach to where the knowledge is, inclusively engaging the organization's expertise, and not "hide" in the meeting-room protected by outer office staffs. Risk management should be tied to performance management with the aim to increase the probability of a good occurrence and to minimise the probability of a bad

occurrence. The more clearly management understands where “we” are and where “we” are going, the better, and participants felt 25-30% of management effort should be spent on this. This clarity is necessary for good risk management, because it provides clear context and objectives. DRDC analysts must make the time to listen to senior managers’ issues and must be present at senior decision making events.

Notwithstanding the recognized importance of changing the culture, it is not simple to do. Culture takes time to change and a period of eight to ten years would not be unexpected to see the desired change fully rooted. Furthermore managing changes to culture should be done in a coordinated, thoughtful manner, not piecemeal as separate initiatives. There are always new ideas and initiatives which seem promising, but they can actually collectively be not only counterproductive but destabilizing. In the area of enterprise risk management it seems evident that neither DND nor DRDC have the experience or expertise to lead in ERM culture change.

> Recommendation: DRDC should employ judiciously over a period of years expertise in enterprise risk management and change management to assist in the capture and co-ordination of internal resources and the adaptation and adoption of risk management principles and framework, specifically supporting the development of the culture of risk. This could be either within the context of DND’s efforts or as a complement with a particular emphasis on the management of risk in research.

4 The Practice of Risk Management

Risk management has always been implicit in leadership and management activity. However while some managers have succeeded many have not and RM has been inconsistent. Modern practice in this area has served to make it explicit and deliberate, consciously and proactively exploring the possible impact of various risk factors on corporate objectives.

The deliberate approach to enterprise risk management brings consistency of approach which is especially relevant to large organizations in industry and government, and those organizations for which the consequences of the risk may have broad societal impact.

The practice of risk management in Government, DND generally and DRDC specifically will now be considered.

4.1 Risk Management in Government Departments

All Government Departments and Agencies are mandated to use integrated risk management. [2] Principles for integrated risk management are being established by Treasury Board Secretariat, in cooperation with Departments, to provide the scope and flexibility for tailored development of risk management practices. Many Departments have already developed guides for the practice of risk management in their areas. Currently IRM does not meet all risk management needs of Departments and there is cooperative work underway, led by TBS, to develop a common guide for Government use. This will draw on existing guides and references from Government, the private sector and academia; in particular the draft for the imminent new ISO 31000 standard for risk management [3] is a source document. DND and DRDC are contributing to the drafting of this guide.

> Recommendation: DRDC should work within the principles and general framework for Risk Management prepared under the auspices of TBS. These are built on broad best practices nationally and internationally, in the private sector and in government. They are general enough that they can be adapted as required.

The effort available and devoted to ERM varies among Departments. Some have small dedicated teams which provide subject matter expertise and support on demand. Most have dedicated individuals within teams that have other responsibilities within organizational entities that are responsible for strategic, long-term planning and management. The size and responsibilities of Departments result in wide divergence in the scope and scale of the need for ERM. DND is one of the few Departments which has (in DRDC) sufficient potential capacity and expertise to provide for developmental work on process and tools. Nevertheless smaller Departments and Agencies have developed tools for their specific needs.

[2] See TBS description at http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254&section=text .
[3] CSA Guideline CAN/CSA-Q850 (R2009) is intended to assist decision-makers in effectively managing all types of risk issues and adopts the general content of the ISO 31000 standard.

Science Based Departments and Agencies have met at the working level to discuss common needs and concerns for IRM/ERM. Research by nature is risky and thus these parts of government may have particular needs in relation to managing risk but more importantly explaining this to the rest of Government.

4.2 Risk Management in DND

Like other Government Departments, DND is working to instill integrated risk management in its operations. As a large organization with major components each with their own perspective and attitude to risk, the enterprise-level coordination of IRM has been slow to develop.

> Recommendation: DRDC should assist DND in enterprise level risk management within DND. It should dedicate sufficient resources, at least a small analytic team, to spearhead this effort and support DND staff. This team would focus on direct support to DND ERM, interact with the most senior levels of DND, support its processes and methods, and draw on expertise across DRDC as required.

A DRDC Contractor report [1] from 2007 addressed the risk management of DND and the CF, especially from the perspective of interoperability under a major threat both internally (joint) and externally (other government agencies). They noted progress towards integrated risk management was slower than expected in this context. They also highlighted the distinct DND and CF cultures with respect to risk management, and the challenges that entails.

Although it does not come under integrated risk management at the strategic level, the operational planning for the CF contributes at its own level with respect to operational objectives. The CF Operational Planning Process [2] includes specific attention to risk management, especially operational risk identification, assessment and mitigation.

4.3 Risk Management in DRDC

Risk management in DRDC will be considered first from the manager's perspective and then from the process perspective.

4.3.1 DRDC Managers Workshop - Issues in the Practice of ERM

The annual DRDC Manager's Meeting held in Ottawa in April 2009 included a half-day session on ERM. A plenary presentation provided background on ERM for the purpose of educating managers. This was followed by parallel breakout sessions which tackled three enterprise risk scenarios. The breakout sessions and their summary reports to a concluding plenary session provided insights on the state of understanding of risk management within DRDC.

The authors were as interested in how managers approached the risk scenarios as what they actually determined about how to manage the risk. The authors did not direct discussion, but simply observed the approach and thinking in the sessions. The observations collected were

obtained more or less at random from short visits to each of six breakout sessions and from the summary reports. Notwithstanding the limitations of this data gathering, the collective observations covered the range of risk management activity and produced useful insights.

The observations and insights gleaned from managers as they considered how to approach the three posed risk scenarios will be discussed first in relation to the first few steps in the simple model for risk management used to structure this paper. We conclude with some meta-observations about the managers' thinking about risk management.

The following resume of the managers' thinking on ERM is a construct. It builds a more reasoned and cohesive picture than was the reality during any of the individual group discussions observed. Nevertheless the composite picture is a fair reflection of DRDC managers' understanding of ERM.

The first step in risk management is to understand the objective and context of the problem. In this respect managers generally recognized the necessity of clear objectives, and understanding the scope of the problem. Some recognized the need to remain at a strategic level, but there was a tendency to "go tactical too soon". As they discussed the context and scope they discovered that a broad look at risk can be too broad to manage effectively by any single group. If all the factors affecting risk were considered, the scope could be vast, with large numbers of actors and the challenge of determining key actors associated with various risk factors quickly became overwhelming.

The managers had several insights into the nature of risk management problems. They realized that the way a problem or question is posed is often too quickly accepted, and that the way it is stated can focus the risk concerns into isolated compartments right away. It was also apparent that managers often talked about risk issues that were outside their areas of expertise. It is important to find and recognize specific pieces in context to which one can speak. High level risk problems usually involve a wide range of actors and stakeholders, with quite different risk concerns and tolerances, but very often with interconnected concerns. Complex risk interdependencies necessitate a team approach to enterprise risk management.

The strength of DRDC is in the areas of risk identification and assessment, especially its analytic approach to problems. S&T output allows DRDC to provide sound basic advice in many areas, to provide support for or conduct strategic environmental scanning and assessment, to challenge assumptions and to offer solutions. DRDC can offer an objective systems approach leading to integrated high-level solutions.

Two particular aspects of risk assessment were highlighted. First, cost modeling is very important and it is critical to understand costs over multiple years. Second, it is possible to do options analysis from a variety of perspectives, and so arrive at different appreciations of risk:

Capability view	integration with other systems
Procurement view	partner with industry
	highlight contributions that Canadian industry can deliver
	advise on offsets
Personnel view	training and recruitment
	right number of people trained for when they are needed

G of Canada view	sovereignty, industrial base, communications with allies being a global player

There were quite a few reflections on DRDC-specific concerns for ERM. Many of these actually relate to general practices and concerns for DRDC. Some reflect a fair and balanced assessment of DRDC's strength and weaknesses in the area of risk management, while others seem to be unrealistic and overly generous in assessing DRDC's past and current capabilities.

DRDC continues to need to develop and nurture its internal coordination and cross-center cooperation. This is especially true for ERM since the expertise to deal with the breadth of issues and the complexity of assessment is unlikely to reside in any one center. It was suggested that DRDC consolidate its contribution to ERM but it was countered that this view of risk problems does not recognize the need to interact with the enterprise risk effort within teams across DND.

Managers generally recognized that DRDC was capable of different levels of support in supporting different actors and stakeholders. While DRDC had good experience and expertise to support tactical and technical perspectives it was less good at supporting strategic and holistic perspectives. It was suggested that DRDC does not currently have the resources or capability to offer comprehensive and balanced support in ERM. Furthermore, DRDC does not have all the answers and would need to recognize when it was possible and necessary to go out to industry, academia and allies.

DRDC managers believe they have become better at risk management but recognize the need for improvement. While DRDC has some expertise to support ERM, it has little expertise in conducting ERM to pass on to the rest of DND. Further development of links and influence would be required for DRDC to effectively support ERM in DND. Embedding more teams with the client was seen as necessary to better understand the client's risk environment. The need is for a balance in advice and support development roles in RM. At one extreme, however, is an unhealthy view that DRDC can do anything and provide help to any aspect of ERM.

DRDC needs to be able to see the big picture, the complexity of the problem and solution spaces. An honest concern was expressed that DRDC needed to understand when it is part of the problem, advocating S&T solutions and products when a more holistic enterprise outlook is required.

In ERM there are invariably a broad set of stakeholders, actors or targets for support. Not only does DRDC need to be able to identify the stakeholders but to tailor outputs to the stakeholders, talking their language about the issues. DRDC needs to identify champions to partner with "external" actors and to understand decision making processes and structures. DRDC must recognize the value and impact possible through decision-making bodies, but also through the staffs which support those bodies.

While DRDC can provide a systems view, it needs to evaluate and improve its own systems view: seeing the big picture, considering synergies, ensuring options don't conflict and taking a through-life view when addressing capability risk.

Finally there were some concerns with supporting ERM that relate more to Departmental concerns. A lack of single point of contact often complicates and slows interaction in DND.

Coordination is often an issue, perhaps because of limited manpower stretched too thin at the working level. RM should work hand-in-glove with strategic advice and ERM should follow whatever high-level scheme (PRICIE, DOTMLPF, etc.) is used to support strategic planning. DND should anticipate and get ahead of issues and risk areas before they arise in practice.

We conclude this discussion of managers' perceptions of DRDC risk management with some general observations. It should be apparent from the above synopsis that collectively there is some insight into and depth of understanding of ERM concepts and issues. Whether this is reflected in DRDC management practice is less clear. Certainly each breakout group in the workshop had a distinctive flavour to its approach. Some were thoughtful and strategic, while others appeared more reactive and focused on details. Individuals within the groups also seemed to have a wide variation in their understanding of RM and certainly ERM.

> Recommendation: DRDC should find a focal point for its support to risk management within DND, and not seek to provide support everywhere. DRDC should focus its initial efforts to support ERM in the area of its strengths – risk identification and assessment – and seek to engage senior decision makers by that route. There is fertile ground for both advice and tools development in these two aspects of ERM. Furthermore support in this area should derive insights and provide alternatives for risk mitigation.

4.3.2 DRDC Processes - Issues in the Practice of ERM

In the previous sub-section we created a picture of the general understanding of ERM by DRDC managers. While collectively there appeared to be a reasonable understanding and even significant insights, it remains to examine whether in practice risk management is well incorporated in DRDC processes and daily decision making. Certainly effective managers will individually incorporate risk management in their thinking – even if only intuitively. However, the question is whether risk management is properly and explicitly incorporated into strategic, program and project management.

It is easiest to start with well documented and defined processes. Thus program management, TDPs, and TIFs should be examined with risk management in mind. While some of these processes do ask for risk identification, the risk assessment and mitigation aspects are often not fully pursued. While there is some attention given to risk in Program and TDP management, it is not systematic and it is more to cover the bases than to exploit for prudent management. The issue may be as much a matter of the emphasis and seriousness with which risk is addressed as anything.

New technology or technology concepts naturally introduce elements of risk – both positive and negative. There is a need to examine the risk carefully before introducing new technology or technology concepts as viable operational options within DND. This is not routinely done in DRDC, but should begin in the TIF and early applied research aspects of the program. There is potentially a huge gap in the ability to manage risk from concept through to mature technology. Very early on the research concept may not have sufficient definition to identify risks, and the risks are more associated with the technical aspects of developing the idea than with the operational aspects of using the idea. Nevertheless the operational risk needs to be studied early

on, to confirm the value and ease the eventual insertion when the technology or methodology is mature.

For more mature technology development there is a need to include risk management in several dimensions – not just project risk, but risks associated with eventual operations, procurement, personnel, "politics", engineering, etc.

It is harder to determine whether risk is carefully managed at the strategic level by DRDC. The senior managers are experienced and much of this comes intuitively. The fact that no risk identification, assessment and mitigation is done in association with the S&T PAA, for example, does indicate that ERM is not conducted at the strategic level of DRDC.

> Recommendation: Expedition 11 should include activity to develop ERM support to DND and to identify changes required to adapt DRDC planning, program, and project processes to explicitly include RM.

5 Research in Risk Management

Research in risk management can be pursued in several different directions. Research in risk management can either support some aspect of the risk management process or it can apply risk management techniques to technology research. In addition there are of course aspects of risk management research in numerous specific areas such as human resources, concepts, strategy, resource allocation and so on.

Research on development of process at its most basic would require building upon the copious fundamental research of broad significance in applied mathematics. This research at its most applied would develop or tailor specific processes, tools and methods to support the specific activity of DND enterprise management, including strategic planning and risk management.

A unique DRDC role in the research community could be to apply risk management techniques to technology research. This will be discussed briefly later.

5.1 Theoretical Risk Management Research

The general process of risk management has been well developed, and its general principles are being incorporated into government. The main challenge here would be to tailor this general guidance, and determine the particular implementation of risk management process which is most intuitive and efficient within the DND and CF environment. There are multiple variations of process which could be considered.

The general process must be supported with identification and assessment of risks for specific factors and objectives within the broader context. There are some risk factors for which risk identification and assessment is a well developed art or science (e.g. financial) while there are other factors for which it is not (e.g. political). There are also some technical areas within the general process that are left unspecified. Some of these technical issues will be discussed shortly. The degree to which these are resolved is the degree to which there can be confidence in the robustness of the risk management process and the accuracy of risk assessment.

The difficulty with knowing what assessment tools and techniques may be most worth developing for enterprise risk assessment relates in part to the different nature of risk in different areas.

Earlier the complexity of enterprise risk management was discussed, and the diverse nature of risk factors and the possible synergies between them were noted as areas which complicate risk management. The disparate nature of risk across diverse factors makes enterprise risk assessment a challenging component of strategic planning. The possible synergies and interrelationships between risk factors suggests work on risk logic models, factor grouping and normalization of factors might be valuable areas of research for high-level assessment and decision making with respect to risks.

At the enterprise level objectives may be simple to state, but complex and inter-related in practice. At this level, someone's result or output is someone else's input. The translation of objectives into measurable proxies, even if these are qualitative, is important. The outcome measures (or proxies) must be clearly defined however. It is important to make a clear distinction between uncertain results related to objectives and risk factors that contribute to that uncertainty and potential impacts. As noted above, simple structural logic models may hold promise. The recognition of complexity and interdependent factors could be captured by expert assessment without explicit dependency models. For example, "political" risk could influence schedule risk which could influence cost risk although each of these is of a different nature and would be subject to expert assessment.

Although some work has been done, a question that seems not to be well addressed in the literature is cost benefit analysis of risk management. There seems to be a presumption that risk management is good and always worth doing. Intuitively it makes sense that being aware of the possibility of risks and working to mitigate negative effects of risk can only be beneficial. However, there must be limits to this. It is not worth creating large systems (with ongoing cost) to avoid financial risk, for example, if the cost of doing so outweighs the expected loss. The literature does certainly make estimates of savings or cost risk avoidance by the use of risk management after the fact. There are certainly examples where risk has not been well managed with attendant loss of life or money, but it is difficult to know how to determine in advance or in a general way the benefit that research on risk assessment techniques might provide. Even harder to know is which research on risk assessment techniques would be most worth pursuing.

In relation to costs and benefits it has been observed that managers and their staffs consistently overestimate benefits and underestimate costs [2]. Indeed, forecasts are "constantly and remarkably inaccurate". There are a variety of reasons for this but they are not essentially technical in nature (i.e. related to data and models). Instead the reasons have mainly psychological and political causes. This has great significance for the assessment of risk at the enterprise level. It suggests that the nature of uncertainty and risk *perception* is an essential element in risk assessment and management. This must be well understood in order to clearly recognize bias, overconfidence, alarmism, and the like and its impact on risk assessment.

Risk management at its heart involves the likelihood estimate of risk. The likelihood of risk is estimated in different ways according to the different manner in which uncertainty is described and measured. Thus, for example, political uncertainty (non-repeatable, chaotic, perception-based, hard to measure, etc.) is of quite a different nature than the uncertainty of component failure (statistical, highly predictable, objective, physically measurable, etc). There are various probabilistic and other models for assessing uncertainty in different domains (e.g. Bayesian, frequentist, fuzzy, possibilistic, …) and it is important to know what models are appropriate in which domains, how they relate, and how best to use them. With simple probabilistic expressions of uncertainty, for example, it is best to use distributions rather than point estimates in risk assessment. It should be clear, then, the difficulty in enterprise risk management where different models of uncertainty underlie different risk factors, and make them hard to compare.

The authors began looking into enterprise risk management with the expectation that there might be classes of enterprise risk management types, that is groups of different domains in which the nature and treatment of risks is similar or conversely quite different. Thus, for example, the health care domain might have a lot in common with military operations, say, but little in

common with the financial domain. It was expected that domains might be classed based on complexity, nature and degree of uncertainty, dominant factors and the like. This kind of class association was not immediately evident in the literature, but might bear further consideration.[4]

Some research attention has been focused on risk where the likelihood is low but the consequences are extreme, so-called Low Probability/High Impact Scenarios. These kinds of risks are typical concerns in military and security domains. These considerations have led to various concepts such as Taleb Distributions, the Hurst Exponent (to deal with long time events), Life Extinction Events, Zero-Infinity Dilemmas (which characterize the choice of nuclear power: the risk of a mishap is incredibly small (close to zero) but if one does occur, the cost and repercussions are enormous (approaching infinitely large) [3].

The above discussion illustrates the fertile domain for fundamental research which would support risk assessment and management. Not all of this is necessarily appropriate for DRDC to pursue itself, but familiarity with the research in these areas should improve the understanding and effective implementation of risk management.

More practical, applied research by DRDC in support of DND is discussed next.

5.2 Applied Risk Management Research in DRDC

RM research in DRDC could be pursued along both fundamental lines as noted above or on more applied lines which will be addressed now.

DRDC should build on its existing strengths. Thus it should focus its support and research firstly in the areas of risk identification and risk assessment. It should also use its expertise in the development of high-level planning processes to aid DND in tailoring, adapting and customizing the general process to its specific needs. Risk assessment should also be exploited to gain insights into risk mitigation through techniques such as sensitivity analysis and experiment.

In a general way DRDC research and tools development in systems modeling, systems dynamics, systems analysis and complex systems all should support the enterprise-level management of risk.

Military capability development in DND is a complex activity which inherently is full of risk – future operational risks, policy risks, and program risks. Just as capability development must measure and assess quite divergent types and nature of capability, so the risks are diverse and of different natures.

Applied research in multi-factor risk analysis should be designed around whatever high-level scheme(s) (PRICIE, DOTMLPF, etc.) might be used for strategic planning. This involves both the notion of "aggregating risk" and defining simple robust metrics to describe capability portfolios. Techniques developed in the financial services sector for risk management of investment portfolios may be transferable to defence planning. Specifically tools are required to examine force structure risks such as: the likelihood and impact of required force elements being

[4] The DRDC Center for Security Science is currently working on an All-Hazards Risk Taxonomy which might be of relevance.

available in the future; the likelihood and impact of mission success in future horizon scenarios; and the likelihood and impact of stated policies being followed. The assessment of future operational risks requires development of OR&A tools to assess outcomes at the joint force level. The assessment of policy risks requires method and tools to combine assessment of future operational risks and force structure risks to assess likelihood of policy objectives being met. All of this would naturally build on and into force structure capability analysis already supported by DRDC.

Risk analysis is in various ways a key element of strategic planning. Program risk must assess the likelihood and impact of the investment plan (IP) delivering to cost and schedule. There must be a clear understanding of the relationship between project level issues and overall cost and schedule. In particular future costs, or at least the variability in these and their impact, must be well assessed. Program risk also involves risks associated with the overall effectiveness and long term sustainability and affordability of the entire capability portfolio. The capability to simulate the IP under different assumptions is required.

Creating systems to work inside constraints relies on risk management. For example, the use of UAVs for surveillance purposes in domestic airspace is an exercise in risk management which has implications for system design and operations. Similarly, consider applying the tools of risk management to developments in urban warfare where constraints on rules of engagement and "collateral damage" are vital concerns.

The use of risk management in assessing technology concepts should begin early and continue through development. Thus operational risk assessment should be conducted early on new concepts to gauge likely effectiveness against various planning scenarios.

Risk management is ultimately about improving decisions so research into techniques to assess decision quality would be appropriate.

> Recommendation: DRDC should undertake a mix of fundamental and applied research in ERM, short-, mid- and long-term as it applies to DND risk factors. At the enterprise level key aspects of this research will involve both human aspects of risk, multi-factor risk assessment and tools and methods for the evaluation of ERM implementation itself. This work aligns with research capability development in complex systems.

5.3 Risk Management in Other TTCP Nations

The defence departments in all nations have to consider risk in their high-level planning. DRDC scientists have links to peers in Allied nations working in the same area. This is currently a topic of some interest, especially in the UK and the US. Recent and ongoing initiatives include the following:

- A new 3-star level Strategy Director organisation has been stood up in the UK. OR&A staffs there are seeking to develop improved approaches to risk management at the strategic level and are interested in developing approaches with Allied nations.

- As part of the preparations for the 2010 Quadrennial Defence Review the Military Operations Research Society held a workshop in Washington DC *Strengthening the Next QDR Through Timely and Relevant Analysis*, 13-15 January 2009. This workshop covered analytical approaches to achieving balance at the strategic level, which is essentially a risk management problem. Information on the Integrated Cross-Capability Assessment and Risk Management (ICCARM) strategic risk assessment methodology developed by the Institute for Defense Analyses, used in the previous QDR, has been provided to the authors. The opportunity exists to work with the ICCARM developers if such an approach was considered suitable for exploitation in DND. ICCARM represents an approach aligned to ERM in that it captures the sensitivities to risk of senior leadership.

- The US has recently implemented a Capability Portfolio Management (CPM) instruction. This is to cover a level of aggregation between individual capabilities and the whole of force, similar to the Canadian capability Domains. CPM is a component of Capability Based Planning and US implementation staffs recognise the need to develop appropriate risk management approaches to ensure balanced capability portfolios.

- A new project has been created under TTCP JSA TP-3 (Joint and Combined Analysis) to link the US CPM implementation effort to UK, Canadian and Australian OR&A staffs working in higher-level risk management. The intent is to propose risk management approaches appropriate to supporting the intermediate (portfolio) and high (whole of force) levels of aggregation in defence planning, with a specific aim of providing a robust risk management approach for Capability Based Planning. This study also overlaps in its areas of interest and membership with the NATO SAS-076 study into CPM.

The international links available through DRDC collaborative activities will ensure that any proposals developed are benchmarked against Allied best practice and benefit from exposure to the state of the art thinking in those nations.

6 Two Partial Case Studies in Enterprise Risk Management

The following partial case studies are meant to illustrate the nature of ERM, from the strategic level perspective. They look at first ERM itself and second ERM and the S&T Program.

The two case studies show, among other things, the use and value of both qualitative and quantitative elements in risk management. Qualitative risk management can be used when it is not possible to quantify factors and measures; it can be systematic and adhere to RM principles and logic.

The case studies also demonstrate the value in RM facilitation DRDC could play to guide and frame strategic discussions.

6.1 Enterprise Risk Management for Enterprise Risk Management

The introduction of ERM is a project which can itself be considered for risk management. This example is not intended to be thorough or complete, rather to provide an abbreviated bullet-point version of the steps in risk management in some key risk areas. This case study does, effectively, summarize key issues and recommendations of this paper.

Context:

Senior management establishes an agreed context for implementation:

- Integrated RM is mandated for Government Departments and Agencies.
- ERM is used widely in government and industry.
- Uncertainty is a natural part of highly complex systems.
- Risk can and should be managed.

Objective:

Senior management provides objective for implementation:

- ERM informs all decision making especially to reduce force of negative impacts

Risk Identification:

Implementation team conducts exercises with senior management to elicit key risks to the implementation of ERM. These are identified as:

1) Culture
2) Cost
3) Technical
4) Resources
5) Scope

Risk Assessment:

Implementation team builds on senior management risk identification to develop appreciation of issues:

1) Possible lack of strong leadership will limit broad uptake and overall effectiveness. Cultural differences are very likely to cause misunderstanding, and miscommunication.
2) Highly likely costs will not be well predicted with cost of implementing risk management becoming uncontrolled. Highly likely cost of not doing ERM is ignored causing occasional catastrophic outcomes.
3) Highly likely that improper risk assessment will lead to lack of success and confidence in ERM. Possible that lack of consistent and scientifically based assessment techniques will lead to improper assessments, confusion and conflict among major stakeholders.
4) Likely that money and people resources required to properly implement ERM will overtax working level and lead to slowdowns in productivity.
5) Likely that scope of effort is too ambitious with resultant disillusionment and abandonment of broad deliberate RM.

Risk Mitigation:

Implementation teams develop mitigation approaches to identified risks.

1) Leadership assumes active lead. External experts in ERM work with all levels over a period of time to instill good practice and proper mindset. Research on fundamental natures of uncertainty which cause cultural differences to get at roots of cultural problems.
2) Determine actual marginal costs to include various degrees of risk management in practice. Research into costing ERM. Cost actual efforts.
3) Develop expertise in assessment of risk in different strategic areas. Use teams of experts to assess risk in critical risk areas. Research theory and best practice in multi-factor risk environments. Research nature of uncertainty and risk assessment in diverse risk areas.
4) Provide adequate resources for risk management. Provide some dedicated resources for risk management support and assessment. Monitor resources actually required to implement ERM and resulting timeline changes for projects across their whole life.
5) Incremental introduction of ERM. Limit marginal increases in process requirements due to RM to most significant risk areas.

Risk Monitoring:

Implementation team develops plan to monitor progress and create feedback

1) Monitor and report resources actually required to implement ERM.
2) Monitor and report resulting timeline changes for projects across their whole life.
3) Report and communicate good practice tips.
4) Foster open “no-blame” culture to encourage the sharing of learning experiences including reports of errors and failures.

End State:
Through taking a top-down approach building upon senior management perspectives an implementation plan has been developed. The feedback mechanisms will identify whether the mitigation strategies are working and if new issues are emerging. The ERM implementation is thus dynamic and responsive to management direction and emerging data from the business.

6.2 Enterprise Risk Management and the DND S&T Program

DRDC RDEC proposed conducting a case study for ERM on the S&T PAA. This not only could be highly instructive and useful, but it could be a good example to the rest of the Department. Other Departments and Agencies use the PAA as a basis for their ERM.

This partial case study will be presented as a work in progress, which eventually will require RDEC involvement. We follow the basic structure of the previous example and weave discussion through it, indicating issues and questions which will need to be resolved.

Context:

Senior management establishes an agreed context:

- The DND Program Activity Architecture (PAA) with associated Performance Measurement is mandated by Government.
- The PAA demonstrates the linkage between program activities DND delivers and the outputs and outcomes it is trying to achieve.
- The S&T Program is one component of the DND program activity and so the S&T PAA is a sub-set of the DND PAA.
- The S&T Expedition Series is the change agent for S&T Program delivery within DND.

Clarification is required in the nature of the PAA and how this relates to objectives. On the one hand, the PAA may be seen to embody the objectives of DND or DND S&T as realized in its outputs and outcomes. However, the objectives of DND and DND S&T are more clearly stated elsewhere, e.g. in the Canada First Defence Strategy and in the S&T Strategy, respectively. On the other hand, the PAA may be seen as a risk mitigation tool used to aid decision making and ensure DND objectives and DND programs are aligned. In other words, the PAA is the result of an ERM process which determines that a PAA is required to mitigate the risk of not meeting objectives. The risk management associated with implementation of the PAA is thus tactical rather than strategic, oriented to the project rather than enterprise level.

It is worth noting that S&T contributes to DND PAA outputs and outcomes, in addition to its own assigned branches of the PAA. The two are not strictly orthogonal as they are inter-dependent.

There is or should be strong connections between S&T objectives, the S&T PAA and the S&T Expedition series. Expedition 09 as the change agent for the delivery of S&T to the DND

enterprise should reflect the objectives of DRDC within the DND enterprise. There should thus be a close association between the DND S&T PAA and the thrusts of Expedition 09. Presumably Expedition 09 is aimed at mitigating the most important risks to meeting the objectives of DRDC within the DND enterprise. We will use the thrusts of Expedition 09 as a framework for talking about risk.

Objective:

Senior management establishes the objective:

- *S&T PAA:* S&T knowledge and innovation informs defence and security decisions.

OR

- *Expedition 09:* DRDC has maximum impact on defence and security.

Alternatively there may be some other objective that is really what RDEC would like to develop its ERM strategy around. Here the "objectives" are taken from wording in the S&T PAA and Expedition 09. Neither is very concrete or measurable. This makes it difficult to be specific about risks and relative importance of risks but still provides an opportunity to force a clarification of objectives.

Risk Identification:

Implementation team conducts exercises with senior management to elicit key risks to the objective of the PAA.

These can be identified within the framework used for Expedition 09, which is:

1) S&T Capabilities & Capacity
    a. Capability management
    b. Corporate services capability
    c. Management capability
    d. Resource allocation
2) S&T Program & Activity
    a. Enterprise governance
    b. Technology management
    c. Procurement practices
    d. Program management
3) S&T Influence and Relationships (connection to Departmental and Federal agendas)
    a. Link to federal S&T strategy
    b. Link to public security S&T strategy
    c. Link to DND core processes
    d. Link to DND risk management

Each of these areas will have a list of risk factors associated with them.

The scope of the risk identification is thus huge. To form a strategy for dealing with identified risks, it is essential to focus on the most critical issues affecting the S&T Program within DND. David Apgar proposes a "simple" process to planning which we can adapt and use to illustrate

how to filter the many risks and identify the few that need to be managed.[5] He progressively simplifies the list of risks and focuses on those which have the greatest impact, are most uncertain or uncontrollable and the most harmful.

At this point, then, he would first ask which risk factors have the greatest impact. It is expected the risk factors with the greatest impact probably occur in the following areas:

1) S&T Capabilities & Capacity
    a. Capability management
    d. Resource allocation
2) S&T Program & Activity
    b. Technology management
    d. Program management
3) S&T connected to Departmental and Federal agendas (Influence and Relationships)
    b. Link to public security S&T strategy
    c. Link to DND core processes
    d. Link to DND risk management

Next Apgar would ask which risks from within this smaller selection of risk areas are the most variable, uncertain or uncontrollable. We expect the most variable, uncertain or uncontrollable risk factors are probably in the following areas:

2) b. Technology management
3) c. Link to DND core processes
1) a. S&T Capability management
2) d. Program management

Specific risks of high impact that are highly variable, uncertain or uncontrollable identified within these key areas are:

1) Technological barriers
2) Operations
3) Organizational barriers
4) Time to respond
5) Knowledge growth
6) Political priorities

For Apgar the focus would be on developing a strategy around managing these risks.

Risk Assessment:

Implementation team builds on senior management risk identification to develop appreciation of issues:

[5] Apgar's process is outlined in a presentation given to the January 2009 Conference Board of Canada Conference on ERM. The philosophy may be found in Apgar's book listed in the Bibliography.

1) Variable likelihood that failure of technology concept development will lead to technology insertion failures. Possible that over-(under-)estimation of value of technology value will lead to lack of confidence in S&T advice.
2) Highly likely that nature of future operations will not be well predicted resulting in misdirected research efforts and poor S&T advice. Likely that successful direct S&T support to operations will lead to better acceptance of S&T advice.
3) Highly likely that lack of participation in organizational decision making will mean S&T is ignored. Probable that close association with decision makers leads to improved S&T inputs to decision making. Highly likely that complex indirect S&T support system will result in marginalization. Highly likely that constant organizational change in S&T and/or DND will cause disconnects from decision making and inefficiencies.
4) Highly likely that late S&T response to DND needs leads to support not being sought in future. Highly likely that proactive preparation leads to better response times and greater appreciation of value of S&T. Highly likely that long-term view of research not appreciated in short-term demands of DND resulting in lack of influence.
5) Probable that breadth of knowledge required in S&T advice to DND grows beyond means to support it all resulting in missed opportunities. Probably that in some areas knowledge will grow at a rate that makes it impossible to develop S&T expertise either internally or externally quickly enough resulting in ill-informed advice.
6) Highly likely that political priorities change frequently resulting in abandonment or shifts in DND and S&T priorities. Possible that political aspirations are unachievable or unrealizable with resultant disillusionment and drift in objectives.

Apgar would continue his strategy development by further focusing on those risks which are the most harmful. For this exercise suppose that organizational barriers are the most harmful risk factors.

Risk Mitigation:

Implementation teams develop mitigation approaches to identified risks.

The strategy will focus mainly on the most harmful risk factor(s) – in this case organizational barriers.

3) Full integration in decision making bodies. Co-locate with key DND decision makers. S&T staff “shadow” and develop relationships with decision support staff at all levels. Simplify access to S&T support. Keep organizational changes to a minimum; develop long-term stability.

Risk Monitoring:

Implementation team develops plan to validate choices taken and to monitor progress and create feedback

End State:

The result should be a focused strategy for meeting the objectives of S&T within the DND enterprise. The strategy focuses on the risks with the most impact which are the most variable, uncertain or uncontrollable and ultimately the most harmful. This strategy will provide a basis for change in an Expedition plan.

Clearly this is illustrative. It combines the process for ERM with a simplifying process to develop a focused strategy for ERM. RDEC managers should participate in such a process clarifying context, objectives, measures of success and key risk areas. The key risk areas are those which would keep RDEC managers from meeting their S&T objective(s). These need to be then simplified to the most critical elements for management focus and deployment of resources.

> Recommendation: To define Expedition 11, DRDC RDEC should engage external expert support in ERM to work with them in an ERM approach which serves to simplify and focus the strategy to achieve S&T objectives within the DND enterprise.

7 Concluding Discussion

Risk management is an integral part of doing business and it is not a new activity. But it can be done more or less well, more or less deliberately, more or less systematically and more or less effectively. DND is like other Departments in its intent to do it better, more deliberately, more systematically and more effectively at all levels.

What DRDC is already doing in much of its activity supports DND risk management at various levels. DRDC's knowledge, studies and innovation are necessary, if not sufficient, to support decisions and risk management at many levels. DRDC needs to build on the strengths of its current capability in a focused manner, beginning at the strategic level where the broadest impact will result.

Risk management at the enterprise level has not been effectively conducted in a deliberate manner in DND or DRDC. At this level, different skills and capabilities are required than at other levels. The nature of the risk space is diverse and interconnected across risk factors. Senior managers will have experience and judgment which provide insight into risk management, but they need support to do it deliberately, consistently and on a solid analytic basis. Risk assessments at the enterprise level are not simple (or complex) rollups of lower level risks. The risks and risks assessment are different in nature at the high level.

A risk management culture is the essential ingredient for success. Risk management cannot be seen as a means to cover one's backside from audit. It is about making decisions with a broad awareness of the positive and negatives impacts of various factors and their likelihood. This leads to more robust and proactive decision making.

Taking a deliberate approach to risk management at the enterprise level allows decisions to be taken in a holistic way at the level which affects organization objectives, rather than piecemeal at the lower levels and within silos. Risk management is not conducted in a separate silo. To be most effective it is necessarily an activity integrated across areas and between levels.

Risk management can help shape the questions to be addressed at the enterprise level – it clarifies the organizational objectives and the high-level risks that affect them. By clearly analyzing how the objectives are affected by risk, it is possible to better respond with more robust solutions across the risk space. Risk management must be perceived as helping management tune their filters and not as second-guessing them.

Risks are often defined in terms of both likelihood and impact. Both must be considered as distributions reflecting a range of possibilities within a 'space' rather than as prescriptive single point cases. Doing so avoids "point scenario trap" where possibilities are too narrowly or specifically defined with resulting lack of robustness. This avoids optimizing on narrow parameters to determine "best" solutions, and leads to solutions which are more robust across a range of likely alternatives.

Finally, whether in DND or DRDC, some general pointers should be reinforced which represent a synthesis of lessons learned from many organizations involved in implementation of Risk Management at the Enterprise level [6]:

1) focus on corporate objectives;
2) ask senior managers what will prevent them from achieving their objectives
    a. capture their assumptions
    b. help define action items to respond to risks
    c. run workshops to assess/validate risks and probabilities
3) keep risk assessment simple
    a. accept subjective assessments supported by data
    b. don't be over-reliant on tools and trust the judgement of experienced managers
4) monitor progress and create feedback process to improve risk identification

And remember that changes take time to implement!

[6] This is taken from the January 2009 Conference Board of Canada Conference on ERM.

References

[1] Barbara D. Adams, Sonya Waldherr and Kenneth Lee, *Interoperable Risk Management in a Joint Interagency Multinational Environment*, DRDC No. CR2007-068, August 2007

[2] *The Canadian Forces Operational Planning Process*, Canadian Forces Joint Publication 5.0 (CFJP 5.0) B-GJ- 005-500/FP-000GOvenrment of Canada, April 2008

[3] Bent Flyvbjerg, "From Nobel Prize to Project Management: Getting Risks Right", Project Management Journal, August 2006, Vol 37, No 3, 5-15

[4] Risk Enumeration And Utility: Risk Views Draft 0.C, Uncontrolled Abstract, Source: CA001/YF910/IA010/06/124 19 January 2007

Bibliography

This bibliography lists resources relevant to enterprise risk management. It is a sampler which is organized to provide pointers in a variety of different directions on the subject. It is not intended to provide a comprehensive or foundational basis for understanding risk management.

General Risk Management

1. Enterprise Risk Management – Integrated Framework, COSO Executive Summary, Sept 2004

2. Institute of Risk Management (IRM) Risk Management Standard, 2002

3. Donald L Kohn, "Crisis management - the known, the unknown, and the unknowable", Wharton/Sloan/Mercer Oliver Wyman Institute Conference, "Financial Risk Management in Practice", Philadelphia, 6 January 2005

4. Bent Flyvbjerg, "From Nobel Prize to Project Management: Getting Risks Right", Project Management Journal, August 2006, Vol 37, No 3, 5-15

5. Courtney, H. et al., Strategy under Uncertainty, Harvard Business Review, Dec 1997

6. Hubbard, D. The IT measurement Inversion, CIO Magazine, Jun 2007

7. Hubbard, D. *How to measure anything: Finding the Value of Intangibles in Business*, Hubbard Decision Research 2007

8. Hubbard, D. *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley and Sons, 2009

9. Buehler, K et al. Owning the Right Risks, Harvard Business Review, Sept 2008

10. Wittenberg A. McDowell T. Engaging the Board in Risk-Adjusted Decision Making, Ivey Business Journal, Mar/Apr 2007

11. David Apgar, *Relevance: Hitting Your Goals by Knowing What Matters*, John Wiley and Sons, 2008

12. Paul Slovic, *The Perception of Risk*, Earthscan, 2000

13. D. Del Bel Belluz, Chapter: "Operational Risk Management" forthcoming in John R.S. Fraser and Betty J. Simkins (editors), *Enterprise Risk Management Compendium*, John Wiley & Sons, Inc. 2009

14. D. Del Bel Belluz, Risk Management Made Simple E-Zine, https://riskwise.net/eZine.html (last visited 6/8/09)

Defence and Security Risk Management

15. *Risk Management Guide for DOD Acquisitions*, Sixth Edition, Version 1, DOD, August 2006

16. Svetoslav Gaidow and Seng Boey, *Australian Defence Risk Management Framework: A Comparative Study*, DSTO Systems Sciences Laboratory, DSTO-GD-0427, February 2005

17. DSTO Tiger Team for Technical Risk Assessment: Jim Smith (Chairman) et al, Technical Risk Assessment of Australian Defence Projects, DSTO Information Sciences Laboratory, DSTO-TR-1656, December 2004

18. George Haddow, *Case Studies in Emergency and Risk Management* (Final Book Outline submitted to Department of Homeland Security/FEMA), Request No.: HSFEEM-04-P-0345, Requisition/Reference No. E393172Y, September 20, 2004

19. David R. Mandel, "Threats to Democracy: A Judgment and Decision Making Perspective", Analysis Social Issues and Public Policy, Vol 5, No 1, 2005

20. David R. Mandel, "Are Risk Assessments of A Terrorist Attack Coherent", Journal of Experimental Psychology: Applied, 2005, Vol 11, No 4, 277-288

21. David R. Mandel, *Toward a Concept of Risk for Effective Military Decision Making*, DRDC Toronto TR 2007-124, December 2007

22. Barbara D. Adams, Sonya Waldherr and Kenneth Lee, *Interoperable Risk Management in a Joint Interagency Multinational Environment*, DRDC No. CR2007-068, August 2007

23. Schneier, Bruce, "The Psychology of Security", January 21, 2008 http://www.schneier.com/essay-155.html (last visited 7/7/09)

24. GAO Report on Defence Acquisition: Fundamental changes are needed to improve Weapons Program Outcomes, 25 Sep 2008

25. Camm, Frank, et al, *Managing Risk in USAF Planning*, RAND Corporation, 2009.

26. Ward, D. Quaid, C. The Pursuit of Courage, Judgment, and Luck, Defence AT&L, Mar-Apr 2007

Non-Defence Risk Management

27. Enterprise Risk Management: Discussion Document [ERM for the Health Industry], Powerpoint Presentation, July 30, 2003 www.casact.org/education/rcm/2003/ERMHandouts/health5.ppt (last visited 7/7/09)

28. Ward R. H. Ching, “Enterprise Risk Management: Laying a Broader Framework for Health Care Risk Management” http://catalogimages.wiley.com/images/db/pdf/0787967971.01.pdf (last visited 7/7/09)

29. Rogachev, A. Enterprise Risk Management in a Pharmaceutical Company, Risk Management 2008, 10, (76-84), Palgrave

30. Enterprise Risk Management in the Insurance Industry, Powerpoint Presentation, July 30, 2003 www.casact.org/education/rcm/2003/ERMHandouts/health5.ppt (last visited 7/7/09)

31. HLB Decision Economics Inc., “Canadian Firearms Program Review: Business Case Assessment and Risk Analysis, Final Report”, Department of Justice, Canada, 31 January 2003

32. “The Financial Policymaker's Bind: "The Known, the Unknown and the Unknowable"”, February 23, 2005, Knowledge@Wharton http://knowledge.wharton.upenn.edu/article.cfm?articleid=1139 (last visited 7/7/09)

Technical Issues in Risk Management

33. Risk Enumeration And Utility: Risk Views Draft 0.C, Uncontrolled Abstract, Source: CA001/YF910/IA010/06/124 19 January 2007

34. A. Carbone, G. Castelli, and H.E. Stanley, “Time dependent Hurst exponent in financial time series”, Physica A 344 (2004) 267-271

35. Yoav Ben-Shlomo and Diana Koh, “A Life Course Approach to Chronic Disease Epidemiology: conceptual models, empirical challenges and interdisciplinary perspectives”, International Journal of Epidemiology, 2002: 31: 285-293

36. De Stavola, Bianca L. et al, “Statistical Issues in Life Course Epidemiology”, American Journal of Epidemiology Vol. 163, No. 1, 2005

List of symbols/abbreviations/acronyms/initialisms

CB	Conference Board (of Canada)
CF	Canadian Forces
CORA	Center for Operational Research and Analysis
CPM	Capability Portfolio Management
DND	Department of National Defence
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DRDC	Defence Research & Development Canada
ERM	Enterprise Risk Management
ICCARM	Integrated Cross-Capability Assessment and Risk Management
IP	Investment Plan
IRM	Integrated Risk Management
ISO	International Standards Organization
NATO SAS	North Atlantic Treaty Organization Systems Analysis and Studies
OGD	Other Government Department
OR&A	Operational Research and Analysis
PAA	Program Activity Architecture
PRICIE	Personnel; Research & Development and Operations Research; Infrastructure and Organization; Concept, Doctrine and Collective Training; Information Management; and Equipment, Supplies and Services
QDR	Quadrennial Defense Review
RDEC	Research and Development Executive Committee
RM	Risk Management
S&T	Science and Technology
TBS	Treasury Board Secretariat
TDP	Technology Demonstration Program
TIF	Technology Investment Find
TTCP	The Technical Cooperation Panel
TTCP JSA TP3	TTCP Joint Systems Analysis Group Technical Panel 3
UAV	Unmanned Aerial Vehicle

Distribution list

Document No.: DRDC CORA TR 2010-035

LIST PART 1: Internal Distribution by Centre

1	DG DRDC CORA	by email:	ross.graham@drdc-rddc.gc.ca
1	R Dickinson, DRDC CORA (HC + PDF)		
1	B Taylor, DRDC CORA (HC + PDF)		
1	DRDC CORA Library (HC + PDF)		
4	TOTAL LIST PART 1		

LIST PART 2: External Distribution by DRDKIM

1	ADM(S&T) (HC)		
1	COS(S&T)	by email:	rene.larose@drdc-rddc.gc.ca
1	DGSTO	by email:	rick.williams@drdc-rddc.gc.ca
1	DGRDCS	by email:	Lesley.ullyett@drdc-rddc.gc.ca
1	DG DRDC ATLANTIC	by email:	JamesS.Kennedy@drdc-rddc.gc.ca
1	DG DRDC VALCARTIER	by email:	guy.vezina@drdc-rddc.gc.ca
1	DG DRDC TORONTO	by email:	ross.pigeau@drdc-rddc.gc.ca
1	DG DRDC SUFFIELD	by email:	cam.boulet@drdc-rddc.gc.ca
1	DG DRDC OTTAWA	by email:	maria.rey@drdc-rddc.gc.ca
1	DG DRDC MPRA	by email:	susan.truscott@drdc-rddc.gc.ca
1	DG DRDC CSS	by email:	Anthony.ashley@drdc-rddc.gc.ca
1	E Pitula, PM Expedition 09	by email:	ed.pitula@drdc-rddc.gc.ca
1	K Dalvi, DDFP 4-2	by email:	kumar.dalvi@forces.gc.ca
1	G Clark, DGIMSP	by email:	gail.clark@forces.gc.ca
1	DRDKIM (PDF)		
15	TOTAL LIST PART 2		

5 TOTAL COPIES REQUIRED

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Enterprise Risk Management

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Dickinson, R.G.; Taylor, B.

5. DATE OF PUBLICATION (Month and year of publication of document.)

March 2010

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

49

6b. NO. OF REFS (Total cited in document.)

0

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC CORA TR 2010-035

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Enterprise Risk Management (ERM) is the process of managing risk from an organization-wide perspective, in order to achieve an organization's overall corporate objectives. This is often a high-level view of the general process of Integrated Risk Management (IRM) which brings a systematic and deliberate approach to the management of risk, integrated throughout the management culture at all levels. This paper examines the nature of ERM in order to make recommendations on the way ahead on ERM for DRDC within the DND enterprise. It explores ERM both from the perspective of DRDC's understanding and application internally, but also from the perspective of DRDC's possible contributions to the research and development of ERM tools and practice within DND. This paper describes: the general ERM process; the importance of a supportive ERM culture; the results of a DRDC management workshop on ERM; the practice of ERM within peer organisations; and suggestions for possible research areas in ERM. Two partial case studies demonstrate the application of enterprise risk management to high-level objectives, first to enterprise risk management itself and then to the science and technology program within DND.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Risk; Risk Management (RM); Integrated Risk Management (IRM); Enterprise Risk Management (ERM); Risk research

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca