DEPARTMENT OF FISHERIES AND OCEANS

Initial IRM Implementation Guidelines

Approved

December 2004

TABLE OF CONTENTS

1) INTRODUCTION....1
2) IRM KEY CONCEPTS....4
3) CRITICAL SUCCESS FACTORS....7
4) APPLICATION OF IRM....8
5) ROLES AND RESPONSIBILITIES....11
APPENDIX 1 – COMPONENTS OF RISK MANAGEMENT....12
RISK IDENTIFICATION: UNDERSTANDING WHAT CAN GO WRONG....13
RISK ASSESSMENT....17
RISK RESPONSE AND TREATMENT....23
RISK COMMUNICATION AND REPORTING....26

1) INTRODUCTION

This Initial Guidelines document has been prepared to serve as a high level document that identifies in general terms where and how Integrated Risk Management can be useful within DFO.

The document will be supported by implementation handbooks and procedures manuals that address, in a step by step fashion, how Integrated Risk Management will be conducted in specific program areas. These more detailed handbooks and manuals will be developed as they are required. It is expected that there will be handbooks and manuals for major activities in DFO by April of 2006.

The Initial IRM Guidelines document will be revised by April of 2006. These IRM Guidelines will reflect the approaches and elements that have proven to be appropriate and effective for DFO during the initial IRM implementation period. These guidelines will also reference all IRM manuals and handbooks that have been developed and are in force at that time.

Background

DFO recognizes that delivering on its priorities with limited resources requires concerted planning and analysis of trade-offs. In this context, it is sound business practice to proactively, systematically and explicitly manage risks, to support informed decision-making by managers in the pursuit of strategic objectives. In response, the Department of Fisheries and Oceans (DFO) is implementing Integrated Risk Management (IRM).

In addition to representing sound business practice, the implementation of IRM also satisfies DFO's obligations to Treasury Board Secretariat (TBS). Both the TBS *IRM Framework*[1] and the recently released *Management Accountability Framework*[2] (MAF) encourage the use of IRM to strengthen risk management across the government, increase accountability and better achieve results.

DFO's IRM Policy took effect on September 1, 2004. The policy outlines the objectives, principles, roles and responsibilities surrounding the deployment of IRM.

These initial IRM Guidelines represent a strategic overview of where and how Integrated Risk Management is expected to be implemented in DFO. Their purpose is to help

[1] Treasury Board Secretariat. 2001.

[2] Treasury Board of Canada, Secretariat. 2003.

operationalize DFO's IRM policy by providing high-level guidance to managers throughout the department in order that DFO's risks can be proactively managed.

The guidelines are intended to establish a common management culture and language surrounding risk management across the department and while they provide general direction on risk management, they are not intended to dictate in a prescriptive manner, risk management procedures.

DFO's IRM deployment will be further guided by a formal IRM Implementation plan, which is currently under development.

IRM Implementation

DFO has entered into an 18-month implementation phase for IRM. The work is being conducted by an IRM Implementation Team, which is seeking guidance and direction from a formal IRM Implementation Committee[3]. The implementation effort began in the summer of 2004 and is characterized by the following key deliverables, each of which represents a key element of DFO's IRM regime.

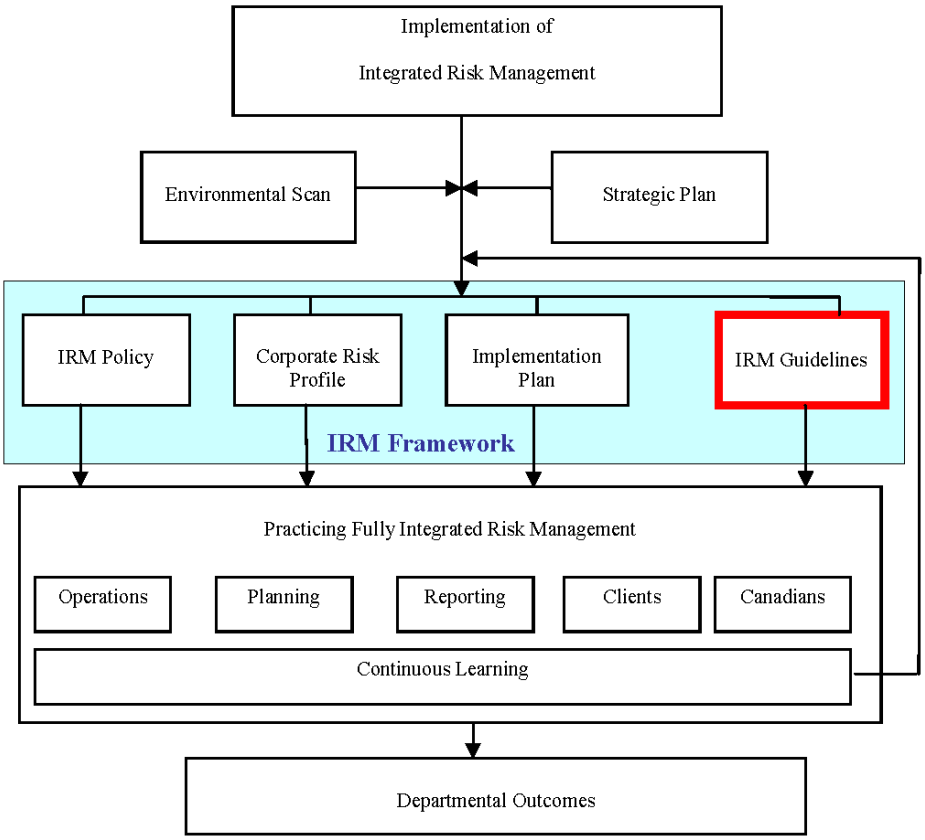
a) An Integrated Risk Management Policy (published in September 2004)

b) An Initial Corporate Risk Profile (currently in draft)

c) Initial Integrated Risk Management Guidelines (this document)

d) An IRM Implementation Plan, including detailed work plan to guide the full deployment of IRM.

[3] Please see Section 5 of these guidelines for a description of the roles of the IRM Team and the IRM Committee.



Upon completion of the 18-month implementation phase, we expect to have an updated and approved Corporate Risk Profile[4] and a final version of Integrated Risk Management Guidelines. The IRM Implementation Plan will also be developed and will provide critical details on the methods and focus of the roll-out of IRM.

Objective

The objective of these initial guidelines is to assist managers at all levels in implementing IRM by providing general information and strategic direction. It is anticipated that the guidelines will be updated and refined as DFO gains experience from our implementation of IRM. The appendix to this document provides some guidance on elements and approaches that can be applied. More detailed procedures manuals for specific activities or areas may be developed at a later date.

[4] It is expected that the Corporate Risk Profile will be updated regularly as part of IRM framework. The frequency of the updates will be defined during the IRM Implementation phase.

2) IRM KEY CONCEPTS

Some Guiding Principles for IRM

- Risk management is everyone's responsibility. Section 5 of these guidelines outlines specific accountabilities across the department with respect to risk management; however, more generally, all staff are responsible for identifying and managing the risks to their objectives.
- Risk management is not the same as risk avoidance. The goal is manage risk at an appropriate level.
- Risk management done properly is proactive in nature. While we cannot always predict the occurrence of negative events, a reactive approach to risk management is generally costly and limits our ability to prevent and correct harmful events and their consequences.
- The full value of risk management is realized when it is practiced in an integrated fashion and when it is tied to other corporate functions such as planning, resource allocation, and management of performance. If risk management is practiced as a separate exercise, its true value will not be harnessed.

IRM will not be sustainable unless it is integrated and linked with other management processes.

DFO's IRM Objectives

DFO's Policy on IRM establishes the following objectives for IRM in the department:

- To recognize that integrated risk management is integral to achieving business objectives and effective governance;
- To establish the discipline of integrated risk management as an departmental strength that is integrated with other management practices and is comprehensive;
- To promote integration through horizontal collaboration and pro-active systematic management of all key risks (strategic, operational and project) to facilitate a unified and consistent decision making approach to help achieve corporate priorities;
- To consistently and explicitly apply integrated 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.

What is 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 objective.

In its most basic terms, risk can most easily be thought of as something that can go wrong[5] and which can prevent you from achieving your objectives.

What is Risk Management?

A central part of everyday business, risk management is a management tool that uses a systematic approach to identify, analyze and respond to the risks to which your objectives are exposed.

Current Forms of Risk Management

Risk management, in many different forms, takes place throughout the department. The goal of *integrated* risk management (IRM) is to integrate and leverage the results from this risk management, for the benefit of middle and senior managers.

While 'intuitive' risk management can sometimes make the most sense, more formal risk management is necessary to proactively manage the risk to a project, program or entire operation.

The Benefits of Integration

Risk management can be performed in silos across the department and will yield value by proactively identifying issues that must be managed in order to better achieve objectives. However, the full value of risk management to the department will not be realized unless and until it is performed in an integrated fashion.

Integrated risk management is a set of business practices, supported by a risk-smart culture, which assesses, communicates and manages risk at a level appropriate to the department's risk profile and opportunities. IRM enhances decision-making, strengthens corporate governance and provides a greater capacity to achieve objectives. IRM will help the department develop a more unified and consistent decision-making approach, improving our ability to capitalize on opportunities, enhance predictability, and protect corporate assets.

---

[5] Some risk practitioners define risk as any kind of uncertainty and thus, include opportunity in the definition of risk. For practical reasons these guidelines define risk only as the potential for events to occur which can *negatively* impact the achievement of objectives. Nonetheless, it is important to note that opportunities can be gleaned from responsible risk-management. For a discussion on this, please see Appendix One, Risk Response and Treatment.

The 'integrated' nature of risk management has many facets, as described below:

- Risks need to be assessed across the department such that a comprehensive, horizontal picture (e.g. across regions and sectors) of the department's risk profile can be ascertained and monitored (horizontal integration);
- Risks should be assessed at multiple levels so that detailed risks within a program or sector can be understood (vertical integration);
- All types of risks are examined (e.g., strategic, operational, financial, etc.), such that the complete exposure is understood; and
- Risk management is integrated into departmental planning and decision-making.

There are a number of concrete benefits that are realized from IRM:

- The proactive identification, assessment, mitigation and monitoring of risks provides a vital early warning system and helps to avoid surprises that can be costly and that can disrupt or derail an operation, program or project;
- Risk creates friction in the system. By understanding and managing risk, friction can be minimized and performance enhanced. Important management objectives such as efficiency, effectiveness, compliance and the safeguarding of assets are thus achieved with greater reliability. This is particularly important in a time of resource constraints; and
- Having up-to-date and meaningful information on risk provides management with important information they need to make informed and responsible decisions.
- Likewise, formal and integrated risk management promotes departmental learning and knowledge transfer. Creating a 'risk-aware' department strengthens operational effectiveness and efficiency.
- When risk management is practiced in a comprehensive and integrated fashion, management's planning process is strengthened. Resources can be allocated to the areas of highest risk, which not only supports the achievement of objectives, but also greatly increases efficiency by streaming resources to the area of greatest need.

At the end of the day, we have a greater chance of success when we practice integrated risk management.

3) CRITICAL SUCCESS FACTORS

To be successful, IRM must be a sustainable, pragmatic and valuable exercise for the department. As with any initiative, management leadership, with clearly defined accountabilities will be necessary. Beyond this the following critical success factors will be borne in mind as DFO moves towards full IRM implementation.

Integration with Existing Management Framework:

In an effective IRM regime, the department's IRM objectives are tied directly to the strategic, operational and project objectives. Risk management practices are to be integrated with existing management practices such as standard operating procedures, business planning, resource allocation and performance management. Risk-related activities of various departmental groups must be coordinated and consistent with one another. Thus, DFO is implementing a common risk management framework, policy and practices. To the extent possible, existing practices would be leveraged to avoid duplication of effort and unnecessary expenditure.

Simple and Efficient Risk Management Tools and Techniques:

An effective IRM regime has efficient and effective tools and techniques in place to continuously identify, assess, manage and report on risk levels. To the extent possible, the DFO approach to risk management will be standardized and applied consistently across the department, although allowances will be made for unique aspects of an operation that require different approaches. As noted above, risk management techniques need to be integrated with existing management practices, operating procedures and systems. The sophistication, and by extension, the cost associated with the practices and tools will be commensurate with the level of risk to which DFO is exposed as well as our IRM objectives.

Implementation Plan:

The implementation of IRM can represent a considerable change in an organization. Key to a successful implementation of IRM will be a well-developed implementation plan, with clear activities and milestones. The plan, which is currently under development, will articulate DFO's IRM objectives, the desired end goals and the measures that will be used to demonstrate their achievement. The plan will also identify roles and responsibilities for implementation, the timing and priority of various activities, the nature and number of required resources and the link between IRM and existing priorities. A targeted communication strategy will be included in the implementation plan, to generate awareness and commitment to IRM across the department. Finally, the plan will be used to articulate a continuous learning process that will be critical to sustain IRM.

4) APPLICATION OF IRM

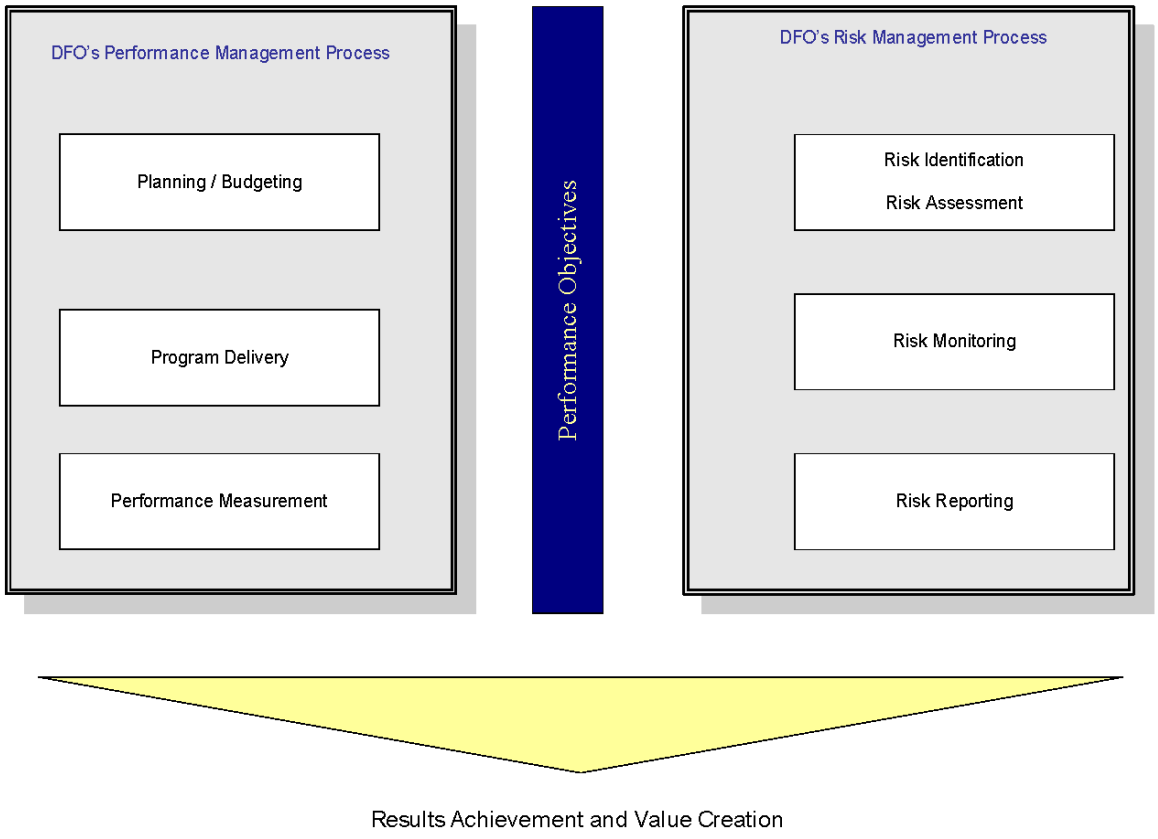
SCOPE

IRM will be implemented enterprise-wide with a view to providing a department-wide picture of risks, in support of strategic and operational decision-making and resource allocation. The risk management methods that will comprise the IRM regime will provide tools to help identify the nature, impact and likelihood of risks at all levels in the department, from small field stations to national programs.

ALIGNMENT WITH EXISTING CORPORATE PRACTICES

The IRM Implementation Plan will provide detailed guidance on where specific risk assessments will be conducted and how they will be integrated to provide an enterprise-wide view of risks. At a minimum risk management will be tied to existing corporate functions such as planning, resource allocation, and performance management. The following diagram illustrates this alignment.

Integrating Risk Management into Decision-making



When and How should You Manage Risk?

The department's overriding objective surrounding IRM is to integrate risk management into the regular operations of DFO, including decision-making. As such, the fundamental principle that underpins this initiative is that risk management should be done by everyone. While informal, intuitive approaches to risk management are appropriate in many cases, a more rigorous and integrated approach is important to support and communicate, in a transparent and meaningful way, strategic decision-making. Recognizing this, the department is committed to implementing a formal risk management process that supports the explicit assessment of risk at the Regional and Sectoral levels, as well as at the level of specific initiatives. As noted earlier, the precise nature of the IRM activities, i.e., exactly when and how risk management should be executed, will be developed in the coming months and will be outlined in the IRM Implementation Plan.

The level of formality with which risk management is executed will necessarily vary, depending on a number of factors including:

- **Cost/Benefit:** The application of risk management should normally meet the test of cost effectiveness.
- **Strategic Importance:** Given that the mission of DFO includes impacts on commerce, navigation, safety, security and trade, a direct test of cost effectiveness should not be the only test or the overriding consideration. The strategic importance of DFO's initiatives should also be considered when deciding how formally to manage risks.

An initial planned conceptual approach for integrated risk management is illustrated below, which includes both top-down (CRP development) and, potentially, bottom-up (targeted risk assessments) components. The actual approach adopted may well be different.

Process	Description	Outputs and Their Usage
Enterprise-wide		
Corporate Risk Profile Development	Annually, in preparation for the planning exercise, the Integrated Risk Management Team would consolidate all significant risks from Sectoral and Regional process. Through a formal assessment process, the Departmental Management Committee would review these risks in the Corporate context. Action plans would be developed, risk tolerance discussed and resources assigned to address any risks that are considered unacceptable.	Risk management strategies (action plans) established based on the risk profile would be integrated with existing long-term strategic and annual business planning and priority-setting, as well as, day-to-day operational decision-making. Risk levels would be monitored as part of program delivery, through the performance management process.

Process	Description	Outputs and Their Usage
Sectoral and Regional Risk Assessment		
Sectoral Risk Assessments	On an annual basis, as part of the sectoral business planning process, strategic risk assessments would be conducted in each sector[6]. Risks to sectoral objectives would be identified, and risk management strategies assessed with a view to determining residual risk levels in each sector. Action plans would be developed and monitored in the course of program delivery.	Risk management strategies (action plans) would be established out of the risk assessments. The strategies would then be integrated with, and inform existing long-term strategic and annual business planning. Priority-setting, as well as, day-to-day operational decision-making would also be improved when considered in the light of the results of Integrated Risk Management analyses. Risk levels would be monitored as part of program delivery. Top risks would be escalated for consideration in the Enterprise-wide risk assessment process, as part of the CRP development exercise.
Program and Activity Level Risk Assessment		
Targeted Risk Assessments	ADMs/RDGs and other managers would direct risk assessment in areas of high risk (e.g. new initiatives, areas of major change, areas where specific incidents have occurred) Where ongoing activities face constant change or are subject to an external environment that brings changed risks and risk levels each year, annual Integrated Risk Management assessments would be recommended.	Risk management strategies (action plans) established out of the risk assessments would be implemented by an appropriate level of management, in accordance with their sphere of influence. Risk levels would be monitored in accordance with the existing performance management process. Risks that cannot be managed at this level would be escalated to the next level. As well, the highest risks and risks pertaining to horizontal issues would be escalated to the sectoral or regional risk assessment process.

[6] Note that with the changes to the departmental planning framework, e.g., a departmental business plan with chapters structured around the Program Activity Architecture (PAA), risk assessments might be done on the basis of the PAA rather than sectors

5) ROLES AND RESPONSIBILITIES

The following responsibility matrix outlines the anticipated roles and responsibilities of key parties within DFO as they relate to the deployment of IRM. The specific activities and roles will ultimately depend on the integrated risk management processes defined during the IRM implementation phase.

Party	**Expected Roles and Responsibilities**
The Departmental Management Committee (DMC).	On an annual basis, the DMC will be provided with reports that identify, assess and provide direction on how to communicate key risk areas for the department. The precise nature of these reports will be determined though the IRM Implementation Planning exercise, which is currently underway. In response, management will develop action plans to address and communicate those risks that are deemed to be unacceptable. These action plans will be integrated with existing long-term strategic and annual business planning and priority-setting and will also be integrated, as appropriate, into day-to-day operational decision-making. As well, as serious risks arise or threaten to arise, these issues will be brought before the DMC for their consideration and, if necessary, action.
All Executives	Senior Executives will participate in the annual risk assessment exercises, e.g., conducted corporately and at the sectoral/regional level. The precise nature of these risk assessment will be determined though the IRM Implementation Planning exercise, which is currently underway. Action plans resulting from the risk assessments will be implemented into existing planning processes and will help to direct resources to the areas of greatest risk. More fundamentally, executives will provide leadership in practice of IRM.
All Managers	In the course of daily operations, managers will identify, assess and monitor risks. They may also be called upon to participate in risk assessments that will take place annually, e.g. at the sectoral / regional levels. More generally, managers should support a culture within their organizations that encourages risk awareness and how best to communicate risk within the department and with the public.
Managers and employees, at the project and team level	In the course of daily operations, everyone should identify, assess, manage, communicate and monitor risks.
The Departmental Audit and Evaluation Committee	The Committee meets on a regular basis to discuss progress on IRM Implementation, key risk assessment results and outstanding risk mitigation strategies (action plans).
The Chief Risk Officer	The Chief Risk Officer (CRO) will act as the centre of expertise during the period of IRM Implementation. Upon completion of the IRM Implementation period, the CRO will direct and oversee the annual CRP exercise as well as other annual risk assessments, e.g. sectoral/regional. More generally, the CRO will provide guidance to DFO personnel on risk management principles and practice. In support of effective risk information management, the CRO will be responsible for managing the risk information system, on behalf of the department.

Party	Expected Roles and Responsibilities
The Integrated Risk Management Team	The IRM Team is responsible for leading the IRM Implementation exercise. Fulfilling the project management role of the IRM implementation, they are responsible for developing all the key elements of the IRM regime, including the Implementation Plan that will lead to full implementation of IRM practices across DFO by April of 2006. They will prepare status reports and updates as necessary. They will work with Integrated Risk Management committees in Regions and Sectors to support the full cross-sectoral integration of approaches and results. Directed by the CRO and by the IRM Implementation Plan, the IRM Team will conduct risk assessments on key priority areas.
The Integrated Risk Management Implementation Committee	This advisory committee provides leadership and direction in support of the IRM Implementation exercise. It is a senior level committee with representation at the DM minus two level from each Region and Sector. To support the implementation of Integrated Risk Management in all sectors and regions by April of 2006. The Committee's objectives are: ➢ For IRM to be a fully implemented component of the annual planning process. ➢ For all major decisions, including policy, regulatory and financial are conducted in the light of an Integrated Risk Management analysis. ➢ To have DFO seen as a leader in Integrated Risk Management. ➢ To ensure that the work of the IRM Team is well founded and compatible with DFO's mission. ➢ To review documents and plans for pilot projects to ensure that they address the needs of the department. ➢ To share IRM information among the members of the Committee. ➢ Provide important input on the development of IRM approaches so that the needs of DFO Sectors and Regions are met.
Clients and Partners	DFO will communicate with affected clients and partners on key initiatives and changes that affect them. Where appropriate DFO will also seek input from clients (including First Nations, fish harvesters shipping industry, recreational boaters, etc.) on specific IRM analyses.
Stakeholders	DFO's programs and activities are important to Canadians in general and as well to members of specific non-government organizations. DFO will communicate with Canadians on major initiatives and operational changes. Where appropriate DFO will also seek input from Canadians in general and NGO's and ENGO's as appropriate.

Table 1 IRM Accountability Framework

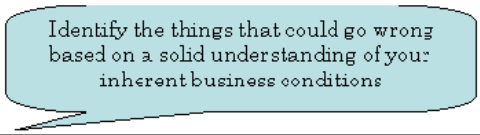
APPENDIX 1 – COMPONENTS OF RISK MANAGEMENT

As noted in the introduction, these guidelines do not provide detailed procedures on how to manage risk. Nonetheless, they do provide a good opportunity to establish a common language and framework at the outset of the IRM Implementation period. Accordingly, this appendix contains some information on the risk management process and provides guidance – not a prescription – for all key phases of risk management, namely:

- Risk Identification
- Risk Assessment
- Risk Response and Treatment
- Risk Communication and Reporting

RISK IDENTIFICATION: UNDERSTANDING WHAT CAN GO WRONG

The first step in managing risk is to understand what can go wrong in your operation. This involves understanding why and how you are inherently exposed to risks and on that basis, identifying specific events which, if they materialize, may prevent you from achieving your objectives. This section of the guidelines provides guidance and tools in support of a thorough, yet efficient risk identification.



Risk Identification		Risk Assessment				Risk Response
Risk Source	Risk Event	Control Effectiveness	Likelihood	Impact	Residual Risk Level	Action Plans
						Action _____ Owner:_____ Due Date:_____
						Action _____ Owner:_____ Due Date:_____

Figure 1 Risk Identification

UNDERSTANDING THE CONTEXT

The first step in identifying your risk is to understand and document the business context in which the risk is likely to materialize. To do this, it is important to identify the objectives that are 'at risk' and the likely sources, or drivers, of risk.

Documenting the Business Objectives "At Risk"

Your business context is first and foremost defined by the objectives you wish to achieve. These objectives can be the strategic objectives of the department, the operational objectives of a program or a specific project objective. Whatever the case, any of these types of objectives can be exposed to unwanted events.

Understanding the Sources of Risk

Any operation or project is inherently characterized by certain business conditions that may lead to risk. These business conditions can be thought of as risk sources and can be internal or external in nature. Some key risk sources include the following:

Risk Source (Business Condition)	**Causal Relationship to Risk**
Degree and recentness of change	The more change in the internal and external environments, the more exposed the department is to risk. This category encompasses both the magnitude and the recentness of the change as well as the impacts these factors may have on risk levels
Degree of complexity	The more complex the business, the higher the exposure to operational risk. This category refers to the complexity of business processes, technology and regulatory environment; however the complexity of governance, the arrangements with key stakeholders and the relationships with stakeholders are also considered.
Legislative or other compliance requirements	The higher the degree of compliance requirements, the more stringent the control requirements. This inherently exposes the department to risk stemming from insufficient adherence to obligations, whether statutory or otherwise and can expose the department to reputational consequences.
Degree of knowledge	The higher the level of knowledge, across the department and among partners, the lower the exposure to risks. At the same time, the higher the knowledge requirements, the higher the exposure to risk that may stem from loss of key personnel, operational or relational knowledge. This category incorporates personnel and corporate knowledge that may reside in processes, business rules, and systems.
Degree of dependencies	The more dependent the entity is on other parties, the more it is exposed to risk that may originate from a lack of control. In addition, the greater the dependencies, the more coordination is required and thus, the higher the exposure to risk. Dependencies to consider include dependencies on external 3rd-parties (i.e. service providers, suppliers, etc.), internal parties and information systems.

Table 2 Risk Sources

IDENTIFYING SPECIFIC RISK EVENTS

As a result of your business conditions, you will be inherently exposed to specific events which, if they materialize, can prevent you from achieving your objectives. These events can be termed "risk events" and can most simply be thought of as 'things that can go wrong'. The following table contains some examples of risk events and categorizes them into Key Risk Areas.

Risk Area	Definition	Examples of Risk Events
Accidental hazards	All types of chemical, biological, nuclear or other hazards, with the exception of those resulting from pre-meditated activities.	♦ Chemical spills. ♦ Power black-out.
Acts of nature	An event arising out of natural causes, with no human intervention, which could not have been prevented by reasonable care or foresight.	♦ Hurricane. ♦ Flood.
Employee risk	Risk that arises from the actions or inactions of employees, whether intentional or unintentional. This category encompasses the risks associated with insufficient human resource capacity and/or competence. Employee fraud is excluded and is captured under "Fraud / Corruption".	♦ Errors and omissions. ♦ Excessive turnover.
Financial risk	Risk arising from insufficient funding for operational and/or strategic priorities.	♦ Insufficient program funding. ♦ Inability to recapitalize in S&T infrastructure.
Fraud / corruption	The risk of loss or damage to assets due to an intentional misrepresentation (by an employee or the public) with an intention to deceive for personal gain.	♦ Misappropriation of assets. ♦ Mis-use of departmental assets.
Hostile actions from others	Malicious or premeditated actions against the department, including action from clients.	♦ Sabotage. ♦ Acts of terror.
Legal risk	Violation of laws, regulations and international treaties / agreements and any resulting legal liability that may result from these violations.	♦ Non-compliance with regulations, legislation.
Partner and supplier risk	Risk that actions (or inactions) taken by partners or suppliers may negatively	♦ Insufficient capacity on the part of delivery agents and/or recipients to manage program

Risk Area	Definition	Examples of Risk Events
	affect the achievement of objectives.	funds and demonstrate accountability.
Process risk	Inadequate or failed processes or management practices, including non-compliance with internal policies and procedures, but excluding system failure.	♦ Contracting procedures not adhered to. ♦ Inability to collect relevant, reliable and measurable performance information to support decision-making and demonstrate performance.
Public opinion risk	The risk that public opinion may impede the Department's ability to achieve its objectives.	♦ Reduced support and funding due to competing / shifting public and political priorities.
Technology / Infrastructure risk	The risk arising from inadequate IT infrastructure including system failure.	♦ Security breach leading to loss, damage, or disclosure of data, and potential damage to reputation. ♦ Business disruption due to IT system failure.

Table 3 Risks, Definitions and Examples

RISK ASSESSMENT

Once you've identified the risks that could potentially harm your operation, you now have to determine how well they are currently being managed and, on that basis, determine how much 'real' risk is left-over. This section provides guidance to help you answer the following key questions:

- How much control do I have over this risk?
- What are the existing management processes that prevent, detect and correct the risk?
- Considering my current management processes, what is the likelihood that the risk will materialize?
- Considering my current management processes, what impact would this risk have on my objectives if it did materialize?

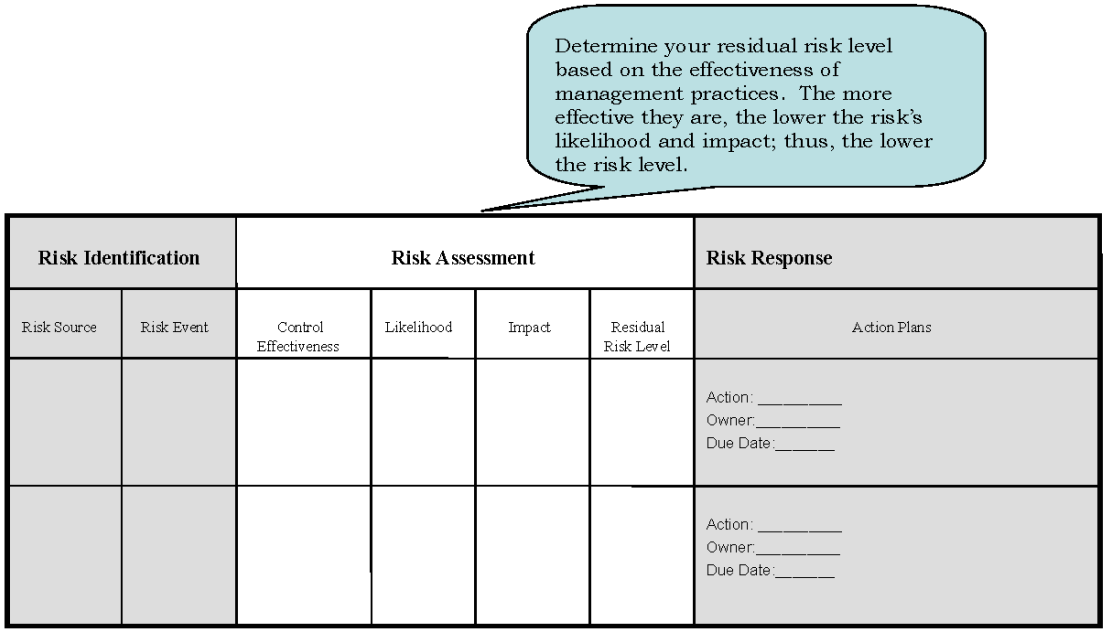


Figure 2 Risk Assessment

EVALUATING YOUR MEASURES TO MANAGE RISK

The assessment of net or residual risk requires that a judgement be made on the likelihood of each risk event occurring and the impact it will have on the stated objectives. One of the key

determinants of likelihood and impact is the effectiveness of your risk management (or risk mitigation) practices. Risk mitigation practices include those elements of the department (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the departmental objectives. These practices reduce both the likelihood of risk (by helping to prevent its occurrence) and its impact (by preventing, limiting the impact of, and/or correcting a risk event).

Assigning a Risk Level

Risk assessment is typically done through the use of simple and intuitive risk maps such as the one illustrated below. These maps can be used to analyze, by risk, the likelihood of occurrence and the impact it may have on the business objectives. The plotting of each risk according to these two attributes provides management with a risk rating (Red, Yellow, Green). The placement of the risk in either one of these zones will dictate or guide management's action plans. For example, any risk which falls into the red zone is typically (but not necessarily) considered unacceptable. The various "risk zones" should reflect management's risk tolerance levels; accordingly, the map should be customized to reflect the specific circumstances of DFO.

The DFO Integrated Risk Management Policy shows that the enterprise level reporting of risk will normally be done with a matrix that shows three levels of likelihood and three levels of impact. In order to provide a higher level of detail, so as to better understand risks and identify those where additional mitigation is a high priority, a matrix with five levels of impact and five levels of probability is proposed. This additional "granularity" will more fully separate the areas of extreme risk and situations where the risk is virtually certain.

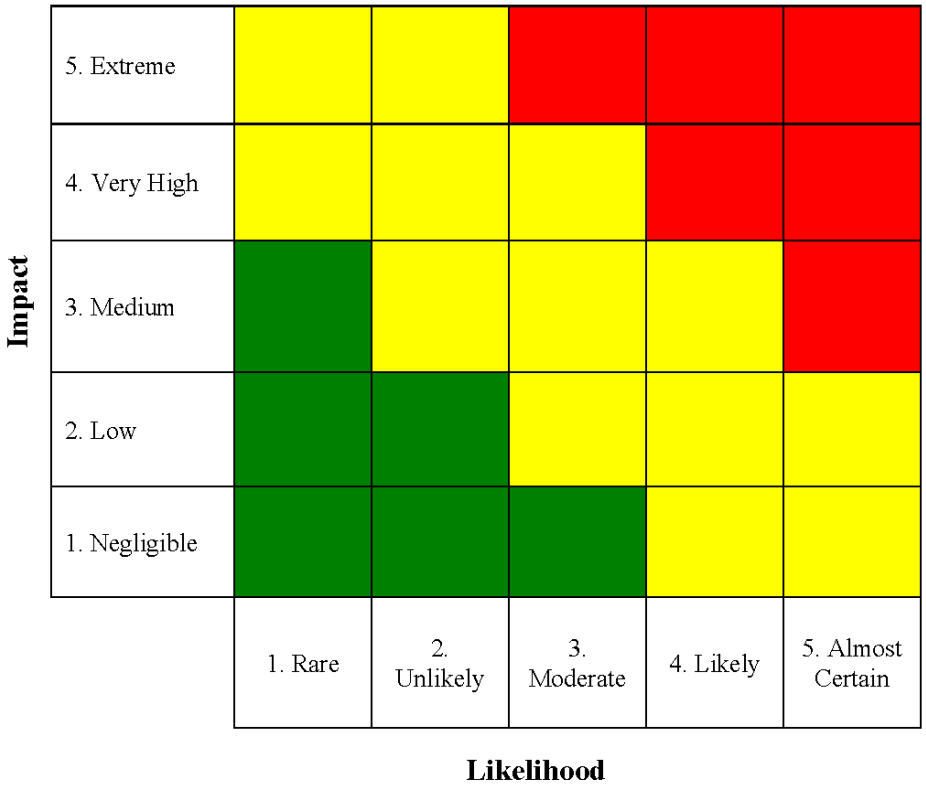


Figure 2 Risk Map

Impact

Description	Scale	Definition	Sample Indicators
An estimate of the impact of the risk on the operations under review. It is the consequence of non-achievement of the objective(s).	1. Negligible	An event, the consequences of which can be absorbed through normal activity.	♦ limited and temporary disruption of program or support operations of less than one hour, ♦ minor health and safety issues for employees, ♦ minor financial loss.
	2. Low	An event, the consequences of which can be absorbed but management effort is required to minimize the impact. The consequences could threaten the efficiency or effectiveness of some aspects of the operation, but would be dealt with internally.	♦ limited and temporary disruption of operations of less than one day, ♦ limited health and safety issues for employees in the program area, ♦ environmental or political issues in the program area that are contained within 1 to 2 days, ♦ limited financial loss, ♦ set-back in client / public trust.
	3. Medium	A significant event which can be managed under normal circumstances by the department. The consequences could mean that the activity could be subject to significant review or changed ways of operation	♦ temporary loss of capability (1-2 days), ♦ environmental or political issues contained with outside assistance with some short term effects, ♦ moderate financial loss, ♦ negative media attention / public criticism, ♦ some loss of client trust, ♦ serious disability / long-term illness, ♦ disclosure of sensitive data.
	4. Very High	A critical event that with proper management can be endured by the department.	♦ loss of operating capability (3-6 days), ♦ environmental or political issues resulting in major long-term detrimental effects on ability to achieve objectives, ♦ loss of some corporate knowledge, ♦ significant public fear / concern.
	5. Extreme	A disaster with the potential to lead to permanent or long-term	♦ loss of departmental capability of one week or greater, ♦ major financial loss.

Description	Scale	Definition	Sample Indicators
		damage to the department's ability to achieve its objectives. The consequences could threaten the survival of not only the activity, but also the Department, possibly causing major problems for clients / public.	♦ loss or disclosure of highly sensitive data, ♦ death / permanent disability or illness (employees and others), ♦ significant disruption in essential services, ♦ significant loss of corporate knowledge, ♦ public / media outrage, outcry to remove minister or senior public servant, ♦ significant loss of client / public trust.

Table 4 Attribute Criteria - Impact

Likelihood

Description	Scale	Definition
An estimate of the probability of the threat occurring.	1. Rare	This event may occur only in exceptional circumstances. It will occur less than 5% of the time.
	2. Unlikely	This event could occur at some time. It will occur between 5% and 20% of the time
	3. Moderate	This event should occur at some time. It will occur between 21% and 59% of the time.
	4. Likely	This event will probably occur in most circumstance. Will occur from 60% to 94% of the time.
	5. Almost Certain	This event is expected to occur in most circumstances. Will occur 95% of the time.

Table 5 Attribute Criteria – Likelihood

Description	Scale	Definition
A subjective rating of the current residual risk related to a specific threat or risk after considering the current mitigation estimate.	Green	Low Risk: no action required
	Amber	Moderate Risk: monitor closely
	Red	High Risk: Action required

Table 6 Attribute Criteria – Residual Risk

RISK RESPONSE AND TREATMENT

At this stage in the risk management cycle, you should have a good understanding of your residual risk profile. You must now determine the following:

- Are the risks within tolerable limits?
- If not, can you do anything to better manage the risks?
- If the risks are within the control of the decision-maker, how much additional mitigation is required? What are the corresponding costs and who should be responsible?
- If the risks are not within the immediate sphere of control, do they need to be escalated or simply accepted?
- Are there any opportunities to be gained through calculated risk taking?
- What are the costs arising from putting additional management controls in place?
- Can you share information early and then regularly to help mitigate stakeholder/public perceived risks?

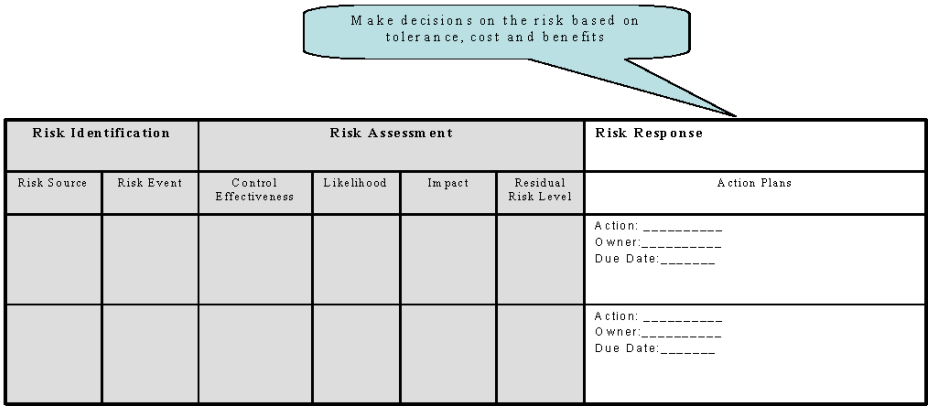


Figure 3 Risk Response

The following is a checklist that can be used to assist you in developing the most appropriate risk treatment and devising realistic and effective action plans.

Issues to Consider when Responding to, and Treating Risk	
Given the risk exposure, the time frame, management's level of tolerance for this risk, and other factors, what should be done about this risk? ***Avoid:*** The risk owner will not undertake the activity as the risk associated with it is unacceptable. ***Mitigate:*** The risk owner will take action prior to the occurrence of the risk to either reduce the likelihood that it will occur, and/or mitigate the impact should it occur. ***Contain:*** The risk owner will not do anything prior to the risk's occurrence to reduce its likelihood of occurrence or the associated impact, but will develop a contingency plan to manage the impact if it does occur. This strategy is often chosen when there is an alternative approach that can be taken if the risk materializes. Typically, the contain response consumes minimal resources prior to risk materialization, but acknowledges that resources may be required if the contingency plan needs to be implemented. ***Assume:*** The risk owner accepts the risk and does not intend to do anything to prevent its occurrence or mitigate its impact. ***Transfer/Escalate:*** The risk owner cannot deal with the risk because it has no control and requires the transfer of its management to another party for mitigation. At this stage, the choice of a transfer response does not take into consideration the willingness of the other party to accept responsibility for the risk.	
Who should take responsibility for developing and implementing the action plan?	

Issues to Consider when Responding to, and Treating Risk	
Are there any preferred strategies for mitigating the risk? *Things to consider:* ♦ How robust should the action plan be? Do we need to substantially reduce the risk exposure, or would a less robust plan suffice? ♦ Is the primary goal to reduce the chance that the risk will occur? ♦ Is the primary goal to reduce the impact if the risk does occur? ♦ Should we be looking at contingencies, in addition to avoidance strategies? ♦ Are there any constraints that the planner needs to know about when developing the mitigation plan?	
When is an action plan due?	
Risk Transfer: If the resources and knowledge regarding this risk lie outside the project and the risk assessor has the authority (or agreement) to transfer or escalate the risk, to whom should this risk be transferred and/or escalated?	
Risk Monitoring: What are the indicators that might signal that the risk is starting to materialize?	
What data should be tracked and monitored?	
How often should risk information be communicated?	
With whom should this information be shared?	

Table 7 Risk Treatment Checklist

RISK COMMUNICATION AND REPORTING

Risk communication and reporting is an integral element of the integration of risk management across the department. It is also critically important to harnessing the full value of IRM as a decision-making tool. An effective and meaningful IRM regime is characterized by the appropriate access to, and usage of risk information, by those who require it. In addition, value is also generated by more effectively communicating important risks to clients and stakeholders.

To ensure risk information is shared and acted upon in an integrated fashion, a number of pre-requisites are required:

- To facilitate comparability of risk information, the department should have a standardized approach to risk – including a common terminology and standardized data. This will also help to ensure that risks affecting horizontal objectives can be easily identified and acted upon.
- Risk information management is a basic requirement to support useful communication of risk issues. DFO may consider a central store for this information.
- To achieve the full integration of risk management, it will be important for risk communication to be routine within DFO, between and among: regions; sectors; programs; parts of programs; regions; and the national capital region. The consideration of risk information as part of the planning process offers an ideal, meaningful, and practical way to accomplish this. The planning process must, therefore, permit a meaningful dialogue on risk issues.
- Risk information need only be shared with those parties who need access to it. To support the efficient sharing of information, a formal escalation process is needed to help aggregate the risk information gathered at lower levels of the department and share it with more senior management, as required.
- External communication of key decisions, especially those where key risks are important to Canadians will be a key component of DFO's Integrated Risk Management strategy.