INTERNATIONAL MARITIME ORGANIZATION

IMO

E

COUNCIL WORKING GROUP ON RISK REVIEW, MANAGEMENT AND REPORTING
1st session
Agenda item 2

CWGRM 1/INF.2
6 June 2007
ENGLISH ONLY

DEVELOPMENT OF A RISK MANAGEMENT FRAMEWORK, INCLUDING A RISK MANAGEMENT POLICY AND A WORK PROGRAMME FOR ITS COMPLETION

Risk Management Framework documents

Note by the Secretariat

SUMMARY

Executive summary:	This document contains substantive risk management documents considered by the Intersessional Correspondence Group on risk management established by the ninety-sixth session of the Council
Action to be taken:	Paragraph 3
Related document:	C 97/3(b) (annex, paragraph 3.2)

1 The Council, at its ninety-sixth session, established an Intersessional Correspondence Group to prepare terms of reference for the Risk Review, Management and Reporting Working Group and further advance development of the risk framework and detailed review of the Organization's risks. In undertaking its work, the Intersessional Correspondence Group took into account the Secretary-General's proposals in document C 96/5(b) and discussions in the Council. During the course of the Intersessional Correspondence Group, a number of participants provided examples of risk management frameworks presently in use in Member States and international organizations, and substantive proposals for a risk management framework for the Organization, and these were also considered by the Group.

2 Attached at annex are the four substantive documents used by that Group which, as requested by the first session of the CWGRM, are being circulated to all Member States to provide relevant information in support of further discussions on the Organization's work on risk management. The documents are:

- Risk Management Framework for IMO – submitted by Australia;
- Treasury Board of Canada Integrated Risk Management Framework;
- Risk Management Framework for IMO – submitted by South Africa; and
- IALA Guidelines on Risk Management.

Action requested of the Working Group

3 The Working Group is invited to note the information provided in the attached annex.

***

ANNEX

RISK MANAGEMENT FRAMEWORK DOCUMENTS

APPENDIX 1

Risk Management Framework for IMO – submitted by Australia

Risk Management Framework for IMO

Definition of Risk and Risk Management

Risk can be defined as “the combination of the probability of an event and its consequences.” (ISO/IEC Guide 73).

“Risk management is a central part of any organisation’s strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.” (A Risk Management Standard – published by AIRMIC, ALARM, IRM 2002)

Managing risks involves both threats and opportunities. Risk management is about identifying potential variations from what we plan or desire and managing these to maximize opportunity, minimize loss and improve decisions and outcomes. Managing risk means identifying and taking opportunities to improve performance as well as taking action to avoid or reduce the chances of something going wrong.

Consistent with initial views offered in C 96/5 (b), management of risk should be integrated into the management philosophy of the organisation, should become part of a formalised process, not as a one-off event. A risk management framework should facilitate development of a culture where risk is managed effectively and consistently, where losses are avoided or mitigated and where opportunities are identified. The framework should be consistent with the range and complexity of risks with which the organisation must contend.

International Maritime Organisation Risk Environment/Context

The goals of risk management in IMO are:

1. to minimise the cost of risk to IMO, both in financial and non-financial terms
2. to provide an assurance that the organisation has identified its highest risk exposures and has taken steps to properly manage these
3. to ensure that IMO strategic planning processes include a focus on areas where risk management is needed and;
4. to maintain a process across IMO that integrates the various risk control measures in place.

[Insert something about IMO’s service provision, aims and objectives? Or is the coverage below enough? Would welcome comment from the Correspondence Group on this.]

IMO’s risk environment is established by the trends and developments in the shipping industry and the associated challenges facing the organisation, which have been described in the Strategic Plan under eight broad headings (see paper C90/14/Add.1, Annex 3).

a) Globalisation

- Shipping is a major facilitator of global trade and growth in shipping reflects the expansion of global commerce and the free movement of people, goods and information.

- Globalisation has also given rise to new players in the maritime arena, including mega shipping conglomerates and alliances as well as global terminal operators, who wield increasing influence on global trade, maritime transport and shipping at large.

- There is concern that shipping standards may be compromised by the forces of liberalisation and competition in the maritime sector.

- Increased interaction between IMO and other international organisations, industry and special interest groups requires a more proactive, comprehensive and inclusive approach in identifying and responding to trends, incidents and developments in shipping to stave off regional and unilateral tendencies which are in conflict with IMO's regulatory framework.

b) Heightened maritime safety concerns

- Enhancing maritime safety through ensuring each link in the chain of responsibility fully its obligations is a priority.

- Flag, port, and coastal States, shipowners, classification societies and other stakeholders all have an important role to play in collectively implementing, maintaining and raising the standards of shipping.

- Access to information, transparency and an inclusive approach to developing measures for the uniform and effective implementation of IMO instruments are critical success factors.

- IMO needs to enhance technical, operational and safety management standards and to eliminate shipping that fails to meet and maintain those standards at all times.

- IMO also needs to identify and evaluate factors influencing a safety culture and to turn them into practical and effective mechanisms for further developing a quality and safety culture through out the maritime community.

c) Heightened maritime security concerns

- Terrorism has propelled collective action between IMO member States, other intergovernmental and non-governmental organisations to introduce new measures to enhance maritime and port security and to safeguard against interruptions to global trade. The challenge is the effective implementation of the new IMO measures to enhance global maritime security.

- There is also a need to instil a security consciousness in ship and port facility operations and at the same time to ensure the right balance is struck with trade facilitation, ie that new security measures should not unduly affect the efficiency of shipping and port operations in an interconnected world highly dependent on seaborne trade.

d) Heightened environmental consciousness

- There is clearly growing public intolerance to environmental pollution from shipping incidents as experienced from several accidents.

- There is also heightened concern over the impact of global shipping activities on the environment, giving impetus to the protection of aquatic systems and not allowing introduction of harmful substances from ships into the marine environment.

- IMO, in line with the global emphasis on sustainable development, needs to be proactive in identifying and addressing shipping activities that could have an adverse impact on the environment and in developing effective responses to shipping incidents to mitigate the impacts on the environment, should they occur.

e) People at Sea

- IMO's fundamental principle is to protect the lives of all those at sea. The advent of large passenger ships with capacities of several thousand persons, increased use of ferries and high speed craft to provide essential regional and archipelagic links, the growing number of migrants transported by sea and the continuing loss of seafarers' lives at sea have heightened concerns over safety of life at sea and the success of search and rescue operations in the case of distress.

- Concerns include the safe operation of ships and whether current response capabilities to deal with emergencies are adequate.

- IMO needs to ensure that all systems related to ensuring the safety of life at sea are adequate, including dealing with large concentrations of people.

f) Capacity building for universal and uniform application of IMO instruments

- IMO's ITCP is crucial in helping developing countries to implement IMO instruments for safer and more secure shipping and enhanced environmental protection, particularly with every new IMO instrument introduced.

- There are concerns about the capacity of IMO to meet the growing needs of developing countries for technical assistance and in particular the longer term financial sustainability of the ITCP.

- IMO need sot ensure an equitable and sustainable means of funding the ITCP and to improve its delivery and effectiveness.

g) Shifting emphasis onto people

- Human performance in all sections of the maritime industry is a major cause of shipping incidents and will continue to be the focus of IMO efforts to address the problem.

- The effectiveness of IMO instruments will come under scrutiny with each shipping mishap resulting from human error, as the IMO strives for full compliance with the instruments.

- Technological advances affecting the human element offer new opportunities which the IMO can harness to enhance the human element in safer shipping.

- IMO needs to increase its emphasis on the human element in safer and more secure shipping and continuously improve measures to enhance human performance in the maritime industry.

h) Technology as a major driving force

- Technological developments have created new opportunities but may also have negative consequences.

- New opportunities exist for advancing various IMO initiatives from safety to security to environmental protection.

- Development sin communications and information technology provide opportunities for knowledge management to increase transparency and accessibility to information.

- IMO's challenges are to ensure that when adopting new technological developments they enhance maritime safety security and environmental protection, and to ensure the proper application of technology to information management within the organisation and to provide enhanced access to that information by the shipping industry and others.

In addition, the IMO, like many other government agencies and industries, faces continuing cost and financial pressures, and well as continually facing new demands for services from members. It must maintain a flexibility in its structure, methods of work, sources of finance and internal management systems in order to adjust to these pressures.

Risk Management Framework

A risk management framework might contain:

a) a risk management policy that should communicate the potential value and ongoing benefit of risk management to the organisation in context of

its organisational objectives, strategic ambitions and overall management framework. Organisations that effectively implement an enterprise wide approach to managing risk seek to assess and manage all types of risks in a cohesive, consistent and integrated way, avoiding organisational silos. A statement of the risk management policy could contain:

- objectives and rationale for managing risk
- links to strategic and corporate plans
- extent or range of risks to be managed
- guidance on what level of risk is acceptable
- who is responsible for managing risks
- support and expertise available
- documentation required
- requirements for monitoring and review.

For illustrative purposes, an example/suggestion of a starting point for a risk management policy for IMO is at Annex A.

b) a risk management process consisting of:
   - communication and consultation internally and externally with stakeholders
   - review of the context in which the process is to operate, including internal and external environment, objectives and limitations on the risk assessment, criteria to be applied
   - risk identification
   - risk analysis
   - risk evaluation/assessment
   - risk treatment
   - monitoring and review

c) business continuity planning – defining what are IMO's critical services and putting in place a plan and or arrangements to maintain continuity of those services eg IT. Business continuity planning has the aim of reducing the impact of an incident hence the extent of degradation of IMO critical services and functions. This is achieved by implementing appropriate work arounds, minimising the time delay for the recovery of those services and outlining to staff and stakeholders a clear recovery process

d) security planning – in executing its functions and responsibilities IMO needs to ensure it is safeguarded from sources of harm that could weaken, compromise or destroy its ability to undertake its functions. A security plan aims to control risk to IMO's people, assets, resources, information and intellectual property at an acceptable level. It would also provide security assistance, guidance and instructions on security matters including overarching security strategies and operational security needs of IMO.

e) fraud control planning – identifying areas of potential exposure to fraudulent or corrupt practices and developing procedures that aim to eliminate or prevent fraud.

Annex B provides a good depiction of the risk management process.

The risk management framework would be linked to organisational strategic, business and project planning.

Risk Identification

A very good first draft risk identification for IMO was included in C96/5 (b). To develop this risk identification further, will rely on those identifying risks to draw on their experience or the experience of others. Often 'what if' scenarios assist in risk identification. Informal inspections, reviews of incidents or events, reports from staff or external sources and workshops are all sources for identifying organisational risk. While a strong methodology in risk identification and measurement is important, judgements on these matters, while informed, are ultimately subjective. Next steps in risk identification for IMO may be to conduct a workshop to refine/expand the existing list of risks and apply measurement and analysis techniques outlined below.

Measurement /Risk Analysis

When undertaking the risk assessment process, the assessment should relate to the goals, objectives, strategies, scope and parameters of the organisation or activity under review.

There are basically two elements to be considered when reviewing risk.

1. The likelihood of the risk event occurring
2. The consequence or impact should the event occur.

In recognizing the adverse consequences of risk, there is also a natural aversion to risk. Also, as the probability of a loss event moves from remote to impending, it invariably becomes the focus of concern. The concern or risk aversion then, will invariably lead to some efforts to prevent the event or at least minimize its effects, introducing the concept that the events can either be prevented from occurring or that their effects or losses can be minimized.

Risk assessment can be qualitative, quantitative or a combination of both. [*The correspondence group may wish to consider the degree to which this blend might be appropriate to IMO. Some suggestions are made below.*]

Inherent risk

When assessing or measuring risk the process should commence with an assessment of the inherent risk. Inherent exposure can be defined as the maximum financial or other impact of a single instance of a risk incident should one occur in the area under consideration, without taking into account any measures which are already in place to ameliorate that risk.

Outlined below are some suggested options for scoring inherent risk. To determine the inherent risk score an assessment needs to be made of the consequences of the impact of the risk identified occurring.

A basis for making that assessment could be:

Consequences

Option 1

A number between, say 1 and 5 that is determined by combining an exposure measure with a likelihood measure. The table below provides some guidance in determining the maximum financial or other impact of a single instance of risk should one occur in the area under consideration:

	Financial Impact	***Information***	***Political Impact***	***Safety Impact***
1 – Negligible	<£20,000 [1]	Unclassified, routine policy information.	The embarrassment is restricted to within the agency, the public remain unaware	Minor injuries to an individual
2 – Low	Between £20,001 and £1,000,000	In confidence information or personal information.	Public made aware of 'embarrassment' through local media.	Injury of more than a minor nature but expected to be restricted to a single individual.
3 – Medium	Between £1,000,001 and £10,000,000	Confidential information eg Commercial or confidential member state information.	Complaints raised with member state or a political representative of that member state.	Injury to several people
4 – Very High	Between £10,000,001 and £50,000,000	Member state or other UN body information which if provided would have substantial political or security implications for that country.	Widespread adverse publicity reaching national press, radio and television. Questions likely to be raised in member state country or other UN body, possibly in Parliament.	Serious injury to one or more people
5 - Extreme	£50,000,000 or more	Information which if provided to other parties might have extreme security or political implications or other information that would threaten the ongoing operations of the IMO.	Widespread adverse publicity with calls for Secretary General to resign. Some public outcry, civil unrest or strikes likely.	Loss of life(s)

[1] [Members may wish to provide comment on whether these values and other measures are struck at an appropriate level]

In general terms, an extreme exposure is one that would threaten the continuing existence of the Agency.

Option 2

An alternative methodology might be to score inherent risk through identifying the consequences of the impact of the risk occurring as outlined below:

Descriptor	Definition of Consequences	Score
Extreme (E)	Threatens the survival of IMO. UN restructures or closes IMO down	10
High (H)	Threatens the Secretary General/ Senior management. Major restructure sought from Council	5
Moderate (M)	Results in major disruption across IMO. Major diversion of resources	2.5
Low (L)	Results in significant challenge to one business unit of IMO	1
Negligible (N)	Is addressed as part of day to day business	0.4
Absent (A)	Nil consequences/impact	0

Likelihood

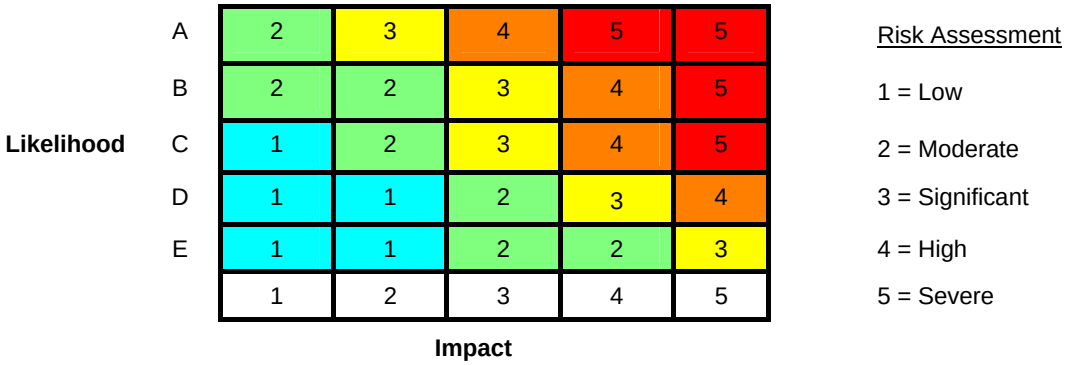
While likelihood and impact are generally considered separately, they are linked. Likelihood can be defined as 'without specific controls within IMO to prevent, detect or correct the action, how frequently would the risk occur in the operation under consideration.'

Option 1

Without specific controls within IMO to prevent, detect or correct the risk, how frequently would the risk event occur in the operation under consideration?

Risk event would be:
A – Almost Certain
B – Likely
C – Moderate
D – Unlikely
E – Rare

Using the first methodology suggested above, thus if you combine the impact and the likelihood as indicated in the table, this will obtain an inherent risk score:



Option 2

The assessment of likelihood and impact can be either quantifiable or semi-quantifiable. A fully quantifiable method should provide more accurate outcomes but is likely to be more difficult to use. Quantifiable measures are those that use direct attribution of numerical values to frequency or likelihood and consequence.

Frequency is measured in terms of the expected number of times the scenario is likely to occur in the period under review. If the period is a year and the event is likely to occur once a month, the frequency would be 12. Under this form of measurement, a likelihood of .01 (once in ten years) is usually used as the lowest measure.

Likelihood is measured in terms of probability of the event occurring in the period under review on a scale from 0 to 1, with 0 being impossible and 1 being certain to occur.

Likelihood	Score
Extreme (E)	0.95
High (H)	0.6
Moderate (M)	0.4
Low (L)	0.2
Negligible (N)	0.1
Absent (A)	0

Consequence is measured in terms of the actual expected outcome each time the scenario occurs. This is recorded in the same units as the measures applied to the objective. Thus if the objective is financial in nature the impact would be the expected financial cost arising from the occurrence of the scenario, based on the experience of the participants.

Likelihood \ Consequence	0.4	1	2.5	5	10
0.95	0.38	0.95	2.375	4.75	9.5
0.6	0.24	0.6	1.5	3	6
0.4	0.16	0.4	1	2	4
0.2	0.08	0.2	0.5	1	2
0.1	0.04	0.1	0.25	0.5	1

Risk Value		
	Extreme	3 or more
	High	1 to 3
	Moderate	.3 to 1
	Low	.1 to .3
	Negligible	Below .1

Semi quantifiable measures are those that use non-quantified terms to express likelihood and impact and then ascribe a suitable value to the term. “Extreme, High, Medium, Low and Negligible” are commonly used terms.

Likelihood values are usually described in terms of probability. “Extreme” could represent 95% certainty of occurrence and “Negligible” could represent 1% potential for the event to occur. The other terms could then be distributed between these two values. The distribution may be evenly spread or may be skewed to reflect the experience of the participants.

Consequence values can be described in a simple table of equivalents based on the units of measure ascribed to the objective. For example, if the objective is financial, each term could be given a fixed dollar value. Alternatively, the values for terms can be described by reference to the tolerance for the objective. “Extreme” could represent 50% of the tolerance for the objective, “High” could represent 25%, “Medium” 12%, “Low” 6% and “Negligible” 1%.

Once inherent risk has been established, an assessment of controls which are in place needs to be undertaken.

Controls

Controls are measures, systems or actions in place that would prevent, detect and correct any occurrence of the risk identified. The assessment is of the likelihood that the control system will prevent, detect and correct any risk occurrence.

Option 1

Prevention or detection & correction would be:
5 – Almost Certain
4 – Likely
3 – Moderate
2 – Unlikely
1 – Rare
0 – Control Systems not known

Alternatively, controls could be measured by describing the control measure and assessing its adequacy:

Option 2

Descriptor	Definition
Adequate	Reasonable controls are in place to manage the risk
Less than Adequate	Controls that are in place will only partly manage the risk. Further controls need to be developed to control the risk adequately.
Inadequate	There are no controls, or the controls in place will not manage the risk.

Residual Risk

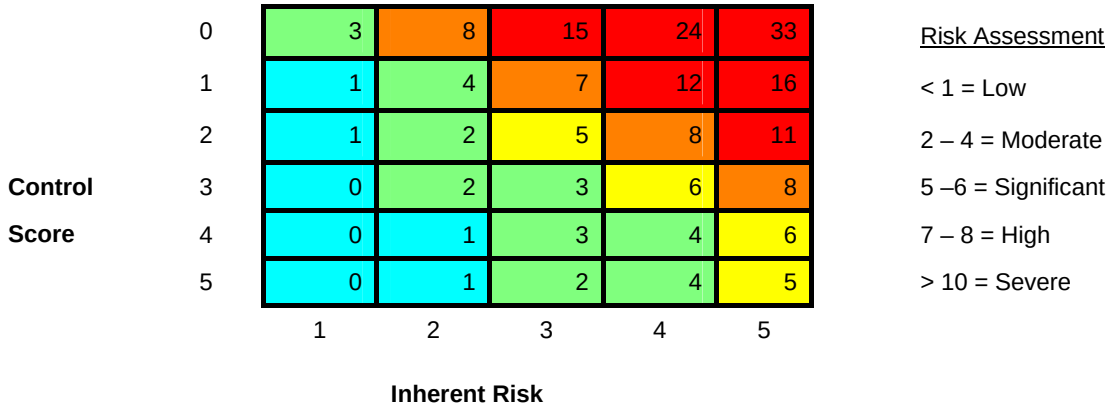
Finally, residual risk can be measured.

Option 1

The residual risk score is a calculated value between 0 and 33. It is calculated as:

$$RR = \frac{3xIRx\sqrt{IR}}{(IC+1)}$$

This provides a weighted scale in which inherent risk carries more weight than control systems. The residual risk score is determined as follows:



Based on this scale, residual risk scores of 10 or above require immediate attention. Scores of 5 or more indicate areas where risk treatment action might be useful.

Option 2

Residual risk is the risk that remains after consideration of the effect of existing controls. This model is well suited to both a single event analysis or a more complex undertaking which incorporates organisational objectives and allows to set risk tolerances at that level. The spreadsheet performs the calculations to multiply the likelihood by the expected impact for each scenario for each objective to produce the expected outcome of each risk for each objective.

The outcomes are summed for each objective to provide a total risk level for the objective and ultimately the organisation. Risk ranking is also possible with this model. They can also be normalised against one selected measure and summed across objectives for each scenario then the total summed to provide an overall risk level.

The total (summed) risks for each objective can then be compared with the risk tolerance for each objective to see whether the objective is under threat. Risks can also be sorted by the value of the expected outcome for each objective and for the overall value to arrive at the top risks for each objective and for all objectives. Other analysis can be done to determine where the risks lie in terms of the organisation, accountability, level of control and what is driving them. A copy of a typical spreadsheet used to manage the risk data is at Annex C. When completed, this forms the Risk Register.

Option 3

An alternative, purely qualitative assessment model using a non numerical value set which might be considered is outlined below. Note that this form of assessment restricts quantitative risk ranking and should IMO wish to combine with strategic planning, it can only focus on one objective/or strategy at a time, whereas Option 2 has the potential to measure risks against IMO strategic objectives.

	Consequences

Likelihood	N	L	M	H	E
E	Moderate	Moderate	High	Extreme	Extreme
H	Low	Moderate	High	Extreme	Extreme
M	Low	Moderate	High	High	Extreme
L	Negligible	Low	Moderate	High	High
N	Negligible	Low	Low	Moderate	High

Extreme Risk:	Immediate action required
High risk:	Senior management attention needed
Moderate Risk:	Management responsibility must be specified
Low Risk:	Manage by routine procedures, monitor
Negligible Risk:	Nuisance.

Risk Treatment

Based on the assessment outlined above, a decision needs to be taken on which risks need to be addressed, by whom, defining responses to be used and in what priority.

Risk treatment consists basically of four techniques:

1. *Risk Avoidance* - the technique of avoiding the activity that creates the risk. For example the risk created by persons travelling by helicopter can be avoided by not following this activity. It is a technique, which should always be explored, but will rarely provide a practical approach.
2. *Risk Control* - the technique applied to either removing or reducing the risk using a variety of techniques. Can the risk be eliminated? Can the risk be substituted by one that does not present a risk? Can the risk be contained so that control is maintained? Can the damage or loss be made minor or inconsequential should the risk eventuate? Can the risk be kept separate from the item most prone to damage. This is the technique, which has most to offer in reducing the level of risk.
3. *Risk retention and Risk Financing* - the technique of reducing the impact of losses, but does nothing to reduce the likelihood of the loss event. It consists of assigning organisational funds to cover all or part of losses using a variety of techniques and is an insurance related activity.
4. *Risk Transfer* is the activity of transferring all or part of the risk of loss to a third party for a financial consideration or premium. This may be via insurance and also includes contractual arrangements where the counter party indemnifies the organisation against liability in specified circumstances.

A risk response initiative should be prepared that address individual risks or groups of risks. These indicate who is responsible for the project, what controls are in place, what actions are to occur, who is to take the individual action and what is the timetable. A copy of a typical template for a risk response initiative is at Annex D.

Monitoring and Review

It is essential that, having established the risk treatment technique to be applied, a system of regular monitoring is implemented to ensure the treatment

is continuously applied and effective. This generally consists of monitoring loss events to ensure they are contained within acceptable limits. However, this has a basic flaw in that losses have to be incurred in order for the failure in the control mechanisms to be detected. Therefore, the risk treatment arrangements should be periodically audited to ensure they are still in place, effectively controlling or minimising the risk. Where defects are located, they need to be rectified to restore control.

The response reports should be reviewed at least annually recording the following:

1. Developments - what has gone on since the last update
2. Current status - what is the current status of each project
3. New risks - what new risks/ issues have arisen since the last review, and what risks previously identified warrant treatment now
4. New responses - what projects are to be developed to address the currently identified risks
5. Effect on the risk register - what is the effect of all these actions on the risk register (spreadsheet or other measure)
6. Opportunities - what opportunities are seen in the course of this review.

[Once IMO's initial risk management plan, including endorsement of risks identified, risk responses and priority are agreed, a report should be regularly provided to Council. Reporting formats could be established by the working group in conjunction with the Secretariat, but any initial comment from the Correspondence Group are welcome, including the role of IMO Committees in this process.]

Annex A

Example/illustration of a risk management policy appropriate to IMO

Objectives and rationale for managing risk

The International Maritime Organisation (IMO) has a commitment to minimising losses emanating from foreseeable risks.

IMO will foster and promote a risk management culture at all levels within the organisation.

IMO will be proactive in identifying areas of potential risk and establishing appropriate treatment. {if appropriate, consistent with the requirements of [cite an appropriate UK, UN or international standard or reference]}

All IMO staff are responsible for identifying, assessing and treating risks as part of their day-to-day duties.

IMO will adopt a uniform risk management approach to identifying risks and their drivers, and planning for management of risks will be reflected in business plans and the IMO strategic plan.

Risk identification and risk evaluation will be linked to practical and cost effective risk control measures commensurate with IMO operations.

IMO will be proactive in its monitoring and responses to risk to reduce the impact and possibility and impact of accidents and losses, whether caused by IMO or externally.

IMO will seek to:

- Minimize the cost of risk to IMO, both in financial and non-financial terms
- Provide an assurance that the organisation has identified its highest-risk exposures and has taken steps to properly manage these.

Links to strategic and corporate plans

See text under International Maritime Organisation Risk Environment/Context
This could be supplemented with chart from Australia's first paper co-sponsored by Netherlands, Canada etc?

Extent or range of risks to be managed

Would be content included in IMO risk register.

Guidance on what level of risk is acceptable

Could include definition of risk tolerances by strategic plan broad headings. Otherwise a general statement should be included following workshop with IMO management and consideration by Council.

Who is responsible for managing risks

In conjunction with the Secretary General, the IMO Council is responsible for setting strategic direction for IMO. The Secretary General is responsible for whole of business risk management. IMO Council is responsible for oversight of IMO's risk management program, its implementation, agreeing risk tolerances and treatment plans and regular monitoring. [Would welcome Correspondence Group comment on the role IMO Committees might play here].

The Secretary General has responsibility for ensuring that the risk management policy and plan is effectively implemented within IMO and its principles communicated at all levels in the organization. The Secretary General will provide the necessary profile to advance a risk management culture in IMO, including participation in its monitoring and reporting.

IMO's senior management team is responsible for ensuring that business units regularly review and update their risk registers and treatment plans.

Business unit managers are accountable for ensuring that high-level risks are managed appropriately through a business unit risk management program and included on a business unit risk register. The Business unit manager is responsible for overseeing the business unit risk management program and endorsing risk mitigation strategies and action plans as outlined in the risk response of each business unit.

All line and project managers are responsible for managing risk within their span of control, for promoting the application of risk management by contractors, and assisting with the identification of global or broadly based risks that could impact on IMO as a whole.

The [name the manager/person] who might be responsible to the senior management group for:

- Coordinating business units' activities to review and update their risk registers and treatment plans;
- Maintaining organisation wide risk and risk control information;
- Promoting and facilitating risk management within IMO.

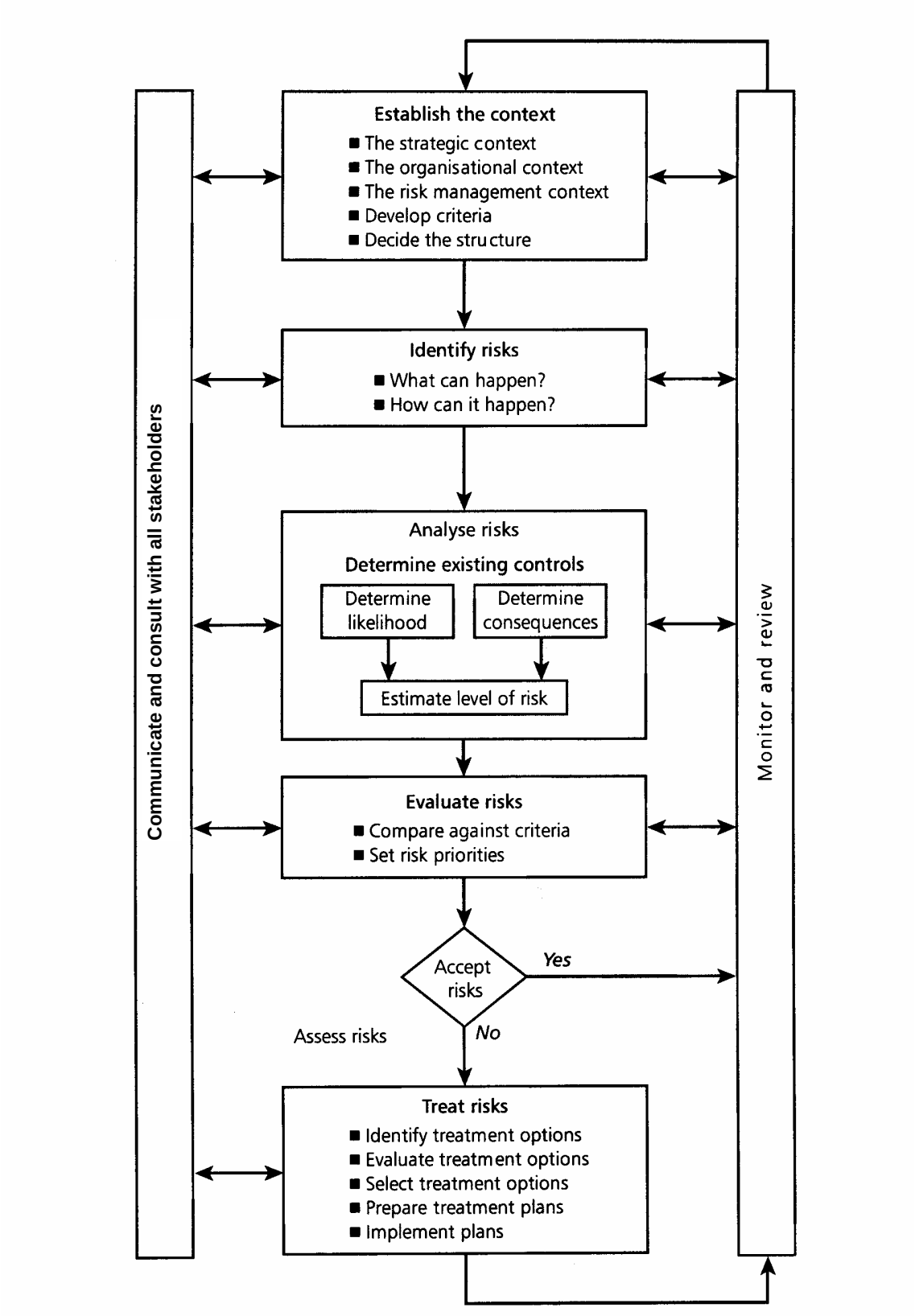
Documentation required

Would include final text of measurement/assessment methodology and other final proformas for risk response plans etc.

Requirements for monitoring and review

Would include final text agreed with regard to monitoring and review discussed above.

Risk Management Process Annex B



Annex C

Typical Risk Spreadsheet/ Risk Register

Key Objectives												
Key performance Indicator												
Average Past Performance												
New Set Target												
Minimum acceptable level												
Tolerance												
Variance Ratio												
WBS-No	Term S/L	Process	Risk No	Risk scenario	Accountability	Potential damage from risk	Existing or planned Process and Controls (Description)	Adequacy of controls (Adequate, Less than Adequate, Inadequate)	Likelihood or Frequency per Year (A)	Expected impact per incident (B)	Risk Level (C) . (=A x B)	Expecte impact pe incident (F
0.0	.											
1.0												
2.0												
3.0												
4.0												

Risk Response Initiative Template Annex D

Risk response initiative No…

NNNNN

OVERALL RESPONSIBILITY			
DESCRIPTION:		SCOPE	
General description of the project		Addresses risks: k No …(Description)	
Project Manager		Deliverable	
CURRENT CONTROLS STATUS			
1			
2			
ACTIONS PLANNED			

Action		Due Date	Output	Resp	Status as at (date)
1					
2					
3					
4					
5					
6					

APPENDIX 2

Treasury Board of Canada Integrated Risk Management Framework

Integrated Risk Management Framework

Cat. No. BT22-78/2001
ISBN 0-662-65673-3

This document is available in alternative formats
and on the TBSWeb site at the following address:
http://www.tbs-sct.gc.ca

President's Message

In March 2000, I had the pleasure of tabling the Government of Canada's new management framework, entitled *Results for Canadians*. It outlines how we are modernizing management practices in order to make the Government of Canada more citizen-focused and better prepared to meet Canadians' changing needs and priorities. This *Integrated Risk Management Framework* is an essential part of these modernization efforts.

In an increasingly complex public policy environment, it is important that Public Service employees are encouraged to approach their work with creativity and a desire to innovate. At the same time, however, we must recognize and respect the need to be prudent in protecting the public interest and maintaining public trust. Achieving this balance is what this *Integrated Risk Management Framework* is all about.

This framework is a practical guide to assist public service employees in their decision-making. At the organizational level, it will help departments and agencies to think more strategically and improve their ability to set common priorities. At the individual level, it will help all employees to develop new skills and will strengthen their ability to anticipate, assess and manage risk.

I invite you to read the framework and make use of the concepts, guidelines and examples that relate to your particular needs. I am confident that this framework will lead to the adoption of a more holistic approach to risk management and foster a working environment which supports employees in pursuing new and innovative ways to better serve Canadians.

The paper version was signed by

Lucienne Robillard

President of the Treasury Board

Table of Contents

Introduction

The Integrated Risk Management Framework delivers on the commitment set out in *Results for Canadians—A Management Framework for the Government of Canada* (March 2000) to strengthen risk management practices within the Public Service. In doing so, the Integrated Risk Management Framework supports the four management commitments outlined in *Results for Canadians*: citizen focus, values, results and responsible spending. The Integrated Risk Management Framework advances a citizen focus by strengthening decision-making in the public interest and placing more emphasis on consultation and communication. Similarly, it respects core public service values such as honesty, integrity and probity at all levels, and contributes to improved results by managing risk proactively. Integrated risk management also supports a whole-of-government view grounded in rational priority setting and principles of responsible spending.

The need for more affordable and effective government combined with trends towards revitalizing human resources capacity and redesigning service delivery are dramatically affecting the structure and culture of public organizations. The faster pace and need for innovation, combined with significant risk-based events from computer failures to natural disasters, has focused attention on risk management as essential in sound decision-making and accountability.

Responding to the need to strengthen risk management as a priority on the government management agenda, the Treasury Boardof Canada Secretariat (the Secretariat) led research and consultations on risk management in collaboration with federal organizations, academics and private interests. The results highlighted the need for a common understanding of risk management and a more corporate, systematic approach. Informed by knowledge and experience from the public and private sectors in Canada and internationally, the Secretariat and its partners collaborated on the development of an Integrated Risk Management Framework.

This Framework is designed to advance the development and implementation of modern management practices and to support innovation throughout the federal Public Service. It provides a comprehensive approach to better integrate risk management into strategic decision-making.

The Framework provides an organization with a mechanism to develop an overall approach to manage strategic risks by creating the means to discuss, compare and evaluate substantially different risks on the same page. It applies to an entire organization and covers all types of risks faced by that organization (e.g., policy, operational, human resources, financial, legal, health and safety, environment, reputational).

The purpose of the Integrated Risk Management Framework is to:

- provide guidance to advance the use of a more corporate and systematic approach to risk management;
- contribute to building a risk-smart workforce and environment that allows for innovation and responsible risk-taking while ensuring legitimate precautions are taken to protect the public interest, maintain public trust, and ensure due diligence; and

- propose a set of risk management practices that departments can adopt, or adapt, to their specific circumstances and mandate.

Application of the Framework is designed to strengthen management practices, decision-making and priority setting to better respond to citizens' needs. Moreover, practising integrated risk management is expected to support the desired cultural shift to a risk-smart workforce and environment. More specifically, it is anticipated that implementation of the Framework will:

- **support the government's governance responsibilities** by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavourable impacts and to benefit from opportunities;

- **improve results** through more informed decision-making, by ensuring that values, competencies, tools and a supportive environment form the foundation for innovation and responsible risk-taking, and by encouraging learning from experience while respecting parliamentary controls;

- **strengthen accountability** by demonstrating that levels of risk associated with policies, plans, programs and operations are explicitly understood, and that investment in risk management measures and stakeholder interests are optimally balanced; and

- **enhance stewardship** by strengthening public service capacity to safeguard people, government property and interests.

Integrated risk management respects and builds on core public service values. Outcomes of applied integrated risk management must be ethical, honest and fair; respect laws, government authorities and departmental policies; and result in prudent use of resources.

The Integrated Risk Management Framework responds to the recommendations contained in the *Report of the Independent Review Panel on Modernization of Comptrollership in the Government of Canada* (1997), which were approved by Treasury Board ministers. The report highlights a new guiding philosophy for comptrollership. This new philosophy combines a strong commitment to four key elements: performance reporting (financial and non-financial); sound risk management; the application of an appropriate system of control and reporting; and values and ethics. In identifying as a priority the strengthening of risk management across the Public Service, the report stressed the need for:

- "… executives and employees [to be] risk attuned—not only identifying but also managing risks …";

- "… matching more creative and client-driven decision making and business approaches with solid risk management…"; and

- "… creating an environment in which taking risks and the consequences of doing so are handled within a mature framework of delegation, rewards and sanctions."

The Framework builds on existing risk management practices, reflects current thinking, best practices and the value of well-recognized principles for risk management. It is linked with other federal risk management initiatives across government, including recent efforts to strengthen internal audit and increase focus on monitoring. Risk management frameworks are also being developed in areas such as legal risk management and the precautionary approach. In addition, the Integrated Risk Management Framework complements the concepts and approach described in the Privy Council Office report—*Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management* (2000). Collectively, these individual initiatives are contributing to strengthening risk management across the federal government in line with modern comptrollership and to improving practices in managing risk from a whole-of-government perspective.

Management Challenges

In today's world, change and uncertainty are constants. With increased demand by parliamentarians for greater transparency in decision-making, better educated and discerning citizens, globalization, technological advances, and numerous other factors, adapting to change and uncertainty while striving for operating efficiency is a fundamental part of the Public Service. Such an environment requires a stronger focus on integrated risk management practices within organizations in order to strategically deal with uncertainty, capitalize upon opportunities, and inform and increase involvement of stakeholders (including parliamentarians), to ensure better decisions in the future.

The challenge for the Public Service of Canada is to approach risk management in a more integrated and systematic way that includes greater emphasis on consultation and communication with stakeholders and the public at large. In meeting this challenge, the Public Service can fulfil its increased responsibility to demonstrate sound decision-making, in line with increasing expectations of due diligence, more intense public and media scrutiny, and initiatives for transparency and open government. Risk management is now seen as an organization-wide issue that, as one of several co-ordinated initiatives, will improve decision-making, enabling the shift to results-based management. Integrated risk management requires looking across all aspects of an organization to better manage risk. Organizations that manage risk organization-wide have a greater likelihood of achieving their objectives and desired results. Effective risk management minimizes losses and negative outcomes and identifies opportunities to improve services to stakeholders and the public at large.

A systematic, integrated but adaptable approach to risk management requires an organization to build capacity to address risk explicitly, to increase the organization's and stakeholders' confidence in its ability to achieve its goals. It contributes to better use of time and resources, improved teamwork and strengthened trust through sharing analyses and actions with partners. In emphasizing the need for more active and frequent consultation and risk communication, an integrated approach to risk management leads to shared responsibility for managing risk. It also increases confidence in the organization's process, and improves public and stakeholder understanding of trade-offs.

Developing a Risk-Smart Workforce and Environment

Application of the Integrated Risk Management Framework, in conjunction with related risk management activities, will support a cultural shift to a risk-smart workforce and environment in the Public Service. Such an environment is one that supports responsible risk management, where risk management is built into existing governance and organizational structures, and planning and operational processes. An essential element of a risk-smart environment is to ensure that the workplace has the capacity and tools to be innovative while recognizing and respecting the need to be prudent in protecting the public interest and maintaining public trust.

Departments whose core mandate focuses directly on public health and safety have traditionally been very proactive in practising systematic risk management. These departments have a long history of addressing the public's low risk tolerance in the areas of health and safety and have, as a result, developed an effective risk management culture. The emerging trends in the public sector environment and challenges associated with the need to adapt to change and uncertainty are contributing to the increased interest in risk management in other public policy areas. This higher level of awareness around risk management and the need to better understand and manage different types of risks in addition to health and safety risks requires a cultural shift. The aim of this cultural shift is to develop a risk-smart workforce throughout the Public Service by ensuring that public servants at all levels are more risk aware and risk attentive, that mitigation measures are proportionate to the issue at hand, and that the necessary tools and processes are in place to support them.

Achieving this cultural change will require sustained commitment throughout the Public Service over a number of years as practices evolve.

Key Concepts

There are three critical concepts that are cornerstones of the Integrated Risk Management Framework: risk, risk management and integrated risk management. These concepts are elaborated on below.

Risk

Risk is unavoidable and present in virtually every human situation. It is present in our daily lives, public and private sector organizations. Depending on the context, there are many accepted definitions of risk[1] in use.

The common concept in all definitions is uncertainty of outcomes. Where they differ is in how they characterize outcomes. Some describe risk as having only adverse consequences, while others are neutral.

While this Framework recognizes the importance of the negative connotation of outcomes associated with the description of risk (i.e., risk is adverse), it is acknowledged that definitions are evolving. Indeed, there is considerable debate and discussion on what would be an acceptable generic definition of risk that would recognize the fact that, when assessed and managed properly, risk can lead to innovation and opportunity. This situation appears more prevalent when dealing

with operational risks and in the context of technological risks. For example, Government On-Line (GOL) represents an opportunity to significantly increase the efficiency of public access to government services. It is acknowledged in advance that the benefits of pursuing GOL would outweigh, in the long term, potential negative outcomes, which are foreseen to be manageable.

To date, no consensus has emerged, but after much research and discussion, the following description of risk has been developed for the federal Public Service in the context of the Integrated Risk Management Framework:

> **Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.**

The phrase "the expression of the likelihood and impact of an event" implies that, as a minimum, some form of quantitative or qualitative analysis is required for making decisions concerning major risks or threats to the achievement of an organization's objectives. For each risk, two calculations are required: its likelihood or probability; and the extent of the impact or consequences.

Finally, it is recognized that for some organizations, risk management is applied to issues predetermined to result in adverse or unwanted consequences. For these organizations, the definition of risk in the Privy Council Office report[2], which refers to risk as "a function of the probability (chance, likelihood) of an adverse or unwanted event, and the severity or magnitude of the consequences of that event" will be more relevant to their particular public decision-making contexts. Although this definition of risk refers to the negative impact of the issue, the report acknowledges that there are also positive opportunities arising from responsible risk-taking, and that innovation and risk co-exist frequently.

Risk Management

Risk management is not new in the federal public sector. It is an integral component of good management and decision-making at all levels. All departments manage risk continuously whether they realize it or not—sometimes more rigorously and systematically, sometimes less so. More rigorous risk management occurs most visibly in departments whose core mandate is to protect the environment and public health and safety.

As with the definition of risk, there are equally many accepted definitions of risk management in use. Some describe risk management as the decision-making process, excluding the identification and assessment of risk, whereas others describe risk management as the complete process, including risk identification, assessment and decisions around risk issues. For example, the Privy Council Office's report refers to risk management as "the process for dealing with uncertainty within a public policy environment."[3]

For the purposes of the Integrated Risk Management Framework:

Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.

In order to apply risk management effectively, it is vital that a risk management culture be developed. The risk management culture supports the overall vision, mission and objectives of an organization. Limits and boundaries are established and communicated concerning what are acceptable risk practices and outcomes.

Since risk management is directed at uncertainty related to future events and outcomes, it is implied that all planning exercises encompass some form of risk management. There is also a clear implication that risk management is everyone's business, since people at all levels can provide some insight into the nature, likelihood and impacts of risk.

Risk management is about making decisions that contribute to the achievement of an organization's objectives by applying it both at the individual activity level and in functional areas. It assists with decisions such as the reconciliation of science-based evidence and other factors; costs with benefits and expectations in investing limited public resources; and the governance and control structures needed to support due diligence, responsible risk-taking, innovation and accountability.

Integrated Risk Management

The current operating environment is demanding a more integrated risk management approach. It is no longer sufficient to manage risk at the individual activity level or in functional silos. Organizations around the world are benefiting from a more comprehensive approach to dealing with all their risks.

Today, organizations are faced with many different types of risk (e.g., policy, program, operational, project, financial, human resources, technological, health, safety, political). Risks that present themselves on a number of fronts as well as high level, high-impact risks demand a co-ordinated, systematic corporate response.

Integrated Risk Management

"Whatever name they put on it—business … holistic … strategic … enterprise—leading organizations around the world are breaking out of the 'silo mentality' and taking a comprehensive approach to dealing with all the risks they face."

—Tillinghast – Towers Perrin

For the purposes of the Integrated Risk Management Framework:

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

Integrated risk management requires an ongoing assessment of potential risks for an organization at every level and then aggregating the results at the corporate level to facilitate priority setting and improved decision-making. Integrated risk management should become embedded in the organization's corporate strategy and shape the organization's risk management culture. The identification, assessment and management of risk across an organization helps reveal the importance of the whole, the sum of the risks and the interdependence of the parts.

Integrated risk management does not focus only on the minimization or mitigation of risks, but also supports activities that foster innovation, so that the greatest returns can be achieved with acceptable results, costs and risks. Integrated risk management strives for the optimal balance at the corporate level.

The Government of Canada has already used an integrated risk management approach to manage risk related to Y2K and is currently applying the approach to other major initiatives such as Government On-Line and Program Integrity.

An Integrated Risk Management Framework

The Integrated Risk Management Framework provides guidance to adopt a more holistic approach to managing risk. The application of the Framework is expected to enable employees and organizations to better understand the nature of risk, and to manage it more systematically.

Four Elements and Their Expected Results

The Integrated Risk Management Framework is comprised of four related elements. The elements, and a synopsis of the expected results for each, are presented below. Further details on the conceptual and functional aspects of the Framework are provided in subsequent sections of this document.

Element 1: Developing the Corporate Risk Profile

- the organization's risks are identified through environmental scanning;
- current status of risk management within the organization is assessed; and
- the organization's risk profile is identified.

Element 2: Establishing an Integrated Risk Management Function

- management direction on risk management is communicated, understood and applied;

- approach to operationalize integrated risk management is implemented through existing decision-making and reporting structures; and
- capacity is built through development of learning plans and tools.

Element 3: 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; and
- consultation and communication with stakeholders is ongoing.

Element 4: 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; and
- experience and best practices are shared, internally and across government.

The four elements of the Integrated Risk Management Framework are presented as they might be applied: looking outward and across the organization as well as at individual activities. This comprehensive approach to managing risk is intended to establish the relationship between the organization and its operating environment, revealing the interdependencies of individual activities and the horizontal linkages.

While it is acknowledged that some departments are more advanced than others in moving towards the implementation of an integrated risk management approach, there is growing appreciation across the Public Service of the need to strengthen risk management practices and develop a more strategic and corporate-wide focus. Implementing integrated risk management will depend largely on an organization's state of readiness, overall priorities and the level of effort necessary to implement the various elements. As a result, developing a more mature risk management environment will require sustained commitment and will evolve over time. This Framework is a step in establishing the foundation for integrated risk management in the public sector. It is acknowledged that to support and facilitate implementation, the development of specific tools and guidelines as well as sharing of best practices and lessons learned will be required.

Element 1: Developing the Corporate Risk Profile

A broad understanding of the operating environment is an important first step in developing the corporate risk profile. Developing the risk profile at the corporate level is intended to examine both threats and opportunities in the context of an organization's mandate, objectives and available resources.

In building the corporate risk profile, information and knowledge at both the corporate and operational levels is collected to assist departments in understanding the range of risks they face, both internally and externally, their likelihood and their potential impacts. In addition, identifying and assessing the existing departmental risk management capacity and capability is another critical component of developing the corporate risk profile.

An organization can expect three key outcomes as a result of developing the corporate risk profile:

- *Threats and* opportunities *are identified through ongoing internal and external environmental scans, analysis and adjustment.*

- *Current status of risk management within the organization is assessed—challenges/*opportunities*, capacity, practices, culture— and recognized in planning organization-wide management of risk strategies.*

- *The organization's risk profile is identified—key risk areas, risk tolerance, ability and capacity to mitigate, learning needs.*

External and Internal Environment

Through the environmental scan, key external and internal factors and risks influencing an organization's policy and management agenda are identified. Identifying major trends and their variation over time is particularly relevant in providing potential early warnings. Some external factors to be considered for potential risks include:

- **Political:** the influence of international governments and other governing bodies;

- **Economic:** international and national markets, globalization;

- **Social:** major demographic and social trends, level of citizen engagement; and

- **Technological:** new technologies.

Internally, the following factors are considered relevant to the development of an organization's risk profile: the overall management framework; governance and accountability structures; values and ethics; operational work environment; individual and corporate risk management culture and tolerances; existing risk management expertise and practices; human resources capacity; level of transparency required; and local and corporate policies, procedures and processes.

The environmental scan increases the organization's awareness of the key characteristics and attributes of the risks it faces. These include:

- **type of risk:** technological, financial, human resources (capacity, intellectual property), health, safety;

- **source of risk:** external (political, economic, natural disasters); internal (reputation, security, knowledge management, information for decision making);

- **what is at risk:** area of impact/type of exposure (people, reputation, program results, materiel, real property); and

- **level of ability to control the risk:** high (operational); moderate (reputation); low (natural disasters).

An organization's risk profile identifies key risk areas that cut across the organization (functions, programs, systems) as well as individual events, activities or projects that could significantly influence the overall management priorities, performance, and realization of organizational objectives.

The environmental scan assists the department in establishing a strategic direction for managing risk, making appropriate adjustments in decisions and actions. It is an ongoing process that reinforces existing management practices and supports the attainment of overall management excellence.

Assessing Current Risk Management Capacity

In assessing internal risk management capacity, the mandate, governance and decision-making structures, planning processes, infrastructure, and human and financial resources are examined from the perspective of risk. The assessment requires an examination of the prevailing risk management culture, risk management processes and practices to determine if adjustments are necessary to deal with the evolving risk environment.

Furthermore, the following factors are considered key in assessing an organization's current risk management capacity: individual factors (knowledge, skills, experience, risk tolerance, propensity to take risk); group factors (the impact of individual risk tolerances and willingness to manage risk); organizational factors (strategic direction, stated or implied risk tolerance); as well as external factors (elements that affect particular risk decisions or how risk is managed in general).

Risk Tolerance

An awareness and understanding of the current risk tolerances of various stakeholders is a key ingredient in establishing the corporate risk profile. The environmental scan will identify stakeholders affected by an organization's decisions and actions, and their degree of comfort with various levels of risk. Understanding the current state of risk tolerance of citizens, parliamentarians, interest groups, suppliers, as well as other government departments will assist in developing a risk profile and making decisions on what risks must be managed, how, and to what extent. It will also help identify the challenges associated with risk consultations and communication.

In the Public Service, citizens' needs and expectations are paramount. For example, most citizens would likely have a low risk tolerance for public health and safety issues (injuries, fatalities), or the loss of Canada's international reputation. Other risk tolerances for issues such as project delays and slower service delivery may be less obvious and may require more consultation.

In general, there is lower risk tolerance for the unknown, where impacts are new, unobservable or delayed. There are higher risk tolerances where people feel more in control (for example, there is usually a higher risk tolerance for automobile travel than for air travel).

Risk tolerance can be determined through consultation with affected parties, or by assessing stakeholders' response or reaction to varying levels of risk exposure. Risk tolerances may change over time as new information and outcomes become available, as societal expectations evolve and as a result of stakeholder engagement on trade-offs. Before developing management strategies, a common approach to the assessment of risk tolerance needs to be understood organization-wide.

Determining and communicating an organization's own risk tolerance is also an essential part of managing risk. This process identifies areas where minimal levels of risk are permissible, as well as those that should be managed to higher, yet reasonable levels of risk.

Element 2: Establishing an Integrated Risk Management Function

Establishing an integrated risk management function means setting up the corporate "infrastructure" for risk management that is designed to enhance understanding and communication of risk issues internally, to provide clear direction and demonstrate senior management support. The corporate risk profile provides the necessary input to establish corporate risk management objectives and strategies. To be effective, risk management needs to be aligned with an organization's overall objectives, corporate focus, strategic direction, operating practices and internal culture. In order to ensure risk management is a consideration in priority setting and revenue allocation, it needs to be integrated within existing governance and decision-making structures at the operational and strategic levels.

To ensure that risk management is integrated in a rational, systematic and proactive manner, an organization should seek to achieve three related outcomes:

- *Management direction on risk management is communicated, understood and applied—vision, policies, operating principles.*
- *Approach to operationalize integrated risk management is implemented through existing decision-making structures: governance, clear roles and responsibilities, and performance reporting.*
- *Building capacity—learning plans* and *tools are developed for use throughout the organization.*

Strategic Risk Management Direction

The establishment and communication of the organization's risk management vision, objectives and operating principles are vital to providing overall direction, and ensure the successful integration of the risk management function into the organization. Using these instruments can reinforce the notion that risk management is everyone's business.

It is essential that management provides a clear statement of its commitment to risk management and determines the best way to implement risk management in its organization. This includes establishing a corporate focus and communicating internal parameters, priorities, and practices for the implementation of risk management. To reinforce the corporate focus on risk management, organizations may dedicate a small number of resources to provide both advisory and challenge functions, and to specifically integrate these responsibilities into an existing unit (for example, Corporate Planning and Policy, Comptrollership Secretariat, Internal Audit).

In establishing the strategic risk management direction, internal and external concerns, perceptions and risk tolerances are taken into account. It is also imperative to identify acceptable risk tolerance levels so those unfavourable outcomes can be remedied promptly and effectively. Clear communication of the organization's strategic direction will help foster the creation and promotion of a supportive corporate risk management culture.

Objectives and strategies for risk management are designed to complement the organization's existing vision and goals. In establishing an overall risk management direction, a clear vision for risk management is articulated and supported by policies and operating principles. The policy would guide employees by describing the risk management process, establishing roles and responsibilities, providing methods for managing risk, as well as providing for the evaluation of both the objectives and results of risk management practices.

Integrating Risk Management into Decision Making

Effective risk management cannot be practised in isolation, but needs to be built into existing decision-making structures and processes. As risk management is an essential component of good management, integrating the risk management function into existing strategic management and operational processes will ensure that risk management is an integral part of day-to-day activities. In addition, organizations can capitalize on existing capacity and capabilities (e.g., communications, committee structures, existing roles and responsibilities, etc.)

While each organization will find its own way to integrate risk management into existing decision-making structures, the following are factors that may be considered:

- aligning risk management with objectives at all levels of the organization;
- introducing risk management components into existing strategic planning and operational processes;
- communicating corporate directions on acceptable level of risk; and

- improving control and accountability systems and processes to take into account risk management and results.

The integration of risk management into decision-making is supported by a corporate philosophy and culture that encourages everyone to manage risks. This can be accomplished in a number of ways, such as:

- seeking excellence in management practices, including risk management;
- having senior managers champion risk management;
- encouraging innovation, while providing guidance and assistance in situations that do not turn out favourably;
- encouraging managers to develop knowledge and skills in risk management;
- including risk management as part of employees' performance appraisals;
- introducing incentives and rewards; and
- recruiting on risk management ability as well as experience.

Reporting on Performance

The development of evaluation and reporting mechanisms for risk management activities provides feedback to management and other interested parties in the organization and government-wide. The results of these activities ensure that integrated risk management is effective in the long term. Some of these activities could fall to functional groups in the organization responsible for review and audit. Responsibility may also be assigned to operational managers and employees to ensure that information affecting risk that is collected as part of local reporting or practices is incorporated into the environmental scanning process. Reporting could take place through normal management channels (performance reporting, ongoing monitoring, appraisal) as part of the advisory and challenge functions associated with risk management.

Reporting facilitates learning and improved decision-making by assessing both successes and failures, monitoring the use of resources, and disseminating information on best practices and lessons learned. Organizations should evaluate the effectiveness of their integrated risk management processes on a periodic basis. In collaboration with departments, the Treasury Board of Canada Secretariat will review the effectiveness of the Integrated Risk Management Framework and make the necessary adjustments to ensure sustained progress in building a risk-smart workforce and environment.

Building Organizational Capacity

Building risk management capacity is an ongoing challenge even after integrated risk management has become firmly entrenched. Environmental scanning will continue to identify new areas and activities that require attention, as well as the risk management skills, processes, and practices that need to be developed and strengthened.

Organizations need to develop their own capacity strategies based on their specific situation and risk exposure. The implementation of the Integrated Risk Management Framework will be further supported by the Treasury Board of Canada Secretariat, which, through a centre of expertise, will provide overall guidance, advice and share best practices.

To build capacity for risk management, there needs to be a focus on two key areas: human resources, and tools and processes at both the corporate and local levels. The risk profile will identify the organization's existing strengths and weaknesses vis-à-vis capacity. Areas that may require attention include:

Human Resources

- building awareness of risk management initiatives and culture;
- broadening skills base through formal training including appropriate applications and tools;
- increasing knowledge base by sharing best practices and experiences; and
- building capacity, capabilities and skills to work in teams.

Tools and Processes

- developing and adopting corporate risk management tools, techniques, practices and processes;
- providing guidance on the application of tools and techniques;
- allowing for development and/or the use of alternative tools and techniques that may be better suited to managing risk in specialized applications; and
- adopting processes to ensure integration of risk management across the organization.

Element 3: Practising Integrated Risk Management

Implementing an integrated risk management approach requires a management decision and sustained commitment, and is designed to contribute to the realization of organizational objectives. Integrated risk management builds on the results of an environmental scan and is supported by appropriate corporate infrastructure.

The following outcomes are expected for practising integrated risk management:

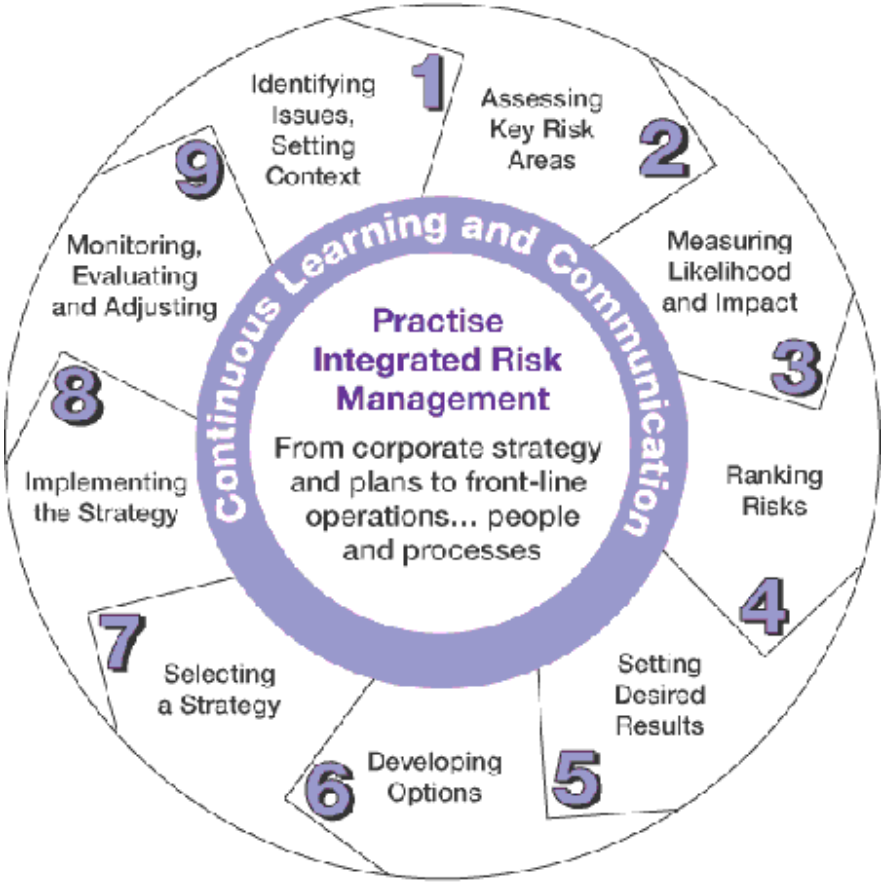
- *A departmental risk management process is consistently applied at all levels, where risks are understood, managed and communicated.*
- *Results of risk management practices at all levels are integrated into informed decision-making and priority setting*—strategic, *operational, management and performance reporting.*

- *Tools and methods are applied as aids to make decisions.*
- *Consultation and communication with* stakeholders *is ongoing—internal and external.*

A Common Process

A common, continuous risk management process assists an organization in understanding, managing and communicating risk. Continuous risk management has several steps. Emphasis on various points in the process may vary, as may the type, rigour or extent of actions considered, but the basic steps are similar. In the exhibits that follow, Exhibit 1 illustrates an example of a continuous risk management process that focuses on an integrated approach to risk management, while Exhibit 2 presents a risk management decision-making process in the context of public policy.

Exhibit 1: A Common Risk Management Process



Internal and external communication and continuous learning improve understanding and skills for risk management practice at all levels of an organization, from corporate through to front-line operations. The process provides common language, guides decision-making at all levels, and allows organizations to tailor their activities at the local level. Documenting the rationale for arriving at decisions strengthens accountability and demonstrates due diligence.

The common risk management process and related activities are:

Risk Identification

1. Identifying Issues, Setting Context

- Defining the problems or opportunities, scope, context (social, cultural, scientific evidence, etc.) and associated risk issues.
- Deciding on necessary people, expertise, tools and techniques (e.g., scenarios, brainstorming, checklists).
- Performing a stakeholder analysis (determining risk tolerances, stakeholder position, attitudes).

Risk Assessment

2. Assessing Key Risk Areas

- Analyzing context/results of environmental scan and determining types/categories of risk to be addressed, significant organization-wide issues, and vital local issues.

3. Measuring Likelihood and Impact

- Determining degree of exposure, expressed as likelihood and impact, of assessed risks, choosing tools.
- Considering both the empirical/scientific evidence and public context.

4. Ranking Risks

- Ranking risks, considering risk tolerance, using existing or developing new criteria and tools.

Responding to Risk

5. Setting Desired Results

- Defining objectives and expected outcomes for ranked risks, short/long term.

6. Developing Options

- Identifying and analyzing options—ways to minimize threats and maximize opportunities—approaches, tools.

7. Selecting a Strategy

- Choosing a strategy, applying decision criteria—results-oriented, problem/opportunity driven.

- Applying, where appropriate, the precautionary approach/principle as a means of managing risks of serious or irreversible harm in situations of scientific uncertainty.

8. Implementing the Strategy

- Developing and implementing a plan.

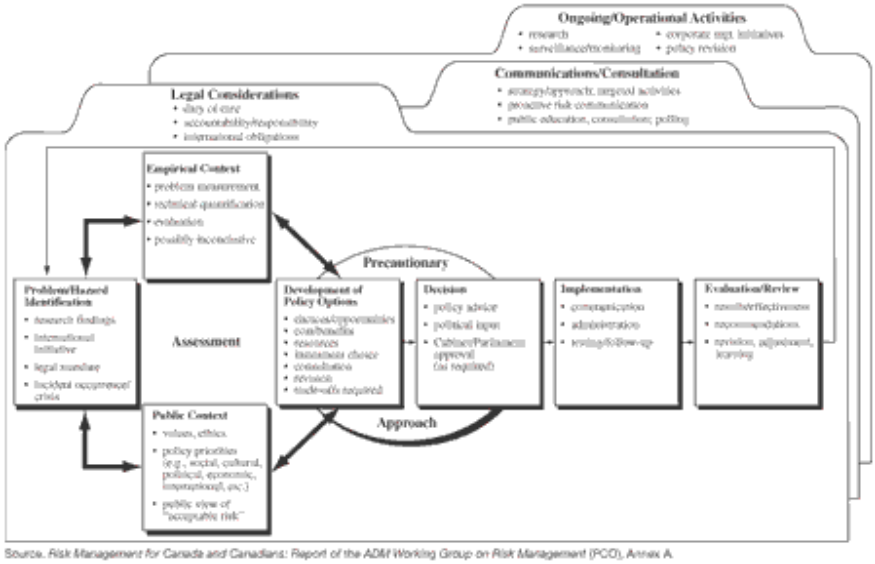
Monitoring and Evaluation

9. Monitoring, Evaluating and Adjusting

- Learning, improving the decision-making/risk management process locally and organization-wide, using effectiveness criteria, reporting on performance and results.

Organizations may vary the basic steps and supporting tasks most suited to achieving common understanding and implementing consistent, efficient and effective risk management. A focused, systematic and integrated approach recognizes that all decisions involve management of risk, whether in routine operations or for major initiatives involving significant resources. It is important that the risk management process be applied at all levels, from the corporate level to programs and major projects to local systems and operations. While the process allows tailoring for different uses, having a consistent approach within an organization assists in aggregating information to deal with risk issues at the corporate level.

Exhibit 2: Risk Management in Public Policy: A Decision-Making Process



Source. *Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management* (PCO), Annex A

Exhibit 2 presents the model, developed by the PCO-led ADM Working Group on Risk Management, which addresses the issue of risk management in the context of public policy development. This model presents a basis for exploring issues of interest to government

policy-makers, and provides a context in which to discuss, examine, and seek out interrelationships between issues associated with public policy decisions in an environment of uncertainty and risk (i.e., a model of public risk management).

As in Exhibit 1, this model recognizes six basic steps: identification of the issue; analysis or assessment of the issue; development of options; decision; implementation of the decision; and evaluation and review of the decision.[4]

In this model, several key elements were identified as influencing the public policy environment surrounding risk management:

- There is a *public element* to virtually all government decision-making, and it is a central and legitimate input to the process.

- Uncertainty in science, together with competing policy interests (including international obligations) has led to increased focus on the *precautionary approach*.

- A decision-making process does *not occur in isolation*—the public nature and complexity of many government policy issues means that certain factors, such as communications and consultation activities, legal considerations, and ongoing operational activities, require active consideration at each stage of the process.

Integrating Results for Risk Management into Practices at all Levels

The results of risk management are to be integrated both horizontally and vertically into organizational policies, plans and practices. Horizontally, it is important that results be considered in developing organization-wide policies, plans and priorities. Vertically, functional units, such as branches and divisions, need to incorporate these results into programs and major initiatives.

In practice, the risk assessment and response to risk would be considered in developing local business plans at the activity, division or regional level. These plans would then be considered at the corporate level, and significant risks (horizontal or high-impact risks) would be incorporated into the appropriate corporate business, functional or operational plan.

The responsibility centre providing the advisory and “corporate challenge” functions can add value to this process, since new risks might be identified and new risk management strategies required after the roll-up. There needs to be a synergy between the overall risk management strategy and the local risk management practices of the organization.

Each function or activity would have to be examined from three standpoints:

- **its purpose:** risk management would look at decision-making, planning, and accountability processes as well as opportunities for innovation;

- **its level:** different approaches are required based on whether a function or activity is strategic, management or operational; and

- **the relevant discipline:** the risks involved with technology, finance, human resources, and those regarding legal, scientific, regulatory, and/or health and safety issues.

Tools and Methods

At a technical level, various tools and techniques can be used for managing risk. The following are some examples:

- **risk maps:** summary charts and diagrams that help organizations identify, discuss, understand and address risks by portraying sources and types of risks and disciplines involved/needed;

- **modelling tools:** such as scenario analysis and forecasting models to show the range of possibilities and to build scenarios into contingency plans;

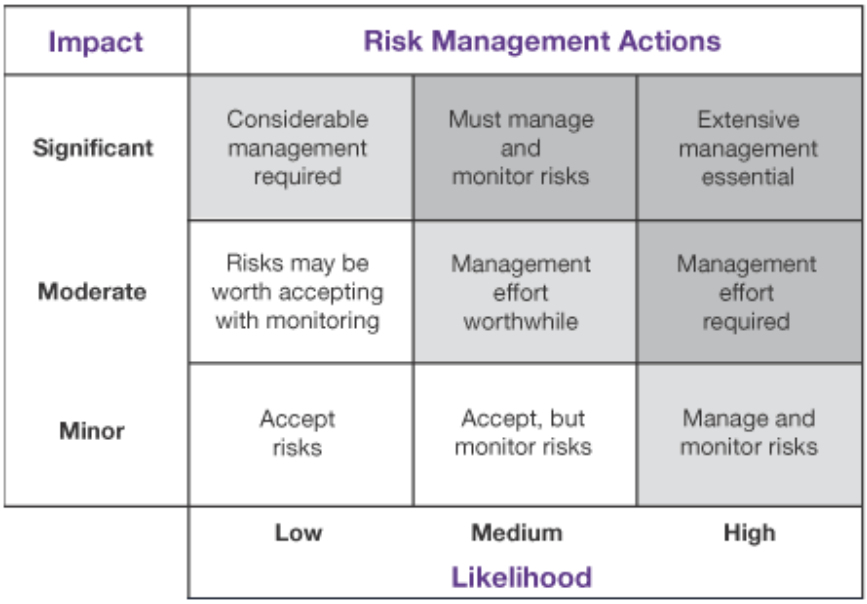
- **framework on the precautionary approach:** a principle-based framework that provides guidance on the precautionary approach in order to improve the predictability, credibility and consistency of its application across the federal government;

- **qualitative techniques:** such as workshops, questionnaires, and self-assessment to identify and assess risks; and

- **Internet and organizational** Intranets**:** promote risk awareness and management by sharing information internally and externally.

Exhibit 3 provides an example of a risk management model. In this model, one can assess where a particular risk falls in terms of likelihood and impact and establish the organizational strategy/response to manage the risk.

Exhibit 3: A Risk Management Model



In developing methods to provide guidance on risk management, the different levels of readiness and experience in a department, as well as variations in available resources need to be recognized. Therefore, methods need to be flexible and simple using clear language to ensure open channels of communication.

Several practical methods that could be used to provide guidance are:

- **a managers'** forum**:** where risks are identified, proposed actions are discussed and best practices are shared;
- **an internal risk management advisory** function**:** dedicated to risk management, either as a special unit or associated with an existing functional unit; and
- **tool kits:** a collection of effective risk management tools such as checklists, questionnaires, best practices.

Communication and Consultation

Communication of risk and consultation with interested parties are essential to supporting sound risk management decisions. In fact, communication and consultation must be considered at every stage of the risk management process.

A fundamental requirement for practising integrated risk management is the development of plans, processes and products through ongoing consultation and communication with stakeholders (both internal and external) who may be involved in or affected by an organization's decisions and actions.

Consultation and proactive citizen engagement will assist in bridging gaps between statistical evidence and perceptions of risk. It is also important that risk communication practices anticipate and respond effectively to public concerns and expectations. A citizen's request for information presents an opportunity to communicate about risk and the management of risk.

In the public sector context, some high-profile risk issues would benefit from proactively involving parliamentarians in particular forums of discussion thus creating opportunities for exchanging different perspectives. In developing public policy, input from both the empirical and public contexts ensures that a more complete range of information is available, therefore, leading to the development of more relevant and effective public policy options. Internally, risk communication promotes action, continuous learning, innovation and teamwork. It can demonstrate how management of a localized risk contributes to the overall achievement of corporate objectives.

Risk communication involves a range of activities, including issue identification and assessment, analysis of the public environment (including stakeholder interests and concerns), development of consultation and communications strategies, message development, working with the media, and monitoring and evaluating the public dialogue. The public sector has the additional responsibility of reporting to and communicating with Parliament.

Within the federal Public Service, it is expected that consultation activities, including those related to risk management, will be undertaken in a manner that is consistent with the *Government Communications Policy*.

Element 4: Ensuring Continuous Risk Management Learning

Continuous learning is fundamental to more informed and proactive decision-making. It contributes to better risk management, strengthens organizational capacity and facilitates integration of risk management into an organizational structure. To ensure continuous risk management learning, pursue the following outcomes:

- *Learning from* experience *is* valued, *lessons are shared—a supportive work environment.*
- *Learning plans are* built *into* organization's *risk management practices.*
- *Results of risk* management *are* evaluated *to support innovation, capacity building and continuous improvement—individual, team and organization.*
- *Experience and best* practices *are* shared—*internally and across government.*

Creating a Supportive Work Environment

A supportive work environment is a key component of continuous learning. Valuing learning from experience, sharing best practices and lessons learned, and embracing innovation and responsible risk-taking characterize an organization with a supportive work environment. An organization with a supportive work environment would be expected to:

Promote learning

- by fostering an environment that motivates people to learn;
- by valuing knowledge, new ideas and new relationships as vital aspects of the creativity that leads to innovation; and
- by including and emphasizing learning in strategic plans.

Learn from experience

- by valuing experimentation, where opportunities are assessed for benefits and consequences;
- by sharing learning on past successes and failures; and
- by using “lessons learned” and “best practices” in planning exercises.

Demonstrate management leadership

- by selecting leaders who are coaches, teachers and good stewards;
- by demonstrating commitment and support to employees through the provision of opportunities, resources, and tools; and
- by making time, allotting resources and measuring success through periodic reviews (e.g., learning audits).

Building Learning Plans in Practices

Since continuous learning contributes significantly to increasing capacity to manage risk, the integration of learning plans into all aspects of risk management is fundamental to building capacity and supporting the strategic direction for managing risk.

As part of a unit’s learning strategy, learning plans provide for the identification of training and development needs of each employee. Effective learning plans, reflecting risk management learning strategies, are linked to both operational and corporate strategies, incorporate opportunities for managers to coach and mentor staff, and address competency gaps (knowledge and skills) for individuals and teams. The inclusion of risk management learning objectives in performance appraisals is a useful approach to support continuous risk management learning.

Supporting Continuous Learning and Innovation

In implementing a continuous learning approach to risk management, it is important to recognize that not all risks can be foreseen or totally avoided. Procedures are paramount to ensure due diligence and to maintain public confidence. Goals will not always be met and innovations will not always lead to expected outcomes. However, if risk management actions are informed and lessons are learned, promotion of a continuous learning approach will create incentives for innovation

while still respecting organizational risk tolerances. The critical challenge is to show that risk is being well-managed and that accountability is maintained while recognizing that learning from experience is important for progress.

In addition to demonstrating accountability, transparency and due diligence, proper documentation may also be used as a learning tool. Practising integrated risk management should support innovation, learning, and continuous improvement at the individual, team and organization level.

An organization demonstrates continuous learning with respect to risk management if:

- an appropriate risk management culture is fostered;
- learning is linked to risk management strategy at many levels;
- responsible risk-taking and learning from experience is encouraged and supported;
- there is considerable information sharing as the basis for decision-making;
- decision-making includes a range of perspectives including the views of stakeholders, employees and citizens; and
- input and feedback are actively sought and are the basis for further action.

Conclusion

The Integrated Risk Management Framework advances a more systematic and integrated approach for risk management. By focusing on the importance of risk communication and risk tolerance, it looks outside the organization for the views of Canadians. Internally, it emphasizes the importance of people and leadership and the need for departments and agencies to more clearly define their roles. The Framework provides a tool that helps organizations communicate a vision and objectives for management of risk based on government values and priorities, lessons learned, best practices and consultation with stakeholders.

The Framework is a fundamental part of the federal management agenda and Modern Comptrollership. It is designed to support the optimization of resource allocation and responsible spending, paramount for achieving results. It also builds on public sector values, knowledge management and continuous learning for innovation. The Integrated Risk Management Framework is the first step in establishing the foundation for more strategic and corporate integrated risk management in departments and in government. In the future, the Framework will be supported by tools and guidance documents as well as complemented by other risk management initiatives.

The Treasury Board of Canada Secretariat intends to work closely with departments and agencies in implementing the Integrated Risk Management Framework and in tracking progress toward building a risk-smart workforce and environment in the Public Service.

Appendix: Shared Leadership—Suggested Roles and Responsibilities

In moving toward an integrated risk management function, everyone has a role to play. Combining shared leadership with a team approach will help contribute to the success of integrated risk management throughout the organization. Suggested roles and responsibilities that could be considered by the different parties involved in integrated risk management are outlined below.

Treasury Board of Canada Secretariat

- communicating and explaining the Integrated Risk Management Framework;
- providing guidance, training and a centre of expertise in support of the Integrated Risk Management Framework;
- providing Treasury Board, other central agencies and Parliament with risk management information and advice appropriate to their responsibilities; and
- periodically examining and evaluating the effectiveness of the Integrated Risk Management Framework, tracking progress and reporting on best practices.

Deputy Heads or Equivalent

- setting the tone from the top that systematic and integrated risk management is valuable for understanding uncertainty in decision-making and for demonstrating accountability to stakeholders;
- determining the best way to implement the Integrated Risk Management Framework in their organization;
- ensuring that a supportive learning environment exists for risk management, including sensible risk taking and learning from experience;
- ensuring, from a corporate perspective, that risks are prioritized, and that appropriate risk management strategies are in place to respond to identified risks; and
- ensuring the capacity to report on the performance of the risk management function (i.e., knowing how well the department or agency is managing risk).

Senior Management

- integrating risk management into overall departmental strategy and management frameworks;
- providing managers and employees with learning opportunities and training to build competencies; and

allocating resources for investment in more systematic risk management.

Managers

- considering risk as a part of their decision-making process; and
- ensuring there is appropriate ongoing operational and corporate-related risk management action, planning, training, control, monitoring and documentation.

Functional Advisors and Specialists

- ensuring that policy and related advice, guidance and assistance is in line with central agency and departmental policies on risk management and senior management's objectives;
- helping managers identify and assess risk and the effectiveness, efficiency and economy of existing measures to manage risk; and
- helping managers design and implement tools for more effective risk management.

Review, Internal Audit

- reporting to the Deputy Head on the department's or agency's performance under the Integrated Risk Management Framework.

All Public Servants

- staying aware of and attentive to risk management issues;
- risk-smart behaviours and outcomes—considering limitations, key risk areas and fundamental rules to understand risks they can and cannot take (i.e., understanding where there is allowance for honest mistakes and where prudence is paramount); and
- documenting decisions and supporting information.

Footnotes

1. *Australian and New Zealand Public Sector Guidelines for Managing Risk* (HB 143:1999) defines risk as the "chance of something happening that will have an impact on objectives. It is measured in terms of consequences and likelihood."

   The Canadian Institute of Chartered Accountants defines risk as "the possibility that one or more individuals or organizations will experience adverse consequences from an event or circumstance."

   The *Canadian Standards Association Risk Management: Guidelines for Decision-Makers* (CAN/CSA-Q850-97) defines risk as "the chance of injury or loss as defined as a measure of the probability and severity of an adverse effect to health, property, the environment or other things of value."

   The November 1, 2000, working draft of the International Organization for Standardization (ISO) Risk Management Terminology defines risk as the "combination of the probability of an event and its consequences. Note 1- In some situations, risk is a deviation from the expected."

2. *Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management* (PCO).

3. This is a general definition and while it includes the assessment of risk as a function of the decision-making process, it is not intended to prescribe a system for prioritizing specific risks.

   Also of note is that in many international fora, *risk analysis* is used as the more comprehensive label, referring to an overall process for dealing with risk, including identification, assessment and implementation of measures. The use of *management* rather than *analysis* is intended to reflect the general applicability of the concepts to be developed, not only in technical or science-based sectors, but also in other public policy areas.

4. For further details, refer to the PCO report, *Risk Management for Canada and Canadians: Report of the ADM Working Group on Risk Management* (March 2000).

APPENDIX 3

Risk Management Framework for IMO – submitted by South Africa

Proposed Risk Management Policy for IMO

1. INTRODUCTION

Council agreed that management of risk should become a formalised on-going process, rather than an individual event. Organisation must ensure the establishment and maintenance of effective, efficient and transparent systems of financial and risk management and internal control. Accounting Officers must facilitate a risk assessment to determine the material risks to which the institution may be exposed to evaluate the strategy for managing these risks. Such a strategy must include a fraud prevention plan. The strategy must be used to direct internal audit effort and priority, and to determine the skills required to manage these risks.

The aim of this framework is therefore to assist the Organisation with the effective and efficient management of risks and exposures. The framework outlines the responsibilities of the different roles players in the management of risk and exposures as well as describes a risk management process that the Organisation will undertake to mitigate or minimise the impact of risks exposures. The framework further seeks to encourage management commitment to risk management and inculcate a risk management philosophy in the Organisation

2. DEFINITION

For purposes of this policy, unless the context indicate otherwise-

"**Organisation**" means the International Maritime Organisation

"Accounting Officer" means the Secretary General of the Organisation

"Audit Committee" means a committee established to evaluate the adequacy, effectiveness and the efficiency of the internal control system and risk management system of the Organisation

"Internal Audit Unit" means the unit that is established in terms of this framework to assess the adequacy of financial management and internal control systems and provide reasonable assurance to management that the established internal control system is functioning as intended and make recommendations for the improvement of the internal control system.

"Internal Control Unit" is a unit that facilitates risk management processes and the development and implementation and performance.

"Internal Controls" are the systems (whether manual, electronic or otherwise) policies, procedures and processes that an Accounting Officer must have in place to minimise the risks which the Organisation might be exposed to, whether as a result of fraud, negligence, error or any other cause.

"Management" means an official from the rank of Assistant Director upwards

"Risk" can be defined as "the combination of the probability of an event and its consequences." (ISO/IEC Guide 73). , means an event, action, situation, etc. that

might cause a financial loss, and/or have negative impact on the organisational operations and its image;

"Risk management" is a strategic process that focuses on effective and efficient processes that identify, monitor and address all risk areas and exposures that might impact negatively on the Organisation and its performance. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities." (A Risk Management Standard – published by AIRMIC, ALARM, IRM 2002)

"Risk Assessment" is a formal and systematic approach to conduct a detailed examination and evaluation of the organisational risks and exposures.

3. APPLICATION

This policy, unless certain parts thereof indicate otherwise, applies to all officials of the Organisations

4. CODE OF PRACTICE FOR RISK MANAGEMENT

Our Code of Practice for Risk Management is to set out a framework to effectively manage the risks involved in all our activities, to maximize opportunities, to minimize adversity and to achieve improved service delivery outcomes and outputs.

The organisation will manage the risks and opportunities in a transparent, honest and responsible manner that will ensure a safe and a conducive environment in the best interest of our department and stakeholders.

Our stakeholders include:

- Member States and other Governments
- Employees
- United Nations and other UN Agencies
- Suppliers
- Environment
- Industry
- Etc

5. OVERSIGHT AND RESPONSIBILITY

The organisational oversight structure is illustrated below:

Executive Authority
Accounting Officer

Auditor General — Audit Committee
Internal Audit

Divisional Managers

Internal Control
Management

5.1 Executive Authority

Management is accountable to the Council which provides governance, guidance and oversight. Council has a major role in defining what it expects in integrity and ethical values and can confirm its expectations through oversight activities. Similarly, by reserving authority in certain key decisions, Council plays a role in setting strategy, formulating high- level objectives and broad-based resource allocation. Council provides oversight with regard to risk management by:

Knowing the extent to which management has established effective risk management in the Organisation;
Being aware of and concurring with the organisation's risk tolerance;
Reviewing the Organisation's portfolio view of risks and considering it against the department's risk tolerance; and
Being aware of the most significant risks and whether management is responding appropriately.

5.2 Accounting Officer/ Secretary General

The ultimate responsibility of risk management in the Organisation lies with the Accounting Officer. The Accounting Officer sets the "tone at the top" that affects integrity and ethics and other factors of the control environment The Accounting Officer must ensure that risk management is integrated into all strategic management processes and that the significant risks are addressed.

The Accounting Officer is responsible for strategic management processes and ensures that the strategic plan of the Organisation indicates specific outputs and service delivery targets and that all significant risks are taken into consideration in the development of the strategic plan. In managing these risks, the Accounting Officer must, amongst other things, put in place a performance management system that links management performance to strategic objectives of the department.

All in all, the Accounting Officer must ensure that s/he is apprised of the significant risks; along with actions management is taking and how management is ensuring effective risk management.

5.3 Division Director

The Accounting Officer shall delegate risk management to Division Directors. Division Directors are responsible for risk management in their area of responsibility. Division Directors must ensure that the system of financial management and internal control established for the Organisation is carried out within their area of responsibility.

Division Directors must maintain a risk register for their areas of responsibility and update it continuously which is to ensure that risks are properly managed.

5.4 Audit Committee

The Organisation's Audit Committee, which has non-executive status, plays an advisory role to the Accounting Officer. It validates the independent role of the Internal Audit Function and the effectiveness of risk management and internal control system. Its role is to independently monitor the activities within the Organisation. It is responsible to provide reasonable assurance that critical processes are being performed effectively, key measures and reports are reliable and established policies are complied with.

5.5 Internal Audit

Internal auditors play an important role in the monitoring of risk management and the quality of performance as part of their regular duties or upon special request of senior management, which is approved by the audit committee. They may assist both management and the executive authority or audit committee by monitoring, examining, evaluating, reporting on and recommending improvements to the adequacy and effectiveness of management's risk management processes. Internal Audit Unit therefore provides an independent and objective service that adds value and improves the organisational risk management operations. Internal Auditors have an impartial, unbiased attitude and avoid conflict of interest and they have no authority or responsibility for the activities that are audited by them.

To ensure independence, the Internal Audit Unit shall report directly to the Accounting Officer and report functionally to the Audit Committee.

5.6 Internal Control Unit

Internal Control Unit is responsible for ensuring that there are effective and efficient systems of internal controls and facilitates the designing and the implementation of such controls.

The main responsibility of Internal Control Unit is to:

- Continuously identify, assess and evaluate risks.
- Facilitate and implement risk management plan.
- Facilitate implementation of effective and efficient internal control measures.
- Monitor implementation of internal controls.
- Review the organisational policies to ensure a sound effective and efficient internal control environment.

Internal Control unit shall work with other divisions in establishing and maintaining effective risk management in their areas of responsibility. The unit

shall also monitor progress and assist other divisions in reporting relevant risk information up, down and across the organisation

5.7 Management

It is the responsibility of the management to establish and maintain controls and control systems as delegated by the Accounting Officer. Management supports the departmental risk management philosophy, promote compliance with risk management processes and good corporate governance and manage the risks within their spheres of responsibility.

5.8 Risk Management Committee (RMC)

RMC is a standing committee chaired by the Accounting Officer or his/her delegated official and it comprises of senior management within the Organisation. The terms of reference of the committee are as follows:

- Develop and communicate a risk management philosophy within the Organisation.
- Ensure that operations are carried out in line with the risk management policy.
- Review effective compliance with the risk management policy and its objectives
- Integrating risk management into planning, monitoring and reporting processes within the Organisation.
- Approving and reviewing risk management policy, including the approval of acceptable levels of risks based on ongoing risk assessments.
- Ensure that risk management becomes an integral part of the day-to-day planning, management and general culture of the Organization.

5.9 Other officials

Other officials are responsible for executing risk management in accordance with established directives and protocols and must ensure that the system of financial management and internal control established is carried out within their areas of operation and responsibility and that financial and other resources allocated to them are used effectively, efficiently, economically and transparently. Employees are responsible for communicating risks such as problems in operations, non-compliance with the code of conduct, other policy violations or illegal actions.

6. AREAS OF RISK MANAGEMENT

The organisational risk management plan can be categorized but not limited to the following risk management areas:

- Business Risk Management
- Financial Risk Management
- Fraud and Corruption Risk Management
- Physical Risk Management
- Environmental, Health and Safety Risk Management and
- Information Security Risk Management

6.1 Business Risk Management

Business risk is the level of uncertainty that the Organisation may not effectively and efficiently executes its strategies to achieve its service delivery objectives.

In order to ensure effective and efficient delivery of services to Member States and industry, the organisation must identify internal and external events/factors that might hamper or enhance service delivery. Events with a negative impact (risks) represent risks and must be managed to ensure that its impact on service delivery is minimized. Events with a positive impact represent opportunities and must be incorporated into the strategy or objective-setting processes, formulating plans to seize the opportunities.

6.2 Financial Risk Management

Financial risk is the risk associated with the effective, efficient and transparent use of the resources of the Organisation.

The Organisation must maintain sound and effective financial and operating controls that are designed to provide reasonable assurance regarding amongst others:

- The maintenance of proper accounting records;
- The adequacy and reliability of financial information;
- The safeguarding of assets;
- Compliance with statutory laws and regulations; and
- Efficient and effective use of organisational resources.

6.3 Fraud and Corruption Risk Management

Fraud risk is risk that results from the intentional misrepresentation of fact or event by individuals or organizations which when acted upon by the Organisation may result in the Organisation suffering loss.

Corruption risk is risk associated with the offering, giving, soliciting or acceptance of inducement or reward which may improperly influence the action of an official in order to or not to perform his/her duties resulting in contravention of any organisational and/ or United Nations policies, regulations and procedures.

The Organisation shall maintain and implement an Anti-Corruption and Fraud Prevention Strategy to manage the risks related to fraud and corruption. The aim of the strategy is to minimize the risk of fraud and corruption through:

- Creating a positive control environment (includes a culture of zero tolerance to fraud and corruption)
- Cost-effective utilization of information systems,
- Implementation of effective, efficient and transparent control procedures,
- Creating fraud and corruption awareness amongst the stakeholders (officials, suppliers, society, etc)
- Investigate all reported cases of fraud and corruption and take appropriate disciplinary action against offenders

6.4 Physical Risk Management

Physical Risk is the risk of damage and theft of organisational property, including acts of nature and human actions.

The focus is to manage and safeguard the physical assets of the Organisation. An asset management system shall be established and maintained to continuously identify and evaluate the exposure of assets to risk with an intention to minimize losses and/ or damages. Security system will be put in place to minimize theft of assets.

6.5 Environmental, Health and Safety Risk Management

This is the risk that the Organisation might achieve its objectives at the expense of environmental sustainability and compromise healthy and safety standards.

The Organisation shall promote environment, health and safety principles and practices to create a safe and healthy environment for all and to meet the requirements of all relevant environments, health and safety legislation as a minimum standard. Compliance with Occupational, Health and Safety (OHS), ISO 14001 are of particular importance.

6.6 Information Security Risk Management

Information security risk is the risk associated with the protection of the confidentiality, integrity and availability of information required by the Organisation to meet its objectives.

Security risks relate to access controls into the building as well as other security measures in place to ensure that departmental resources/assets are safeguarded.

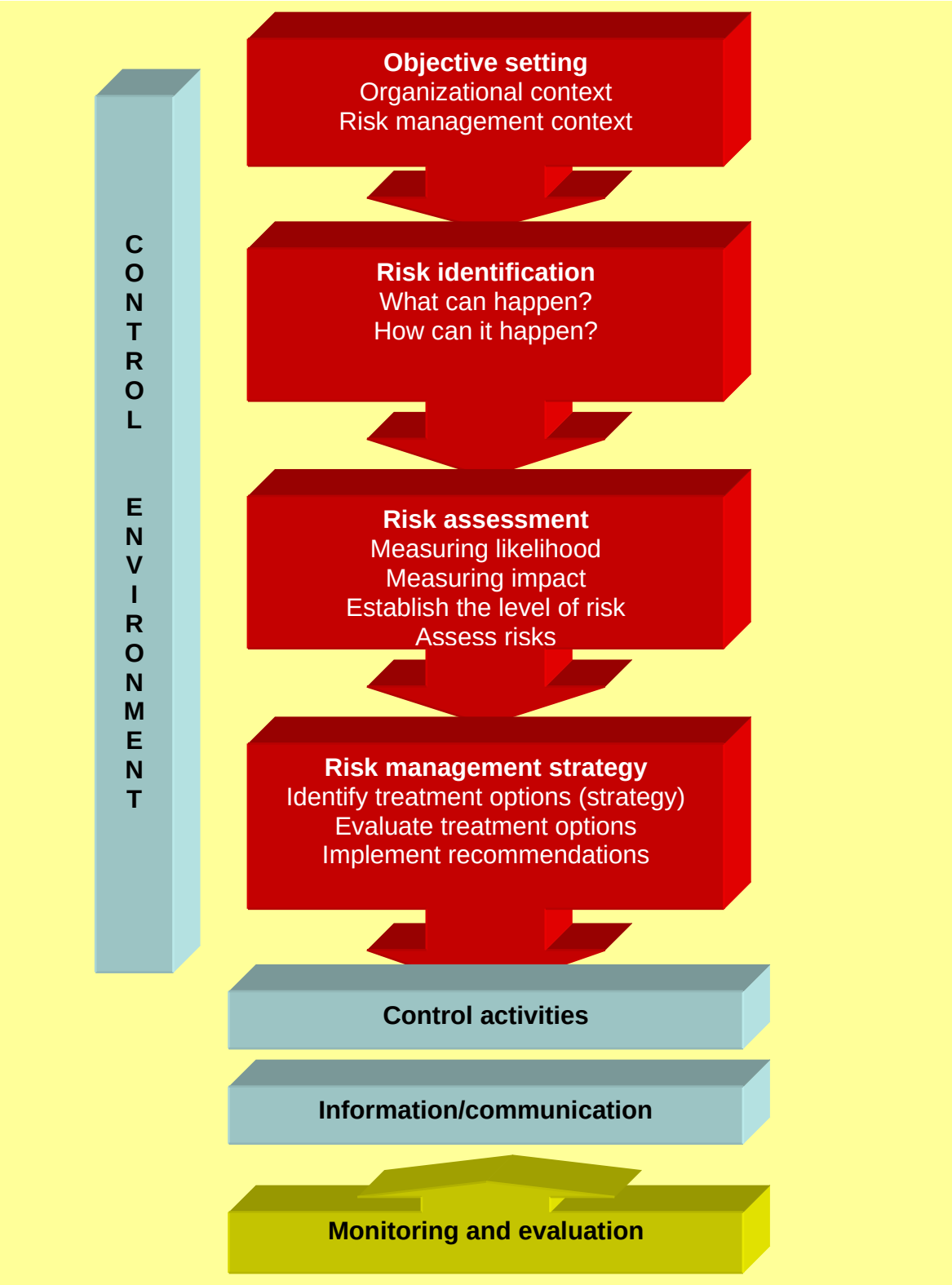
7. RISK MANAGEMENT PROCESS

The process of managing risk is a structured approach for incorporating risk management into the daily, broader management process. Risk management is more than an exercise of risk avoidance. It is as much about identifying opportunities as avoiding or mitigating losses.

The departmental risk management shall be an ongoing process at every level, and consists of eight interrelated components, namely:

- the control environment;
- objective setting;
- risk identification;
- risk assessment;
- risk management strategy;
- control activities;
- information and communication; and
- Monitoring.

The following table indicates the different relationships between the components:
Eight components of risk management



The organisation control environment is the foundation of risk management, providing discipline and structure. The control environment influences how strategy and objectives are established, Organisation activities are structured, and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities.

7.1 Control Environment

The control environment encompasses the tone of the organisation and sets the basis for how risk is viewed and addressed by the organisation's officials. The control environment consists of different layers including, amongst others, risk management philosophy, risk tolerance or appetite, integrity and ethical values, organizational culture and structure as well as management operating style.

The organisation shall conduct an internal environment survey at once every three years.

7.2 Objective Setting

Objectives must exist before management can identify events potentially affecting their achievement. Risk management ensures that management has a process in place to both set objectives and aligns the objectives with the organisation's mission/vision and is consistent with the organisation's risk tolerance or appetite. This objectives setting process include both the strategic and operational objectives and it must happen annually during the strategic planning and budgetary process.

7.3 Events identification

Internal and external events and/or factors affecting achievement of organisational objectives must be identified, distinguished between those with negative and positive impact. Events or factors with a positive impact must be channelled back to management strategy or objective setting process. During this identification phase, all financial and non-financial factors must be identified.

The Organisation shall use various methods of identifying risks and exposures. Some of the methods are:

- interview/focus group discussion;
- audits or physical inspections;
- brainstorming;

- survey/questionnaire;
- history, failure analysis;
- examination of past department or public entity experience;
- incident, accident and injury investigation;
- scenario analysis;
- strengths, weaknesses, opportunities, threats (SWOT) analysis;
- flow charting, system design review, systems

7.4 Risk Assessment

Risk assessment is a formal and a systematic approach to conduct a detailed examination and evaluation of the Organisation's risks and exposures. Risks assessment should focus on all significant possible areas of impact relevant to the Organisation or its activities. In this phase, risks are assessed, considering their likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on both an inherent and residual basis.

7.5 Risk management strategy

Management identifies risk management strategy options, which should include a fraud prevention plan, and consider their effect on event likelihood and impact, in relation to risk tolerances, costs versus benefits, and thereafter designs and implements response options. The consideration of risk management strategies and selecting and implementing a risk management strategy is integral to risk management and requires that management select a response that is expected to bring risk likelihood and impact within the Organisation's risk tolerance level.

Risk management strategic options shall be classified under the following broad categories:

- **Risk Avoidance.** A decision not to be involved with a risk or in a risk situation. The decision will be not to proceed with a particular activity or project because upon assessment, the activity represents such a great risk that there is limited ability to control the risk and that there is little benefit in pursuing the activity.

- **Risk Control –** Is the pro-active control of adverse consequences of a risk by implementing preventative measures. It is the risk, which is cost effective to control or treat.

- **Risk Transfer/sharing –** It is the risk that upon assessment shall be considered cost effective to transfer to third parties or otherwise sharing a portion of the risk with the third party.

- **Risk Retention –** It is the risk that upon assessment shall be considered cost effective to be accepted or tolerated due to its limited impact on the department.

7.6 Control Activities

Risk responses serve to focus attention on control activities needed to help ensure that the risk responses are carried out properly and in a timely manner. Control activities are part of the process by which an organisation strives to achieve its business objectives.
Control activities therefore refer to policies, procedures, processes and systems that the organisation maintains to minimize the impact of risk and help ensure risk management strategies are properly executed. They occur throughout the organisation, at all levels and in all functions.

7.7 Information and Communication

Relevant information – both from internal and external sources, financial or non-financial – must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities. Effective communication occurs in a broader sense, flowing down, across and up the department, as well as the exchange of relevant information with external parties, such as suppliers, regulators and other stakeholders.

Management shall keep the executive authority up-to-date on performance, developments, risks and the functioning of risk management, and other relevant events and issues.

Management shall provide specific and directed communication addressing behavioural expectations and the responsibilities of personnel. This includes a clear statement of the organisation's risk management philosophy and approach and delegation of authority.

Communication about policies, processes and procedures shall take different forms including:

- Information sessions and presentations
- Workshops
- Circulars
- Distribution of hard copies and
- Email and Intranet

7.8 Monitoring

Risk management shall be regularly monitored – a process that assesses both the presence and functioning of its components and the quality of their performance over time. Monitoring can be done in two ways: through ongoing activities or separate evaluations. This will ensure that risk management continues to be applied at all levels and across the department.

8. APPROVAL OF POLICY

This risk management policy becomes effective upon approval by the Accounting Officer of the Organisation

Approved on the _____day of _____00_____ at _____

_____
Secretary General/ Delegated Official

APPENDIX 4

IALA Guidelines on Risk Management

IALA Guidelines on Risk Management

December, 2000

TABLE OF CONTENTS

PART A - INTRODUCTION

A.1 SCOPE OF THE GUIDELINES

These Guidelines are intended to outline a general risk assessment and risk management methodology for Marine Aids to Navigation including Vessel Traffic Services (VTS) so that all types of risks are effectively managed. The Guidelines may be used when assessing the optimum mix of aids to navigation and other facilities, including injury or loss of life, property, the environment, or something else of value. The annexes to the Guidelines include an example application as well as definitions for some of the risk terms used herein. Other examples of the application of the methodology described in the Guidelines will be published on the IALA website (http://www.iala-aism.org) as they become available.

In order that different Marine Aids to Navigation Authorities can consistently apply the Guidelines it is important that the process is clearly documented and formally recorded in a uniform and systematic manner. This will ensure the process is transparent and can be easily understood by all parties irrespective of their experience or background in the application of risk assessment and related techniques.

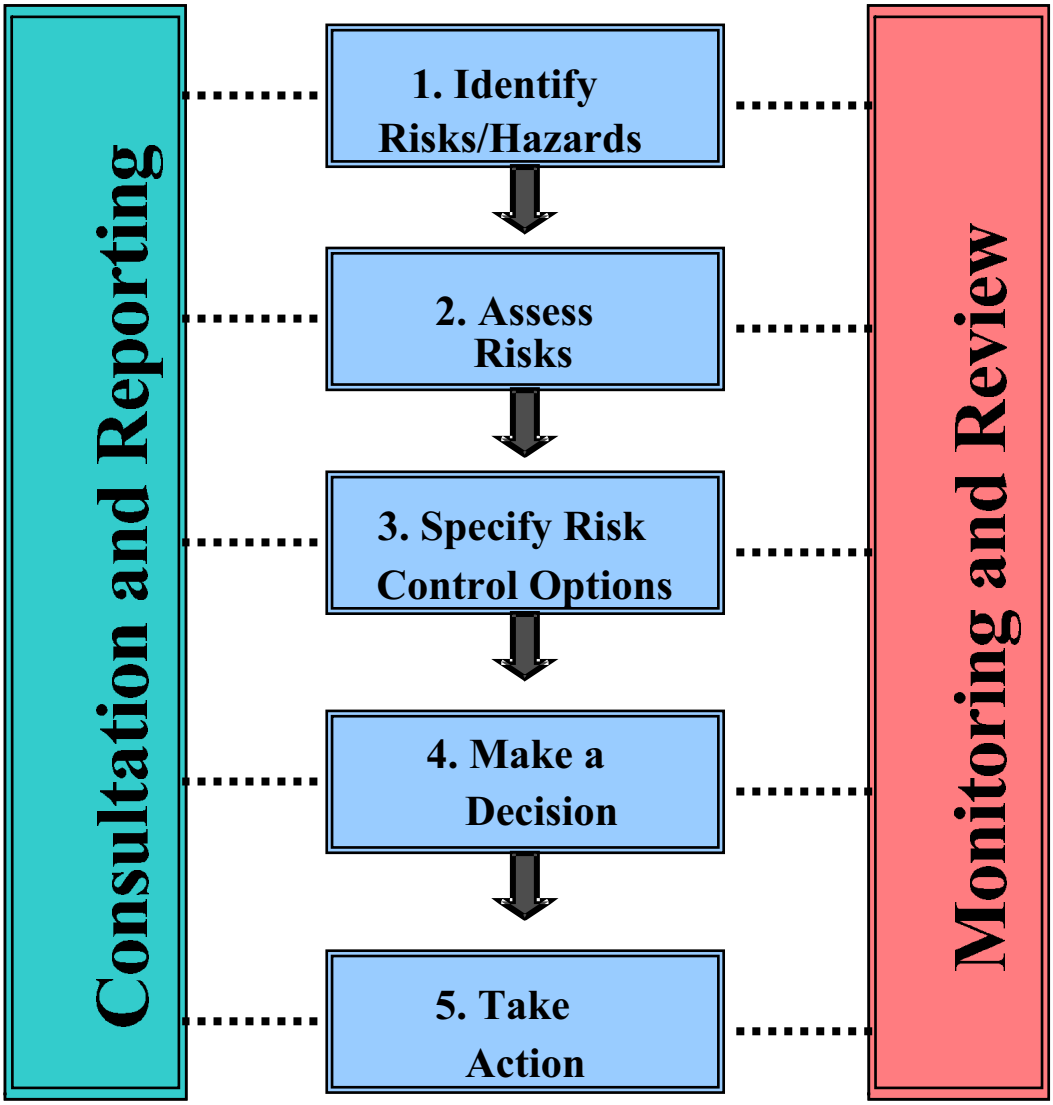
In the interim period, these Guidelines provide the basis for trial applications aimed at demonstrating the potential of utilizing a formal risk management process. The Guidelines will be reviewed, after a period of practical application, to amend and update as deemed necessary.

A.2 RISK MANAGEMENT DECISION PROCESS

The Risk Management process described in the Guidelines comprises five steps that follow a standardized management or systems analysis approach:

a. Identify risks/hazards;
b. Assess risks
c. Specify risk control options
d. Make a decision; and
e. Take action.

Figure A.1: IALA Risk Management Process



A.3 THE IMPORTANCE OF USING A RISK MANAGEMENT PROCESS

Organizations should evolve on an ongoing basis in order to remain relevant and to meet their mandate and objective as changes occur. Mastering risk is becoming essential as part of the current evolutionary context.

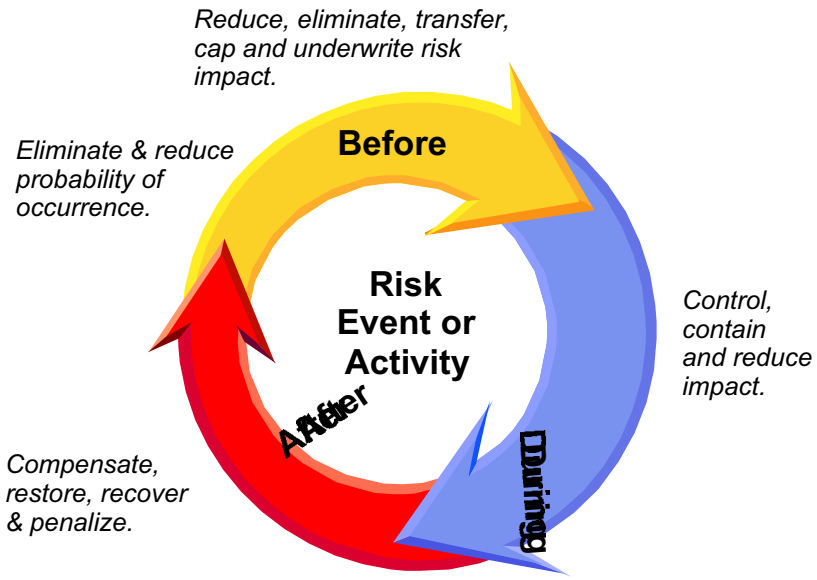
Risk is about something that may happen in the future. Factors such as technological innovation and complexity and growing social and cultural awareness are making it increasingly difficult to anticipate what may occur in the future. Risk management involves the analysis of scenarios about future events, their likelihood, impact and acceptability to stakeholders. This information is critical to issues such as the balancing of "program integrity" and "limited resources." Simply put, limitations on resources can adversely affect program integrity that involves the ability of organizations to ensure the continued achievement of results consistent with priorities. Organizations need modern management approaches including risk management to make judgements about maintaining program integrity. Competency in conducting intuitive and systematic analyses of the level of risk involved in organizational transition and new opportunities will support timely decision making and demonstrate due diligence across and down the organization.

Individuals and organizations manage risk every day consciously and unconsciously. The need to do so more systematically and explicitly is also a matter of transparency, accountability and credibility. Transparency gains are occurring as a matter of public sector reform and technology advances. Transparency leads to accountability and potential effects on credibility. Integrating risk management into management and operational practices provides a basis for anticipating transparency issues, managing accountability expectations and maintaining credibility. Credibility is maintained when stakeholders gain assurance that the organization is "in control." Such assurance is gained in part when it is transparent in plans, reports and stakeholder interfaces that the organization systematically and continually identifies, assesses and manages its risks. In effect, an organization must incorporate risk assessment and risk management into its own management system.

A.4 TEMPORAL NATURE OF RISK MANAGEMENT

Risk also has a temporal nature and it should be recognized that the process is iterative, and that a return to a previous step can be made at any time.

Figure A.2: Temporal Nature of Risk Management



Event and time-based risk management solutions.

A.5 FLEXIBILITY IN A RISK MANAGEMENT PROCESS

Risk management involves estimation, assumptions and implementation of strategies and procedures carried out by people. In many cases it is necessary to take a decision where all these elements have degrees of uncertainty. Most risk management approaches will examine these uncertainties and devise strategies to monitor events in order to be timely in adjusting a decision as a result of an uncertainty unfolding in a manner other than expected.

Risk management includes the objectives of sensible risk taking in order to support the achievement of results. Because zero risk situations are by and large not affordable in today's resource environment, some level of risk taking will always be a part of decisions. However, the climate for promoting timely decisions involving risk will be undermined if there is not an attitude of allowing for adjustments after a decision has been made. Allowing for adjustment should be built into the risk management process. Allowing for adjustment should involve learning from the adjustment so that it will be avoided in the future. Managers can be taken to task for not avoiding a known problem but they need to feel supported in terms of there being an allowance for adjustment on areas of new uncertainty.

Monitoring the estimations, assumptions and actions by the people implementing strategies and procedures will ensure adjustments are identified and implemented in a timely manner.

A.6 CONSULTATION AND COMMUNICATION

Reforms aimed at becoming more fiscally sound have increased the need for trades-off in the options and services provided by most organizations. Risk is generally a factor in these trades-off. Over and above trades-off, however, there are three compelling rationales for continued consultation and communication among stakeholders in the development of policies for managing risk.

First is the principle that program managers should consult with stakeholders, with a related agreement that stakeholders have the right to participate meaningfully in decision-making and be informed about the basis of decisions. It should be acknowledged that, notwithstanding the benefits of broad consultations, the program manager usually has the final decision. Virtually all public involvement processes have to address the question of the stakeholders role in the decision process regardless of whether participants are empowered to set policy or not.

Second is the belief that relevant wisdom is not limited to scientific specialists and officials of the organization and that stakeholders often contribute relevant information that might otherwise not be available to decision-makers.

Third is the rationale that broad consultations may decrease the conflict and increase the acceptance of, or trust in decisions by Marine Aids to Navigation Aauthorities. Related to this is the growing recognition of the importance of trust as a factor affecting how all stakeholders perceive risk.

Effective communications and consultations with stakeholders can provide the decision-makers with improved insight into risk problems since stakeholders often have a unique perspective or relevant information not otherwise available to decision-makers. This leads to better, more informed decisions. Just as important, effective communications provide a unique opportunity for decision-makers to improve their credibility with stakeholders. Improved credibility increases safety as a result of increased acceptance of and compliance with a safety program. Conversely, inappropriate or poorly conducted communications can reduce credibility and seriously inhibit the achievement of objectives.

A.7 INFORMATION AND DATA

Suitable data are necessary for each step of the Risk Management process. When data are not available, expert judgement, physical models, simulations and analytical models may be used to achieve valuable results.

Data concerning incident reports, near misses and operational failures may be very important for the purposes of making more balanced, proactive and cost-effective decision. A judgement on

the value of data that are to be used should be carried out in order to identify uncertainties and limitations, and to assess the degree of reliance that should be placed on the available data.

A more detailed list of data and information that should be considered in evaluating risk specific to Marine Aids to Navigation is attached in Annex II.

A.8 DOCUMENTATION REQUIREMENTS

There is a requirement for extensive documentation throughout the risk management process, especially if risk to life, property or the environment is being evaluated. If the issues under review are relatively inconsequential, documentation requirements may be modest, but still necessary.

Documentation:

a. helps in explaining decisions;
b. helps in defending decisions after they have been made;
c. provides a reference for future risk management processes, so as to facilitate continuous improvement;
d. provides for the monitoring function;
e. provides the basis of all decisions, in that all decisions are based on information;
f. provides a record of proceedings; and
g. helps in communicating reasons for decisions to stakeholders.

It may be critical that documentation is detailed and comprehensive, as in cases of possible litigation. However, the need for documentation should reflect the importance to stakeholders of the risk decisions to be taken, the level of concern regarding these issues and/or the resources available to the decision-maker. Reasonable efforts should be made to document the process without generating excessive paperwork.

Documentation may be an important resource for future decisions, just as a lack of documentation may generate serious problems. The amount of documentation to be provided should be a matter of serious consideration. While it is cautioned against being secretive, some information may need to remain confidential.

PART B - THE RISK MANAGEMENT PROCESS

B.1 STEP 1 – IDENTIFY RISKS/HAZARDS

B.1.1 Scope

The purpose of Step 1 is to identify and generate a prioritized list of risks/hazards, specific to the problem under review. This is achieved by the use of standard techniques to identify risks/hazards, which can contribute to incidents, and by screening these risks/hazards using a combination of available data and judgement.

B.1.2 Define Problem/Trigger

The problem under analysis and its boundaries should be carefully defined stating associated risk issues. This is often the most difficult phase in the process. However, it is also fundamentally the most important.

The risk management process may be initiated for a number of reasons, including:

a. a periodic safety review;
b. monitoring the system (including the effects of previous systems);
c. an emergency, accident or incident;
d. a public request or complaint;
e. other decisions, changes, or modifications to the operations of the organization; and
f. any number of internal or external events, including funding, operational and technical changes.

To avoid confusion, problems and issues must be specifically defined and documented, and should be dealt with one at a time. It is important to prioritize issues. Issues may also change throughout the process, as more information becomes available. For example, new issues may arise, issues may dissolve, or priorities may change.

B.1.3 Consult Stakeholders

During this stage, depending on the situation, it would be beneficial to identify and consult with stakeholders in order to validate or define the scope of the issues. Decision-makers in an organization often perceive the importance of an issue differently from external stakeholders.

Obviously, it is not necessary to involve all outside stakeholders in the validation of every identified issue. However, the greater the effect of a decision, the greater the concern, and the greater their involvement should be. When dealing with a more complex problem, in order to explain the resulting decision better, greater stakeholder involvement is required.

B.1.4 Hazard Identification Methodology

The approach used for hazard identification generally comprises a combination of both creative and analytical techniques, the aim being to identify as many relevant hazards as possible. The creative element is to ensure that the process is proactive, and not confined only to hazards that have materialized in the past. It typically consists of structured group reviews aimed at identifying the causes and effects of accidents and relevant hazards. Consideration of functional failure may assist in this process. The group carrying out such structured reviews should include experts in the various appropriate aspects, such as navigational aid design, and specialists to assist in the hazard identification process and incorporation of the human element. A structured group review session may last over a number of days. The analytical element ensures that previous experience is properly taken into account and typically makes use of background information (for example applicable regulations and codes, available statistical data on incident categories and lists of hazards to personnel, hazardous substances, ignition sources, etc.).

A coarse analysis of possible causes and outcomes of each accident category should be made using standard techniques that are chosen according to the problem under review.

B.1.4.1 Types of Hazards

In general terms, five types of hazards generate risks:

a. natural hazards such as floods, wind storms, earthquakes, biological hazards, and other natural phenomena;
b. economic hazards such as inflation, depression, and changes in tax and fee levies;
c. technical hazards such as system or equipment failure, fire, explosion, obsolescence, and air/water pollution; and
d. human factors such as errors or omissions by poorly trained persons or fatigued persons, or acts of willful negligence, sabotage or terrorism.
e. operational hazards such as groundings, collisions, strikings and other unwanted events.

B.1.4.2 Types of Loss

The five types of hazards have the capability to generate seven different types of loss:

a. health losses include death and injury;
b. property losses including real and intellectual property;
c. economic losses leading to increased costs or reduction to revenues;
d. liability loss resulting when an organization is sued for an alleged breach of legal duty, such cases must be defended even if no blame is assigned. Liability losses are capable of destroying or crippling an organization;
e. personnel loss when services of a key employee is lost;
f. environmental losses (negative impact on land, air, water, flora or fauna); and
g. loss of reputation or status.

B.1.4.3 Hazard Identification

Hazard identification can be summarized in terms of three sub-tasks:

a. structured and comprehensive consideration of known sources of hazards or initiating events, usually identified by reviewing past incidents and losses;
b. brain-storming by a team that understands all aspects of the system under consideration. Led by a team leader, this includes following the structured list of hazards to identify how a hazard might lead to a risk; and
c. preliminary assignment of frequency and consequence to the risk scenarios. This task is useful in assisting the decision-maker in selecting those scenarios to be analyzed further in the Risk Estimation Step (for action or a more detailed estimation of frequency and consequence), and for those risk scenarios to be set aside.

B.1.4.4 Major Contributors to Risk

Care should be taken to ensure that the list of hazards including items such as failure of Management to have adequate change management procedures; lack of investigation and follow-up when process failures occur; the lack of an incident investigation protocol within the organization, etc.

B.1.5 Incorporation of the Human Element

The human element is one of the most important contributory aspects to the causation and avoidance of incidents. Human element issues should be systematically treated within the Risk Management framework, associating them directly with the occurrence of incidents, underlying causes or influences. Appropriate techniques for incorporating human factors should be used.

B.1.6 Risk Identification

Risk may be established by using the identified hazards and a variety of means, including:

a. failure mode and effects analysis;
b. analysis of historical incident data, utilizing existing experience and reports if possible;
c. fault-tree analysis;
d. event-tree analysis;
e. hazard and operational studies;
f. professional judgement (of internal and external experts); and
g. personal observation (e.g., site visits).

Because most issues are quite complex, it is unlikely that all risks will be identified. There will usually be some risks that will only be identified following an incident.

B.1.7 Results

The output from Step 1 comprises:

a. prioritized list of risks/hazards/unwanted events; and
b. preliminary description of the risks/hazards/unwanted events.

B.2 STEP 2 – ASSESS RISKS

Risk assessment is assumed to include two major sub-activities, risk estimation and risk evaluation.

B.2.1 Step 2a – Risk Estimation

B.2.1.1 Scope of the Risk Estimation Sub-Activity

In this step of the decision process, the frequency and consequences associated with each risk scenario selected for analysis are estimated.

B.2.1.2 Methods for Estimating Frequency and Consequences

The first step in this process is to identify the method or methods that will be used for any analyses. The estimates should be based on historical data, models, professional judgement, or a combination of methods. Preferably an established scientific or statistical protocol should be followed. It is necessary to explicitly define these applied methods to avoid conflict between technical experts and laypersons when judging the technical merit of the results. The choice of method will reflect the accuracy needed, cost, available data, the level of expertise on the team, and the acceptability of the method to stakeholders.

It is essential that technical experts clearly explain the methods that will be used in the technical analyses. It is not necessary that laypersons understand these methods in detail, as long as they know that they can have the analyses reproduced and vetted by their own experts. The process should be open and transparent at all times to build trust between decision-makers and other stakeholders, and provide confidence in the results.

Methods For Estimating Frequency and Consequences (i.e., risk or expected loss)

There are a number of methods and associated measures that are used to estimate risk/expected loss (i.e., the combined effect of the frequency and consequences of hazards or unwanted events)

a. Monetary Estimates

Technically, risk is defined as the likelihood (chance, probability) of an unwanted event or hazard times its impact (consequence).[1] Such a product produces an estimate of the expected or likely losses associated with the unwanted events or hazards. If the probability is expressed as a frequency of occurrence, for example, the mean number of occurrences per year, and the impact, given that it occurs, is expressed in monetary terms, then the product yields the mean expected or average monetary loss per year. For example, if it is estimated that one grounding would occur

[1] While, technically, risk is defined as probability x impact, the term risk is also commonly used to refer to the unwanted event itself, which is defined formally as a hazard.

once every ten years, on average, and that it would produce losses totaling $500,000 each time it did occur, the average expected loss would be $50,000 per year ($500,000/10 years).

b. Count Estimates

It is not always easy to estimate possible losses in monetary terms, however. Sometimes, simple physical loss counts are more appropriate. For example, where monetary values are difficult to assign to wildlife losses, it is sometimes easier to simply estimate the number of individuals that could be lost each year.

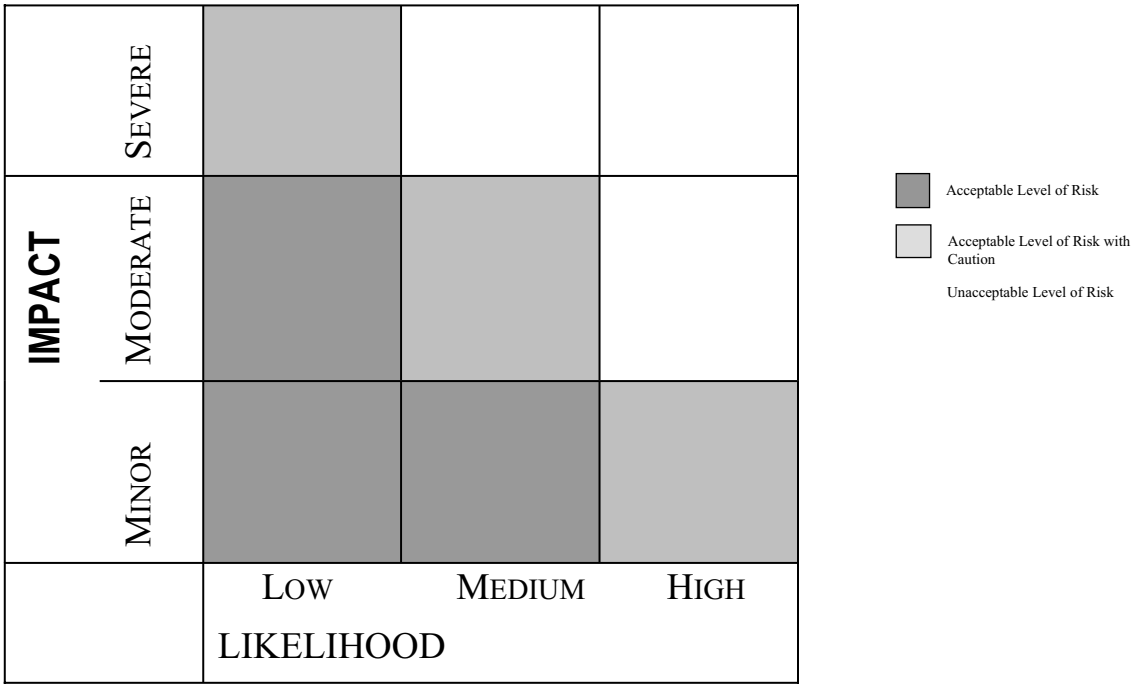
c. Risk Matrix Estimates

Even more often, resort must be made to assigning relative scores to the frequency and consequences associated with the identified hazards (e.g., low, medium, high) and plot these on a risk matrix – see Figure B.1. Usually, these assessments must be based on intuition, experience and expert knowledge where no data are available or quantitative analysis is not warranted (e.g., where the risk is expected to be low).

d. Index Estimates

Sometimes it is possible to compute an index for different waterway areas of interest such that the index represents the relative rank of the risk in these areas (i.e., the combination of frequency and consequences). This index approach is often called *Multi-Criteria Decision Analysis (MCDA)* and is commonly used to order complex RFPs, alternate policies, options and strategies. Risk index values for given waterways can then be compared to study area expenditures and potential anomalies identified.

FIGURE B.1: RISK MATRIX



B.2.1.3 Third-Party Review

Having technical analyses reviewed and validated by trusted outside experts lends further credibility to the results. Universities and government agencies tend to be trusted because of the public perception that they are independent and, therefore, unbiased. It is important for the decision-maker to understand whom stakeholders trust vis-à-vis the particular issue being considered. This is accomplished through dialogue with stakeholders and is an important component of the stakeholder analysis.

It is recommended that a formal third-party review be used to confirm the integrity of the analysis process. This review can be accomplished using internal or external resources, depending on the situation, but not by the analysts themselves. For example, it can save the organization embarrassment if analyses are vetted internally for accuracy prior to the information being given to outside stakeholders. It may also be necessary to have the analyses vetted by some credible external body as a matter of policy, and especially if trust is an issue for stakeholders.

B.2.1.4 Validation

Validation should include the following steps:

a. checking that the scope is appropriate for the stated objectives;
b. reviewing all critical assumptions and ensuring that they are credible in light of available information;
c. ensuring that the analysts use appropriate models, methods, and data;
d. checking that the analysis is reproducible by personnel other than the original analyst(s);
e. checking that the analysis is not sensitive to the way data or results are formatted; and

f. checking to ensure that all assumptions and uncertainties associated with the estimation process have been acknowledged and documented.

Analysts should ensure that all analyses and methods employed by technical experts are fully documented and explained. A distinction should be made between estimations based on related historical data and those based on derived models.

B.2.1.5 Estimating Frequency

The purpose of frequency analysis is to determine how often a particular scenario might be expected to occur over a specified period of time. These estimates are often based on historical data, where judgements about the future are based on what has occurred in the past. If there are no relevant historical data available, or if these data are sparse, other methods such as fault-tree, or event-tree analysis, or other mathematical or econometric models may be used. Estimates may also be based on expert experience and judgement. Most often, frequency estimates are based on a combination of these methods.

What usually results from this analysis is an expected range of frequencies with some estimate of uncertainty, rather than a single number.

B.2.1.6 Estimating Consequences

Consequence analysis involves estimating the impact of various scenarios on everyone and everything affected by the activity. The impact of the consequence on the needs, issues, and concerns of stakeholders is the consideration, and it should be noted that consequences could be both negative and positive.

Consequences are often measured in financial terms, but they can also be measured by other factors: numbers of injuries or deaths, numbers of wildlife affected, impact on quality of life or on lifestyle, impact on an organization's reputation, and others. The benefit of measuring consequences in financial terms is that it provides a common measure for comparing dissimilar conditions. Another strong benefit of using a monetary measure is that it motivates decision-makers to take action.

It should be noted that non-financial consequences, especially loss of reputation, could be much more damaging to an organisation than initially thought. It is important to try to quantify these types of consequences.

There are numerous scientific and statistical methods available for making these estimates of frequency and consequence, and the literature associated with estimation technologies is extensive. It is recommended that the decision-maker employ a technical expert or experts familiar with these techniques.

B.2.1.7 Presenting Frequency and Consequence Estimates

Sometimes data resulting from frequency and consequence analyses are presented separately, but often the results are combined (multiplied together) in what is termed the expected value of the loss. The expected value of the loss is often used to compare one risk to another and is also

incorporated in the analysis of the benefits of risk control options. The expected value of the loss can give some indication of how much should be spent on risk control to correct a situation. For example, if the expected loss is $1,000 per annum, it is probably not prudent to spend $10,000 per annum to reduce it. The expected value also provides a baseline from which to measure the performance of risk control strategies. A measures of the change in expected value, brought about by control measures, is compared to the cost of implementing the control option. In this case, the change in expected value acts, in a benefit/cost analysis, as a measure of the benefit of the risk control option. It is beneficial to include an economist on the team to perform these and other economic analyses.

B.2.1.8 Results

The output from Step 2a comprises:

a. the expected range of frequency with an indication of uncertainties; and,
b. the potential consequence of the risk.

B.2.2 Step 2b - Risk Evaluation

B.2.2.1 Scope of the Risk Evaluation Sub-Activity

The purpose of Risk Evaluation is to identify the distribution of risk, thus allowing attention to be focused upon high-risk areas, and to identify and evaluate the factors, which influence the level of risk.

The risks, as estimated in section B.2.1, are evaluated in terms of the needs, issues, and concerns of stakeholders, the benefits of the activity, and its costs. The result of this exercise is a determination of the acceptability of these risks.

One of three conclusions will result from the risk evaluation exercise:

a. the risk associated with the activity is acceptable at its current level;
b. the risk associated with the activity is unacceptable at any level; or
c. the activity might be acceptable but risk control measures should be evaluated.

If the risk is considered acceptable, then the activity can move forward as proposed and no further action is required. The decision process ends here, although there will still be a need to monitor the activity for possible changes in the risk.

If no level of risk is considered acceptable, and if the activity is not a mandatory or inevitable one, the activity as proposed may need to be abandoned. Again, the decision process ends here.

If the decision is that the activity might be acceptable if the risk can be reduced, then proceed to Step 3 in the decision process and specify risk control options.

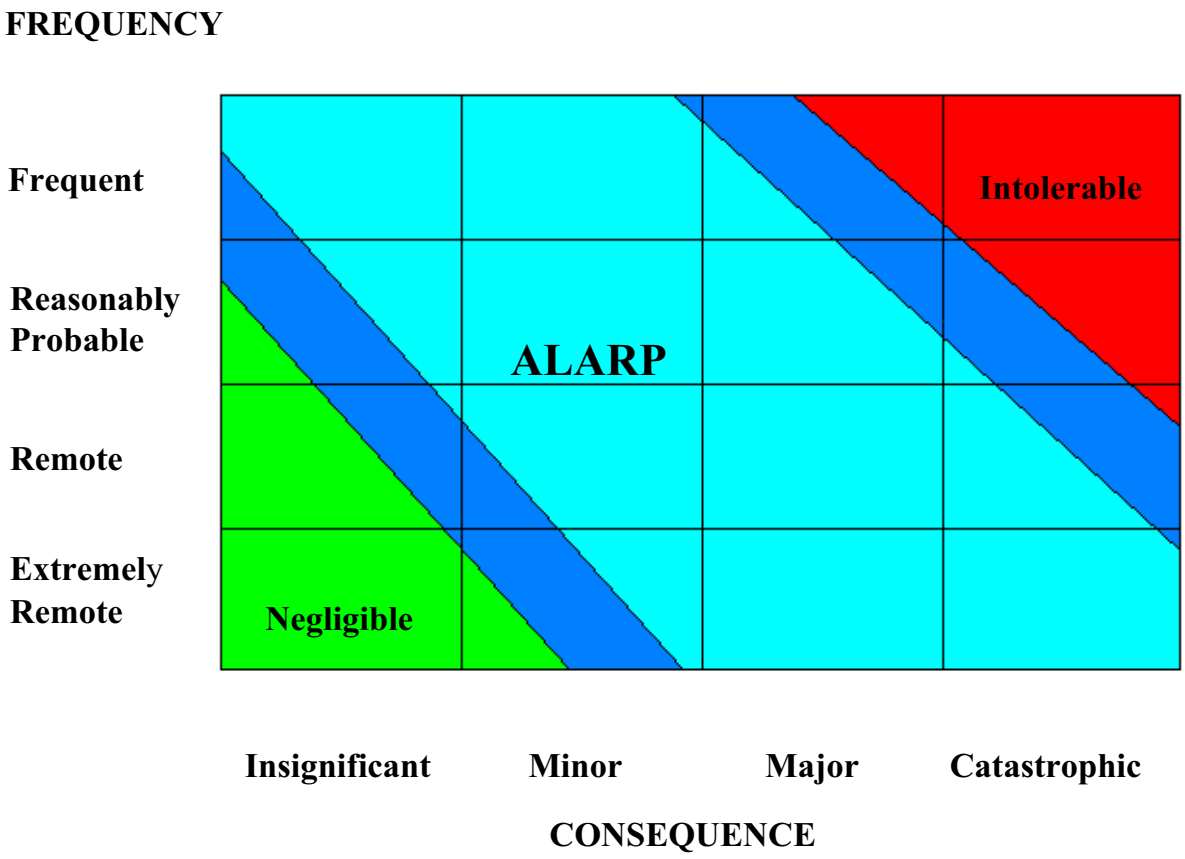
There may be a need to return to a previous step(s) if the current information is deemed inadequate for making decisions about the acceptability of the risk.

B.2.2.2 Acceptability of the Risk to Stakeholders

Once all the risks are assessed they are then evaluated in terms of the documented needs, issues, and concerns of the stakeholders, and the benefits of the activity, to determine the acceptability of the risk.

Zero risk is something that is not often realized, unless the activity generating the risk is abandoned. Rather than striving to reduce risk to zero, Authorities should strive to reduce risk to as low as is reasonably practicable. This concept is known as ALARP (see Figure B.2).

Figure B.2: ALARP Matrix



ALARP = As Low As Reasonably Practicable
Note: Risk level boundaries (Negligible/ALARP/Intolerable) are purely illustrative

B.2.2.3 Risk Perceptions

There are a number of factors, other than expected value of the loss, that effect stakeholder acceptance of risk. This introduces the area of risk perception, that is, what factors affect a person's perception of risk, and how do perceptions affect decision-making around the acceptability of risk?

While experts emphasize technical factors, such as the probability of an event or its consequences on human health or safety, the public emphasizes factors such as:

a. the degree of personal control that can be exercised over the activity - people are less accepting of risks over which they have little or no control (public transportation vs. driving their own car);
b. the potential of an event to result in catastrophic consequences – one versus multiple deaths;
c. whether the consequences are "dreaded" - people are less accepting of risks where the consequences are dreaded; they would prefer to die quickly from a stroke than from a long, painful (dreaded) battle with cancer, although the ultimate consequence is the same;
d. the distribution of the risks and benefits - people accept higher risk if they also receive benefits from the activity (e.g., recreational boating, swimming); they are less accepting of uncompensated loss;
e. the degree to which exposure to the risk is voluntary - voluntarily moving next to a chemical plant vs. having the plant move next to you; and
f. the degree of familiarity with the activity - people are less accepting of risks associated with activities with which they are not familiar (e.g., irradiation of food).

One additional factor is that people tend to accept higher levels of risk if the manager of that risk is trusted. Again, this speaks to the need for effective and open communications with stakeholders to develop and maintain this trust.

An event or issue that is characterized by an extremely low probability may be disregarded by experts because of the low value resulting from an expected-value calculation. However, it may become a major source of concern for the public because of the perceived severity of the consequences and/or because of inequity in the distribution of the associated gains and losses.

Whether a risk is considered acceptable or not is based on stakeholders' needs, issues, and concerns. These needs, issues, and concerns derive from an individual's or organization's basic objectives and values, as well as the social environment within which the individual or organization exists. If people are concerned about the trustworthiness of an organization they may be less accepting of risks associated with these entities.

Influences on Perception of Risk

It is important for the risk management team to remember that, when communicating with stakeholders about risk issues, perception is reality. The public will make judgements of the acceptability of a risk based on its perceptions of the consequences of the risk, rather than on scientific factors like probability.

The public's perception of risk may be influenced by many things, including age, gender, level of education, region, values, and previous exposure to information on the hazard or activity of interest. Public perceptions of risk may differ from those of technical experts. Discrepancies may result from differences in assumptions, conceptions, and the needs, issues, and concerns of stakeholders as they relate to the hazard or activity under discussion.

B.2.2.4 Results

The output from Step 2b comprises:

a. an identification of the high risk areas needing to be addressed;
b. an identification of the principle influences within the overall system that effect the level of risk; and,
c. a determination of whether the risk is acceptable and whether there is a need to reduce the estimated level of expected loss associated with the identified risk.

B3. STEP 3 – SPECIFY RISK CONTROL OPTIONS

B.3.1 Scope

The purpose of Step 3 is to propose effective and practical risk control options, comprising the following three principal stages:

a. focusing on areas of risk needing control;
b. identifying potential risk control measures and their associated costs; and
c. grouping risk control measures into practical regulatory options.

If the decision at the risk assessment step is that the risk is unacceptable and should be reduced, then at the risk control step, options are considered to reduce the risk. The effectiveness of risk control options is evaluated by estimating the risk before and after control options have been applied. The costs, benefits, and risks associated with the proposed control measures, as well as the residual risk, are considered in the evaluation. The residual risk, and any other actions taken to manage the residual risk, should also be evaluated.

The risk control step can proceed in a batch mode or a sequential mode. In batch mode, all of the control options being considered are evaluated in a comparative manner. In sequential mode, control options are evaluated one at a time. The process stops when an option results in an acceptable evaluation of the residual risk and the conclusion that other options are not likely to be significantly better.

B.3.2 Areas Needing Control

The risk control options must be focused on the areas most needing risk control. The main aspects to making this assessment are to review:

a. risk levels, by considering frequency of occurrence together with the severity of outcomes. Incidents with an unacceptable risk level become the primary focus;
b. probability, by identifying the areas of risk that have the highest probability of occurrence. These should be assessed irrespective of the severity of the outcome;

c. severity, by identifying the areas of risk that contribute to high severity outcomes. These should be assessed irrespective of their probability; and
d. confidence, by identifying areas where risk has considerable uncertainty either in risk, severity or probability.

B.3.3 Identifying Risk Control Options

Risk control options are designed to reduce either the frequency of the loss or the consequences of the loss should it occur, or both. It should be remembered that new strategies must be acceptable to stakeholders and that application of control options may introduce new risks, new stakeholders, or new issues.

There are six broad strategies for controlling risk:

a. avoid the exposure altogether, thereby reducing the probability (frequency) of a loss to zero;
b. reduce the frequency of the loss (e.g., through training, ongoing monitoring and maintenance programs, use of higher quality materials);
c. reduce the consequence of the loss should it occur (e.g., emergency response plans and capability, evacuation plans, diking and ditching around hazardous materials containers, wearing protective safety equipment);
d. separate the exposures (e.g., traffic separation schemes, land-use controls around hazardous facilities);
e. duplicate assets, including redundancy in safety systems (e.g., backing up computer records, keeping important materials in several locations, maintaining several suppliers of critical materials, arranging with other organizations to provide backup capability); or
f. transfer the obligation to control losses to some other party through a contractual arrangement. This is a transfer of the risk and not a risk reduction strategy. The benefits accrue to the organization transferring the risk and not necessarily to other stakeholders.

There is usually more than one control option available to manage a particular risk, and most often control strategies will consist of implementing several risk control options. To be effective, the full range of feasible control options should be considered and evaluated.

B.3.4 Evaluating Risk Control Options

Alternative strategies for controlling risk are evaluated in terms of their effectiveness in reducing losses, the cost to implement the option(s), and the impact of control measures on other stakeholder objectives, including the introduction of new risks or issues.

Until the control options have actually been applied, and results observed, estimates of their effectiveness are conjecture. The same methods used to estimate frequency and consequence in the risk estimation step can be applied to estimate the potential change in these parameters expected to result from the application of risk control measures: historical data, fault- and event-tree analysis, professional judgement, etc. As with other estimates, all associated assumptions and uncertainties should be acknowledged and documented.

Not only should control measures be effective in reducing risk, they should also be cost-effective. The cost of the control measure should not normally exceed the reduction in the expected value of the loss.

Implementing a control option may also generate new risks. The new risk scenario generated by the control option should be assessed like other scenarios, beginning with the risk assessment step.

In general, preferred risk control options are those that cost the least, effect the greatest reduction in losses, and create the least adverse side effects.

B.3.5 Costing Risk Control Options

The control options identified above must now be costed – whether they are intended to reduce risk and therefore most likely to cost the program more, or whether they are intended to save money and likely to maintain/increase risk.

The cost of an option should be evaluated over a timeframe equivalent to the economic or useful life of the facilities and assets associated with the option. Because most options involve assets with differing economic lives, it is usually recommended that the analytical time frame be set to the useful life of the most durable assets. However, some assets, such as civil works, can perform satisfactorily for 40 years, a timeframe that is unnecessarily long. Because most electronic and other equipment has a useful life in the 10 to 15 year range, 15 to 20 years appears to be a reasonable timeframe for analysis, with adjustments made for any residual asset values at the end of the period.

Option costs must cover capital, labour and other resources needed for planning and implementation, as well as costs related to the maintenance and operation of the option throughout the life-cycle period under review. In other words, those costs that would be avoided if the option were not to proceed should be included, no matter who incurs them.

Past expenditures, which are not affected by an option, are not relevant and can be regarded as "sunk" costs, provided they have no opportunity cost (alternative use). Land or a building in a remote location that is already owned but with no alternative use could be considered a "sunk" cost. However, the same land or building in a metropolitan area, which has an alternative use, would have to be costed at the value of this alternative use.

Costs can be divided into three broad categories:

a. Planning Phase
   This category includes all costs incurred prior to procurement, construction, or implementation. Typical costs would include those related to planning, engineering and design, including costs related to a project team.

b. Construction/Development
A large number of costs items will be involved at this stage. They could include some of the following (as well as others):

- Land acquisition and/or the opportunity cost of land already held.
- Construction costs (related to both new and existing facilities).
- Aids to navigation and other equipment purchases, including spares.
- Other capital expenditures.
- Training related to implementation.
- Moving expenses.
- Other start-up costs.

c. Operational Phase
Once the option is in place, an estimate must be made of its life-cycle costs. These could include:

- Salaries (including regular wages, overtime, bonuses, allowances and fringe benefits).
- Maintenance of equipment, electronics and civil works.
- Periodic capital outlays (such as mid-life refits)
- Operating expenses (e.g. removal and placement of aids to navigation).
- On-going training.
- Lease costs (landlines, etc.).
- Other O&M costs.

Costs should be recorded in a spreadsheet format, with a column representing each year in the life-cycle period, and rows representing cost items. Discounting, using appropriate rates, should be applied in order to treat all costs, whether incurred early or late in the planning period, in an equitable manner.

B.3.6 Assessing Stakeholder Acceptance

Before risk control decisions are made, they should be communicated through the stakeholder consultation process. A proposed option may appear acceptable to the decision-maker, in terms of its effectiveness and costs, but may be unacceptable to other stakeholders because of other factors. There is a need to evaluate any proposed control or financing strategy in terms of the needs, issues, and concerns of affected stakeholders.

B.3.7 Residual Risk

Any risk left after the implementation of risk control options is termed residual risk. The residual risk must be evaluated by returning to the risk assessment step, to determine if it is acceptable. If

the residual risk is not acceptable, then the activity may need to be abandoned, or alternative risk control strategies implemented to reduce the risk to an acceptable level.

One means of increasing acceptability is to increase the benefits associated with the activity. The risks are evaluated in terms of the overall needs, issues, and concerns of stakeholders. Therefore, if concerns about risk can be balanced against gains in other areas of stakeholder interest (greater income, cleaner water, fewer incidents, etc), then the activity may be seen as acceptable.

Determining the level of acceptable risk is best achieved through effective dialogue with stakeholders. In deciding whether or not a risk is acceptable, it may be useful to determine whether the risk:

a. is so great or the outcome so unacceptable that it must be refused altogether;
b. is, or has been made, so small as to be negligible; or
c. falls between (a) and (b), and it has been reduced to the lowest achievable or practicable level.

B.3.8 Results

The output from Step 3 comprises:

a. a range of risk control options, along with their costs, which are assessed for their effectiveness in reducing risk;
b. a list of factors and stakeholders affected by the identified risk control options; and
c. the residual risks deemed acceptable to the stakeholders.

B.4 STEP 4 – MAKE A DECISION

B.4.1 Scope

The purpose of Step 4 is to define, in consultation with stakeholders, the recommendations that should be considered. The recommendations should be based upon the comparison and ranking of risks and their underlying causes; the comparison and ranking of the risk control options as a function of associated costs and benefits; and the identification of those risk control options which keep risks as low as reasonably practicable (ALARP).

B.4.2 Estimate Option Benefits

The risk-reduction benefits that would be derived from implementing each of the options identified and costed in Activity B.3 above must now be estimated. This is probably the most difficult and problematic activity of the entire risk management process.

If the current levels of risk in the area of interest were estimated in terms of annual expected monetary losses, then it must be determined what proportion of this existing risk is eliminated by each option (in order to calculate a monetary benefit for each option). Conversely, if it is proposed to eliminate aids to navigation or reduce availability or otherwise reduce service levels, then it must be determined by what proportion existing risk is increased (in order to estimate the monetary value of the increased risk). Once determined, comparisons of the monetary value of the program risk change to the cost or savings resulting from the option can be made (as discussed in B.4.3 below).

In most cases, however, it will only be possible to say whether or not the option produces no change in risk levels, increases/decreases it somewhat, significantly and so on. In this case, where it is possible only to project a non-monetary value to changes in the aids to navigation addressable risk, it becomes more difficult to evaluate the net societal benefit/cost of the option(s). If an option is projected to save the aids to navigation program $1,000,000 per year, and it has been determined that no change in risk will follow, the net benefit to the option is $1,000,000. But, if it has been estimated that risk will increase marginally or somewhat, what is the value of this increase? Threshold analysis can be used here to help answer this question.

A threshold analysis is designed to establish the amount of benefit required to make any particular option cost-beneficial. In using this technique, a judgement is required on the likelihood that the benefit would exceed these thresholds. These thresholds are also known as “switching values”, because they are the values at which the decision could switch from one option to another.

For example, let us assume that the studies have identified three options that will cost, respectively, $1,000,000, $800,000 and $500,000 annually. In threshold analysis, expert opinion

must be used to determine firstly, if each option is likely to reduce annual risk by at least annual costs, and secondly, which of the options will produce the greatest return.

B.4.3 Compare Costs to Benefits and Make a Decision

When monetary estimates of benefits and costs are available, discounting can be used to rank options in terms of benefit/cost ratios, net present values, and so on. Where monetary estimates of the benefits are not directly available, threshold values can be used to at least rank the options. Even so, balancing estimated risk-reduction benefits against option costs is never straightforward. Society usually demands more risk-reduction effort where human life and health are at risk than where only property is involved; and the public usually demands a high level of effort be expended to prevent environmental damages. Public perception of the risks involved often plays as much or more of a role as does the actual estimate of the expected losses.

Balancing risk-reduction benefits against risk-reduction costs is an important issue today. In a risk-averse organizational setting, people minimize expected losses, to the extent possible, irrespective of the probability or impact of the risk. In a risk-taking environment, people compare expected risk-reduction benefits to the cost of the initiative which would produce these benefits. They take actions that would optimize the overall benefit to society (keeping in mind the type of losses involved, whether associated with life, health, property, the environment, revenue, etc.). A risk-smart organization does not simply take more risks, however, it takes calculated risks that optimize the benefits derived from its risk-reduction activities.

It is important here to consider more than the obvious, hard, financial benefits and costs of the activity. There may also be a number of associated indirect benefits and costs that may not be readily recognized - for example, ecosystem health, sustainable development, employment benefits or other spin-off benefits. These so-called soft benefits and soft costs should also be considered, in the Risk Assessment process.

It is important that both direct and indirect effects of an activity be considered and factored into any analysis of acceptability. The use of a multidisciplinary risk management team, coupled with an extensive consultation program, may aid this effort.

In summary, the following considerations are usually involved when comparing benefits and costs,:

a. consider the risks assessed, both in terms of frequency and consequence, in order to define the base case in terms of risk levels of the situation under consideration;
b. arrange the risk control options in a way to facilitate understanding of the costs and benefits resulting from the approval of an option;
c. estimate the pertinent costs and benefits for all risk control options;
d. estimate and compare the cost effectiveness of each option, in terms of the cost per unit risk reduction by dividing the net cost by the risk reduction achieved as a result of implementing the option; and
e. rank the risk control options from a cost-benefit perspective in order to facilitate the decision making recommendations.

B.4.4 Results

Output from Step 4 can provide an objective comparison of alternative options, based on potential reduction of risks and cost effectiveness. Recommendations should be easily usable by decision-makers at all levels, in a variety of contexts, without a requirement for specialist expertise. This step should also provide feedback information for reviewing the results generated in the previous steps.

B.4.5 Presentation of the Results

To facilitate the common understanding and use of the Guidelines, a report should be produced that:

a. provides a clear statement of all recommendations;
b. lists the principle hazards, risks, unwanted events, costs and benefits identified;
c. explains the basis for significant assumptions, limitations, data models and inferences used or relied upon in the assessment or recommendations;
d. describes the sources, extent and magnitude of significant uncertainties associated with the assessment or recommendations; and
e. describes the composition and expertise of the group that performed the risk management process.

Timely and open access to relevant and supporting documents should be provided. A reasonable opportunity to incorporate comments should also be provided.

B.5 STEP 5 – TAKE ACTION

B.5.1 Scope

The purpose of Step 5 is to implement the chosen risk control option or options; evaluate the effectiveness of the decision process; and to establish a monitoring and evaluation program to monitor the outcome of implementation (an explicit decision to take no action constitutes action as defined here). If a decision were taken to implement a new risk-reduction process or control, then the usual planning and implementation activities necessary for the introduction of a new activity would have to be undertaken. Monitoring, reporting, communication and review must be planned and introduced. It is equally important to periodically review all existing risk-reduction activities to ensure that they are still relevant and beneficial. Furthermore, an Authority must always be aware of residual risk, and if appropriate, loop back in the process to determine if it should be further reduced.

B.5.2 Implementation Plan

Prior to implementing any of the chosen risk control options, it is important to develop an implementation plan. In the organization's implementation plan, the decision-maker should consider the technical decisions that need to be made in order to execute chosen strategies (e.g., the timing of implementation, resource availability, technical decisions to set up monitoring programs). Managerial decisions that are made in co-operation with other managers and staff also need be considered (e.g., training requirements, staffing requirements, job shifting or new positions, financing requirements).

B.5.3 Implementation

During implementation, selected risk control options are implemented, and the stakeholder outreach, dialogue, media contact, and key messages are delivered using contacts developed throughout the risk management process. A broader public communication effort (e.g., through the media and community meetings) may be necessary in order to facilitate delivery of messages related to the decisions being made and implemented.

B.5.4 Monitoring

B.5.4.1 Primary Functions

Monitoring is a key function of the risk management process and has four primary functions:

a. to detect and adapt to changing circumstances;
b. to ensure that the risk control options are achieving the results expected of them;
c. to ensure proper implementation of control and communication strategies; and

d. to verify the correctness of assumptions used in the various analyses.

B.5.4.2 Changing Conditions

When monitoring for changes in the system, six broad issue categories should be considered:

a. the environment in which the activity takes place, including the regulatory environment;
b. the potential losses to health, property, income, the environment, etc;
c. the hazards causing the losses (natural, economic, technical, human);
d. the acceptability of the losses (a function of needs, issues, and concerns);
e. stakeholders; and
f. new technology.

A change to one or more of these parameters changes the risk. Hazards often change with the seasons and there may be a need for ongoing seasonal adjustments.

Over a time, the value (market or replacement) of assets may change, either rising (due to inflation) or falling (due to depreciation or obsolescence). These changes in the value of assets will affect the consequence of a loss should it occur, and there may be a need then to change control and financing strategies.

New technologies may be made available that affect the choice of risk control, or communication strategies.

Any changes to these factors may necessitate a return to the Risk/Hazard Identification step if new issues result. Stakeholders may also change, and will need to be kept informed about the ongoing risk management program.

B.5.4.3 Monitoring Performance

To ensure that the risk management program, including specific control measures, is effective in achieving the results expected of it, the decision-maker should:

a. establish standards of what constitutes acceptable performance;
b. compare the actual performance of the program against these established standards; and
c. make corrections for substandard performance.

Performance standards may be goals the organization wishes to achieve, such as a 50% reduction in incidents within two years. The realized incident rate is compared to the goal to determine whether the program was successful. If actual performance does not meet the established goal, it may mean that the goal was too high (or too low), or that some new control strategy may need to be considered.

If performance is less than expected, before developing new strategies, it is best to ensure that the chosen strategy has been implemented properly. Improper implementation is often the cause of substandard performance.

B.5.4.4 Correctness of Assumptions

Assumptions are guesses about what may happen in the future and, as such, are subject to varying levels of uncertainty. It is important that all assumptions used throughout the analysis be verified where possible. If the assumptions prove correct, this lends strength to the decisions arising from the process. If assumptions prove not to be valid, then the analysis may need to be redone.

Assumptions should be routinely reviewed to avoid costly mistakes. The monitoring function should be an ongoing responsibility for the risk management team, providing for continuous improvement within the risk management program.

The financial and non-financial benefits of monitoring include:

a. the identification of new or changing risks:
b. the accumulation of evidence to support assumptions and results of analyses;
c. the development of a more accurate portrait of the risks; and
d. reduction in costs associated with improper or redundant implementation of risk control measures.

B.5.4.5 Timing

All risk management strategies should be reviewed periodically. Sometimes a "sunset" date is established, where a particular control option, such as a regulation, will cease to exist unless extended. Extension requires an analysis to justify the continuation of the control option. If no justification can be established, the control option is terminated. "Sunsetting" aids in ensuring that ineffective or unnecessary actions are not continued indefinitely.

B.5.5 Risk Management Decision Process Evaluation

After having undergone the extensive decision process, it is prudent to evaluate the effectiveness of the risk management process in satisfying the objectives of the decision-maker. This facilitates continuous improvement in the decision-process itself, creating efficiencies for future efforts.

This review also provides for greater defensibility of decisions made throughout the process.

ANNEX I – RISK TERMINOLOGY

Aid to Navigation – any device or system, external to a vessel, which is provided to help a mariner determine position and course, to warn of dangers or of obstructions, or to give advice about the location of a best or preferred route.

Benefit-Cost Analysis – an approach, used to assess the gains and losses resulting from a set of alternative actions, that helps one decide whether any of the actions should be undertaken.

Decision-maker - a person or group with the power or authority to make decisions.

Dialogue - a process for two-way communication that fosters shared understanding. It is supported by information.

Hazard/Risk – an unwanted event or occurrence, a source of potential harm, or a situation with a potential for causing harm, in terms of human injury; damage to health, property, the environment, and other things of value; or some combination of these.

Hazard/Risk Identification -the process of recognizing that a hazard or risk exists and defining its characteristics.

Loss - an injury or damage to health, property, the environment, or something else of value.

Organization - a company, corporation, firm, enterprise, authority, agency or institution, or part thereof, whether incorporated or not, public or private, that has its own functions and administration.

Residual risk - the risk remaining after all risk control strategies have been applied.

Risk - the chance of injury or loss as defined as a measure of the probability and severity of an adverse effect to health, property, the environment, or other things of value.

Risk acceptance – a decision to accept a risk.

Risk assessment – as used here, it is meant to include the overall process of risk estimation and risk evaluation.

Risk consultation - any two-way communication between stakeholders about the existence, nature, form, severity, or acceptability of risks.

Risk control option - an action intended to reduce the frequency and/or severity of injury or loss, including a decision not to pursue the action.

Risk control strategy - a program that may include the application of several risk control options.

Risk estimation - the activity of estimating the frequency or probability and consequence of risk scenarios, including a consideration of the uncertainty of the estimates.

Risk evaluation - the process by which risks are examined in terms of magnitude and distribution, and evaluated in terms of acceptability considering the needs, issues, and concerns of stakeholders.

Risk management - the systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and communicating about risk issues.

Risk perception - the significance assigned to risks by stakeholders. This perception is derived from the stakeholders' expressed needs, issues, and concerns.

Risk reduction – actions taken to lessen the frequency, negative consequences, or both, of a particular risk.

Risk retention – acceptance of the expected loss associated with the consequences of a particular risk.

Risk scenario - a defined sequence of events with associated frequencies and consequences.

Stakeholder - any individual, group, or organization able to affect, be affected by, or believe it might be affected by, a decision or activity. The decision-maker(s) is a stakeholder.

ANNEX II – INFORMATION AND DATA

Vessel Traffic Services:

- The maritime traffic (safety and efficiency of maritime traffic).
- Volume and mix of traffic.
- The local conditions in the maritime area concerned (e.g.: geography, hydrography, tidal conditions, weather conditions).
- Protection of the marine environment.
- Protection of the surrounding area.

Maritime Traffic

Traffic statistics to be obtained:

- Traffic safety record in general.
- The number of vessel traffic movements in the area (or part of the area) concerned, including trends in the number of vessel movements, based on data covering the past 3-5 years at least.
- The break-down of vessel traffic in types and sizes of vessels and categories of cargoes carried, including navy and/or other Government owned vessels, fishing vessels, recreational craft, local ferries, sea going or inland high speed craft, inland craft/barges, tugboats, pilot tenders and other service craft, etc.
- Complexity of the traffic pattern.
- Vessels with hazardous cargoes as defined in IMO Res. A.857(20), Annex- 1, para. 1.1 under.11.
- Is there any (statistical) information available on the above five bullet points?
- Are there any recent traffic surveys and an evaluation of these surveys available?
- Does any ship-to-ship cargo transfers take place in or in the proximity of the fairway either at anchor or moored to buoys and do these activities interfere with the safe and efficient flow of traffic? If so, is it possible to quantify this interference?
- If appropriate, is there any interference by vessel traffic with other marine based activities?

Accident data to be obtained:

- Is there an up-to-date and complete record, covering a period of at least 5 years, available on accidents or incidents with vessels in the area, including information on the economic consequences?
- Were thorough accident and incident investigations performed and by whom?
- What are the main recorded causes of the accidents and incidents?

- Are there any "black spots" in relation to these accidents and incidents?
- Where recommendations were contained in reports on accidents and incidents, were these recommendations implemented in full or only in part or not at all?
- Is any information available on the mariners or navigators opinions regarding traffic safety in the area concerned?
- Is any other relevant data on accidents or incidents available?
- In some areas the number of small local craft, usually without any capability to communicate by radio to a VTS or to other vessels, is very high compared to the other traffic. In addition, this local traffic may show "remarkable" behaviour and may not be aware of navigational limitations of larger power-driven vessels. If this is the case, it might be necessary to develop, implement, promulgate and maintain (or enforce) special local rules to ensure the unobstructed and safe passage of the (larger) commercial vessels.

The human element is one of the most important contributory aspects to the causation and avoidance of accidents or incidents. Human element issues throughout the "integrated system of safe and efficient traffic management", within a sound environmental content, should be systematically treated within the risk assessment methodology to be used, associating them directly with the occurrence of accidents, underlying causes or influences. Appropriate techniques for incorporating human factors should be used.

Data on traffic delays to be obtained:

- Efficiency of maritime traffic in general.
- Are there any traffic delays?
- What are the main causes?
- Are there any specific locations in the area concerned where congestion occurs regularly?
- Is there a relation or relations between this congestion and the number of vessel movements and/or with specific conditions in the navigable waters in the area and with any black spots as mentioned above?
- What is the view of shipping companies and mariners regarding the efficiency of traffic?
- Are there any complaints and, if so, how are these handled and addressed?
- Is it possible to quantify the additional costs to the maritime industry, to port operations, onward transport of goods and late delivery of cargoes as a result of congestion and delays?
- Is any other relevant data on efficiency of traffic available?

The maritime area concerned.

The geography of the area:

- Provide an outline of the maritime area concerned.
- Describe the area in terms of its geography, e.g. narrow and winding fairways, port basins, piers, quays along the fairway.
- Shallows shifting shoals.
- Specific navigational hazards.
- Geology of the sea/estuary/bottom and shoreline.
- Stability of the bottom profile.
- Dredging operations in the fairway.
- Locks, including their operations.
- Bridges with restricted air-draught.
- Climatic conditions (prevailing winds, fog, ice conditions).
- Tidal conditions, negative surges, currents.
- Hydrological/meteorological conditions.
- State of hydrographic surveys.

Analyze the data on the geography of the area concerned thoroughly.

Data on present traffic management resources:

- National or IMO adopted ships' routing measures, including if appropriate associated rules and recommendation.
- Conventional aids to navigation,
- Differential GNSS and if appropriate, LORAN-C/Chayka.
- Number, size and location of anchorages, including not only a description of the use of these anchorage(s) by vessels but also reasons for vessels anchoring and the average duration of vessels being at anchor). Is any information available on the quality of the holding-ground in the anchorage's? Are there any specific local rules" applicable for vessels using the anchorages?
- Pilotage, including disembarking locations; and how are the pilots transferred?
- Ship reporting requirements, availability of adequate tug assistance.
- Local navigation rules and recommendations in the area.
- Any other relevant instruments and information.

Protection of the marine environment.

The following items should be addressed:

- Is the area concerned, or part of it, a formally declared "Particular Sensitive (Sea) Area" based on either IMO Res. A.720(17)[, as amended] 14, or regional/national legislation?
- Is there such a sensitive area regardless of the formal status of that area in the proximity where, due to the prevailing wind and current conditions, any marine pollutants, as a result of shipping accidents or incidents, may end up.
- Is the wider area an important fishing ground in particular for local fishermen? Are there any fish farms? Is it possible to quantify these interests to some extent?
- Is there any other formal protection of the area based on international, national or local rules and regulations; e.g. "special area" under MARPOL Annex I?
- Are there any records available concerning marine pollution because of shipping accidents or incidents and the resulting damage to the environment, in terms of clean-up costs, dead birds and other wildlife and e.g. damage to fish stocks?
- Is there an established national or regional policy on the protection of the marine environment?
- Is there any criteria set regarding pollution in that national and/or regional policy?
- What is the attitude of the general public on the environment issue and the marine environment in particular?
- Is a pollution abatement or an emergency response organization available on short notice?
- Is sufficient equipment and qualified manpower available on short notice to fight an accidental pollution of any substantial size?
- Is the protection of the marine environment in the wider area as such, considered to be sufficient reason that it warrants the implementation of a VTS? If not,
- Is it possible to categorize the importance of the protection of the marine environment in the wider area?
- Protection of the environment is very often a matter of national priority. This priority should be considered along with other relevant considerations.

Protection of the surrounding area.

Protection of bridges and other works, work-sites, protection of human life and infrastructure in urban and/or industrial areas in the proximity of busy fairways is very often a valid reason for attempting to counteract against/abate the possible negative effects of maritime traffic by implementing a VTS or improving existing traffic management resources.

- Is any statistical information available on damage, in the widest sense, including loss of human lives, to the surrounding area as a result of maritime accidents or incidents in the area concerned? Is it possible to quantify the consequential costs?
- Is it possible to categorize the importance of the protection of the surrounding area?

ANNEX III

Bay of Fundy Aids to Navigation Availability Assessment

Example Only

The Management Board of the Canadian Coast Guard commissioned Consulting and Audit Canada (CAC) to create a display and risk index computer system containing about 150 columns of marine risk-related data covering 100+ waterways/ports. The data were sub-divided into four categories: *frequency* (e.g., number of cargo vessel movements, number of ferry movements); *impact* (e.g., tonnes of petroleum transported, number of passenger trips); *modifiers* (e.g., visibility, windspeed); and *history* (e.g., vessel groundings, loss of life). The computer system (called ORCA—Oceans Risk & Criteria Analysis) allows a user to automatically display data in barchart, map or scattergram format, and to weight and combine criteria data into a risk index..[2]

The ORCA system was used in this example.

[2] For more details, see *ORCA: Oceans Risk & Criteria Analysis*, Edition II, Prepared by Consulting & Audit Canada for the Canadian Coast Guard, Project No. 570-1411, November, 1998.

B. The Risk Management Process

This example assessment follows the five major steps specified in Section B of the *IALA Guidelines on Risk Management*.[3]

B.1 Identify Risks/Hazards

Canadian Coast Guard (CCG) records for Fundy LOS Area 3 covering Saint John harbour and the upper Bay of Fundy (see Figure 1.1) show that aids to navigation in this

Table 1.1: Navaids Level Of Service History (For Fundy LOS Area 3)

Navaid Importance Rating	Total No. Of Navaids In LOS Area	Number Of Navaids Down In Period	Total Down Occurences	Total Days Down	Avg. Days Down Per Occurrence
1	20	17	106	887	8.4
2	71	56	160	1,231	7.7
3	36	9	13	272	20.9
Total	127	82	279	2,389	8.6

area were not functioning properly on 279 occasions over the last 5 years. As a result, the 82 involved aids to navigation, out of a total of 127, were "down" for 2,389 days (see Table 1.1). The review outlined in this Annex was triggered by the realization that the level of service reflected by this record over the last five years does not meet current objectives.

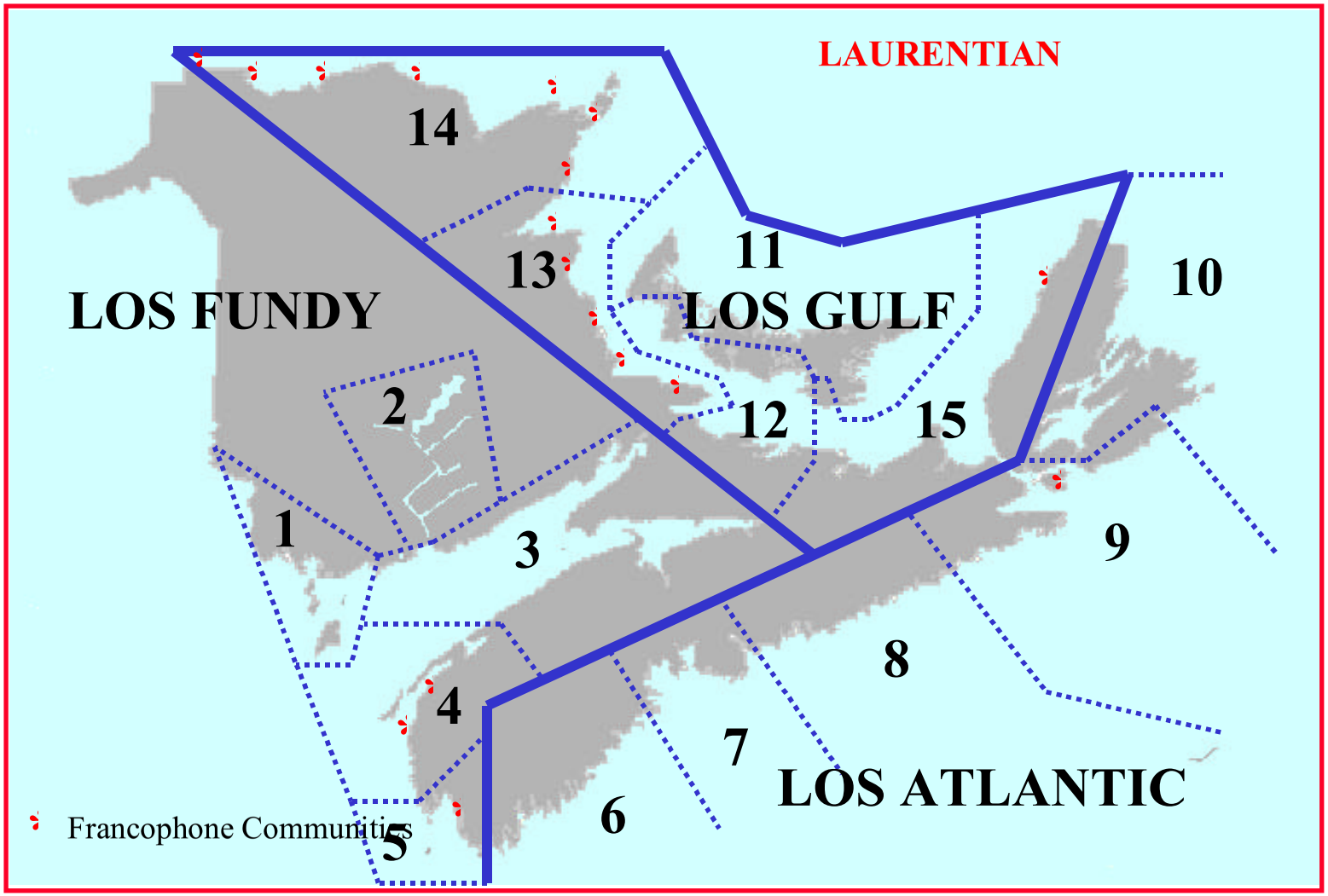
A large number of stakeholder groups use the aids to navigation in LOS Area 3 and would need to be consulted (e.g., operators of ferries, fishing vessels, commercial ships, tugs, port authorities, recreational boaters, environmentalists and so on).

B.2 Assess Risks

Aids to Risk & Criteria Analysis system). A total of 45 groundings were reported to have occurred in our area of interest over the last 25 years. There were no deaths, serious navigation are primarily directed toward the prevention of vessel groundings, although collisions can sometimes be prevented by an appropriate aid to navigation. In this review, however, only groundings as reported by the Transportation Safety Board (TSB) occurring in LOS Area 3 were extracted from the CCG's ORCA system (Oceans

[3] All dollar values mentioned in this example refer to Canadian currency unless otherwise noted.

Figure 1.1: LOS AREAS - MARITIMES



Canadian Coast Guard

Risk & Criteria Analysis system). A total of 45 groundings were reported to have occurred in our area of interest over the last 25 years. There were no deaths, serious injuries, significant spills or serious vessel damages associated with these 45 groundings. Furthermore, after reviewing the circumstances associated with these occurrences, it does not appear that any were caused by a "down" aid to navigation (see Table 1.2).

Table 1.2: Grounding Occurences For 1976 - 2000 (re Fundy LOS Area 3)*

Vessel Type	Total No. Number Of Groundings	Persons Dead Or Missing	Serious Injuries	Groundings Caused By Down Navaids
Barge	1	0	0	0
Bulk Carrier	6	0	0	0
Container Ship	1	0	0	0
Ferry	3	0	0	0
Fishing Vessel	16	0	0	0
General Cargo	3	0	0	0
Research Vessel	1	0	0	0
Tanker	2	0	0	0
Tug / Other	12	0	0	0
Total	45	0	0	0

* As reported by the TSB and recorded in ORCA.

While the 25-year accident history does not indicate any residual risk that should have been addressed by an aids to navigation program, 25 years is still not a long period of time to observe some types of rare but potentially serious accidents – for example, a grounding involving a tanker with associated cargo loss. Thus, we reviewed the annual traffic statistics for LOS Area 3 (see Table 1.3).

Table 1.3: ESTIMATED ANNUAL TRAFFIC (re Fundy LOS Area 3)*

VESSEL TYPE	SAINT JOHN HARBOUR	UPPER BAY OF FUNDY
Barge & Cargo Vessels	1800	200
Cruise Vessels	10	0
Ferries	1500	0
Recreational Vessels	low	low
Fishing Vessels	low	low

* As derived from ORCA.

There are about 1800 barge, cargo, tanker, tug, research and other commercial vessel arrivals and departures each year at the port of Saint John (supertankers are included in this estimate). There are an additional 1500 ferry arrivals and departures for this port. The rest of LOS Area 3 records only about 200 transits per year related to commercial traffic. Recreational activity is low in the LOS area and fishing activity is only moderate when compared to many other LOS areas in the country.

While no grounding during the last 25 years appears to have been caused by a "down" aid to navigation, the traffic statistics shown in Table 1.3 do not preclude the possibility of one occurring over the longer term. Thus, we will continue with this review and look at the benefits and costs associated with some option or options that would address historical service levels in Fundy LOS Area 3.

Estimating Addressable Risk

Risk is defined as the probability of an unwanted event times its consequences. Groundings are the most likely unwanted events that could be prevented by an aids to navigation program. From our discussion above, it is most difficult to estimate the probable frequency of groundings by vessel type that would be caused by the current level of service if it continued into the future. It is easier to estimate the expected consequences of a grounding, given that it did occur, although even this task is problematic. For example, Canadian Coast Guard studies undertaken in the past have estimated the mean impact of a tanker grounding with loss of cargo at nearly $30 million Cdn.[4] The Exxon Valdez was assessed damages amounting to nearly $1 billion US. However, most fishing vessel groundings with no loss of life often exhibit damages in the 100s or 1,000s of dollars Cdn, at most. Thus, we will not attempt to produce an estimate of the expected losses (i.e., risk) that could be caused by the current level of aid outages, but proceed with estimating the cost of an option to improve service levels, and then use "threshold" analysis to draw conclusions about the possible risk-benefit of the proposed option.

B.3 Specify Risk Control Options

Risk Control Options

There are a number of methods that one could use to improve the availability of aids to navigation in Fundy LOS Area 3. For example, one could increase response time in order to reduce the mean number of "down" days by half. Such a solution would likely

[4] For an example application, see *Confederation Bridge VTS Benefit-Cost Analysis*, Prepared by Consulting & Audit Canada for the Canadian Coast Guard, Project 570-1224, May, 1997.

require an additional "1100" series maintenance vessel, costing about $70 million, with attendant increases in personnel costs and other operating and maintenance expenditures. Consequently, this option was not pursued further.

Improved aid to navigation availability could also be achieved by a reduction in the number of "down" occurrences. Most outages associated with floating aids to navigation are related to inadequate anchoring while most outages associated with fixed aids to navigation are related to equipment failures. Thus, it is proposed to improve anchoring and increase equipment reliability.

Control Option Costs

Costs for improving anchoring and equipment reliability were first estimated for each aid to navigation type in the LOS Area (see Table 2.1). For example, three tonne anchors for large floating buoys would be replaced by five tonne anchors at a cost of $9,000 per replacement. These unit improvement estimates were then applied to the number of aids to navigation in each type category to arrive at a one-time cost for this option (again see Table 2.1). Using this method, it is estimated that $1 million dollars would be required to bring aid to navigation reliability to targeted service levels (i.e., future "down" occurrences would likely be reduced by one-half). It could be noted that O&M expenditures for LOS Area 3's 127 aids to navigation are estimated at about $1.4 million per year (the total O&M budget for the Maritimes Region's 5,000+ aids to navigation is around $19 million).

Table 2.1: Reliability Improvement Cost Estimates By Aid Type

Category	Capital Cost Per Navaid ($)	Number Of Navaids	Total Cost ($)
01 -Radiobeacon / DGPS Sites	0	1	0
03b-Major Shore Lights - Unstaffed	30,000	9	270,000
04a-Minor Shore Lights - Small	5,000	8	40,000
04b-Minor Shore Lights - Standard	5,000	9	45,000
04c-Minor Shore Lights - Large	5,000	10	50,000
07b-Radar Reflector*	750	2	1,500
08c-Ranges Lighted - Large	35,000	6	210,000
09c-Sector Light - Large	35,000	1	35,000
10b-Stakes and Bushes*	250	2	500
11- 2.9 m Long Leg Buoy (9 1/2')	9,000	1	9,000
12- 2.9 m Short Leg Buoy (9 1/2')	9,000	27	243,000
14a-Buoys Lighted - 500 to 1000 kg	3,000	1	3,000
14b-Buoys Unlighted - 500 to 1000kg	1,500	11	16,500
16b-Buoys Unlighted - 175 to 500 kg	1,500	15	22,500
17b-Buoys Unlighted < 175 kg	1,000	23	23,000
N/A*	250	1	250
Total		127	969,250

* Yearly costs for five year have been applied here.

B.4 Make a Decision

Option Benefits

As already stated, it is very difficult to estimate the risk-reduction benefit of spending $1 million to reduce "down" time for 127 aids to navigation by approximately one-half. While no groundings appear to have been caused by a non-functioning aid to navigation over the last 25 years, a grounding could be caused by such an occurrence in the future. A grounded tanker would likely produce impacts exceeding $1 million, especially if loss of cargo or bunker fuel were involved; and even the loss of one life would exceed the estimated improvement cost given the value normally placed on a statistical life in these types of analysis. However, the probability of such unwanted events caused by a non-functioning aid to navigation must be very small–no such impacts even resulted from the 45 non-aid related groundings that did occur over the last 25 years in the LOS Area.

Most marine stakeholders would likely conclude that the safety benefits of this option would not exceed its $1 million cost; and perhaps there is a good reason for such a conclusion. When an aid to navigation is "down", a NOTSHIP is issued and mariners then take special care and operate at a heightened degree of awareness for the duration of the outage period. This reaction likely explains why we did not observe any groundings that were caused by "down' aids to navigation over the last 25 years in this LOS area.

Comparing Costs and Benefits

As discussed above, we do not need to further compare an estimated $1 million cost for service improvements to an estimated safety benefit which would likely be significantly less than this amount.

Making a Decision

While the direct safety benefits of reducing aid to navigation outages do not appear cost-beneficial, there are two other issues that could be pursued:

1) Would the long-term reduced maintenance costs resulting from an estimated 50% reduction in aid to navigation outages compensate for the one-time capital investment of $1 million?

2) Should the current level of service goals be revised to conform more to the actual service being delivered in light of the apparent absence of groundings caused by "down" aids to navigation in this LOS area? Perhaps a lower level of service can be tolerated without increased risk as long as only a "reasonable' number of

NOTSHIPS are issued at any one time for a given area? If one cries wolf too many times, all warnings tend to be ignored. Of course, a review of service level standards would require the involvement of all stakeholders from the very beginning.

B.5 Take Action

No implementation of the proposed option for risk-reduction purposes is recommended. However, it is recommended that two additional reviews be conducted as outlined in section B.4 above.