National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

BASELINE STUDY: INTEGRATED RISK MANAGEMENT WITHIN THE DND/CF

Conducted Jointly with Deloitte & Touche

January 2004

1000-6-4 (CRS)



Canada

CAVEAT

Note to Reader: This report captures the results of a study performed on behalf of management. As such, it does not have the rigour of an audit or program evaluation.

SYNOPSIS

This report presents the results of a study, initiated by the Chief Review Services, to assess progress by the DND/CF toward implementation of Integrated Risk Management (IRM). Terminology and processes used in this report are consistent with a framework defining the elements of IRM published by the Treasury Board in 2001. Risk management is also one of the pillars of modern comptrollership and is reflected in the DND/CF modern management agenda. Treasury board Secretariat has recently released the Management Accountability Framework of which risk management is one of the ten essential elements of good management. The conduct of this study follows a recommendation contained in an April 2000 CRS report, prepared at the direction of the Deputy Minister, and entitled, Survey of Risk Management Concepts and Practices.

Risk management is an approach or process that helps set the best course of action under uncertainty by identifying, assessing and acting upon risk issues. It can be performed intuitively or explicitly, in normal day-to-day situations with varying levels of sophistication. Integrated Risk Management needs to be distinguished from more traditional approaches. IRM is defined as a continuous, proactive and systematic process for understanding, managing and communicating risk from an organization-wide perspective. It involves ongoing, structured assessments of risks that can affect the achievement of organizational objectives at the strategic, operational, and/or tactical levels of management. Fully functioning IRM is embedded within, and supports, existing organizational processes, such as strategic planning, business planning, performance measurement and incident reporting. IRM is often referred to as a journey, as it encourages changing the culture from one of risk aversion to one where risks are viewed as uncertain events that can contribute positively or negatively to the achievement of organizational objectives. Open communication of risks is a key element of IRM.

Some of the more significant benefits accruing through the application of IRM, include:

- *Improved decision-making as assumptions are made explicit and analysed;*
- *Strategic partners are engaged and risks shared, based on expertise;*
- *Resources are allocated based on projected benefits, costs and risks;*
- *Improved design of monitoring and early warning systems;*
- *A perspective for discussing the significance of identified gaps between performance measures and targets;*
- *Effective responses for timely risk mitigation;*
- *Improved balance between flexibility and control at all levels;*
- *Synergies/information exchange across the DND/CF organizations;*
- *Better demonstration of due diligence; and*
- *Greater likelihood of achieving organizational objectives.*

IRM is not a stand-alone process, rather, it is an early-warning system embedded in an organization's corporate strategy and way of thinking.

This report links DND/CF IRM practices to the TBS IRM Framework and to a corresponding audit conducted by the Office of the Auditor General. However, our assessment also situates the DND/CF's overall risk management in the context of a five-stage Risk Management Maturity Model, adapted from work by the firm of Deloitte & Touche. The overall rating/placement of the DND/CF, in this respect, is presented at page V of the Executive Summary of this report. Part 3 of the report, provides a discussion of the rationale for this "rating".

Essentially, specific areas within the DND/CF have relatively sophisticated risk management regimes in place. For example, it is practiced in military operational planning, flight safety/airworthiness, nuclear safety, submarine safety, financial and cost validation risk assessments performed by ADM(Fin CS), and as part of capital project planning and delivery. The Departmental Legal Risk Management Committee, chaired by the DM, anticipates instances where litigation may result, and plans strategies to lessen its likelihood or consequences. Additionally, Army, Navy and Air force Environmental Chiefs of Staff use business planning impact assessments to identify specific risks to meeting Defence Plan objectives/tasks – these impacts usually pertain to resource limitations. We have also noted the DCDS initiative to design and pilot-test an IRM framework. There are also synergies within Defence with concepts from CF operational training carried over to the concept of risk management.

Notwithstanding progress within specific areas, overall, the DND/CF does not have a continuous, proactive and systematic process to manage risks on an organization-wide basis, i.e., Integrated Risk Management. This is not to be unexpected, given the complexity of the DND/CF, and that the concepts and techniques for IRM are relatively new. However, this same complexity speaks to the need for relatively advanced risk management. As the TBS has observed, progress toward IRM requires "…sustained commitment at the highest levels and throughout all ranks of management…to ensure the true integration of risk management thinking and principles into strategic planning, decision-making and accountability processes".[1]

The Maturity Model undertakes to rate where the DND/CF is today. The proposed "road map" presents an approach for progressing risk management within the DND/CF. The report also offers six relatively specific recommendations. Key to these are the development of a standard departmental framework under a corporate champion, but allowing Level 1s the implementation flexibility to focus on areas of greatest need in the short term, and learning from these experiences for additional implementation in the longer term. It will be important that the DND/CF continue to demonstrate leadership in risk management within specific spheres/functions while building overarching systems as well as learning from other organizations that have achieved leadership regarding risk management within their key functions.

[1] Treasury Board Secretariat, Integrated Risk Management Framework: A Report on Implementation Progress, March 2003.

The study recommendations address the following:

- *Vice Chief of the Defence Staff (VCDS) to champion IRM;*
- *VCDS to develop a departmental framework for IRM, focusing on the promulgation of a policy, principles, roles, process and common language in which all DND/CF organizations can link efforts;*
- *VCDS, in concert with ADM(Public Affairs), the CF Legal Advisor and the Director Access to Information & Privacy, to develop strategies for communicating risks within the DND/CF and externally, including a full understanding of pertinent provisions of the Access to Information Act;*
- *VCDS to perform a co-ordination role across Level 1 organizations and to develop a corporate risk profile;*
- *VCDS to initiate risk-awareness training and to promote open communication of risks; and*
- *VCDS to prepare a long-term DND/CF action plan for IRM implementation.*

Ultimately, it is hoped that this report will serve as a useful reference tool to assist the progress of Integrated Risk Management within the DND/CF.

Management Comments and Action

The VCDS has accepted the above-presented key recommendations and has expressed strong support for the implementation of Integrated Risk Management (IRM) across the DND/CF. At the same time, the VCDS has described a context for moving forward.

Firstly, the VCDS has observed that it will be crucial to maintain the primacy of operational risk in the development of an IRM Framework and plans. Also emphasized is the importance of avoiding the creation of a separate system(s), but rather to exploit and, where necessary, refine existing systems, including those such as Performance Measurement, Business Planning, and Capability-Based Planning. IRM holds the potential to provide a cross-functional perspective on current Risk Management practices within the DND/CF and to contribute to well-informed decisions.

This CRS report acknowledges the complexity of implementing IRM, and that it will take time to embed the necessary principles and culture into the organization. Experience in other departments has shown that, depending on the level of effort, it can take at least 5 years to implement IRM across an organization as complex as the DND. Accordingly, the report's recommendations are addressed to the VCDS/corporate level initially, in view of the need to establish an overarching DND/CF IRM Framework. It is further recognized that it will be necessary to ensure that individual Level 1s have flexibility to initially implement IRM within their organizations where it makes the most sense to do so and where the benefits are more obvious. Attendant to the VCDS role as champion for IRM will be the responsibility to act as facilitator with the Level 1s to bring IRM to maturity.

It is in the above context that the VCDS has accepted the key recommendations of the CRS report.

More explicit target milestones will be provided respecting the CRS recommendations. The VCDS organization will follow-up with Level 1s to identify an OPI to participate in the development of a more detailed action plan, so that a complete understanding of the requirements can be articulated, and the plan sets the DND/CF on a course to improve risk management DND/CF-wide.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Study Objectives, Scope and Approach

As per approved Review Plans, in 2003, the Chief Review Services (CRS) studied progress by the DND/CF toward implementation of Integrated Risk Management (IRM). Promoting increased awareness of IRM was a secondary objective of the study. The study was also influenced by the Treasury Board Secretariat's (TBS) Integrated Risk Management Framework. Further, risk management is a pillar of modern comptrollership and is reflected accordingly in the DND/CF corporate priorities, which call for the promotion of a modern-management agenda, including risk management.

The study's scope embraced all of the DND/CF. Our approach included:

- Researching recent best public and private integrated risk management practices, both internationally and domestically. A previous CRS study[2] surveyed risk management developments in the private and public sectors;
- Developing a diagnostic/assessment tool based on best practices and the TBS Integrated Risk Management Framework;
- Conducting workshops with a cross-section of military/civilian staff from Level 1 organizations to discuss IRM practices and the presence of these practices in the DND/CF. Workshop results were documented and provided to each Level 1 with respect to their own organization; and
- Interviewing Level 1s to better understand their perceptions of the adequacy of current risk information in their own organizations, and to discuss possible improvements to IRM within the DND/CF.

What Is Integrated Risk Management and what are its Benefits?

IRM is defined by TBS as a continuous, proactive and systematic process to understanding, managing and communicating risk from an organization-wide perspective. IRM involves an ongoing and structured assessment of risks that face an organization at every level. The results are then aggregated at the corporate level to facilitate priority setting, improve decision-making and determine actions to deal with risks.

[2] Risk Management: Survey of Concepts and Practices, Chief Review Services, DND, April 2000.

Successful implementation of IRM fosters a management culture that more openly encourages: the identification and communication of risks by personnel at all levels (e.g., strategic, operational, tactical); structured assessment of risks; the identification of risk mitigation options/strategies; and, decisions made at the lowest possible organizational level (guided by pre-defined risk tolerances). This benefits the organization by the resultant increased efficiency and effectiveness created from a more risk-smart and knowledgeable workforce that has the right information to make or recommend appropriate decisions.

IRM is not a stand-alone process; rather, it is an early-warning system embedded in an organization's corporate strategy and way of thinking. Fully functioning, organization-wide risk management can be integrated seamlessly with existing organizational processes to support business planning, performance measurement and incident reporting. IRM can be viewed as a journey that requires changing the culture of an organization from risk aversion to where risks are viewed as uncertain events that can contribute positively or negatively to the achievement of organizational objectives. IRM can identify and document risks before they happen, attempting to reduce both the likelihood and the consequences of an adverse event. This is important for demonstrating due diligence.

Overall Assessment of the DND/CF's Implementation of IRM

Our assessment of the DND/CF's implementation of IRM is similar to that of the Auditor General's 2003 report on six other federal government departments, the IRM concept is only beginning to take root. Some of these six departments however, are in the process of, or have completed, the first two steps of the TBS IRM Framework: i.e., developing a corporate risk profile and establishing a departmental IRM function/champion. DND/CF has not yet taken these steps.

CRS has endeavoured to take a balanced approach to this assessment – not only pointing out required improvements, but also identifying good risk management practices. Many areas exist within the DND/CF where risk management is practiced to varying degrees. For example, risk management is practiced in the military operational planning process, flight safety/airworthiness, nuclear safety, submarine safety, and as part of capital-project planning. The Departmental Legal Risk Management Committee, chaired by the DM, anticipates instances where litigation may result, and plans strategies to lessen the likelihood, or impact, of such litigation. Additionally, army, navy and air force Environmental Chiefs of Staff use business planning impact assessments to identify specific risks (normally based on identified resource shortages) to meeting Defence Plan tasks. CRS also noted the DCDS initiative to design and pilot-test an IRM framework. **But overall, the DND/CF has not yet embraced IRM.** The chart below summarizes our general assessment of how the DND/CF compares against the key elements of IRM. It should be noted that this assessment is based on the vast majority of DND organizations, as there are always some exceptions in an organization as large as DND.

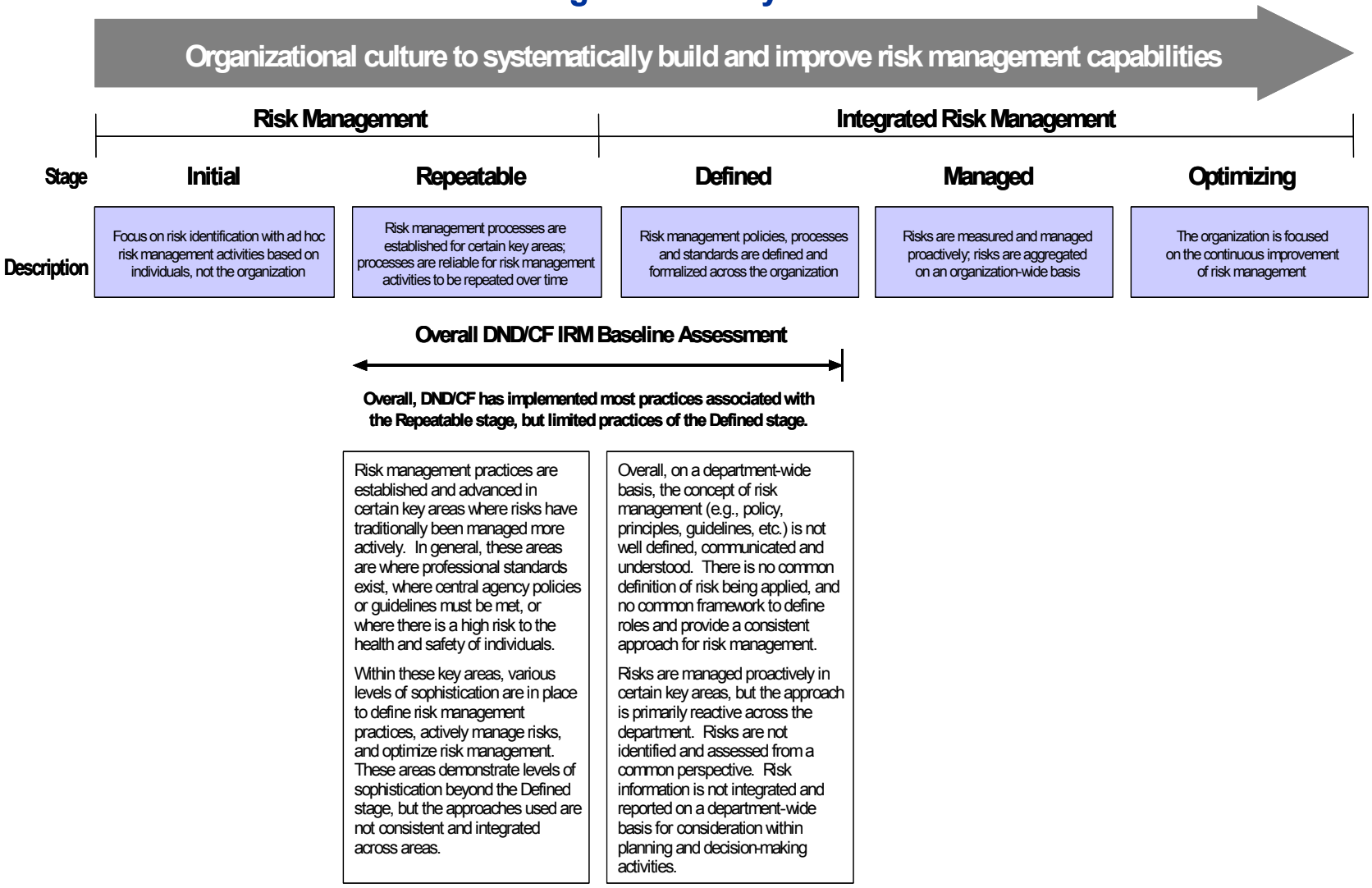
Comparison of IRM Key Elements against DND/CF Practice

IRM Key Element/Characteristic	THE DND/CF Comparison (Generally)
Continuous, dynamic risk identification as early warning	Relatively sporadic & annual identification
Possible risk events proactively identified before occurrence	Largely reactive to risk event occurring
Systematic Process in place	Risks considered principally as they relate to business planning
Structured analysis of likelihood & impact	Mainly intuitive analyses, although pockets where structure used
Everyone identifies risks	Mostly a manager's responsibility to identify risks
Organization-wide process	Process not yet in place
Risk managed at lowest practical level	Risk tolerances often not known or communicated; therefore, difficult for lower levels to manage risks
Risks prioritized	Unstructured prioritization
Reporting of prioritized risks upwards	Reporting partially through annual business planning
Mitigation plans commensurate with severity & likelihood or risks	Few mitigation plans based on risk assessment
Open communication of risks	Limited horizontal communication

In the course of this study, CRS has made a distinction between military *operational* risk management and *corporate* risk management. The DND/CF's mandate is to respond, at the government's direction, to international uncertainties. Its international and domestic defence tasks include preparing for war and peacekeeping, and responding to terrorism, civil unrest, national disasters and requests from Other Government Departments (OGDs). **The DND/CF is an organization founded on the principles of planning and preparing for the unexpected.** Operationally, therefore, the DND/CF has built relatively sophisticated risk/situational-awareness and operational planning systems, demonstrated by the work conducted through the National Command Centre. In fact, risk management activity by the Joint Staff Action Team (JSAT) is an example of fairly sophisticated IRM, albeit not fully developed. CRS however, must differentiate between risk managing in certain well-defined operations and implementing integrated risk management organization-wide. **Although, IRM is already somewhat embedded in military operational activities, it is not evident in other DND/CF corporate and military support activities.**

The evolution of risk management within an organization can be viewed through the Risk Management Maturity Continuum developed by Deloitte & Touche. The diagram on the following page, describes the five stages of risk management maturity, where we believe the DND/CF lies on this continuum, and our overall assessment of the DND/CF's implementation of IRM. The DND/CF, on average, is situated in the *Repeatable* category, tending toward the *Defined* category. It must be stressed that this is our overall opinion based on the sum of the parts in the DND/CF. There are areas within the DND/CF, such as flight safety/air worthiness, that could be considered to be in the *Optimized* category. On the other hand, there are many areas where the *Initial* category would be applicable.

Risk Management Maturity Continuum



Barriers to IRM Implementation

A number of barriers to optimizing IRM implementation are evident in the DND/CF. These barriers are not unique to the DND/CF, and include:

- A requirement for more demonstrable senior management support for the IRM concept and the required organization-wide structured risk analysis;
- Absence of an overarching departmental IRM policy and direction;
- Scepticism regarding the achievable benefits through IRM; and
- A DND/CF organizational culture:
    - Wherein managers may be reluctant to make risks fully transparent to avoid diminishing a proposal's/ project's chances of gaining approval;
    - That may equate the disclosure of high risks with bad news and inadequate job performance;
    - Wherein IRM initiatives may be seen as a competitor for limited resources, as opposed to complementary tools for better management;
    - That does not easily/readily share risk information horizontally;
    - That exhibits concern that documented risk information will be exploited by third parties to bring unwarranted criticism upon the organization; and
    - That, by and large, may not recognize risk management as a key foundation for an ethical climate.

DND/CF IRM Implementation Strategy

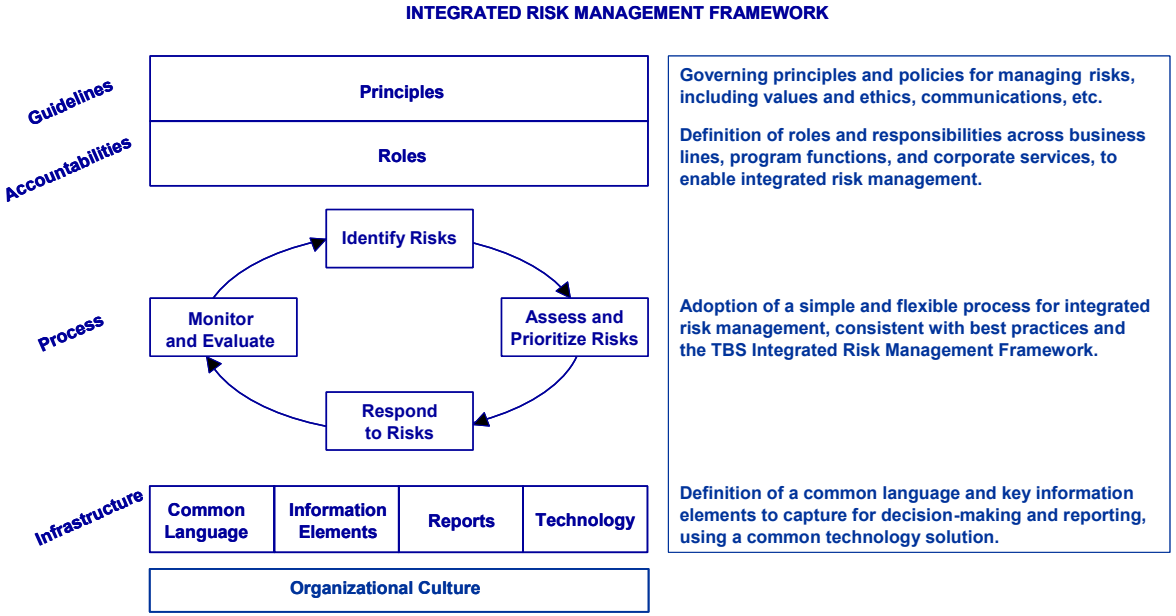
CRS recognizes that IRM represents a change that could well take years to fully implement and embed in an organization's philosophy and culture. As such, sufficient flexibility should be built into the implementation approach to account for the diverse entities in the DND/CF. Initially, management needs to understand where on the risk-management maturity continuum each DND/CF entity is best placed. In other words, CRS foresees different DND/CF organizations establishing different risk management regimes, depending on the importance of their specific work functions to the overall success of DND/CF objectives. In fact, the April 2000 study by CRS cited a paper, which specifically acknowledged that risk management approaches will be customized according to the type of mandate of the organization (e.g., policy, security, operations). All organizations; however, should work toward encouraging open communication in identifying risks, establishing an early-warning system for reporting risks, and defining organizational risk tolerances.

A detailed road map to IRM is proposed in *Part 4.4*. The road map outlines a number of short and long-term activities for the DND/CF to implement. Our recommendations below focus on the short-term initiatives required to develop a departmental framework and to begin addressing some of the barriers, in order to enable longer-term success.

Six Recommendations

1. **Vice-Chief of the Defence Staff (VCDS) should champion IRM.** For IRM to work, senior management needs to be convinced of its benefits and it therefore, needs a high-level champion. The benefits of IRM are further described in *Annex A*. VCDS should increase executive awareness by promoting IRM within senior-management committees such as DMC and PMB. IRM practices, such as structured risk identification, analyses, mappings, and open communication about risks, should be encouraged.

2. **VCDS should develop a departmental framework for IRM, focusing on the promulgation of a policy, principles, roles, process and common language in which all DND/CF organizations can link efforts.** The IRM framework should be simple, clear and flexible. While military operational activities should be subject to the principles underlying IRM, emphasis in the short term should be placed on implementing IRM in corporate and military support activities, allowing the existing military operational risk process to operate where appropriate. We provide a suggested IRM Framework as follows; similar to the framework we designed for DCDS.



3. **VCDS, in concert with ADM(Public Affairs), the CF Legal Advisor and the Director Access to Information & Privacy (DAIP), should develop strategies for communicating risks within the DND/CF and externally, including a full understanding of obligations relative to Access to Information.** Public release of information is perceived as a substantial barrier for openly identifying risks. Other governments and departments have used various legislative-based provisions and arguments, such as damage to the public interest and incomplete advice for decision-making, as rationale for severing risk information from reports.

4. **VCDS should perform a coordination role across various Level 1s and begin to develop a corporate risk profile.** Each Level 1, in conjunction with VCDS, should define areas where a more rigorous IRM approach is required to identify and report risks. As a first step, Level 1s should place emphasis on areas that:

   - Affect safety or security of personnel, such as ammunition, military operations and training, health services, and general safety;
   - Are regulatory or legislative in nature, and areas where the precautionary principle[3] may apply in technical or science-based spheres, such as nuclear, environmental protection, airworthiness and Nuclear, Biological, Chemical (NBC);
   - Directly affect public safety, such as homeland security and emergency preparedness; and
   - Have potential litigation consequences. (Legal Risk Management Committee currently performs IRM in this area.)

5. **VCDS should initiate risk-awareness training for managers and employees, and promote open communication of risks.** To secure the full benefits of IRM, DND/CF management needs to encourage openness and sharing of information. Managers at all levels need to encourage full disclosure of risk information. IRM successes in the Flight Safety/Airworthiness Program, and others noted within this report, should be used to promote the benefits of IRM. Many risks and risk-mitigation strategies have a direct relationship to ethics or values. Ways to leverage the Departmental Ethics Program; therefore, as it pertains to IRM, should be investigated with CRS.

[3] The Federal Government is currently preparing a framework for the application of precaution in science-based decision-making about risk, whereby it is recognized that the absence of full scientific certainty should not be used as a reason for postponing decisions where there is a risk of serious or irreversible harm. The framework intends to apply general principles for precautionary decision-making, and is intended for regulatory departments and agencies. Several areas in DND could be impacted, including CAS – Flight Safety; ADM(HR-Mil) – Health Services; ADM(IE) – Environmental Protection and Nuclear Safety; ADM(Mat) – Airworthiness and Ammunition; ADM(S&T)/DCDS – Nuclear, Chemical, Biological, Radiological.

6. **VCDS should prepare a long-term DND/CF action plan for IRM implementation.** The action plan should specify roles, responsibilities and target dates; it should also consider resource implications. Implementation should include areas where the cultural foundation has already been built and success will be evident quickly. This type of implementation will build momentum and establish the DND/CF on its journey towards IRM.

PART 1 – INTRODUCTION

As approved in the DND/CF Review Plan, Chief Review Services (CRS) conducted a study to determine progress by the DND/CF in implementing integrated risk management (IRM). The study was influenced by a Treasury Board Secretariat (TBS) initiative to report on the level of progress made in implementing the TBS Integrated Risk Management Framework.

The Federal Government's Risk Management policy states: *"it is government policy to identify and reduce or eliminate risks to its property interests and employees, to minimize and contain the costs and consequences in the event of harmful or damaging incidents arising from those risks"* [4]. Further, in an effort to strengthen risk management practices, TBS published in April 2001 an Integrated Risk Framework document, intended to help guide departments in their development of organization-wide risk management. Modern comptrollership is one of four priorities of government departments as established by the Office of the Clerk of the Privy Council. Risk Management is a key element of modern comptrollership. DND corporate priorities for 2003-04, moreover, include promotion of a modern management agenda, which embraces risk management as a vital component of modern comptrollership.

To assist in this study, CRS engaged the assistance of Deloitte & Touche to conduct a baseline assessment of IRM within the DND/CF. This report represents the joint efforts of CRS and Deloitte & Touche staff.

1.1 PURPOSE AND OBJECTIVES

This report provides an assessment of the state of IRM within the DND/CF.

Specifically, we undertook the following:

- A survey of DND/CF practices in relation to IRM;
- Increasing awareness and understanding of IRM in the department, through wide-ranging focus groups and discussions;
- Assessing DND/CF IRM practices against the TBS IRM framework – Part 3 of report; and
- Developing recommendations to strengthen IRM across the DND/CF – Part 4 of the report.

[4] Risk Management Policy, TBS, Page 2.

This report does not attempt to:

- Develop a DND corporate risk profile or identify and assess departmental risks;
- Identify all departmental IRM practices; and
- Provide a statistically valid sample of all DND/CF IRM practices.

1.2 SCOPE

The study included the following DND/CF L1 organizations:

Vice Chief Defence Staff	(VCDS)
Deputy Chief Defence Staff	(DCDS) [5]
Assistant Deputy Minister Human Resources – Military	(ADM(HR-Mil))
Assistant Deputy Minister Materiel	(ADM(Mat))
Chief of Maritime Staff	(CMS)
Chief of Land Staff	(CLS)
Chief of Air Staff	(CAS)
Assistant Deputy Minister Finance & Corporate Services	(ADM(Fin CS))
Assistant Deputy Minister Infrastructure & Environment	(ADM(IE))
Assistant Deputy Minister Human Resources – Civilian	(ADM(HR-Civ))
Assistant Deputy Minister Information Management	(ADM(IM))
Assistant Deputy Minister Science & Technology	(ADM(S&T))
Assistant Deputy Minister Public Affairs	(ADM(PA))
Assistant Deputy Minister Office of Critical Infrastructure Protection & Emergency Preparedness	(ADM(OCIPEP))
Judge Advocate General	(JAG)
Canadian Forces Legal Advisor	(CFLA)

The review was limited to NDHQ/Headquarters activities.

[5] Information collected from the DCDS Risk Management Framework Project, conducted by CRS in June 2002, was considered as part of the study.

1.3 STUDY APPROACH

Research into best practices was conducted and a diagnostic tool developed in relation to the four pillars of IRM proposed by the TBS Integrated Risk Management Framework. Representatives from the aforementioned organizations attended work sessions to discuss the extent to which IRM practices are present in their organizations. Most NDHQ organizations down to Level 3 were represented at these work sessions. Interviews were conducted with Level 1s to improve CRS understanding of the perceptions of the adequacy of risk information provided, along with personal perceptions regarding what could be improved with respect to IRM within the DND/CF.

Information collected from the work session(s) was documented and provided to each DND/CF organization in a separate document. The information from the work sessions and interviews with Level 1s was used as input to the baseline assessment of IRM within the DND/CF and is summarized in Part 3 of this report.

The process of collecting data for this report allowed for information sharing within each Level 1 regarding current IRM practices, and stimulated discussion on the nature and importance of IRM in DND/CF and actions that could move IRM forward.

PART 2 – INTEGRATED RISK MANAGEMENT CONCEPTS

The current business environment demands a more integrated approach to risk management due to the complex interrelationship and reliance across all divisions of an organization. It is no longer sufficient to manage risk by individual or functional area. Organizations around the world now benefit from a more comprehensive approach to dealing with all risks.

IRM involves an ongoing assessment of the risks that face an organization at every level and then aggregating the results of this assessment at the corporate level to facilitate priority setting and improved decision-making. To be effective, IRM should become embedded in an organization's corporate strategy and shape the organization's risk-management culture.[6] To be successful, IRM should not function as a stand-alone process; it should be integrated within existing organizational processes. IRM ensures that risks are openly identified and communicated at appropriate levels of an organization; decisions are made considering risk analysis; actions are taken; and where required, risks are elevated to the next level for resolution. Successful IRM results in clearer accountability, proactive organizational decision-making and a greater opportunity to achieve organizational objectives.

2.1 KEY TERMS AND DEFINITIONS

The following key terms and definitions have been used throughout the baseline assessment:

Risk	Risk refers to the uncertainty that surrounds future events and outcomes. Risk is the expression of the likelihood and impact of an event with the potential to influence organizational objectives.[7]
Risk Management	Risk management is the systematic approach or process that sets the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.[8]
Integrated Risk Management (IRM)	IRM is a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective. IRM is about making strategic decisions that contribute to the achievement of overall DND/CF objectives.[9] IRM involves vertical and horizontal linkages or, in the context of DND/CF, assessment and analysis of risks across and within L1 organizations.

[6] TBS Integrated Risk Management Framework, April 2001.
[7] TBS Integrated Risk Management Framework, April 2001.
[8] TBS Integrated Risk Management Framework, April 2001.
[9] TBS Integrated Risk Management Framework, April 2001.

2.2 RISK-MANAGEMENT MATURITY CONTINUUM

The evolution of risk management within organizations can be viewed through the Risk Management Maturity Continuum presented below. The table below depicts a model, based on risk-management best practices, that was initially developed by Deloitte & Touche. The model has been recently adapted for the public sector. The maturity continuum identifies five stages of risk management maturity. A description is provided for each stage, along with the main capabilities and characteristics associated with each. Outcomes from the various levels of risk management capabilities are also provided.

Risk Management Maturity Continuum

Organizational culture to systematically build and improve risk management capabilities

	Risk Management		Integrated Risk Management		
Stage	**Initial**	**Repeatable**	**Defined**	**Managed**	**Optimizing**
Description	Focus on risk identification with ad hoc risk management activities based on individuals, not the organization	Risk management processes are established for certain key areas; processes are reliable for risk management activities to be repeated over time	Risk management policies, processes and standards are defined and formalized across the organization	Risks are measured and managed proactively; risks are aggregated on an organization-wide basis	The organization is focused on the continuous improvement of risk management
Capabilities & Characteristics	The concept of risk management is not well understood Risk management is ad hoc and few processes are defined Risk management is driven from individual preference and initiative Risks are identified and managed only as required, in reactive mode Risk management is dependent on the competencies of individuals Practices used for risk management are not necessarily repeatable	Risk management policies or guidelines are in place in key operational or priority areas Roles and responsibilities for managing risks are understood within specific areas, and risk management OPIs may be in place to provide support if required Individuals are accountable for managing risk and generally have the required authority to act Resources are specifically allocated to risk management efforts in specific or key areas The environment is scanned within key areas and important risks are assessed using various methods Risk management practices are consistently applied within key or priority areas There is no risk management policy, guideline or framework at the department-wide level	A common definition of risk is used and there is a defined organization-wide risk management framework or process used by all groups Senior management is familiar with risk concepts and the organization-wide framework or process Roles and responsibilities for managing risks are defined and there is a risk management OPI at the department level The environment is scanned on an organization-wide basis to identify risks in relation to objectives Important risks are identified and assessed using a consistent approach; plans are developed to manage risks Technology is used to store risk information and facilitate reporting Important decisions consider risk factors from an organization-wide perspective	Standardized tools and techniques are used for managing risks Training is provided to managers and staff on risk management, and tools and techniques Risk management is integrated across the organization Processes are in place to monitor and report risks on a regular basis Risk tolerances or limits are established and communicated Risk exposures can be anticipated from experience, lessons learned or forecasting techniques When risk tolerances or limits are exceeded, actions are taken to correct the situation Risk information is shared across the organization and with stakeholders on an ad hoc basis	Risk management is fully integrated across the organization and levels of effort are optimized in key areas Risk management priorities are in line with organizational objectives Practices for managing risks are monitored for effectiveness and organized efforts are made to improve risk management practices There is a clear linkage between performance measures and risk management Best practices are identified and shared across the organization Significant risks and implications are communicated across the organization and to stakeholders on an ongoing basis There is formal recognition for effective risk management
Outcomes	There is limited awareness of risks. Risk management is taking place but it is driven from issues and managed based on intuition and individual preferences.	Risks are actively managed in traditional areas where professional standards exist, and in areas of high risk to health and safety. There is limited awareness of risk as an opportunity.	Risks are identified proactively, from a common perspective. Risk information is reported and considered as part of other management processes such as planning and decision-making.	Risks are actively monitored and decisions are made to reduce risk exposures to an acceptable level. There is a good awareness of risk tolerances across the organization.	The performance of risk management activities is measured. Risk management practices are improved on a continuous basis. Stakeholders are informed of risks and engaged in providing input and feedback.

The maturity continuum highlights a number of key IRM elements. Organizational culture, including values and ethics, is an important component to build and improve risk-management capabilities. A supportive IRM culture is influenced greatly by senior-management leadership and commitment to promote and support risk management. With proper leadership, all personnel will recognize that managing risks is everyone's business, and that risk management issues should be discussed openly on the basis of trust and teamwork.

In the *Initial* and *Repeatable* stages of the maturity continuum, an organization practices risk management in various areas where risks may be more tangible or predominant. The concepts of risk management are usually understood in these specific areas, but risk management is reactive, and risks are not identified and managed systematically and consistently across the organization. In the *Defined*, *Managed* and *Optimizing* stages of the maturity continuum, an integrated approach to risk management is being established. Risks are identified on a department-wide basis using a consistent approach, and guidance and support for risk management is provided through a departmental OPI. Active monitoring and sharing of risk management practices occurs. Risk management priorities are in line with organizational objectives and linked to performance measures. Additionally, organized efforts are taken to improve risk management practices.

The maturity continuum has been used in the DND/CF baseline assessment to situate current DND/CF risk management practices along the continuum and to help identify opportunities to move the DND/CF forward to a more integrated, proactive risk management approach. It is important to note that few private or public-sector organizations have yet reached the *optimizing* level of risk management, and that every organization needs to determine how far and how fast movement along the continuum should occur. Depending on the nature of the risks that an organization faces, it may be more useful or cost-effective to have greater sophistication of risk management practices in certain areas than in others. The target *maturity* level for IRM is a strategic decision that should be made based on current risk management activities and the nature of the risks an organization faces. This strategic decision will be explored further in subsequent parts of this report.

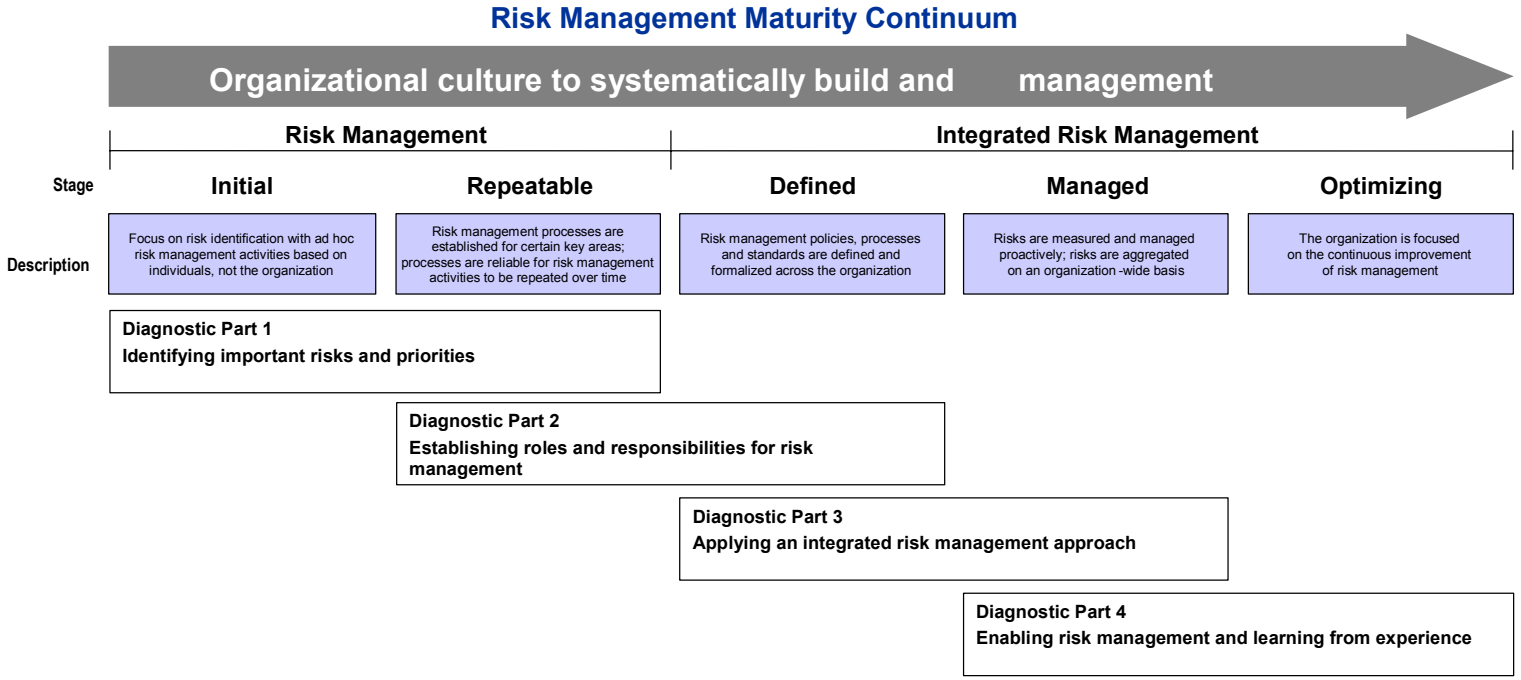
PART 3 – ASSESSMENT OF THE DND/CF INTEGRATED RISK MANAGEMENT PRACTICES

3.1 ASSESSMENT METHODOLOGY

To assess the extent that elements of IRM are in place within the DND/CF, a diagnostic tool was developed based on best practices and organized around the four elements of IRM outlined in the TBS Integrated Risk Management Framework guidance document. A copy of the diagnostic tool is presented in *Annex B*.

The diagnostic tool includes 24 best practice statements that relate to the elements of IRM. For each statement, Level 1 participants used anonymous voting technology to provide an assessment against each best-practices statement as a starting point to discussion. Comments made by participants were recorded to provide information on the context, examples, barriers and improvement opportunities for practicing IRM within each Level 1. A summary report of discussions was produced from each work session and provided to each Level 1 contact.

The following diagram illustrates the links between the four parts of the diagnostic and the Risk Management Maturity Continuum.



Application of the diagnostic tool in work sessions helped to situate the DND/CF along the maturity continuum. Individual interviews were also conducted with Level 1s to discuss the context of IRM and opportunities for improvement. Information collected enabled the identification of common themes across the DND/CF, and the baseline assessment of IRM within DND/CF.

3.2 COMMON THEMES

The following common themes regarding IRM within DND/CF were developed using information collected as part of the work sessions and subsequent follow-up activities, including interviews with Level 1s. Each part introduces context to facilitate a better understanding of the theme. Theme conclusions are then presented in bold and italics, and a description is provided to illustrate the theme across the DND/CF and within specific Level 1s. **It should be noted that the themes provide a summary assessment of the DND/CF as a whole. As such, certain areas within Level 1s may differ with respect to the maturity of risk-management practices in place.** These differences are highlighted and presented as strengths or opportunities. Risk-management practices specific to each Level 1 are detailed within the work session summary report provided to each Level 1 contact.

It is also important to note that the public sector provides a unique context for risk management. Program outcomes in the public sector tend to be difficult to identify and/or measure. The need for public transparency, as well as media scrutiny, can result in risk aversion, making risk management concepts beyond risk avoidance difficult to apply. Policies governing access to information can also suppress the sharing of sensitive risk information. These policies are often developed to avoid information being reported out of context or sensationalized. These factors and barriers should be considered when reviewing the following assessment.

3.3 ORGANIZATIONAL CULTURE

Culture

Culture is one of the basic underpinnings of a sound IRM framework, and is central to the overall organizational risk environment. Culture is a key factor in how an organization sets its goals and objectives, operates and adapts over time. Understanding organizational culture is crucial to building strong IRM tools in the DND/CF. Not surprisingly, a number of cultures are evident within the DND/CF. The two most easily identifiable are the operational culture, and the operations support and corporate culture.

Risk management has long been recognized as an essential element of military operations. The Canadian Forces have formal training and procedures for operation of military equipment, and planning and execution of both domestic and international missions. Military training and doctrine includes many different risk management considerations that relate to monitoring situations, handling equipment in a safe and secure manner, knowing how best to react in specific circumstances, and mounting an effective response to problem situations. The DCDS organization has a draft risk management framework for deployments that outlines specific risk management procedures in relation to various deployment situations. Military decisions are made through a strict chain of command guided by hierarchy, guidelines, protocol and regulation. The approach to passing information up and down the chain of command is formalized and well understood. Planning structures are in place to share knowledge and information, determine a proper course of action, draft contingencies for unexpected situations and for JSAT, ensure integration of effort across responsible Level 1s. In general, risk tolerances and accountability for actions and achieving results among military staff are clear. Within specific tasks, the ability exists to innovate and take acceptable risks to achieve results. Reward and recognition for achieving results is often visible. Although, operators would seem to have a broad base upon which to strengthen the practice of IRM, they tended to be resistant to suggestions that risk-management practices in their areas could be improved. That resistance must be considered a factor in education and change management.

Identifiable sub-cultures are evident within the DND/CF risk environment. The operational-risk environment is distinct from the NDHQ corporate and operations-support environments.

In contrast, risk management within operational support and corporate functions is viewed as a normal part of conducting business in fields such as engineering, computer science, project management, financial management and human-resources management. These fields tend to collect and maintain data as a routine managerial function. As part of training in these fields, risk management concepts are introduced in terms of key controls that need to be in place, rather than as a broader set of management tools. At the functional level within DND/CF, certain risks, such as financial and project risks, are actively managed. In addition, a degree of risk management efforts are dedicated to maintaining compliance with policies, procedures and other central-agency requirements. Within support functions; however, a tendency exists to provide internal clients with information and options for consideration, and to let internal clients make their own decisions with regard to computer systems, infrastructure and materiel. Internal client expectations and risk tolerances are generally not well communicated to support functions. Traditionally, reward and recognition are geared toward results achieved rather than uncertainties resolved or problems avoided.

Both operators and corporate personnel share significant cultural characteristics common with the public sector. Working group participants viewed both operators and corporate staff members as somewhat risk averse – sometimes to the point of missing opportunities. Operators and personnel with professional risk training were seen as less risk averse and more comfortable with risk and reward assessments. Consistent with less advanced concepts still being taught in some areas, risk as an opportunity to achieve objectives is not widely understood or embraced. A risk-averse culture is common within public sector organizations and stems from a need for greater transparency, clearer accountability and greater public scrutiny than is generally required in the private sector.

Communications

Open communications to facilitate the passage of risk information both vertically and horizontally is another best practice and also a key element of the organizational risk culture. Level 1 organizations currently operate somewhat independently, and risk information is not widely shared among Level 1s and across DND/CF. In the DND/CF, risks are discussed in formal meetings such as DEM (Daily Executive Meeting), JSAT (Joint Staff Action Team), LRMC (Legal Risk Management Committee), ARB (Airworthiness Review Board), SRBs (Senior Review Boards) and PMB (Program Management Board). Risk information; however, is rarely identified as such and is typically not analyzed from the perspective of likelihood and impact, or in clear relation to impact on defence objectives. Communicating information about risk is performed mostly on a need-to-know basis to those in authority rather than shared. Informal channels are also used to discuss risks and resolve issues within lower management levels. A commonly held belief is evident within certain groups that risks should not be brought to the attention of senior management unless a solution has been found as this could reflect negatively on an individual's skills and ability to manage problem situations. In some instances, groups expressed frustration over difficulties encountered in notifying superiors of problems due to negative attitudes or reactions toward receiving news of potential problems. Reluctance among personnel to be candid about risks is evident as these risks are communicated up the chain of command.

Significant barriers exist to communicating risk openly.

Regulations quite rightly restrict the free exchange of classified information. Concerns regarding the release of highly sensitive information and the threat of negative publicity or embarrassment may also be contributing factors in the absence of commonly available risk assessments and open information exchange. Policies governing access to information are often perceived to be a deterrent to the documentation of risks and the sharing of information on a broad basis.

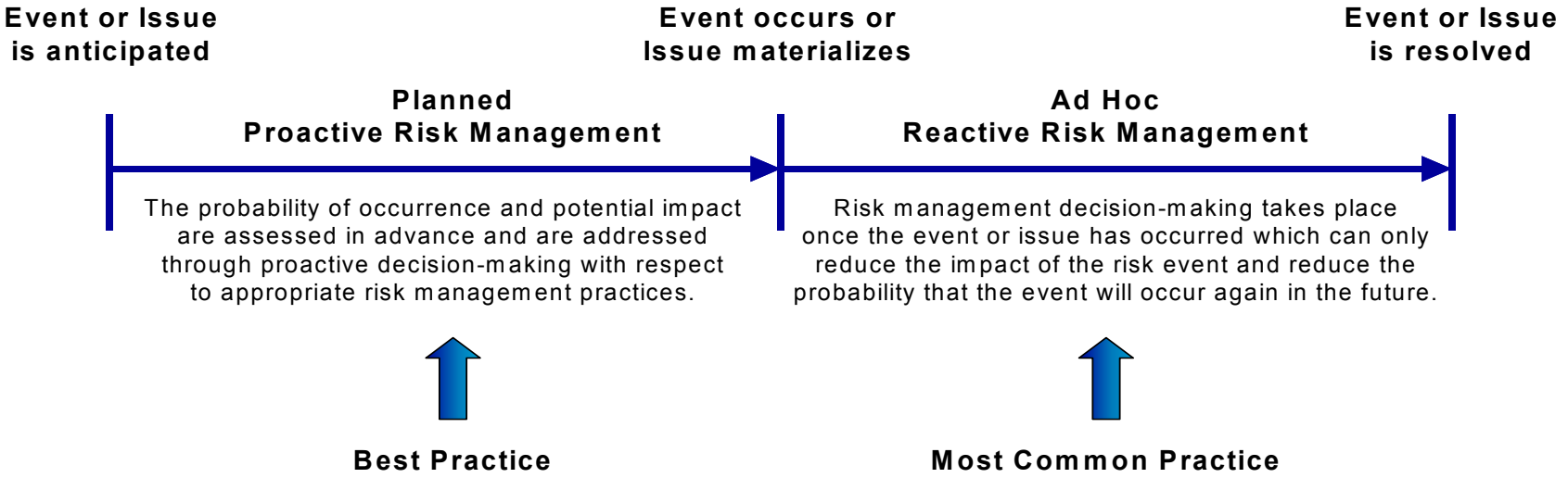
3.4 IDENTIFYING RISKS AND PRIORITIES

Risk Identification

Generally, the first step in any risk management process is risk identification. Clearly, an organization that can identify potential risk well before the event or situation occurs affords itself significant flexibility in mitigating the risk. The nature of risk management within the DND/CF is primarily reactive. In certain areas of the DND/CF, such as military operations, project management, financial management and environmental health and safety, risks are managed proactively using formal or traditional methods. Across the DND/CF; however, proactive risk management is rare. Risk management takes place, but it is primarily instituted once an issue has surfaced. One area within the DND/CF where proactive risk management is practiced is within the Flight Safety/Airworthiness Program. Risk management within this area is used to identify potential issues and take corrective action to prevent potential hazards.

Risk management within the DND/CF is primarily reactive.

The following chart depicts the difference between Proactive Risk Management and Reactive Risk Management.



Environmental scanning is not widely understood or practiced in the DND/CF. A constant check of what is happening in the general environment, as takes place in support of the Legal Risk Management Committee, is one way of making risk identification more proactive.

Risk identification improves with practice and is more effective when practiced by a group in a structured way, such as in a brainstorming session. DND/CF activities and priorities are often dictated by events that are perceived to be, for the most part, unforeseeable and beyond departmental control. But even these events might be foreseen through structured or facilitated risk identification methods.

Assessment and Prioritization

One key process element of IRM is the assessment of risks identified with respect to their likelihood of occurrence, and the impact of the risk should it occur. Using a simple map of likelihood and occurrence, risks can be ranked and compared. Some Level 1 business plans include high-level analysis of risks; however, no consistent processes are in place to identify and assess risks. Working group members believed business planning risk assessments to be of questionable quality. The Level 1 business plans generally do not include clear linkages or alignments among objectives, priorities and risks; nor are there clear linkages with departmental objectives and priorities. As a result, some confusion exists about whether priorities and risk management efforts are directed in areas that are most critical to organizational and departmental success. The quality and consistency of risk analysis may also be a challenge within other areas, such as project management. Workshop participants voiced the opinion that risks affecting projects are sometimes assessed purposely at low levels to better ensure that a project is favourably received and approved.

In general, the approach to assessing risks appears to be mostly intuitive, lacking structured analysis. Limited prioritization of risks is evident, and the linkage of decisions with planned objectives is not always clear at the strategic level.

3.5 ROLES AND RESPONSIBILITIES

Within the DND/CF, individuals perceive risk management as inherent to their jobs. To the extent that risk management is considered everyone's business, this is a strength. However, job responsibilities are not specific with respect to risk management responsibilities and accountabilities. As a result, responsibilities for managing risks are not formalized and are poorly understood. Because risk management responsibilities are not formalized, it is less likely that risk management will consistently move beyond the capabilities of each individual to the point where risks are addressed on an integrated basis across the DND/CF.

Roles and responsibilities for managing vertical and horizontal risks are not clearly defined.

Assignment of risk ownership, or identification of the person who determines what actions should be taken to manage risks and has authority to implement those actions, is usually clear within military operations but not always clear in support or corporate functions. Identifying who is responsible for dealing with risk issues as part of the chain of command is relatively simple. Identifying who should be responsible for risk management of horizontal issues across Level 1s, however, is not nearly as obvious. Nonetheless, when risks occur that need immediate attention, a person who has authority to address the risks can normally be identified, and effective corrective action is usually taken on a timely basis.

Designated Offices of Principal Interest OPIs) exist in some areas where risks are actively managed, such as legal services, project management, financial management, submarine safety, military operational planning and flight safety. But few OPIs provide support specifically for risk management within each Level 1. In general, openness to having designated OPIs for risk management is evident – provided that such infrastructure would add value and would not require significant resources.

Proper accountability for IRM requires that risk tolerances be established and shared. Each person responsible for risk should be able to determine between the risk that can be assumed and acted upon, and the risk that should be passed up the chain for resolution. Personnel in the operational community tend to report significantly greater comfort than personnel in the corporate community with respect to the level of risk that they are empowered and expected to deal with. Operators routinely identify their limits of responsibility as being included in job terms of reference, specific orders or briefings.

3.6 AN INTEGRATED RISK MANAGEMENT APPROACH

Process

While an organization's risk management practices need not be identical across departments, a significant level of commonality in the risk environment of an organization is required for a genuine IRM framework. Risk-management practices across the DND/CF differ significantly from location to location. Military and civilian staffs understand risk within their immediate job responsibilities, but they use various definitions of risk, acquired in formal training or on the job, as part of operational and corporate processes.

No commonly accepted risk process is evident in the DND/CF.

Areas where capital and information technology projects are managed tend to define risk in terms of how it might affect various criteria such as quality, budget and timelines. Specific project management criteria or dashboards are used to monitor the status of projects and report issues to management. To the extent that they exist, DND/CF risk management processes differ substantially. As mentioned, DCDS has drafted a risk management framework for CF operations; however, the framework has not been fully implemented. CMS has indicated that a level of IRM exists within Maritime Command Pacific (MARPAC). The Airworthiness Program has a highly evolved risk management process. Within DGNS (Nuclear Safety), all products are assessed based on likelihood and impact, and controls such as training, inspection levels, and warning and detection equipment, are applied commensurate with risk. Within ADM(Finance and Corporate Services), the Director Strategic Finance and Costing reviews and advises on projects from a financial risk perspective. As could be expected in an organization focused on innovation, risk management within the research and development community is well established. On the other hand, many Level 1 organizations indicated that information to identify and assess risks does not always exist to allow for effective risk management.

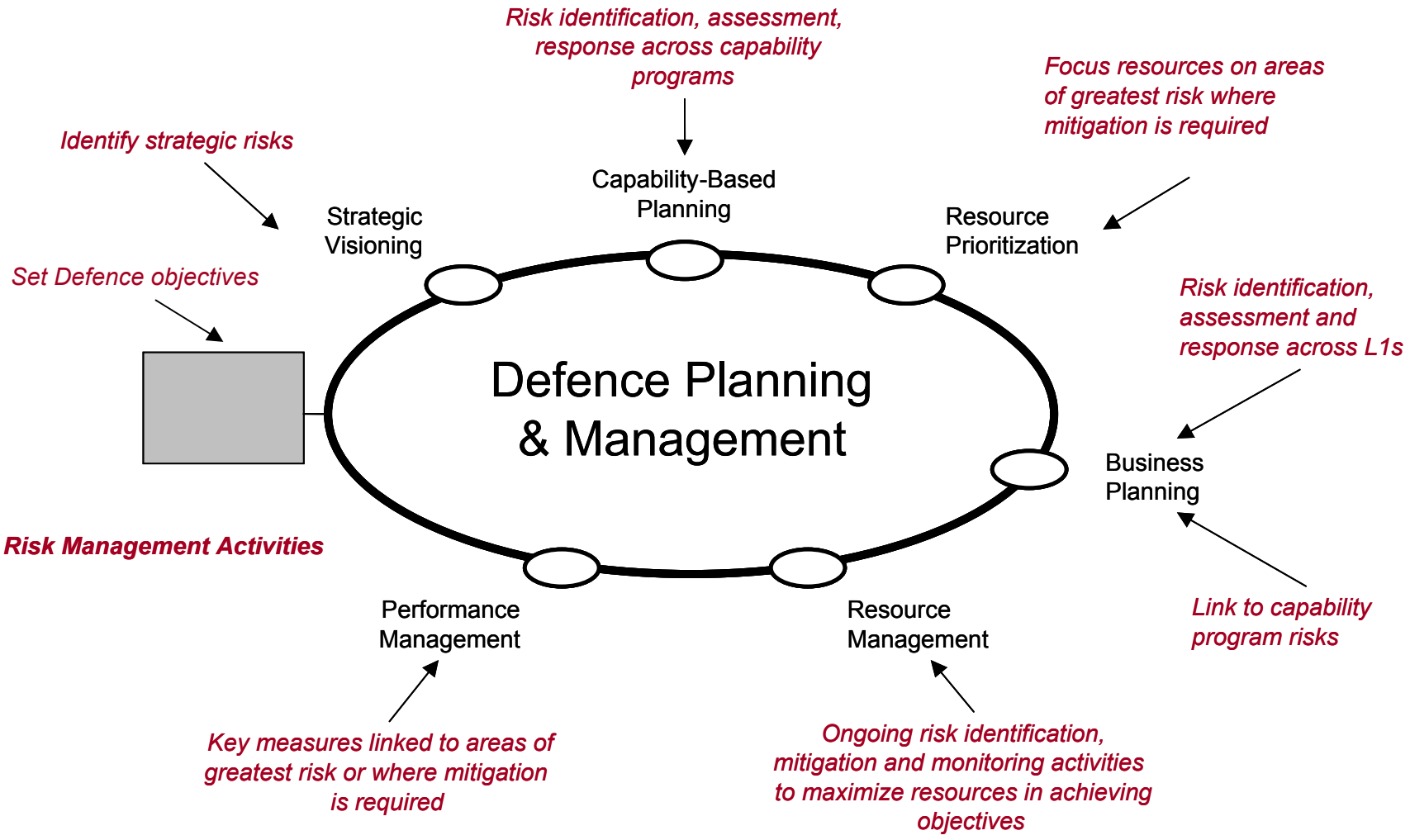
Principles

Formal organizational adoption of risk principles is a best practice and part of a sound IRM framework. Risks are present throughout DND/CF and have significant influence on actions taken by personnel.

> ***Outside of areas where risk management is traditionally used in the DND/CF, little understanding or articulation of the concept of IRM – and how it needs to be integrated as part of normal, day-to-day planning, decision-making and performance management – is evident.***

IRM is not intended to be a separate, stand-alone process. For IRM to be effective, managers must apply IRM as part of their normal duties. Contrary to commonly expressed views in DND, IRM should support business planning, decision-making and performance measurement rather than compete with them. In the following chart titled "Integrated Risk Management as part of Defence Planning and Management", we have shown how IRM information can be used as inputs to the various elements of the Defence Planning and Management model, e.g., Strategic Planning; Capability-Based Planning; Resource Utilization; Business Planning, Resource Management and Performance Measurement.

INTEGRATED RISK MANAGEMENT as part of Defence Planning and Management



When fully functional, IRM will allow all staff to contribute to the identification of risks. In this way, IRM provides an early-warning system for managers.

Currently, risks are used mostly to highlight the impact of resource shortfalls. This is focused at a single point in time and does not consider the dynamic dimension of IRM. When IRM is used properly, staff at all levels are continuously on the alert for significant events that could effect organizational objectives, and report risk information upwards on a real-time basis without fear of reprisal.

3.7 ENABLING RISK MANAGEMENT AND LEARNING FROM EXPERIENCE

Common elements of IRM infrastructure include training, language and definitions, clearly identified elements of risk information, a reporting system, and technology to assist in tracking and reporting risks, and in analyzing risk information for lessons learned.

Military operations have formal training and procedures for key areas, such as the operation of military equipment and the management of missions relating to search and rescue, peacekeeping and military conflict. Operational support and corporate functions have formal training in relation to traditional fields such as engineering, computer science, and project, financial and human-resources management. Across the organization, managers and staff have not been trained on risk management concepts and fundamental theory. Risk management training and continuous learning are primarily addressed with on-the-job coaching and mentoring. Limited direction is provided with respect to risk management training and continuous learning.

The use of a common language and approach to risk and IRM are essential for risk management integration across an organization. Based on TBS guidance, risks are the uncertainties that need to be understood and managed in order for an organization to achieve its objectives. IRM is a continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective. IRM allows for the making of strategic decisions that contribute to the achievement of overall DND/CF objectives. Without a common language and definitions, it is difficult for managers and staff to achieve an understanding of risk and determine risk management priorities in a coordinated manner. VCDS has posted to its website definitions of risk and risk management that are consistent with the TBS Integrated Risk Management Framework. These definitions; however, are not widely understood, communicated or applied across the DND/CF.

Risk information has little value if it is not reported to those empowered to act upon it. In DND/CF, reporting is impacted by a number of factors. As mentioned above, restrictions on the passage of classified information negatively impact reporting, as does concern with respect to risk information being accessed and reported out of context. DND/CF has risk reporting criteria and formats specified for some areas, such as business planning and project approval. Despite these requirements, though, risk information is not consistently reported or, when absent, actively sought by senior management.

A management infrastructure that includes common risk language, information elements, reporting guidelines and technology is not yet in place to enable widespread deployment of IRM.

Lessons learned are an essential part of IRM. Many areas within the DND/CF have lessons learned databases and share lessons learned information as part of training and doctrine. Lessons learned are not specific to risk management, but they do include risk management considerations. In most cases; however, processes and systems for documenting and communicating lessons learned are not very effective, and lessons-learned databases are not easily accessible or widely used. Again, legislation governing access to information and concern over negative consequences may create challenges in certain Level 1 organizations with respect to documenting risk information.

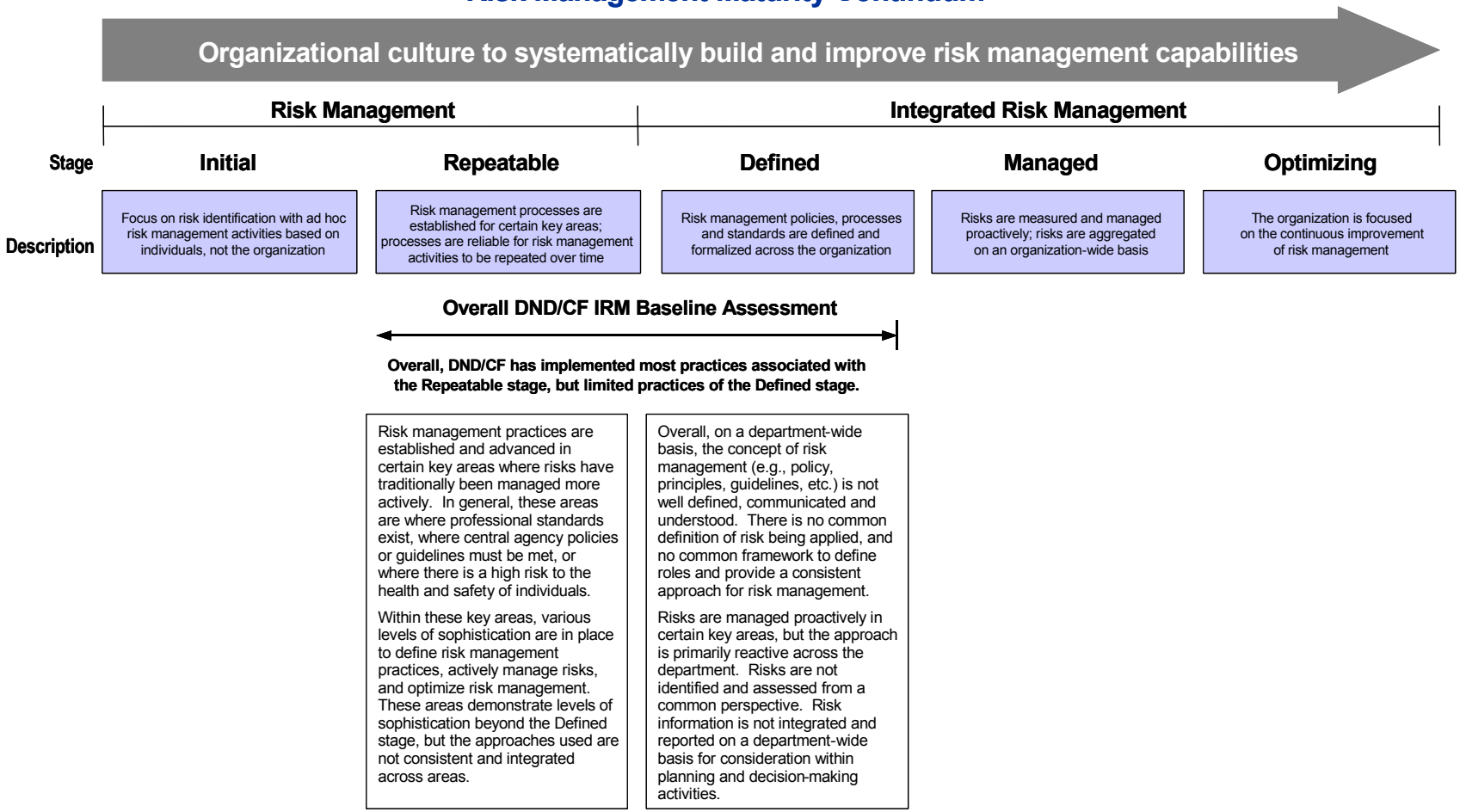
3.8 ASSESSMENT OF IRM WITHIN THE DND/CF

IRM can be considered a journey, and progress is best assessed over time. In relation to the Risk Management Maturity Continuum presented on page 5, the baseline assessment indicates that, overall, DND/CF has implemented most of the practices associated with the *Repeatable* stage and a limited number of practices in the *Defined* stage, indicating that the DND/CF is in the midst of its journey to implement IRM organization-wide.

Certain areas within DND/CF appear to manage risks at a more advanced level of maturity, using characteristics of the *Managed* or *Optimizing* stages. Such functions; however, tend to operate in isolation, with little consistency and limited integration across functions.

The following diagram depicts key observations, drawn from the preceding themes, to support this assessment.

Risk Management Maturity Continuum



Some risks require more sophisticated risk management than others. Since all risks are not equally important, it is impossible to determine objectively whether all risks are properly managed unless a systematic approach is used to identify, assess and prioritize risks in an organization. In addition, a certain amount of sophistication is desirable for managing all risks. A standard framework is considered necessary to ensure that due care is taken for the management of all potential risk issues. DND/CF has an opportunity to achieve a greater level of maturity for IRM. This maturity can be accomplished over time, focusing implementation in the short-term on priority areas that are amenable to IRM.

3.9 ASSESSMENT OF DND IRM PRACTICES IN RELATION TO THE TBS IRM FRAMEWORK

The following table describes current DND/CF IRM practices in relation to the TBS IRM elements and results.

TBS INTEGRATED RISK MANAGEMENT FRAMEWORK ELEMENTS AND EXPECTED RESULTS	DND/CF SUMMARY OF CURRENT CONTEXT
Developing the Corporate Risk Profile • The organization's risks are identified through environmental scanning • The current status of risk management within the organization is assessed • The organization's risk profile is identified	• Across DND/CF, an intuitive approach is generally used for risk identification and assessment, with limited structure for conducting environment scanning. • The current state of risk management in terms of challenges, opportunities, capacity, practices, culture, etc., has been assessed on a department-wide basis in this study. • DND/CF has not developed a department-wide profile of risks, although risk profiles have been developed in certain areas where risks are actively managed.
Establishing an Integrated Risk Management Function • Management direction on risk management is communicated, understood and applied • An approach to operationalize integrated risk management is implemented through existing decision-making and reporting structures • Capacity is built through development of learning plans and tools	• VCDS is the departmental OPI for risk management, although this is not commonly understood. Limited direction has been provided for risk management. • VCDS has accepted responsibility for implementing integrated risk management across the department, and an implementation roadmap is proposed in this study. • There is no coordinated approach for training and continuous learning in relation to integrated risk management. Risk management training and continuous learning is primarily addressed through functional and job specific training.
Practising Integrated Risk Management • A common risk management process is consistently applied at all levels • Results of risk management practices at all levels are integrated into informed decision-making and priority setting • Tools and methods are applied • Consultation and communication with stakeholders is ongoing	• DND/CF does not have a common risk management process consistently applied at all levels within the organization. Risk management processes, methods, tools and practices vary between areas where risks are actively managed. • Risk information is not aggregated and reported on a department-wide basis. At the department level, decision-making and priority-setting considers risks in terms of funding and resources gaps, with limited analysis of the consequences of the gaps. • There is consultation and communication with stakeholders, both internal and external to the department. Communications appear to be mostly issues driven.
Ensuring Continuous Risk Management Learning • A supportive work environment is established where learning from experience is valued, lessons are shared • Learning plans are built into an organization's risk management practices • Results of risk management are evaluated to support innovation, learning and continuous improvement • Experience and best practices are shared, internally and across government	• DND/CF does not have a consistent work environment for risk management. In certain areas where risks are more important, there is active management of risk, learning from experience and sharing of lessons learned. • Learning plans for integrated risk management have not been developed. • Some of the results of risk management activities are reflected in DND/CF doctrine, although evaluation of risk management practices is generally not conducted unless an event occurs or an issue materializes, which has significant implications.

PART 4 – STRENGTHENING IRM WITHIN THE DND/CF

This part provides an approach for the DND/CF to strengthen IRM, an overview of critical success factors, recommendations to commence IRM implementation, and a road map of activities to consider for long-term IRM implementation.

4.1 APPROACH

In many ways, the baseline assessment indicates that effective risk management processes are in place in some areas of the DND/CF; however, opportunities exist to strengthen and integrate risk management. DND/CF does not have a continuous, proactive and systematic process to understand, manage and communicate risk on an organization-wide basis. An opportunity exists; therefore, to introduce a common and organization-wide framework for IRM. A successful IRM regime is evident in the Departmental Airworthiness Program, and recommendations have been developed that reflect the experience and best practices highlighted in this program.

Steps could be taken to build a more supportive culture for IRM within the DND/CF. Integrating risk management with existing management processes will help to maximize the effectiveness of these processes without the need for significant resources. A guiding framework for IRM should be developed and rolled out across the DND/CF. The framework will provide general guidelines but will allow for customization within Level 1s to account for complexities, while maintaining effective risk management processes in military operations and other technical disciplines. The framework's objective is to ensure risk management is embedded in day-to-day activities of DND/CF and not in isolation within each Level 1.

The DND/CF is already actively managing certain risks in some key areas. To further implement IRM, overall guidelines and infrastructure should be developed to provide a standard and consistent framework within which to identify, assess, prioritize and manage risks. An OPI for championing the implementation of IRM should be recognized.

4.2 KEY SUCCESS FACTORS FOR MOVING FORWARD

The main DND/CF challenges for moving forward with IRM are no different from those of other large and complex organizations. Several key success factors should be understood before moving forward with IRM. Examples of organizations that have identified key success factors in implementing IRM include: Human Resources Development Canada, the Office of the Auditor General, and the DND CF Airworthiness/Flight Safety Program.

Human Resources Development Canada (HRDC) is considered a leading adopter of IRM concepts within the federal government. HRDC not only developed a common set of principles and guidelines to identify, assess and prioritize risks, but also continues to refine ways to fold IRM into existing planning processes.[10] In its progress report on IRM, HRDC identified key factors for the successful implementation of IRM; these key factors are outlined in *Annex C*.

In April 2003, the Auditor General of Canada reported on its audit of IRM in Treasury Board Secretariat and six departments. The purpose of the audit was to assess, in each department, the implementation of the Treasury Board Secretariat's Integrated Risk Management Framework.[11] Observations from the audit report are highlighted in *Annex D*.

Within the DND/CF, management has worked on implementing and fostering a culture of proactive and integrated risk management in the area of flight safety. Examples of some of the departmental airworthiness risk-management practices and related lessons learned are highlighted in *Annex E*.

In addition to the key success factors and lessons learned identified by other organizations, DND/CF will need to overcome certain barriers identified in the assessment of IRM practices. The following **key success factors** will help address these barriers. These factors have been incorporated in the proposed road map for moving forward.

- **Fostering a culture receptive to innovation, prudent experimentation and responsible risk taking**
- **Providing adequate resources to establish a framework for IRM**
- **Developing a flexible departmental risk-management framework to allow for customization and Level 1 priorities**
- **Scanning for external influences and changing priorities in order to ensure risk information remains current and relevant**
- **Developing classification guidelines for the protection of sensitive risk-information**

[10] Integrated Risk Management in HRDC, October 2002.
[11] Auditor General Report, April 2003.

Implementing IRM is often done incrementally. Some organizations address one source of risk at a time as part of their existing management processes. Other organizations identify and assess all sources of risk at once and then establish priorities for action. Others consider all risks and actions but only within a sub-component of their operations as a pilot project. But most organizations seek early successes that will help build momentum and promote further development toward their ideal IRM approach.[12]

Sources of risks may be identified from common categories of risks. *Annex E* provides a list of potential categories of risks that could be used as a starting point and then developed based on organizational requirements.

4.3 SIX RECOMMENDATIONS

The DND/CF should focus on six key actions in the near-term to establish and embed IRM.

1. **VCDS should champion IRM.** For IRM to work, senior management must be convinced of its benefits, and it needs to be championed from the top. The benefits of IRM are described in *Annex A*. VCDS should focus on raising executive awareness by promoting IRM within senior management committees such as DMC and PMB. IRM practices, such as structured risk identification, analyses, risk mappings, and open communication about risks should be encouraged.

2. **VCDS should develop a departmental framework for IRM, focusing on the promulgation of a policy, principles, roles, process and common language in which all DND/CF organizations can then link efforts.** The IRM framework should be simple, clear and flexible. We have proposed a framework in the Executive Summary of this report. We also recommend that DND categories of risks be identified for consistent departmental capturing/roll-up. An example of Risk Categories in presented at Annex F.

3. **VCDS should develop, with ADM(Public Affairs), the CF Legal Advisor and the Director Access to Information & Privacy (DAIP), approaches to communicating sensitive information/reporting pertaining to risks.** Other departments have cited various issues, such as damage to the public interest and incomplete advice for decision-making, as rationale for severing risk information from reports, depending on its stage of development and validation.

4. **VCDS should perform a coordination role across various Level 1s and begin developing a corporate risk profile.** Each Level 1, in conjunction with VCDS, should define the areas where a more rigorous IRM approach is required to identify and report risk. As a first step, Level 1s should emphasize areas that:

[12] Institute of Internal Auditors Research Foundation, Enterprise Risk Management: Trends and Emerging Practices, Summary and Conclusions.

- have an impact on safety or security of personnel, such as ammunition, military operations and training, health services, and general safety;
- are regulatory or legislative in nature, and where the precautionary principle may apply in technical or science-based areas,[13] such as nuclear, environmental protection, airworthiness and NBC;
- have a direct impact on public safety, such as homeland security and emergency preparedness; and
- have potential litigation consequences. (Legal Risk Management Committee currently performs IRM in this area.)

5. **VCDS should initiate risk-awareness training for managers and employees, and promote open communication of risk.** To secure the full benefits of IRM, the DND/CF needs to embed an open and sharing information culture. Managers at all levels need to encourage full disclosure of risk information without fear of reprisal. IRM successes in the Flight Safety/Airworthiness Program, and in others noted within this report, should be used to promote the benefits of IRM. Many risks and risk-mitigation strategies, either operational or business practices, have direct relationships to ethics or values. Ways to leverage the Departmental Ethics Program; therefore, as it pertains to IRM, should be investigated.

6. **VCDS should prepare a long-term DND/CF action plan for IRM implementation.** This action plan should specify roles, responsibilities and target dates, and consider resource implications. Given the level of maturity of risk management practices in some areas of DND/CF, implementation should include areas where success will be evident quickly. This practice will build momentum and firmly establish DND/CF on its journey towards IRM.

4.4 A ROAD MAP OF ACTIVITIES TO CONSIDER FOR DND/CF IRM IMPLEMENTATION

This part proposes a road map of key activities to enable DND/CF to move forward and develop additional capabilities for IRM. The roadmap considers the current context of risk management within DND/CF and the opportunities available. Key success factors and lessons learned are integrated within the proposed activities. The suggested approach is flexible and; therefore, dependent on the speed of IRM implementation and the resources devoted to it.

The road map, outlined in the following pages and articulated in the suggested order of implementation, will assist DND/CF in moving further along the Risk Management Maturity Continuum.

[13] The Federal Government is currently preparing a framework for the application of precaution in science-based decision-making about risk, whereby it is recognized that the absence of full scientific certainty shall not be used as a reason for postponing decisions where there is a risk of serious or irreversible harm. This framework intends to apply general principles for precautionary decision-making, and is intended for regulatory departments and agencies. Several areas in DND could be impacted, including CAS – Flight Safety; ADM(HR-Mil) – Health Services; ADM(IE) – Environmental Protection and Nuclear Safety; ADM(Mat) – Airworthiness and Ammunition; ADM(S&T)/DCDS – Nuclear, Chemical, Biological, Radiological.

ROAD MAP ACTIVITY	DESCRIPTION	SUGGESTED APPROACH
1. Establish senior-management commitment	Establishing senior-management commitment involves convincing senior management of the importance of risk management. Senior management should foster a culture receptive to risk management by defining and communicating expectations for risk management, and providing adequate resources to support IRM. Senior management should ensure that risk management receives appropriate visibility by including it on the agenda of key meetings. Senior management can also foster a culture receptive to risk management by enquiring about the progress of implementation efforts.	▪ VCDS should take ownership and responsibility for moving the IRM agenda forward. This will involve a project initiative with dedicated resources. ▪ Discussions should occur at senior management levels (DM/CDS) on the benefits of IRM and the desirability of moving forward on it. ▪ Senior management should communicate the importance of risk management, the decision and reasons to move forward with IRM, and information on what the decision entails in terms of key milestones and timelines. ▪ Senior management should define and communicate expectations for managing risks, including key messages, with respect to the responsibility for managing risk and the openness with which risk should be discussed. ▪ Senior management should demonstrate the need for IRM by leveraging internal success stories such as airworthiness risk management within CAS.
2. Develop an enabling IRM framework	IRM frameworks provide a more formal, structured, continuous and organization-wide approach to risk management. While frameworks provide structure, they are not intended to be inflexible and overly prescriptive. They do; however, promote consistency and provide guidance and assistance in identifying, assessing, managing and reporting on risk on a continuous basis.	▪ VCDS should lead the development of a departmental IRM framework in consultation with Level 1 representatives. This CRS report provides an example IRM framework in the Executive Summary. ▪ The IRM framework should integrate with planning, decision-making and performance management activities where applicable. ▪ The IRM framework should provide high-level guidelines for how risks should be categorized, identified, assessed, prioritized, acted-upon and monitored. ▪ The IRM framework should be flexible to allow for organizational complexities. Level 1 organizations would determine how best to apply the framework in their respective areas to meet expectations for IRM. They would also determine appropriate security classification for the risk information developed.

ROAD MAP ACTIVITY	DESCRIPTION	SUGGESTED APPROACH
3. Develop a corporate risk profile	Developing a risk profile early in the process provides many benefits and may help tailor the desired IRM approach. Risk profiles involve the identification and assessment of risks and the determination of tolerance levels. The Auditor General has reinforced the need to develop a risk profile as part of its action plan to implement IRM in the federal government.	▪ VCDS should take the lead for the development of a DND/CF risk profile by defining the requirements and approach to be followed. ▪ Structure and guidance should be provided by VCDS for identifying, classifying, assessing and prioritizing risks. The definition of tolerance levels requires direction from senior management, and may be dependent on the nature of the risk or the functional area. ▪ VCDS should coordinate data gathered by Level 1s and develop a departmental risk profile. Each Level 1, in conjunction with VCDS, should define the areas where a more rigorous IRM approach is required.
4. Integrate with planning and performance management, and develop risk-reporting guidelines	Effective risk management does not operate as an independent process. Risk management should integrate with other processes such as planning and performance management. Linkages need to be defined to influence priority setting and resource allocation. Performance measures should include activities relating to risk management.	▪ VCDS and Level 1 business planners should work together to determine how risk management should integrate with planning, priority setting and risk reporting. ▪ VCDS should conduct work sessions with Level 1 organizations to determine how risk management should link with performance measures under development. ▪ As a result of these consultations, guidance should be developed on how to consider risks within the planning, priority setting and performance management processes.
5. Provide education and awareness training to managers and staff on IRM concepts	Education and awareness training sessions will help foster a better understanding of IRM concepts and benefits, including the concept of risk as opportunity. These sessions should also include communication regarding how the DND/CF is moving forward with IRM.	▪ VCDS should lead the development of education and awareness sessions across the DND/CF. Coordination will be required with Level 1 representatives to identify existing competencies and skills, and determine who should receive training as well as the nature and extent of the training required. Learning plans and strategies should be developed to improve and maintain competencies and skills.

ROAD MAP ACTIVITY	DESCRIPTION	SUGGESTED APPROACH
6. Implement an enabling IRM framework (as developed in Road Map activity #2)	A pilot-project approach should be used to implement the framework. Based on the results of a pilot project, the framework should be updated and rolled out across THE DND/CF. Implementation of the framework should be monitored for progress.	▪ It is understood that the IRM framework should define expectations only and provide general principles and guidelines for risk management. The framework should be simple and flexible for Level 1s to apply and customize to their context. Consideration should be given to a standard information model to allow for the roll-up and reporting of risk information on a department-wide basis. ▪ The pilots should be selected strategically, based on a number of factors such as support for a risk framework and expected benefits of implementation. ▪ VCDS should provide guidance and advice for the pilots; monitor progress; report progress to senior management; and update the framework as required based on lessons learned.
7. Define roles and responsibilities for IRM	IRM frameworks often include an articulation of key roles. Leadership, coordination, participation, and risk ownership roles should be included. These roles should be incorporated into existing job responsibilities.	▪ Leadership roles involve ensuring that the IRM framework is applied and that risk information is updated and reported on a regular basis during the year. As the OPI for risk management, VCDS should have the overall leadership role; Level 1s would have a leadership role within their organization. ▪ Coordination roles involve coordinating the application of the framework and the reporting of information. Business planners are typically well positioned to act as coordinators. ▪ Participation roles involve the DND/CF managers and staff who need to provide input to identify, assess and prioritize risks within each of their respective units. Managers and staff also need to support coordinators and risk owners. ▪ Risk ownership roles involve determining which actions should be taken for managing risks and defining expected results. Risk owners are persons who can determine how a particular risk should be managed and who has authority to take action. Risk owners are also responsible for reporting the status of risk-management actions and the results achieved. They should be identified at the lowest possible level within the DND/CF.

ROAD MAP ACTIVITY	DESCRIPTION	SUGGESTED APPROACH
8. Define performance targets and build targets into performance agreements	Performance targets and accountabilities for risk management should be defined at individual levels, and incorporated into job descriptions, competency profiles and performance agreements. Targets and accountabilities should be based on the roles and responsibilities defined.	▪ Performance targets could be developed in relation to the achievement of IRM milestones, implementation of the IRM framework and the achievement of results for managing risks. ▪ As a first step, performance targets could be developed for leadership and coordination roles to provide incentive for implementing the framework. Performance targets could be developed for risk owners to provide incentive for the implementation of risk management actions.
9. Make risk management an integral part of planning, decision-making and performance management	Senior management committees across Level 1s should be responsible for the consideration of risks as part of decision-making activities. Consideration of risks is particularly important for planning and priority setting.	▪ Risk management will need to be part of the agenda of specified senior management committees horizontal to the DND/CF and specific to Level 1s. ▪ Based on the IRM framework developed, VCDS should identify departmental committees where risks should be discussed and considered as part of planning and decision-making. Each Level 1 should propose their governance structure for risk management.
10. Publicize and reward successes	Reward and recognition should be provided for risk-management successes. Reward and recognition are effective approaches, setting a positive tone from the top and influencing risk-management culture.	▪ VCDS should establish guidelines for reward and recognition. Emphasis should be placed on team and group recognition. ▪ Senior management should be responsible for managing rewards and recognitions for risk management based on the guidelines developed by VCDS.

ANNEX A – BENEFITS OF INTEGRATED RISK MANAGEMENT

A number of benefits may be anticipated from applying Integrated Risk Management:

- **Early warning system to lessen the impact of negative surprises**

  By having a systematic approach to identify, assess and prioritize risks, managers/COs would be able to plan and implement appropriate actions to manage risks. Ownership of risks and risk management actions will be assigned, and risk information will be considered as part of planning, decision-making and reporting activities on an ongoing basis.

- **Effective responses to limit the impacts of risks that may occur**

  By anticipating and managing risks proactively, staff should be able to lessen the likelihood of unfavourable events, reduce the impact of such events should they occur, or be in a better position to respond effectively to risk issues that surface. By maintaining an inventory of risks and risk management actions, accountabilities for managing risks will be better identified and more clearly defined. There will also be greater opportunity for learning from past experiences.

- **Greater likelihood of success in the achievement of objectives**

  By systematically identifying, assessing and taking action on risks relating to their objectives and assigned defence tasks, it is expected that organizations at all levels will significantly improve their chances of success. Slightly more time would be spent proactively managing risks, and significantly less time should be required to deal with the consequences of risks having occurred.

- **Horizontal synergies across THE DND/CF**

  By sharing risk information with other THE DND/CF organizations, it is expected that a more integrated approach can be used to address risks in a proactive and responsive manner. IRM should provide a better understanding of risk at each organizational level and within other areas, and support the sharing of risk information beyond organizational barriers or stovepipes that may exist.

ANNEX A

- **Demonstrating Due diligence**

  The DND/CF will be able to demonstrate that they took all reasonable effort to identify, analyze and mitigate risks.

Many incidental benefits should materialize through application of IRM, simply from having risk issues discussed openly and acted upon systematically. For example, planning may become more focussed, and resources may be better allocated to activities key to the achievement of objectives and the management of risks. The analysis of risks may provide valuable information for comparison of courses of action or in the development of business cases. The communication of risk information across the organization may create greater awareness for managing risks and may improve ability to anticipate and adapt to change.

ANNEX B – DIAGNOSTIC TOOL

STATEMENTS to help gather relevant information in relation to integrated risk management **Please respond in relation to your Level 1 organization**	**SCALE** to help determine the extent to which integrated risk management is being practiced Never (1) Sometimes (2) (3) (4) Always (5) | Don't know / Doesn't apply	**COMMENTS** to provide examples in relation to the statements and scale
PART 1 – IDENTIFYING IMPORTANT RISKS AND PRIORITIES		
1. A common definition of risk is used across the organization. Eg. When people discuss risk, it means the same thing throughout the L1.	1 2 3 4 5 |	
2. Risk tolerances are understood. Eg. There is an understanding of the degree of risk that is acceptable within your Level 1.	1 2 3 4 5 |	
3. The environment is scanned and potential risks are identified on a regular basis. Eg. Sources of risk, opportunities and threats are regularly reviewed.	1 2 3 4 5 |	
4. Important risks are formally assessed, using established criteria, on a regular basis. Eg. The assessment of risks is done in terms of impact and likelihood.	1 2 3 4 5 |	
5. Important risks are monitored on an ongoing basis. Eg. There are regular forums for L1 senior managers where risks are reviewed. Actions to mitigate these risks are also discussed.	1 2 3 4 5 |	
6. Risk management priorities are in line with organizational objectives. Eg. Risks are prioritized for action, and these priorities line up with the priorities of the L1.	1 2 3 4 5 |	

ANNEX B

STATEMENTS to help gather relevant information in relation to integrated risk management **Please respond in relation to your Level 1 organization**	**SCALE** to help determine the extent to which integrated risk management is being practiced Never 1 ☐ 2 ☐ 3 ☐ 4 ☐ Sometimes 5 ☐ Always | Don't know / Doesn't apply ☐	**COMMENTS** to provide examples in relation to the statements and scale
PART 2 – ESTABLISHING ROLES AND RESPONSIBILITIES FOR RISK MANAGEMENT		
7. Risk management strategies are understood. Eg. There is clear direction as to how risks are to be managed within your L1. Objectives and policies are in place.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
8. A risk management OPI provides support. Eg. There is a designated champion for risk management and this champion provides direction and disseminates information and best practices regarding risk management.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
9. Stakeholders are informed of important risks. Eg. Those that contribute or could be impacted are kept informed of significant risks.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
10. Roles and responsibilities for managing risks are understood. Eg. It is clear that everyone has a role in managing risk within your L1 and they know what they need to do. There are designated risk owners and risk managers.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
11. Individuals with accountability for managing risks have the required authority. Eg. The risk owners and managers, have the necessary authority to act. Risks are not assigned to individuals who do not have authority to deal with them.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	

ANNEX B

STATEMENTS to help gather relevant information in relation to integrated risk management **Please respond in relation to your Level 1 organization**	**SCALE** to help determine the extent to which integrated risk management is being practiced Never 1 ☐ 2 ☐ 3 ☐ Sometimes 4 ☐ Always 5 ☐ Don't know / Doesn't apply ☐	**COMMENTS** to provide examples in relation to the statements and scale
PART 3 – APPLYING AN INTEGRATED RISK MANAGEMENT APPROACH		
12. Overall, there is a defined process for risk management. Eg. The process to be followed within your L1 to identify, act upon and monitor risks is clear to all individuals.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	
13. Practices for managing risks are consistently applied. Eg. The approach to managing risks is aligned throughout your L1.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	
14. Tools, methods and techniques are used for managing risk. Eg. There is a common model, frameworks or template used to identify, assess, record and monitor risks.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	
15. Risks are addressed as part of the planning process. Eg. Risks are identified and monitored, and mitigating strategies and action plans are developed as part of the planning process.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	
16. Important decisions involve an analysis of underlying risks. Eg. Key decisions take into account risk considerations.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	
17. There is a linkage between performance measures and risk. Eg. Performance measures have been established that relate to risks within the Level 1.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ ☐	

ANNEX B

STATEMENTS to help gather relevant information in relation to integrated risk management **Please respond in relation to your Level 1 organization**	**SCALE** to help determine the extent to which integrated risk management is being practiced Never 1 2 3 4 5 Always | Don't know / Doesn't apply	**COMMENTS** to provide examples in relation to the statements and scale
18. Practices for managing risks are monitored for effectiveness. Eg. Risk management activities are regularly reviewed (i.e. using metrics) to ensure they contribute to effectively managing risk, and changes are implemented.	☐1 ☐2 ☐3 ☐4 ☐5 | ☐	
19. Risk management information is reported. Eg. There are reports prepared which highlight risks and risk mitigation activities at every level.	☐1 ☐2 ☐3 ☐4 ☐5 | ☐	
20. Risk information is shared within your L1, with other L1 organizations or on a department-wide basis. Eg. Risk information is discussed with other groups proactively, with the management of risks adjusted accordingly.	☐1 ☐2 ☐3 ☐4 ☐5 | ☐	
21. Technology is used to store risk information and to facilitate reporting. Eg. A software system is used to log risk information and to facilitate the aggregation and reporting of information to senior management.	☐1 ☐2 ☐3 ☐4 ☐5 | ☐	

ANNEX B

STATEMENTS to help gather relevant information in relation to integrated risk management **Please respond in relation to your Level 1 organization**	**SCALE** to help determine the extent to which integrated risk management is being practiced Never 1 ☐ 2 ☐ 3 ☐ 4 ☐ Always 5 ☐ | Don't know / Doesn't apply ☐	**COMMENTS** to provide examples in relation to the statements and scale
PART 4 – ENABLING RISK MANAGEMENT AND LEARNING FROM EXPERIENCE		
22. Organizational culture supports effective risk management. Eg. There is open communication about risks, people are encouraged to identify and discuss risks and propose innovative ways to deal with risk.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
23. Training on risk management concepts and fundamental theory is provided to improve risk management competencies. Eg. Training has been developed and implemented to ensure L1 individuals involved in risk management have the right skills and competencies. Training is available and on going.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	
24. There is recognition for managing risks.	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ | ☐	

ANNEX C – HRDC KEY SUCCESS FACTORS FOR IMPLEMENTING INTEGRATED RISK MANAGEMENT

KEY SUCCESS FACTOR	DESCRIPTION
Supportive environment from key stakeholders	Having stakeholder interest, support, and inquiry on the progress of risk management is helpful for putting integrated risk management on the agenda of corporate priorities.
Commitment from senior management and middle management	Senior and middle management need to support risk management as a concept. To adopt such a perspective, and ultimately change behaviours, managers need to believe that the risk management perspective is of value, and provides a better way of doing business.
Designated group for specialist support	Having an assigned group provide expertise and impose a flexible discipline for practicing integrated risk management is helpful. A clear mandate from senior management to such a group is key for establishing legitimacy and facilitating coordination across groups.
Investment in integrated risk management infrastructure	The start-up of integrated risk management requires time and effort to organize for change, provide adequate training, and develop common method or techniques. Having a simple, clear and flexible framework and a common language is key for integrated risk management.
Central direction and coordination	Central direction and coordination are necessary for integration with corporate planning and priority setting. Since risks tend to be managed within business lines, the heads of business lines should be responsible to identify and assess risks. A corporate level process; however, is needed to set priorities and allocate resources to major risk areas. A corporate level environmental scanning process is also needed to capture broad strategic challenges and opportunities related to the overall departmental mandate. The corporate planning or strategic policy areas may be the best positioned to take the lead for corporate level functions.
Progress reporting to senior management	It is quite effective to establish events or milestones, and to require progress reports to the most senior departmental management levels. This practice is successful in focussing the attention of ADMs and their respective management teams on integrated risk management.
Linkage with corporate planning and priority setting processes	Integrated risk management must impact priority setting and resource allocation if it is to be meaningful. Corporate planning and priority setting can be a catalyst for progress reporting, and provide an impetus for the implementation of integrated risk management.
Scaleable implementation	The implementation of integrated risk management is likely to occur in stages. Having a strategy to move from pilots to full scale implementation, to a deep embedding of integrated risk management into departmental decision processes helps keep implementation on track over long periods. Sustained energy and focus is needed until integrated risk management is just a normal way of doing business.

ANNEX D – REPORT OF THE AUDITOR GENERAL OF CANADA ON INTEGRATED RISK MANAGEMENT

On April 2003, the Auditor General of Canada reported on its audit of Integrated Risk Management, involving Treasury Board Secretariat and six departments. The purpose of the audit was to assess the adequacy of steps that departments are taking to implement the Treasury Board Secretariat's Integrated Risk Management Framework.[14]

In its review of good practices and lessons learned by organizations outside of the federal government department, the Auditor General identified a number of factors that contribute to the successful implementation of integrated risk management:

- Having senior management support
- Having a common strategy and framework
- Having clearly assigned responsibilities for implementing integrated risk management
- Taking a continuous approach for managing risks

As a result of the audit, the following recommendations were made to enable the implementation of integrated risk management within departments:

- More visible commitment and leadership is needed from senior management
- Departments need a well-developed action plan for integrating risk management into their operations
- Departmental risk profiles should be developed, which identify and assess risk, and determine tolerance levels
- Capacity to implement and maintain integrated risk management practices should be assessed
- Learning plans and strategies should be developed to improve and maintain competencies and skills
- Progress on the implementation of integrated risk management should be monitored and reported

The proposed Roadmap for implementing integrated risk management within the DND/CF is responsive to the above good practices, lessons learned, and recommendations.

[14] Auditor General Report, April 2003.

ANNEX E – FLIGHT SAFETY CASE STUDY

In this part, an overview of the Departmental Airworthiness Program is provided as an example of advanced risk management practices within DND/CF.

History

Risk management was formally introduced within Director Flight Safety (DFS) in 1997-98 following a series of flight safety incidents surrounding the Aurora Flight Director Indicator (FDI) and the Tutor Ejection Seats. Prior to this time, risk management was not formalized; it was assumed that risk management was implicitly part of on going flight safety processes already in place.

However, following the Aurora and Tudor incidents, it was realized that these issues had in fact been around for a number of years, but that there had been no accountability for ensuring that these issues were addressed. While there was awareness of risk management in general, the understanding was not consistent, and there were no formalized risk management processes in place. It was at this time that an officer in the Airworthiness Program realized that there was a need to create accountability for managing risks. In 1999, it became mandatory within CAS that a person with the required authority sign-off and become accountable for risk assessments carried out. Formalized processes to identify, assess, manage and report risk were then created in support of this accountability.

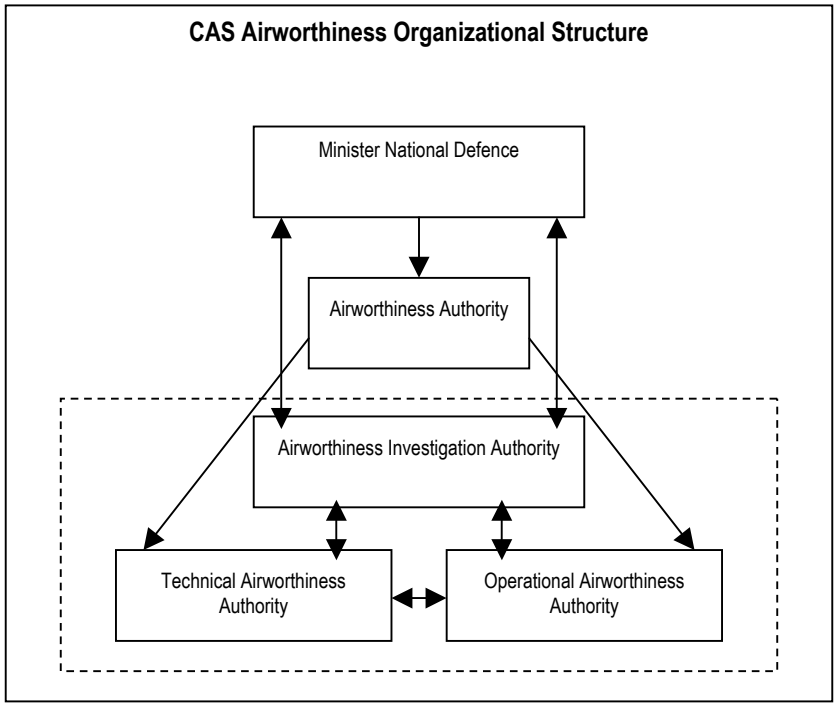
Today

Since 1997, risk management practices have evolved to the point that they are a part of daily flight safety operations, from the working level to the most senior management levels. Risk management processes have, for the most part, successfully been integrated within other processes, so that risk is a natural “filter”, through which individuals involved in flight safety operate.

The Airworthiness Risk Management Program is an example of a DND/CF organization having implemented characteristics of the “Managed Stage” and the “Optimizing Stage” within the Risk Management Maturity Continuum. There is recognition that there are still challenges to overcome and room for continuous improvement; for example, CAS is now trying to standardize flight safety risk management practices across all of its operations. However, there are a number of best practices and lessons learned that can be drawn for consideration of risk management practices within the broader DND/CF organization.

ANNEX E

In reviewing the risk management within the Airworthiness Program, there are selected practices that have been identified as being key in the successful implementation of risk management within the organization such as: organizational structure, accountability, culture and communication. These best practices and lessons learned, along with supporting practices, have been outlined below.



Organizational Structure

Flight safety risk management practices have been rooted within the broader accountability structure for airworthiness. Specifically, the Minister has delegated to the Chief of Air Staff the responsibility for the Airworthiness Program as the Airworthiness Authority (AA). Three other positions are also delegated by the Minister in support of the Airworthiness Program, namely the Technical Airworthiness Authority (TAA), the Operational Airworthiness Authority (OAA) and the Airworthiness Investigation Authority (AIA).

ANNEX E

The roles of these organizations in relation to risk management are as follows:

AA	Responsible for overseeing all aspects of risk management within the Airworthiness Program.
TAA	Responsible for developing and implementing risk management processes as they relate to engineering, manufacturing, maintenance and material support, as well as addressing and managing specific risks as they relate to these areas.
OAA	Responsible for developing and implementing risk management processes as they relate to operational procedures, flight standards, operator training/qualification/licensing and aerospace control operations, as well as addressing and managing specific risks as they relate to these areas.
AIA	Responsible for working with TAA and OAA to support development of risk management processes including on-going monitoring of risk management process effectiveness, as well as on-going education, promotion and accident/incident investigation and reporting.

Embedding risk management practices as part of the organizational structure has made it very clear which groups are responsible and accountable for developing, implementing and monitoring risk management practices, as well identifying, addressing and monitoring risks.

Accountability

Accountability is required to have risk management taken seriously and effectively acted upon. The current risk management program requires that for any risk identified and assessed, an individual be named accountable based on the initial risk assessment results. This same individual is then also accountable for the outcomes associated with the risk. Ensuring accountability has prompted individuals being held accountable to request and review all relevant documentation to ensure completeness and accuracy.

Culture

The success of risk management with respect to flight safety is also attributed to a culture where “flight safety is part of everybody’s business”. As a result, employees are encouraged to identify and assess risks, and report risk information without fear of reprisal. To create this culture, the Director of Flight Safety (DFS), the appointed AIA, has focused on educating the organization on the importance of risk management. DFS strongly emphasizes the need to carry out every risk assessment honestly, discouraging conscious downgrading of a risk to allow sign-off by an individual with lesser authority. DFS has developed some guiding principles, which have been widely accepted within CAS, and also form part of the proposed Airworthiness Risk Management Program. These principles are:

ANNEX E

- Do not accept unnecessary risk;
- Accept risk only if the benefits outweigh the costs;
- Airworthiness risk must be accepted by the appropriate level of airworthiness authority; and
- Assess risk continuously.

CAS makes every effort to actively promote "finding cause, not blame". This culture is supported by policies, processes, open communications, training and on-going education.

An example as to how the culture supports risk management is in the DND/CF publication "Flight Comment", where individuals who have identified risks are celebrated and showcased as key contributors to enhancing flight safety within the Department.

Another example is the way in which DFS tries to discourage military commanders from thinking that an organization (e.g., Wing) that reports more risk is less safe than an organization that reports less risk; when in fact, it may be an inverse relationship. If an organization is more proactive in identifying risks, the organization is also more likely to be proactive is undertaking corrective measures to address any safety deficiencies.

Communication

A key success factor in implementing flight safety risk management has been on-going communication. DFS has been a key contributor in communicating the importance of risk management within CAS. In addition to senior briefings within Headquarters, DFS also spends almost half of the year visiting bases and speaking with personnel from across the organization to gauge the level of understanding of risk management, assess how risk management is being practiced, and identify and monitor broader organization risks impacting flight safety.

One lesson learned by DFS was the need to understand the nuances of the push-pull relationship in terms of communicating flight safety risk management information. At one point, it was felt that given the amount of information available to individuals regarding the status of current risks and risk trends via technology, certain reports could be discontinued. However, following the discontinuation of certain reports, employees commented that the reports were useful in prompting review of the information (push), rather than residing in a database (pull). A decision has recently been made to reinstate some of these discontinued reports, based on demand.

ANNEX E

Other Supporting Practices and Tools

A number of other practices and tools are in place within CAS, which promote and support on-going flight safety risk management:

- **Senior Management Buy-in.** Risk management was introduced to senior management as a way of ensuring due diligence in matters of flight safety. Once risk management was seen as a way to facilitate and not hinder the job, risk management "sold itself". Today, risk management is synonymous with flight safety.

- **Risk Tolerances.** Guidance provided by the TAA and OAA is that unsafe airplanes are not to be flown. Risk management processes developed by these organizations are such that in order to correct a situation to allow a plane to be flown, a risk assessment needs to be carried out and authorized, and corrective actions taken.

- **Roles and Responsibilities.** Roles and responsibilities have been clearly defined in terms of risk owners, risk managers and OPIs. As a starting point, it is made clear at the outset that all individuals have a responsibility for identifying and acting on risk to the extent of their ability, which may include addressing the risk or reporting it upward for assessment and further action. Risk owners are those individuals who take responsibility for and sign-off on the risk assessment. Risk owners then assign risk managers who carry out tasks on behalf of the risk owner. OPIs for flight safety risk management are in place in all bases. These OPIs have the knowledge, skills and abilities to help individuals involved in flight safety better understand and appropriately apply risk management practices.

- **Database.** A database was created, dating back to 1970, called the Flight Safety Information System (FSIS), documenting all occurrences, investigations, corrective and preventive measures taken. This database is accessible to approximately 300 individuals, allowing them to document any concerns and query the system for historical flight safety information. The system has been designed to allow for anonymity of the individuals involved in a particular occurrence, in an effort to encourage use of the system. Strict guidelines exist, in that information in the system is to be used only to enhance flight safety, and not to associate incidents to individuals. This database is a part of the Flight Safety / Airworthiness Program, but plays the dual role of also sharing knowledge and allowing for preventive measures as part of overall risk management.

- **Risk Assessment.** Risk assessments are carried out across the TAA, OAA and AIA using defined criteria for both severity and probability. Descriptions have been provided for each of the different criteria. These same criteria are being proposed as part of the Airworthiness Risk Management Program for CAS.

ANNEX E

Severity	Probability
1. Catastrophic	1. Frequent
2. Critical	2. Probable
3. Significant	3. Occasional
4. Negligible	4. Remote
	5. Improbable / Unlikely

In the event that an individual does not have the technical skill or knowledge to assess an identified risk, the risk is passed on to individuals with the required skills and knowledge via the FSIS for the risk assessment.

- **Prioritization of Risk.** Flight Safety risks are prioritized within CAS. Specifically, all risks identified as causing damage or causing injury to an individual are addressed and corrective action is taken. All other risks are identified and discussed using an issues list and "top ten" approach. This list tracks all potential risks, including both technical and non-technical risks, including frequency of posting, operational levels, supervisor courses, etc. Potential risks included in the issues list are prioritized based on a DFS risk assessment. Other information included in the list includes potential outcomes and mitigating activities. Risks that are deemed to be more serious are more actively risk managed. This list is used as a way of sharing risk information with management across CAS.

- **Reporting.** Reporting on risk and risk management activities takes place both informally via on-going discussions, as well as formally via the FSIS database, issues list, Hazard Reports, etc. All medium and high risks are reviewed and discussed by senior management at the Airworthiness Review Board. Presentations by DFS also leverage risk management techniques, presenting issues as risks with associated risk assessment, mitigating strategies and monitoring activities.

Key lessons learned from the DFS experience…

- Ensure buy-in at senior levels
- Make risk management a requirement
- Involve stakeholders
- Develop standard risk management guidelines, but allow implementation based on an organization's specificities
- Invest in the development of risk management tools and techniques
- Embed existing practices with risk management for optimal integration
- Extensively communicate the importance of risk management

ANNEX E

- **Risk Assessment Repository.** Ensuring that risk assessments are done properly and honestly is a constant challenge of communication and education. While DFS does review some of the risk assessments, it is felt that a central repository for all risk assessments would be useful to ensure that all risk assessments, including lower rated risk assessments, are reviewed for appropriateness.

- **Trend Analysis.** Desk officers throughout the organization actively review information within the FSIS to see if any trends exist and to identify if corrective or preventive actions are required.

- **Training.** Risk management training has been embedded as part of all flight safety training, including: TQ3, Flight Safety Course, Flying Supervisor Course, etc. On-going risk management training and education also takes place on-the-job through dealings with DFS and the flight safety OPIs. There was also a sense that risk management could be introduced even earlier, as part of OTU.

- **Integration with Other Business Processes.** Risk management has been inculcated as part of the Airworthiness Program. As a result, risk is an on-going consideration of all management processes, including planning.

The Airworthiness Program is a successful initiative that has implemented a proactive approach for managing risks. Risks are anticipated and risk management activities are planned and implemented proactively using a structured and consistent approach. Organization structure assigns responsibility for risk management. Risk management culture has evolved to a point where it is considered everyone's responsibility to manage risks, and risk information is shared openly. Common tools and techniques, as shown in this case study, are used for managing risks and reporting risk information.

Within the scope of its operations, the Airworthiness Program has demonstrated an advanced stage of integrated risk management. In relation to the Risk Management Maturity Continuum, the Airworthiness Program is operating at the Managed Stage, with certain characteristics of the Optimizing Stage.

ANNEX F – RISK CATEGORIES AND EXAMPLES

The identification of risks requires the consideration of multiple factors, sources and types of risks that may impede the achievement of objectives and assigned defence tasks across the DND/CF or internal to the functions and business lines. Based on the TBS Integrated Risk Management Framework, sources of risk can be external organization. External sources of risk include economic factors, political factors, environment factors, etc. Internal sources of risk may include factors relating to policy and strategy, goals and objectives. Types of risks include functions such as technology, finance, human resources, etc. [15]

The following risk categories can be used as a starting point to identify risks in relation to their source, their type, or their association to specific DND/CF functions or business lines. These categories of risk are not exhaustive and are meant to provide a starting point for risk identification. Based on the risks that will be identified, the categories of risk may need to be updated or modified to better reflect organization context and provide a better classification of risks.

RISK CATEGORY	RISK EXAMPLES
Business Environment Risks	e.g., risks from industry developments, changing demographics, globalization, etc.
Environmental Protection Risks	e.g., risks relating to specific environment issues.
Culture, Values and Ethics Risks	e.g., risks relating to differences in culture, values, and ethics across the organization.
Health and Safety Risks	e.g., risks relating to workplace hazards and working conditions.
Political Risks	e.g., risks relating to rapid change of government focus, priorities, pressures, etc.
Expectations Risks	e.g., risks relating to stakeholder expectations including the public, media, elected officials, OGDs, etc.
Reputation Risks	e.g., risks relating to the reputation of military and civilian staff, reputation of the organization, etc.
Alliance Risks	e.g., risks relating to allies, vendors, contractors, etc.

[15] TBS Integrated Risk Management Framework, April 2001, p.16.

ANNEX F

RISK CATEGORY	RISK EXAMPLES
Policy Risks	e.g., risks relating to the definition and adoption of policies, the acceptance of policies from stakeholders, etc.
Planning Risks	e.g., risks relating to the setting of adequate goals and objectives, the planning of activities, the identification of priorities, the allocation of resources, etc.
Doctrine Risks	e.g., risks relating to the adoption and communication of doctrine, the training of military and civilian staff, etc.
Organization Risks	e.g., risks relating to organization structure, business model, roles, responsibilities, span of control, reporting relationships, decision-making approach, coordination with other L1s, etc.
Operational Risks	e.g., risks relating to the planning, mounting, conduct, and sustainment of operations, etc.
Supply and Logistics Risks	e.g., risks from procurement, contracting, inventory, equipment storage, protected and proper facilities, business continuity, emergency preparedness, etc.
Human Resources Risks	e.g., risks relating to succession planning, recruiting, retention, competencies and skills development, performance management, classification, compensation, morale, motivation, productivity, etc.
Financial Risks	e.g., risks relating to foreign currency fluctuations, funding appropriations, budget allocations, commitments, expenditures management, capital investments, payments, custom and commodity taxes, accounting, reporting, etc.
Information Risks	e.g., risks relating to information confidentiality, privacy, access to information, information quality and integrity, documentation management, knowledge management, etc.
Technology Risks	e.g., risks relating to information technology strategy, changes in technology, management of technologies, development and implementation projects, user support, system functionality, system capacity, system reliability, physical security, contingency, back-up, recovery, etc.
Change Management Risks	e.g., risks relating to the management of change initiatives.
Compliance Risks	e.g., risks relating to legal and regulatory compliance, central agency policies, contractual obligations, statutory reporting, employment rules, litigation and liabilities, etc.