



Fisheries and Oceans
Canada

Pêches et Océans
Canada

INTEGRATED RISK MANAGEMENT (IRM) POLICY

Fisheries and Oceans Canada

“The executive team clearly defines the corporate context and practices for managing organizational and strategic risks proactively”

- Management Accountability Framework, TBS 2003

Approved

July, 2004

Table of Contents

| | | |
|-----|----------------------------------|----|
| 1.0 | Effective Date | 3 |
| 2.0 | DFO Context..... | 3 |
| 3.0 | Objectives | 3 |
| 4.0 | Definitions..... | 4 |
| 5.0 | Principles and Practices | 5 |
| 6.0 | Roles and Responsibilities | 7 |
| 7.0 | References..... | 10 |

POLICY

Integrated Risk Management

1.0 Effective Date

This policy takes effect September 1, 2004

2.0 DFO Context

As DFO continues to renew and integrate policy, program and management structures, internal and external cultural barriers to meaningful change must be reconciled to achieve strategic and operational objectives with a high standard of accountability and acceptable degree of control.

Delivering on priorities with limited resources requires concerted planning and analysis of trade-offs. It is sound business practice to proactively, systematically and explicitly manage risks in the pursuit of strategic objectives.

3.0 Objectives

- To recognize that risk management is integral to achieving business objectives and effective governance;
- To establish the discipline of risk management as an organizational strength that is integrated with other management practices and is comprehensive;
- To promote horizontal collaboration and pro-active systematic management of all key risks (strategic, operational and project) to facilitate a unified organization and the achievement of corporate priorities;
- To consistently and explicitly apply risk management in decision-making;
- To build upon existing approaches for managing risk while strengthening the capacity to include stakeholders; and
- To support and provide resources for IRM training and learning plans.

4.0 Definitions

Risk

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 important objective.

Integrated Risk Management (IRM)

Integrated Risk Management involves the culture, structures and processes for a proactive, systematic and explicit organization-wide discipline that identifies, assesses, manages and communicates all risks that can have a meaningful impact on the achievement of important objectives. In doing so, it fulfills key management accountability and governance expectations set down by the Treasury Board Secretariat in the Management Accountability Framework.

The department manages risks everyday – IRM builds on existing practices and provides the organization with tools to enhance planning and decision-making processes to meet business objectives. In a mature state, IRM becomes part of the day-to-day management decision-making process.

An integrated Risk Management Model is provided as **Appendix A** to illustrate the infrastructure and operational components of IRM.

The Precautionary Approach

The precautionary approach is an important element of risk management for the department. It applies to situations where there may be serious or irreversible harm together with significant scientific uncertainty. Risk management decision-making processes always require sound and rigorous judgment. The precautionary approach provides direction in making these judgments.

The Oceans Act requires the department to promote a wide application of the precautionary approach to major decisions regarding conservation, management and exploitation of marine resources.

Legal Risk Management - DFO/Justice

Legal risk management (LRM) is a specialized application of risk management. The Treasury Board requires each department to take responsibility for its own legal risk management, in cooperation with the Department of Justice.

DFO's Legal Risk Management Committee decides which of DFO's legal issues/cases meet its "high impact" criteria, and then makes recommendations or takes action as required to manage them. High impact legal issues/cases are those which, for example, could have a significant impact on the national interest; the Charter or Constitution; DFO's policy, legislation, regulations, programs or finances; or relations with Aboriginal or Métis people.

The distinction between LRM and IRM relates to the nature and scope of analysis. While LRM deals primarily with legal risks, IRM involves the assessment of all possible events, circumstances or issues that could influence achievement of the department's business objectives. Those events, circumstances or issues may or may not be legal in nature.

Glossary of Risk Management Terminology

A Glossary of Risk Management Terminology is provided in **Appendix B**.

5.0 Principles and Practices

1. The Departmental Management Committee (DMC) explicitly defines the corporate context, criteria and practices for managing key risks.
2. Managers at all levels across the organization address horizontal issues and strategic risks as required.
3. On an annual basis, the DMC is provided with reports which identify, assess and communicate key risk areas, strategic risks and mitigation strategies that are judged to be tolerable or acceptable.
4. Departmental strategic planning addresses and accounts for key risks and provides a sound analysis of the relationship between strategic business objectives and the environment. This includes identifying organizational strengths, weaknesses, opportunities and threats including financial, operational, competitive, political, social, cultural and legal aspects.
5. Risk profiling is conducted annually to support the development of strategies for managing strategic, operational and project risks.
6. Risk management strategies established through risk profiling are integrated with existing long-term strategic and annual business planning and priority-setting as well as day-to-day operational decision-making.

7. Managers and employees, at the project and team level systematically assess operational and project risks to the achievement of outcomes.
8. All staff manage risk to take advantage of appropriate opportunities and to minimize threats to employees and desirable results.
9. The interests and perceptions of clients, the public and other stakeholders are fundamental considerations in risk management.
10. Management assesses IRM readiness and capabilities to support valuable improvements to processes.
11. Management supports a department-wide continuous learning strategy based on IRM guidelines, tools and learning opportunities.
12. IRM Guidelines are developed and communicated to provide direction to appropriate staff in order to operationalize IRM principles and practices.
13. Risk Management roles, responsibilities and authorities are assigned to the personnel who are in the best position to manage strategic, operational and project risks.
14. A risk management process is documented and fully integrated with major strategic and operational processes.
15. Risk recording and reporting is incorporated into existing performance monitoring and reporting systems to ensure key risk information is available.
16. Managers and staff utilize both intuitive and systematic risk analysis based on the context, urgency and significance of risks.
17. IRM results are measured and monitored at key levels across the department.
18. Experience and best practices are shared internally and across the department.
19. Good risk management practices are recognized and shared across the department.

6.0 Roles and Responsibilities

The Departmental Management Committee is responsible for:

- Providing oversight for the department's fulfillment of management accountability¹ and governance expectations in relation to management of risk, including adherence to the departmental IRM Policy and risk-related policies² and regulatory requirements;
- Reviewing and discussing significant risk issues and ensuring horizontal collaboration in the development of mitigation strategies and the establishment of corporate priorities in resource allocation;
- Communication of an IRM vision and promoting an organizational philosophy and culture that embraces risk management as an integral part of all activities; and
- Providing clear direction on the corporate level criteria for assessing levels of risk and direction on tolerable or acceptable levels of risk and expected management actions associated with specific levels of risk. A Corporate Risk Matrix and Risk Tolerance Table can assist in fulfilling this responsibility – see **Appendices D and E**.

All Executives are responsible for:

- The assignment of risk management roles and responsibilities;
- The management of strategic risks through periodic risk assessments or as new initiatives are undertaken;
- The integration of IRM with existing practices, specifically with planning and reporting practices and annual reporting on the management of strategic risks,; and
- Creating a supportive environment that encourages effective risk management.

¹ Treasury Board of Canada, Secretariat has a risk management expectation as a component of its Management Accountability Framework – See **Appendix C**.

² Treasury Board of Canada, Secretariat has issued policies on Transfer Payments, Internal Audit, Evaluations, Active Monitoring and Communications that have specific risk-based requirements. (See Section 7.0)

All Managers are responsible for:

- The management of strategic risks; operational or project risks through periodic risk assessments or as new initiatives and issues are undertaken;
- The development of direct channels for risk communications with their managers and with employees;
- The monitoring and reporting of risk on a regular basis; and
- Ensuring appropriate ongoing support for the development of IRM capabilities.

All Employees are responsible for:

- The proactive assessment and documentation of significant risks in every business decision; and
- Taking prompt action to manage and communicate risks in accordance with management direction on tolerable or acceptable risk.

The Departmental Audit and Evaluation Committee is responsible for approving:

- Direction on strategies for communicating IRM change requirements throughout the organization;
- Direction on the implementation of the IRM Policy, guidelines and action plans;
- Guidance for the Chief Risk Officer, currently designated as the Director General, Audit and Evaluation Directorate;
- Guidance on the provision of tools, education and sponsorship to develop risk management knowledge and skills of all staff that provide functional advice;
- Guidance on the development of risk recording and reporting structures;
- Reports on the performance of IRM; and
- Ensuring audit and evaluation plans are risk-based and include audits and evaluations of the application of the IRM Policy.

The Chief Risk Officer is responsible for:

- Co-ordination and facilitation of risk profiling activities including strategic risk assessments workshops;
- Summarizing the strategic risk assessment results;
- Coordinating an IRM capabilities survey and summarizing and communicating results;
- Assisting managers in the facilitation of systematic risk assessment sessions;
- Keeping abreast of IRM developments and the department's IRM capabilities; and
- Coordinating the development of the risk recording and reporting tools and the IRM reporting requirements.

The Audit and Evaluation Directorate is responsible for:

- Providing assurance on all aspects of risk management strategy and practices in the department;
- Ensuring recommendations in audit and evaluation reports, consider the risks of implementing and not implementing a given recommendation; and
- Ensuring Management Action Plans developed by program managers in response to audit and evaluation recommendations adequately address the risks identified in audit and evaluation reports.

The Communications Directorate

Communications is to be engaged during the risk management process to:

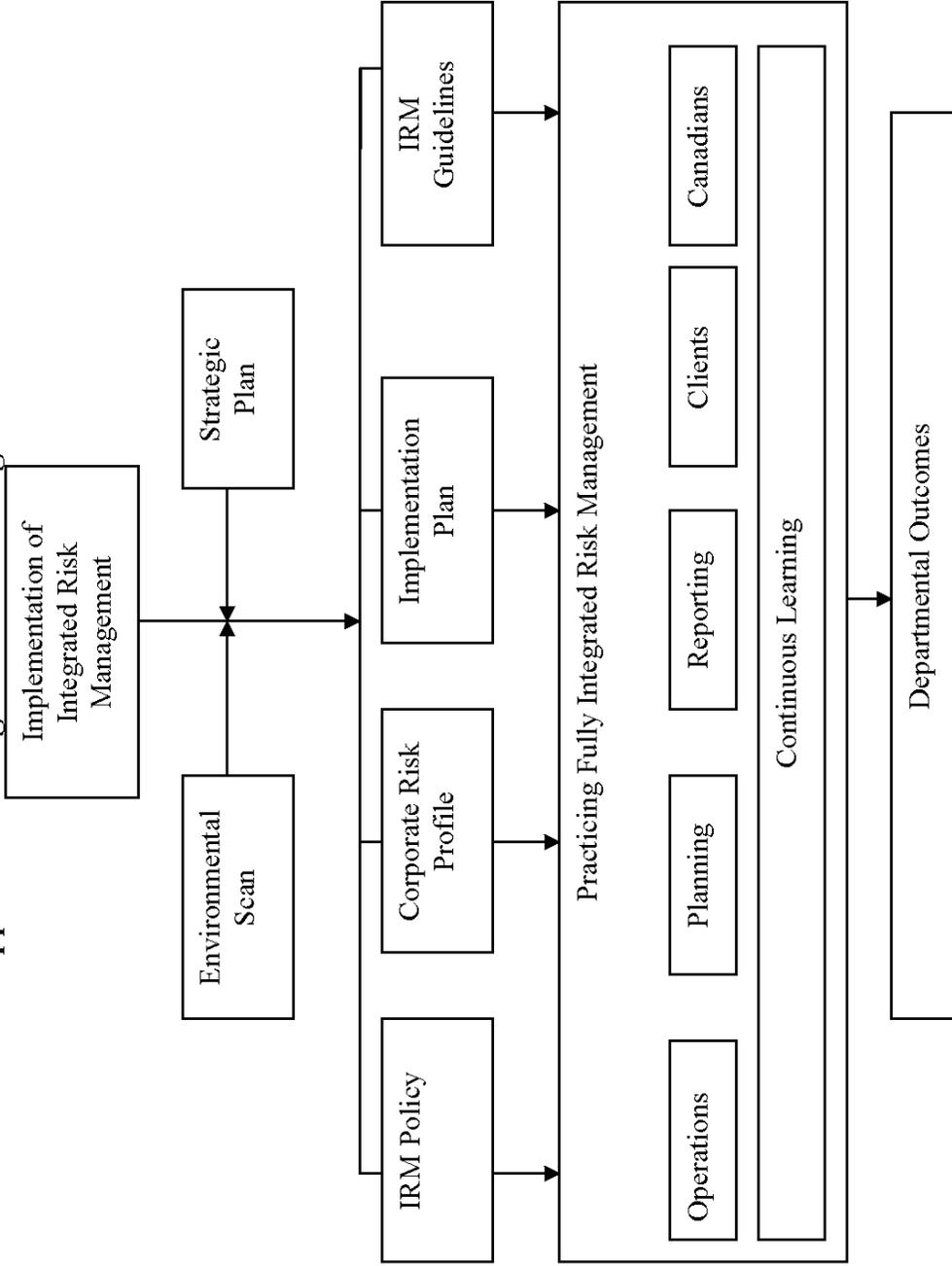
- Provide guidance on the development of a risk communications strategy and practices within the department;
- Include risk communications assessments and recommended approach (based on profile criteria and communications insight into stakeholder needs/wants) in plans and strategies as warranted;
- Act as a catalyst during client/management meeting to provide advice on risk communications during the discussion of issues; and
- Implement the departmental crisis communications plan when an issue has been designated as a crisis by the Deputy Minister.

7.0 References

- Treasury Board of Canada, Secretariat
 - Integrated Risk Management – Implementation Guide, 2004
 - Management Accountability Framework, 2003
 - Risk-Based Audit Framework Guide, 2003
 - Policy on Communications, 2002
 - Integrated Risk Management Framework, 2001
 - Policy on Internal Auditing, 2001
 - Policy on Program Evaluation, 2001
 - Policy on Active Monitoring, 2001
 - Policy on Transfer payments, 2000
 - Enhanced Management Framework, 1996

- Others
 - Risk Management Vocabulary, International Standard Organization, Guide 73, 2002
 - Risk Management: Guideline for Decision-Makers, Canadian Standards Association CAN/CSA-Q850-97

Appendix A Integrated Risk Management Model



Appendix B

Glossary of Risk Management Terms

Event:

Occurrence of a set of circumstances

Impact:

Result of an event

Implementation Risk:

The risk events that may arise as a result of the implementation approach that is chosen.

Inherent Risk:

Events or circumstances that exist before the introduction of any means of mitigation

Key Risk Areas:

The key internal and external inherent sources of risk that evolve from the legislation, mandate, program design and/or operating environment, where there is a potential significant impact on performance. For example, organizations which require employees to travel to remote and/or international locations would likely identify Health and Safety as a Key Risk Area. A specific risk within this Key Risk Area could be Travel by Automobile.

Likelihood:

The potential for the occurrence of an event

Mitigation:

Limitation of the undesirable effects of a particular event

Residual Risk:

The risk remaining after response (existing measure and incremental strategies)

Risk:

Combination of the likelihood of an event and its impact – *Source: International Standard (ISO)*

OR

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 objectives. - *Source: Treasury Board of Canada Secretariat*

Risk Acceptance:

A decision to accept a risk

Risk Assessment:

Overall process of identification, measuring impact, likelihood and risk evaluation

Risk Avoidance:

Decision not to become involved in a risk situation

Risk Communication:

Transfer or exchange of information between stakeholders about risk

Risk Criteria:

Terms of reference by which the significance of risks is to be assessed

Risk Drivers:

Broad factors that generate the need for risk management. Risk drivers often include: the pace of change; the need for due diligence; stakeholders' expectations for good governance, etc.

Risk Estimation:

Process used to assign a magnitude to a risk and its components

Risk Evaluation:

Process of comparing the estimated risk against risk criteria

Risk Identification:

Process to list and describe the source of risk, events and consequences

Risk Management:

Overall application of policies, processes and practices dealing with risk

NOTE 1:

Risk management may include identification, assessment, response, monitoring, review and communication

Risk Matrix:

A tool, which sets out criteria for impact and likelihood of risks. The Risk Matrix ensures all parties involved in assessing the level of residual risk are using common criteria

Risk Perception:

Value or concern with which stakeholders view a particular risk

NOTE 1: This perception is derived from stakeholders' expressed needs, issues, knowledge and concerns

NOTE 2: The risk perception may differ from objective data

Risk Transfer:

Share with another party the benefit of gain or burden of loss from the impacts of a particular risk

Risk Response:

Process of selection and implementation of risk control options

Risk Scorecard:

A tool used to plot and illustrate the likelihood and impact of a given risk area(s)

Source of Risk:

An event, circumstance or activity with a potential for consequences

Source of Risk Template:

A tool listing context specific events, circumstances or activities that facilitates identification of risk areas

Stakeholder:

Any individual, group or organization that may affect, be affected by, or perceive itself to be affected by the risk

Appendix C

TBS Management Accountability Framework – Risk Management Expectations*

| Risk Management a key management expectation of the Management Accountability Framework | | |
|--|--|---|
| Expectation | Indicators | Measures |
| The Departmental Management Committee approves the corporate context and practices for managing organizational and strategic risks proactively | <ul style="list-style-type: none"> ▪ Key risks identified and managed ▪ Evidence that risk is assessed in decision making ▪ Risk smart culture ▪ Capacity to communicate and manage risk in public context | <ul style="list-style-type: none"> ▪ Corporate Risk Profile, reviewed regularly ▪ Tools, training, support for staff ▪ Evidence of risk considerations in strategic planning ▪ Engagement of external stakeholders in assessing and communicating risks |

* TBS Management Accountability Framework is available at www.tbs-sct.gc.ca/maf-crg/maf-crg_e.asp

**Appendix D
DFO Corporate Risk Matrix**

Qualitative Measures of Impact

| Level | Impact | Damage & Liability | Operational Effects | Reputational Loss |
|----------|-----------------|---|--|--|
| 3 | Severe | <ul style="list-style-type: none"> ▪ Death or permanent disability ▪ Fiduciary error or omission > \$1M ▪ Loss of critical client information (e.g. landings) or disclosure of highly sensitive or classified information ▪ Loss of major asset(s) > \$1M ▪ Serious violation of law (e.g., Labour Code) ▪ Permanent environmental damage | <ul style="list-style-type: none"> ▪ Disruption of essential programs/services > 7 days for large numbers of clients ▪ Protests with significant impacts on the public or DFO operations ▪ Will not meet most service objectives ▪ Cancellation/Significant delays of major projects ▪ Loss of Key Corporate knowledge | <ul style="list-style-type: none"> ▪ Significant loss of client group trust ▪ Public outcry for removal of Minister and/or departmental official ▪ Media outcry for removal of Minister and/or departmental officials ▪ Strong criticism by review agencies (e.g., OAG, PAC, etc.) |
| 2 | Moderate | <ul style="list-style-type: none"> ▪ Serious injury/illness ▪ Fiduciary error or omission \$100K - \$1M ▪ Environmental damage ▪ Loss of asset(s) \$100K - \$1M ▪ Violation of law (e.g., Labour Code, Criminal Code, etc.) ▪ Disclosure of sensitive information | <ul style="list-style-type: none"> ▪ Disruption of essential programs/services < 7 days for some clients ▪ Protests with some impacts on DFO operations ▪ Will not meet some service objectives ▪ Some schedule delays to major projects ▪ Some loss of corporate knowledge | <ul style="list-style-type: none"> ▪ Some loss of client group trust ▪ Negative media attention ▪ Criticism by review groups (e.g., OAG, PAC, etc.) |
| 1 | Minor | <ul style="list-style-type: none"> ▪ First aid treatment ▪ Fiduciary error or omission < \$100K ▪ Loss of asset(s) < \$100K ▪ Disclosure of personal information | <ul style="list-style-type: none"> ▪ Some disruption of programs for some clients ▪ Some underachievement of service objectives ▪ Schedule delays to minor projects | <ul style="list-style-type: none"> ▪ Setback in building of client group trust ▪ Some unfavourable media attention ▪ Some unfavourable observations by review groups (e.g., OAG, PAC, etc.) |

Qualitative Measures of Likelihood

| Level | Likelihood | Description |
|----------|---------------|--|
| 3 | High | The event is expected to occur in most circumstances (> 70%) |
| 2 | Medium | The event should occur at sometime (21 – 70%) |
| 1 | Low | The event occurring is unlikely (< 20%) |

Appendix E

Risk Tolerance Model

