Treasury Board of Canada Secretariat Secrétariat du Conseil du Trésor du Canada

RISK-BASED AUDIT FRAMEWORK GUIDE

Treasury Board of Canada Secretariat

Version 4.3.1

June, 2003

RDIMS 170182

TABLE OF CONTENTS

Foreword

About the Guide

This Guide is the result of an interdepartmental collaborative effort of officials from more than 10 federal departments and Wiltshire-Consulting Inc. who contributed to its design and content. The Guide explains the key steps in the development of a meaningful Risk-Based Audit Framework (RBAF).

It is intended that the development of an RBAF will be conducted under the Guiding Principles for the Process (**Appendix A**). The Guide provides numerous appendices including a Risk Scorecard Toolkit (**Appendix E)**.

While this Guide focuses on the development of frameworks for Contributions, it also provides some guidance for the development of frameworks for Class Grants. A Class Grant is a grant program where there is a class of recipients rather than an individual one. RBAFs for class Grants are similar to those for contributions, except that there is no requirement for audit of recipients. **Please Note:** that for Class Grants and other types of transfer payments, the program manager should contact the Centre of Excellence for Internal Audit to discuss the exact requirements prior to developing a framework. The final decision on the type of framework rests with Treasury Board of Canada Secretariat.

Over time, examples of the process and products required for programs, which reflect varying degrees of complexity will be made available on our web site. The methods and tools provided within this Guide will enable the completion of an RBAF for both simple and complex programs.

Executive Summary

Purpose of the Guide

The purpose of this guide is to assist managers in the preparation of a Risk–Based Audit Framework (RBAF) to fulfil the following requirements of the *Policy on Transfer Payments* (PTP June 2000):

(i) That "it is government policy to manage transfer payments in a manner that, is **sensitive to risks**, complexity, accountability for results and economical use of resources..." (Section 5.0);

(ii) That the departments, in their "Treasury Board submissions for program approval of terms and conditions for grants to a class of recipients or for contributions should include the following: a risk-based framework for audit of recipients of contributions, an internal audit plan and evaluation plan of the transfer payment program, including expected funds to be budgeted for costs related to these requirements" (Section 8.1.1, xvi); and

(iii) That "Departments must develop a risk-based audit framework for the audit of contributions including:

- determining which recipients are to be audited;
- selecting appropriate auditors or indicating the acceptability of auditors when retained by the recipient;
- determining whether the scope, frequency and scheduling of audits meet program requirements;
- coordinating audits with others involved in the audit of the same recipients; and
- determining follow-up action required on audit findings.

These PTP requirements place emphasis on the integration of risk concepts into transfer payment management and audit planning procedures. This RBAF guide provides managers with step-by-step directions on how to prepare an RBAF document that clearly and concisely demonstrates that all requirements have been met.

This guide also addresses the potential efficiency and effectiveness gains of integrating, or at least coordinating, the RBAF with the Results-Based Management and Accountability Framework (RMAF) which is required by the PTP to address performance measurement and evaluation strategies.

Summary of the RBAF Sections

In general, the RBAF consists of seven (7) sections, as summarized below. **Section 1.4** of this guide presents the factors that should be considered in determining the appropriate level of detail to be included in each section.

1. Introduction

- The RBAF should be introduced with a concise explanation of the purpose of the RBAF in relation to PTP requirements and demonstration of good governance.
- A brief description on the background of the program, initiative or policy[1] should be provided at the beginning of the RBAF to set the overall context.
- If program management chooses to integrate the RBAF with the RMAF, this section should be used to briefly outline the points and extent of integration.

2. Roles, Responsibilities and Relationships

This section should provide a clear explanation of the roles and responsibilities of management and Internal Audit (IA) in fulfilling PTP requirements. The PTP (Section 8.5) and the Guide on Grants, Contributions and Other Transfer Payments delineate the roles and responsibilities of management and IA as follows:

- **Management** is responsible for ongoing financial and operational monitoring and the audit of recipient's compliance to terms and conditions of contribution agreements and the reliability of results data.
- **Internal Audit's** role is to employ a risk-based approach in planning and conducting audits that provide assurance on the adequacy of integrated risk management practices, management control frameworks and information used for decision-making and reporting in the achievement of overall program objectives.

In addition to overall responsibility for the program, management is also responsible for the development of the RBAF. However, IA can provide valuable assistance in addressing risk in the design and implementation of the overall program. Accordingly, this section should describe:

- consultations between management and IA, early on in the development of the RBAF, to facilitate co-ordination of risk-based decisions on conducting recipient audits; and
- co-ordination of IA input in completing Section 6 of the RBAF which addresses Internal Auditing requirements.

3. Program Profile

The profile should include:

- the underlying rationale, objectives and need for the program;

[1] Throughout this document there are numerous references to transfer payment "programs." In some organizations the word "policy" and "initiative" is used instead of program. In this guide, references to "program" applies equally to instances where initiative or policy is used.

- ❑ the target population, resources, product groups, delivery mechanisms, PTP stacking provisions and governance structure; and
- ❑ the key internal and external inherent risks areas[2] (Key Risk Areas) that evolve from the legislation, mandate, program design and/or operating environment, where there is a potentially significant impact on performance.
- ❑ The key risk areas listed here are developed in the Risk Assessment and Management Summary step (Section 4, below) and are presented in the profile section to explain the risk context of the program.

4. Risk Assessment and Management Summary

The Risk Assessment and Management Summary should include:

- ❑ a methodology section explaining the risk definition and process used;
- ❑ the identification of the parties involved in the process;
- ❑ a Risk Matrix[3] to explain the criteria and define the levels of impact and likelihood;
- ❑ identification of sources of risk, assessment of the likelihood and impact of those risks, including the underlying assumptions made and a discussion of risk mitigation actions (including management controls) taken and planned; and
- ❑ a summary of the key risks and a discussion of how they will be used to inform decisions on the nature and extent of monitoring (including performance measurement), recipient and internal auditing and evaluation.

5. Program Monitoring and Recipient Auditing

Monitoring

It is expected that the level of monitoring will increase proportionally with the importance and/or sensitivity, complexity and materiality of the program.

To the degree that risk mitigation strategies (dealt with in Section 4) take the form of changes in the Management Control Framework (including the Performance Measurement) the Monitoring regime will be considerably influenced by the nature, extent and likely impact of the risks identified. It should be remembered that where the risk mitigation strategy takes the form of controls, monitoring decisions should be based on the level of risk before mitigation.

This section should provide a complete description of overall program monitoring practices and detailed operational and financial monitoring procedures used to assess program performance and compliance with terms and conditions. Any monitoring

[2] “Inherent Risk” refers to events or circumstances that exist before the introduction of any means of mitigation and without consideration of the risk’s likelihood (see Glossary of Risk Management Terms).

[3] “Risk Matrix” is a tool that sets out criteria for assessing the level impact and likelihood of risks. The Risk Matrix ensures all parties involved in the risk assessment are using common criteria (see Glossary of Risk Management Terms).

requirements that will need resources over and above the existing program management resource base should be described, including the incremental costs involved.

Recipient Auditing

Purpose: Recipient auditing is often the only effective way to establish:

- ❑ That funds were used for intended purposes;
- ❑ Compliance with terms and conditions; and
- ❑ Reliability of results data.

This section should summarize the methodology used to select recipients for audits as well as the scope and extent of the audit. This section should also describe the specific assessment techniques employed and the expected cost of the planned audit regime.

According to the Transfer Payments Policy: "Departments must develop a risk-based audit framework for the audit of contributions including:

- determining which recipients are to be audited;
- selecting appropriate auditors or indicating the acceptability of auditors when retained by the recipient;
- determining whe ther the scope, frequency and scheduling of audits meet program requirements;
- coordinating audits with others involved in the audit of the same recipients; and
- determining follow-up action required on audit findings.

The recipient audit plan should be based on an assessment of a list of risks, which includes bringing forward (from Section 4) of those risks identified by program management that pertain to the recipient. That list should be augmented with any relevant risks that may be identified by internal audit or other stakeholders. Finally, it should include "audit risks" (i.e. those having to do with ensuring that the auditees are not cited for not meeting performance criteria when they actually do, or reported as meeting performance criteria when they actually do not).

Note: program managers should consult their audit groups regarding technical audit issues.

6. Internal Auditing

Purpose: An internal audit of a transfer payment program can provide valuable assistance to management by providing assurance as to the soundness of the risk management strategy and practices, the management control framework and practices and the information being used for decision making and reporting.

This section should include:

- ❑ a description of the results of any recent internal audits of relevance;

- a description of the risk-based audit planning methodology used for all departmental programs (including transfer payment programs);
- an explanation of when and how the transfer payment program, in question, was considered in the overall audit planning process; and
- anticipated audit objectives, scope and timing and expected cost in cases where the need for an internal audit has been affirmed by Internal Audit;

The internal audit plan should be based on an assessment of a list of risks, which includes bringing forward (from Section 4) of those risks identified by program management. That list should be augmented with any relevant risks that may be identified by internal audit or other stakeholders. Finally, it should include "audit risks" (i.e. those having to do with ensuring that the auditees are not cited for not meeting performance criteria when they actually do, or reported as meeting performance criteria when they actually do not).

7. Reporting Strategies

The reporting strategies section should indicate:

- the scope, timing and source and user of periodic reports which are produced for monitoring purposes;
- the recipient audit reports that will be produced and how they will be used;
- the internal audit reports that will be provided;
- who is responsible (especially when multiple parties are involved) for producing reports; and
- the mechanisms (e.g. annual progress requests, mid-term reports, Departmental Performance Reports) and timeframes for reporting on operational monitoring, recipient and internal audits to the lead department, TBS, TB Ministers and/or Parliament.

Glossary of Risk Management Terms

Risk Management Terms

Audit Risk Factor: (facteur de risque de vérification)
Source of Audit Risk (risk of the auditor drawing the wrong conclusion; e.g. declaring the auditees as compliant when they are not or as non-compliant when, in actual fact, they are)

Event: (événement)
An occurrence or a happening

Expected Risk: (risque attendu)
Expected Risk (ER) = Inherent Risk (IR) * Probability of occurance (P).

External Audit: (vérification externe)
Independent audit performed by auditors who are external to the organization being audited. Three types of external audit are private sector audits of an organization's financial statements, financial or comprehensive audits of federal government departments or agencies (or their provincial/municipal counterparts) and recipient audits.

Impact: (impact)
The result of an event or occurance, if its likelihood of occurance is a certainty (i.e. if the probability of occurance is 100%).

Implementation Risk: (risque de mise en oeuvre)
The risk events that may arise as a result of the implementation approach that is chosen

Inherent Risk: (risque inhérent)
Intrinsic risk of an event or circumstances that existed before the introduction of any means of mitigation (mitigation may affect either the impact or the likelihood of its realization or both).

Interested party: (partie intéressée)
Person with an interest, or group having a shared interest in the success of an organization [ISO/CD2 9000:2000]

Internal Audit: (vérification interne)
To provide sufficient and timely assurance services on all important aspects of its risk management strategy and practices, management control frameworks and practices, and information used for decision-making and reporting;

Key Risk Areas: (secteurs de risques principaux)
The key internal and external inherent risk areas that evolve from the legislation, mandate, program design and/or operating environment, where there is a potential significant impact on performance.

Likelihood: (probabilité)
The probability of occurrence of an event or circumstance

Mitigation: (atténuation)
Limitation and the undesirable effects of a particular event or circumstance (which may affect likelihood or impact of a risk being realized):

- Before the event (minimization):
  - Prevention
  - Reduction
  - Avoidance
- During the event
  - Containment
- After the event
  - Compensation
  - Restoration
  - Recovery

Recipient Audit: (vérification de bénéficiaires)
A recipient audit is an external audit of recipients of contributions. It may include financial audit, compliance with terms and conditions of a contribution agreement, audit of whether funds are being used for the purpose intended and/or audit of stewardship of public funds.

Residual risk: (risque résiduel)
The risk remaining after response or mitigation (existing measures and incremental strategies)

Risk: (risque)
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 an organization’s objectives. - *Source :Integrated Risk Management Framework, Treasury Board of Canada Secretariat (TBS)*
(See **Expected Risk** for a mathematical description of **Risk**).

Risk acceptance: (acceptation des risques)
A decision to accept or live with a risk, rather than trying to mitigate it

Risk assessment: (évaluation des risques)
Overall process of identification, measuring impact, likelihood and risk evaluation

Risk avoidance: (évitement des risques)
Decision not to become involved in a risk situation (i.e. to choose another path, which does not encounter that risk)

Risk communication: (communication sur les risques)
Transfer or exchange of information about risk between interested parties

Risk criteria: (critère de risque)
Terms of reference or standards by which the risks are to be assessed

Risk drivers: (éléments générateurs de risques)
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: (estimation des risques)
Process used to assign a magnitude to a risk and its components

Risk evaluation: (évaluation des risques)
Process of comparing the estimated risk against risk criteria

Risk Factors: (facteurs de risques)
Sources of risk that are categorized either as Impact or Likelihood risk factors, for the purpose of facilitating risk assessment or mitigation.

Risk identification: (identification des risques)
Process to list and describe the source of the risk and its consequences

Risk Management: (gestion des risques)
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: (matrice de risques)
A tool that sets out criteria for the assessment of impact and likelihood of risks The Risk Matrix ensures all parties involved in assessing the level of risk are using common criteria

Risk Mitigation: (atténuation des risques)
A means of risk minimization before the event, containment during the event, or compensation, restoration or recovery after the event

Risk Perception: (perception des risques)
Value or concern with which stakeholders view a particular risk
NOTE 1: This perception is derived from the stakeholder's expressed needs, knowledge, concerns and tolerance of uncertainty
NOTE 2: The risk perception may differ from objective data

Risk Response: (réponse aux risques)
Process of selection and implementation of risk management options, including controls.

Risk Scorecard: (feuille d'évaluation des risques)
A tool used to plot and illustrate the likelihood and impact of a given risk or risk area

Risk Sharing: (partage des risques)
Share with another party the benefit of gain or burden of loss from the impacts of a particular risk

Risk transfer: (transfert des risques)
Transfer of the risk to another party, who will accept the risk and/or reap the rewards

Source of risk: (source de risque)
An event, circumstance or activity with a potential for consequences; for risk assessment purposes, sources of risk need to be converted to/categorized as Impact or Likelihood risk factors.

Source of Risk Template: (modèle de source de risque)
A tool listing context, specific events, circumstances or activities that facilitates identification of risks or risk areas

Stakeholder: (détenteurs d'enjeux)
Any individual, group or organization that may affect, be affected by, or perceive itself to be affected by the risk

Section 1 - Introduction to the Risk-Based Audit Framework

This guide is intended to assist managers in meeting the *Policy on Transfer Payments* (PTP June 2000) risk-related requirements that support government-wide directions for more corporate and systematic management of risk in the design and delivery of programs. For example, emphasis is placed on incorporating risk in the initial stages of program planning by stipulating that:

- ❑ "The type of transfer payment that a department uses to meet its program objectives is determined by the departmental ma ndate, business lines, clients and **an assessment of risks."**

The PTP also refers to the following two requirements that are fulfilled through the development of an RBAF:

- ❑ "It is government policy to manage transfer payments in a manner that is **sensitive to risks**, complexity, accountability for results and economical use of resources…" [Section 5.0];
- ❑ "Departments must develop a **risk-based audit framework** for the audit of contributions…" [Section 8.5].

A primary impetus for the government-wide management-change initiative on risk arose from observations and recommendations made in the *1997 Report of the Independent Panel on Modernization of Comptrollership in the Government of Canada*. The report found that:

- ❑ "…key responsibilities for governing bodies … [include]: understanding **the risks associated with the type, level and quality** of the service government decides to (or not to) provide, whether directly or indirectly, and **ensuring that appropriate means are in place to manage these risks**…"
- ❑ "…areas that increasingly demand managerial excellence …[include]: matching more creative and client-driven decision making and business approaches with **solid risk management**…"

In this context, Treasury Board of Canada Secretariat (TBS) acknowledged the importance and benefits of systematic risk management as a strategic investment in the attainment of overall business objectives and demonstration of good governance. As a result, increased emphasis is being placed on working together, at all levels, to create management regimes which are based on leadership and values, well-defined standards and control systems as well as **solid risk management**.

In addition to the PTP, TBS has promoted the integration of systematic risk management practices in other key policies and guidelines, such as:

- ❑ the *Integrated Risk Management Framework* (April 2001) which establishes the expectation that implementing the Framework will "strengthen accountability by demonstrating that **levels of risk are explicitly understood**"; and
- ❑ the *Active Monitoring Policy* (June 2001) which stipulates that "departments must actively monitor their management practices and controls **using a risk-based approach**."

The sections which follow describe the underlying objectives and components of an RBAF and provide guidance in its development and preparation.

1.1 What is an RBAF?

The RBAF is a management document that explains how risk concepts are integrated into the strategies and approaches used for managing programs that are funded through transfer payments. The RBAF provides:

- ❑ background and profile information on the transfer payment program including the key inherent risk areas (internal and external) that the program faces;
- ❑ an explicit understanding of the specific risks which may influence the achievement of the transfer payment program objectives;
- ❑ a description of existing measures and proposed incremental strategies for managing specific risks; and
- ❑ an explanation of monitoring, recipient auditing, internal auditing, and reporting practices and procedures.

1.2 Why Do We Need an RBAF?

Transfer payment programs operate in an environment which involves many interconnections, including those that stem from global expectations, governance requirements, authorities and various risk drivers[4]. All these factors affect the design and implementation of the program. Overview and detailed models which reflect the transfer payment program environment are illustrated in **Appendix D**.

Risk-Based Audit Frameworks can cost-effectively and efficiently assist managers in operating in this complex environment by:

- ❑ enhancing managers' and employees' understanding and communication of risk and related mitigation options;
- ❑ strengthening accountability for achieving objectives and stewardship over public funds;
- ❑ facilitating managers' achievement of government-wide requirements for solid risk management;
- ❑ providing a basis upon which to create contingency plans;
- ❑ helping to secure funding for new or renewed programs; and
- ❑ enhancing information for decision-making.

[4] Risk drivers are the 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. (see Glossary of Risk Management Terms).

1.3 Who Should be Involved in the Development and Implementation of the RBAF?

The key parties that should be involved in the development and implementation of an RBAF are as follows:

- Managers of the program who have primary responsibility for ensuring that the RBAF reflects an accurate and comprehensive analysis of potential risks to the achievement of objectives as well as cost-effective monitoring, mitigation and reporting strategies;
- Internal Audit and program staff who could provide expert advice and technical support in risk identification, assessment and monitoring as well as take a lead role in preparing the Internal Auditing section of the RBAF;
- Evaluation staff who could provide knowledge and expertise, in recognition of the potential for overlap between RMAFs and RBAFs and in cases where the RMAF and RBAF are being integrated; and
- TBS Program and Centre of Excellence for Internal Audit analysts, who have assigned responsibilities and knowledge of program and RBAF requirements respectively, and can provide advice during their preparation.

Delivery partners/co-deliverers and interested parties may also be involved as collaborators.

1.4 What Factors Should be Considered in Planning and Preparing an RBAF?

The level of detail included in an RBAF document will vary according to the nature, complexity and sensitivity of the programs. In planning and developing the level of information and effort required to prepare the RBAF, consideration should be given to the following:

- uncomplicated programs with low materiality and a straightforward accountability and risk management environment would require a less detailed and resource intensive RBAF;
- high priority and complex programs with significant materiality (relative to the overall departmental budget) and a diversified and complex environment would require a more detailed RBAF and a larger investment of time and effort;
- the breadth and complexity of the program's RMAF could be used as a guidepost for RBAF development; and
- meaningful information should be provided in each section of the RBAF.

The next sections of this document will guide the reader through the components of an RBAF and the steps involved in their development.

Section 2 - Components of an RBAF

The RBAF consists of the following key components:

1. **Introduction** – a description of the purpose of the RBAF, background, as well as the level of integration with the RMAF, if required.

2. **Roles, Responsibilities and Relationships** – a description of the roles and responsibilities between management, Internal Audit and recipients.

3. **Program Profile** – an explanation of the objectives, underlying rationale and nature of the program, the key areas of inherent risk (Key Risk Areas) as well as a description of recent audit and evaluation findings, which have affected the program profile.

4. **Risk Assessment and Management Summary** – a description of specific risks as well as existing and incremental risk mitigation strategies.

5. **Program Monitoring and Recipient Auditing** – a description of the ongoing monitoring and auditing of recipients that will be undertaken by management. This component would include a description of the risk-based methodology used to make decisions on auditing recipients and possible third party agents who may be permitted to fund other parties through sub-agreements. Relevant details about the objectives, scope, focus, cost, timing, researching and co-ordination requirements for recipient audits would also be provided.

6. **Internal Auditing** – a description of the objectives and timing of a planned internal audit of the transfer payment program. A description of when and how the program will be considered for an internal audit should be provided if it has not yet been considered by the internal audit planning process.

7. **Reporting Strategies** – a description of the plans in place to systematically report on the results of program, monitoring and recipient and internal auditing.

The purpose of each component, suggested development processes and the resulting products are described in the next section.

Section 3 - Steps in the Process

The preparation of the RBAF involves a systematic and analytical process. This section of the guide takes managers and specialist advisors through the distinct steps in this process – the product of each step being a key element of the final framework.

3.1 Introduction

- ❑ The RBAF should be introduced with a concise explanation of the purpose of the RBAF in context of PTP requirements and the demonstration of good governance.
- ❑ A brief description of the program background should be provided to set the overall context. Background information would include events giving rise to the program, the nature of the contribution agreement (i.e. payable, non-repayable), magnitude of the transfer payments and the timeframe of the funding authority.
- ❑ If program management chooses to integrate the RBAF with the RMAF, this section should be used to briefly outline the points and extent of integration.

3.2 Roles, Responsibilities and Relationships

a) Purpose

This section should clearly delineate the respective roles and responsibilities of management and IA in fulfilling the PTP monitoring, auditing and RBAF requirements. A summary of the recipient's role and responsibilities for complying to terms and conditions should also be provided.

b) Process

The PTP (Section 8.5) and the Guide on Grants, Contributions and Other Transfer Payments delineate the roles and responsibilities of management and IA.

- ❑ **Management** is responsible for ongoing financial and operational monitoring and the audit of recipient's compliance to terms and conditions and the audit of recipients. The audit of recipients can also examine whether results data is reliable.

- ❑ **Internal Audit's (IA)** role is to employ risk-based methodologies in planning and conducting audits to provide assurance on the adequacy of integrated risk management practices, management control frameworks and information used for decision-making and reporting on the achievement of overall objectives.

Management is responsible for applying and describing the risk-based approach in the selection of recipient audits. If management is not familiar with a risk-based methodology, IA could be of assistance in discharging this responsibility.

While management has overall responsibility for the RBAF, IA is responsible for employing a risk-based approach in establishing whether the overall transfer payment program should be subject to audit. As such, IA should complete the Internal Auditing section [Section 6.0] of the RBAF.

Managers and IA should consult as soon as the RBAF requirement had been identified. They should reach an agreement on the collaboration needed to complete the Recipient Auditing and Internal Auditing sections of the RBAF.

To facilitate a common understanding of compliance and ongoing monitoring requirements, it may also be beneficial to articulate recipients' roles and responsibilities for meeting contribution agreement terms and conditions.

c) Product

A statement of roles, responsibilities and relationships between PTP management, IA and recipients.

3.3 Program Profile

a) Purpose

The Program Profile should provide the context and the key areas of inherent risk (Key Risk Areas) that evolve from the transfer payment program's objectives and environment. Overall, the profile assists the manager in:

- ❑ meeting good governance expectations through a sound understanding of the accountability and risk management environment; and
- ❑ conducting a more efficient and effective detailed identification and assessment of risk for the Risk Assessment and Management Summary in the next RBAF component.

b) Process

The Program Profile should be developed with reference to the organization's outcomes and design information that has been compiled during recent business planning and the development of the RMAF. As a first step in the process, the "Performance Profile" and other pertinent RMAF data should be verified with participating managers.

Clearly articulated objectives and context will provide the basis for further internal and external environmental analysis and identification of the Key Risk Areas that evolve from the mandate. In this context, for ongoing programs, any recent internal audit or evaluation should be described, particularly the effect that their results may have had on the program.

In the case of a small, uncomplicated program, the Profile can be developed by the manager alone. However, as the complexity and magnitude of the program increases, greater detail will be required from key knowledgeable stakeholders to ensure all Key Risk Areas are identified and adequately described.

Knowledgeable stakeholders include experienced program staff, internal audit and evaluation advisor(s) and, if deemed necessary, external stakeholders. The involvement of a risk management advisor may also be required, depending on the degree of program complexity.

c) Product

The Profile should include:

- ❑ the background, underlying rationale, objectives and need for the program;
- ❑ the target population, resources, product groups, delivery mechanisms, TPP stacking provisions and governance structure; and
- ❑ the key internal and external areas of risk (Key Risk Areas) that evolve from the legislation, mandate, program design and/or operating environment where there is a potential for significant impact on performance (i.e. anticipates, in macro terms, the work to be done in the next section).

3.4 Program Risk Identification, Assessment and Management Summary

Explanatory Note: The key risks should ideally be identified, assessed, and associated mitigation measures either implemented or in progress, prior to the development of the proposed Treasury Board submission (in the case of new policy initiatives, prior to the Memorandum to Cabinet). If available, the departmental Integrated Risk Management Framework (IRMF) would be a primary source of reference or at least a starting point.

a) Purpose

The purpose of this component is to ensure an explicit understanding of the level of key risks. Through systematic risk identification, assessment and development of response or mitigation procedures, managers will acquire an explicit understanding of all aspects of key risks.

Furthermore, this component provides insight into the main operational measures, including controls used to mitigate key risks and thereby contributes data relevant to the explanation of Program Monitoring presented in **Section 3.5**.

b) Process

The preparation of the Risk Assessment and Management Summary section generally requires input from a team of managers and knowledgeable staff within the program area, supported by various functional groups.

The team should carry out the following steps:

Preparation Steps

- ❑ Consider who should participate
- ❑ Clearly define risk
- ❑ Establish a time horizon
- ❑ Customize a risk matrix
- ❑ Consider other tool requirements

Process Steps

1. Understand Objectives

- ❑ Clearly articulate and understand the program's objectives with reference to the outcomes established in the RMAF Logic Model.

2. Risk Identification

- ❑ Identify risk areas (sources of risk) related to the achievement of objectives (e.g. events, hazards, issues, lost opportunities and circumstances that could lead to an impact on stewardship, delivery, outputs, outcomes, etc.); and
- ❑ Conduct a preliminary intuitive analysis of the risk level of each area (high, medium, low) to select the risk areas that require further analysis.

3. Risk Assessment

- ❑ Articulate the particular concerns and existing mitigation measures for the risk areas selected for detailed analysis; and
- ❑ Assess the likelihood and impact of an undesirable effect, given existing mitigation measures, to arrive at a residual level of risk.

4. Risk Response or Mitigation

- ❑ Establish incremental response strategies to avoid, share, transfer, accept and manage the risk.

5. Key Risk Summaries

- Summarize the Key Risks and related particular concerns, existing measures, and Incremental Risk Management Strategies.

A more detailed explanation of these steps is provided in **Appendix B**. A sample set of worksheets that have been designed to support the risk assessment process is also provided in **Appendix E.**

c) Product

The Risk Assessment and Management Summary should include:

- A methodology section which explains the risk definition and model;
- A brief description of the process steps followed;
- The identification of parties involved in the process;
- A Risk Matrix to explain the criteria and define the levels of impact and likelihood
- An elaboration of the Key Risk Areas that were used in the Profile section to explain the overall risk context of the program; and
- summaries of the Key Risks that were identified including particular concerns, existing mitigation measures and incremental risk response strategies, if required.

3.5 Program Monitoring and Recipient Auditing

a) Purpose

The purpose of this section is to provide a description of the monitoring and recipient auditing practices, which are to be undertaken by management. It should reflect the risk identification and elaboration work done in the previous section; in particular, it should reflect the mitigation (in this case, monitoring or recipient auditing) of those risks for which the response was to implement controls.

This section should reflect all activities related to monitoring of the overall program and the recipient's compliance with terms and conditions through detailed operational and financial procedures.

b) Process

Monitoring

The description of overall monitoring should demonstrate that management has those risks for which the mitigation strategy was controls covered by adequate means and measures. Typical monitoring objectives would include:

- ❑ Achievement of established outputs/outcomes;
- ❑ Risks or impediments to the achievement of outputs/outcomes;
- ❑ Due diligence in determining eligibility of recipients and the expenditures of funds;
- ❑ The efficient, effective and economical use of resources, and
- ❑ Whether or not the program is being administered in accordance with appropriate terms and conditions at all stages of the transfer payment life cycle (i.e. selection, administration, delivery and reporting).

The description of detailed monitoring of compliance should outline the operational and financial procedures, including:

- ❑ Interviews and documentation reviews to assess milestone achievements;
- ❑ Expense claim verification procedures;
- ❑ Stacking requirements verification procedures; and
- ❑ Reviews of recipient financial statements.

The existing and incremental mitigation measures for key risks, included in the Program Risk Assessment, Identification and Management Summary section, provide relevant and current information for the preparation of the overall monitoring section. The Results-based Management and Accountability Framework (RMAF) should also provide relevant information with regard to monitoring the achievement of outcomes.

Recipient Auditing

Recipient auditing is often the only effective way to establish:

- ❑ That funds were used for intended purposes;
- ❑ Compliance with terms and conditions; and
- ❑ Reliability of results data.

Recipient Auditing is applicable to contribution agreements due to their conditional nature. In cases where contribution agreements allow recipients to establish sub-agreements, management may also choose to audit the third, fourth, etc. party recipient’s sub-agreement activities; i.e. all the links of the chain through to the end recipient (and the original Terms and Conditions of the Contribution Agreement should provide for this).

Particular attention should be paid to Alternative Service Delivery (ASD) arrangements, i.e. where another party delivers the funds to the end recipient on behalf of the program manager, as this arrangement is inherently higher risk than direct delivery to the recipient.

Grant programs conduct strict eligibility checks before issuing grants. However, once grants are issued, there is no further requirement to verify the recipients' use of funds, i.e. recipient auditing is not applicable in this instance.

The PTP sets out the requirement for a "risk-based" approach for determining whether or not an audit should be conducted and if conducted, its objectives, scope and extent. The risk methodology used here should be consistent with that used in the previous section for program risk identification, assessment and management.

In fact, the results of the risk assessment performed in the previous section (particularly those risk factors having to do with the recipient) should be brought forward and augmented, as needed, by factors that may not have been identified there (e.g. knowledge of the recipient known by the Finance or Internal Audit groups, but not to the program manager) and further augmented by "audit risk" factors (i.e. risk factors having to do with the possibility of the auditor drawing the wrong conclusion – concluding that all is well when it is not or that all is not well when it, in fact, is).

This section should describe the process used for deciding on and planning recipient audits, considering the following steps:

1. Audit Objectives

   ❑ Establish the audit objectives to verify compliance with terms and conditions and, if required, the reliability of results data.

2. Risk Identification and Assessment Criteria

   ❑ Development of a risk-based matrix and criteria to analyse the level of risk associated with recipients of contributions.

3. Risk Factors Rating

   ❑ Consider each audit risk factor and assign a rating. Calculate the overall risk rating, as LOW, MEDIUM or HIGH risk.

4. Audit Planning Decisions

   ❑ Based on overall risk ratings, determine the nature, scope and timing and sampling strategy, if any, for conducting recipient audits (or, where the second, third, etc. party is acting on behalf of the program manager (i.e. an ASD arrangement), end party audits).

A more detailed description of the audit selection process and planning considerations is provided in **Appendix C**.

c) Product

This section includes:

- ❑ a complete and concise explanation of existing and planned monitoring activities; and
- ❑ a summary of the methodology used and decisions taken on conduct of recipient audits, including cost.

3.6 Internal Auditing

a) Purpose

An internal audit of a transfer payment program can provide valuable assistance to management by providing assurance as to the soundness of the risk management strategy and practices, the management control framework and practices and the information being used for decision making and reporting. Specifically, internal audits may examine whether:

- ❑ Due diligence is exercised with regard to the expenditure of public funds;
- ❑ The program is administered in accordance with the terms and conditions of the funding authority;
- ❑ Relevant legislation and policy (e.g. Sections 32, 33 and 34 of the Financial Administration Act and Transfer Payment Policy) are being respected;
- ❑ The program has a risk management strategy and whether systematic risk management is used, where the magnitude and complexity of issues would warrant; and
- ❑ The quality of information is adequate for decision-making.

b) Process

The process for planning internal audits is risk-based and the responsibility of IA. Transfer payment program management should consult with IA as soon as the need for an RBAF is identified (preferably at the Memorandum to Cabinet stage or at least when the need for a submission has been identified) in order to make arrangements for IA input to the relevant RBAF components.

To maintain consistency, the risk assessment methodology used for internal audit decisions should be the same as the one used for program and recipient audit risk assessment; i.e. the results of the program risk assessment should be brought forward and augmented by risk factors that the internal audit group may be aware of, but that the program managers were not (e.g. corporate support risk factors and "audit risk"). Refer to Appendix C for details.

It is recognized that the internal audit function and related planning are ongoing and that, in the case of an ongoing program, they may have already considered the relative risk of the subject program and scheduled, or not, an audit of the program for a specific time in the future or an audit of the program may have already been performed recently. If that is the case, then it would suffice to indicate the results of the audit performed and/or the details of future plans, including expected costs. However, in the case of a new program a complete risk assessment would have to be retrofitted to the existing internal audit plan and the results described here, including objective, scope, timing and expected costs.

c) Product

The products, which should be provided by IA are:

- ❑ A description of the results of any recent internal audits performed;
- ❑ Anticipated audit objectives, scope timing and expected cost, in cases where the need for an audit has been affirmed by IA; and
- ❑ A description of the risk-based audit planning methodology used for all departmental programs (including Transfer Payment Programs);
- ❑ If it is decided that no internal auditing will be performed, there should be an explanation of that decision.

3.7 Reporting Strategies

a) Purpose

The final component of the RBAF ensures that plans are in place to systematically report (both internally and externally) on the results of ongoing monitoring, recipient auditing internal auditing and evaluation. (Note, if reporting of evaluation results is already provided for in the RMAF, it may simply be copied here for completeness purposes).

b) Process

There are many potential users of this information and the reporting strategy should consider all of their needs (e.g. management decision-making, accountability and communication/information sharing). Potential users of risk information include program management, central agencies and internal and external stakeholders.

c) Product

At the minimum, the reporting strategy should include a description of:

- ❑ Periodic reports which are produced for monitoring purposes;
- ❑ Agreed upon recipient audit reports;
- ❑ Evaluation reports;
- ❑ Internal audit reports that will be provided;
- ❑ Who is responsible (especially when multiple parties are involved) for producing reports; and
- ❑ The mechanisms (e.g. annual progress reports, mid-term reports, Departmental Performance Reports) and timeframes for reporting on operational monitoring, recipient and internal audits to the lead department, TBS, TB Ministers and/or Parliament.

Section 4 – RBAF/ RMAF Integration

4.1 Benefits of Integrated Performance and Risk Assessment and Reporting

The PTP also requires that management develop a Results-Based Management and Accountability Framework (RMAF) to provide measurement and evaluation strategies for assessing the performance of a transfer payment program. The RBAF and RMAF are complimentary documents that provide managers with the means and measures for enhancing program monitoring and reporting.

In this regard, the RBAF and RMAF have natural points of integration that relate to the typical analytical and planning approaches used by managers to monitor program operations and performance. For example, it is quite natural for program managers to simultaneously contemplate performance and risk issues when considering whether or not program objectives will be achieved. This integrated thinking facilitates the development of practices and procedures that fulfil the dual function of promoting the achievement of objectives and mitigating risks to performance.

The links between performance and risk, including data collection elements (baseline data) and control frameworks, should be considered at the beginning of the program lifecycle. This integrated approach will assist in clearly identifying all objectives, the program context as well as potential internal and external risks to the achievement of objectives. In this regard, it is recognized that the RBAF must be “risk sensitive” and that the RMAF must be “performance sensitive”, i.e. linking risk to the program outcomes and performance measurement strategies.

Set out below is a proposed outline of an integrated RBAF/RMAF report, which could be referred to as an “Accountability, Risk and Audit Framework”.

Integrated Report

1. Introduction
   - □ Background
   - □ Level of Integration

2. Roles Responsibilities and Relationships
   - □ Roles and Responsibilities of Management and Internal Audit

3. Program Profile
   - □ *Key Objectives and Results*
   - □ Key (Inherent) Risk Areas

Current Source
- □ RBAF
- □ *RMAF*

4. Logic Model
   - □ *Outputs and Outcomes*
   - □ *Risks*

5.. Risk Assessment and Management Summary
   - □ Key Risks and other Risks
   - □ Existing Mitigation Measures
   - □ Incremental Strategies
   - □ Sources:
   - □ *Resources & Activities*
   - □ *Measurement Challenges*
   - □ Influence Challenges

6. Performance Measurement Strategy
   - □ *Performance Indicators*
   - □ Risk Indicators
   - □ *Measurement Strategy*
   - □ Implementation Risk[5]

7. Evaluation Strategy
   - □ *Evaluation Issues*
   - □ *Data Collection Strategy*
   - □ Data Collection Risk

8. Program Monitoring and Recipient Auditing
   - □ Monitoring
     - □ Control Related
     - □ *Performance related*
     - □ Risk Assessment
     - □ Agreement Auditing

[5] Implementation risk refers to the risk events that may arise as a result of the implementation approach that is chosen (see Glossary of Risk Management Terms).

9. Internal Auditing
   - ❑ <u>Internal Audit of the Program</u>

10. Reporting Strategies
    - ❑ *Performance Evaluation*
    - ❑ <u>Risk Audits</u>

Appendix A – Guiding Principles for the Process

The development of a Risk-Based Audit Framework should be conducted under the following guiding principles:

- ***Forward-Thinking*** (Réflexion prospective) – to ensure the framework establishes strategies and controls to address the events and issues which have the potential to influence the achievement of objectives to the end of the funding approval term.

- ***Credibility*** (Crédibilité) - to ensure that the process followed is systematic and respected by stakeholders and that appropriately qualified personnel are involved in the risk assessment process.

- ***Communications*** (Communications) – to ensure a clear and simple language is used to facilitate common understanding so everyone can contribute.

- ***Shared Ownership*** (Co-propriété) – to facilitate collaboration between managers and all stakeholders in the assessment and mitigation of risks as well as meeting accountability requirements for risk management and reporting.

- ***Transparency*** (Transparence) – to ensure stakeholders are aware of the nature and level of risk involved in management and operational service delivery.

- ***Utility*** (Utilité) – to ensure that the framework serves as a useful management tool for explaining and integrating risks factors and strategies at all levels of planning, decision-making and reporting.

- ***Flexibility*** (Flexibilité) – to respond to the ever-changing context within which policies, programs and initiative operate and to thereby ensure that the frameworks are regularly revisited and adapted as necessary.

Appendix B - Process for the Risk Assessment and Management Summary

Preparation Steps

□ **Consult your Corporate Integrated Risk Management Framework**. Use this as the first line of inquiry, if available.

□ **Consider who should participate**. For more complex programs, it is generally advisable to use a multi-disciplinary team approach. This team would normally include a risk management advisor. In addition, leader/facilitator/author roles should be considered.

□ **Clearly define risk**. Two definitions of risk are included in the Glossary of Risk Management Terms. The International Standards (ISO) definition presents a basic and essential meaning of risk. The other definition, which is derived from the *TBS Integrated Risk Management Framework,* provides additional context in relation to achieving objectives.

□ **Establish a time horizon**. The time-span should reflect the number of years for which funding is requested.

□ **Establish the Risk Matrix**. In estimating the level of risk, the analysis of the likelihood (high, medium, low) and level of impact (severe, moderate, minor) should be based on an agreed upon Risk Matrix comprised of quantitative and qualitative criteria, which reflect damages/liabilities, operational effects, reputation loss and loss of opportunity concerns particular to the circumstances. These criteria are generally collected together in what is commonly called a Risk Matrix. The Risk Matrix ensures consistent assessments and enhances communication (See **Appendix E** for a sample Risk Matrix).

□ **Explore the availability of other risk management tools.** A **Sources of Risk Template** illustrated in **Appendix F** is a useful tool to help identify possible risk areas. A **Risk Management Action (Tolerance) Model,** as suggested in the TBS Integrated Risk Management Framework, could be used in considering the actions that should be taken to address the various levels of risk (see **Appendix G**). Other samples of these tools may exist as part of your Corporate Integrated Risk Management Framework.

□ The five process steps explained below employ various worksheets and tools from the Risk Scorecard Toolkit presented in **Appendix E.**

Step 1: Understanding of Objectives

□ Clearly articulate and understand the program's objectives with reference to the outcomes established in the RMAF.

Step 2: Risk Identification

- ❑ Brainstorm and list all possible significant Risk Areas (e.g. events, hazards, issues, problems, opportunities and circumstances that could lead to an impact) on a Risk Identification Worksheet, such as is shown in **Exhibit B1** below. A Sources of Risk Template could be used to prompt and verify whether or not all risks have been explored (see **Appendix F**).

- ❑ For each identified Risk Area, conduct a preliminary intuitive analysis of the risk level (high/medium/low; considering both Inherent Risk and Likelihood Factors) to determine the most significant/sensitive risks that might require further detailed analysis.

- □ Select the Risk Areas that should be subject to a more detailed analysis. Usually, all of the items that have been given a preliminary rating of "high" and "medium" are analysed in more detail. However, items that have been rated as "low" could also be analysed in more detail, depending on time and cost considerations (NB: having a complete listing of risks may be advantageous to the program manager, in the long run, as environmental events may result in shifting risk profiles over time and those risks currently rated as low may increase in importance and vice versa).

- □ Once the list of risk areas is considered reasonably complete, and a preliminary risk assessment has been established for each risk area, conduct a preliminary risk assessment of the "potential for surprise." If the "potential for surprise" is considered to be a HIGH Risk, additional effort should be invested in articulating specific risk areas that reflect the "potential for surprise" events in order to reduce the level of risk to MEDIUM or Low.

Exhibit B1: Risk Areas Identification Worksheet (example only)

Risk Areas	**Project Objective:** To achieve stated outcomes based upon a sound management control framework *(including an estimate of "potential for surprise" events)*			
		Preliminary Risk Assessment		
		High	**Med**	**Low**
1.	Regional Capacities		🗐	
2.	Cut backs within Third Party Delivery Agents	🗐		
3.	Partnerships	🗐		
4.	Information Systems		🗐	
5.	Challenges to Branch Decisions (external stakeholders)			🗐
6.	Information for Decision-Making		🗐	
7.				
8.				
9.				
10.	Potential for Surprise		🗐	

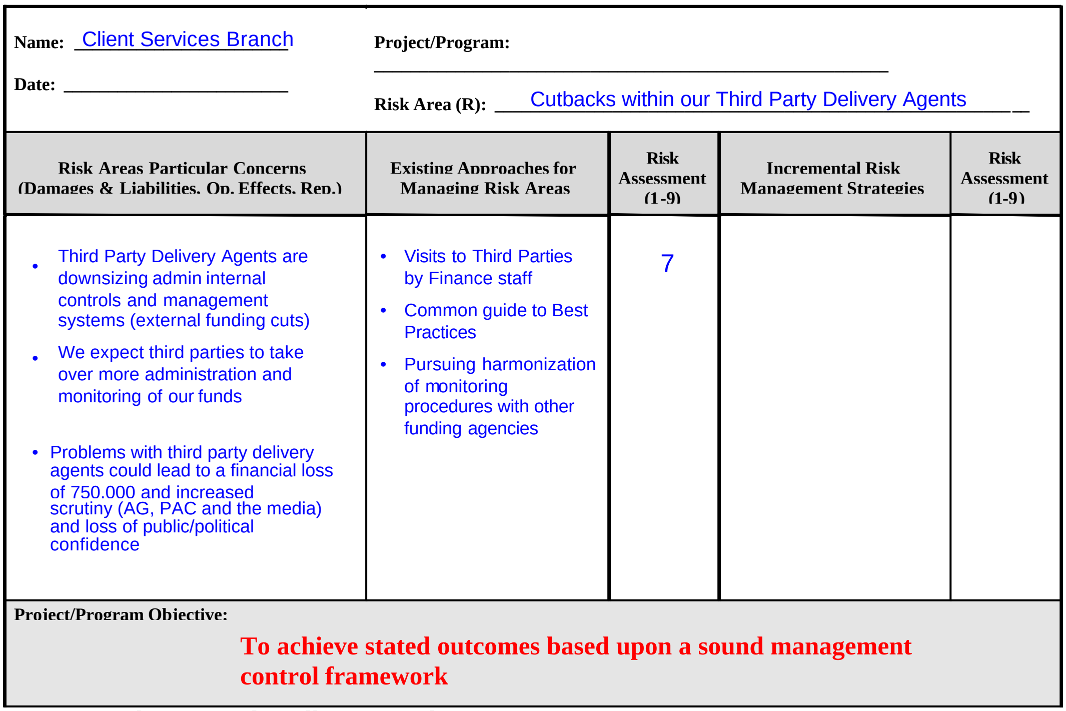
Source – *Risk Scorecard Tool Kit* (Appendix E)

Step 3: Risk Assessment

- Using separate Risk Analysis Worksheets for each Risk Area indicate, on the first column, your particular concerns and impacts related to the achievement of objectives (see example, **Exhibit B2**)

- On the second column of the Risk Analysis Worksheet, indicate the existing measures for mitigating the concerns and impacts. Existing measures can directly or indirectly mitigate risk.

Exhibit B2: Risk Analysis Worksheet (example only)



Name: Client Services Branch

Date: ____________________

Project/Program: ______________________________

Risk Area (R): Cutbacks within our Third Party Delivery Agents

Risk Areas Particular Concerns (Damages & Liabilities, Op. Effects, Rep.)	Existing Approaches for Managing Risk Areas	Risk Assessment (1-9)	Incremental Risk Management Strategies	Risk Assessment (1-9)
• Third Party Delivery Agents are downsizing admin internal controls and management systems (external funding cuts) • We expect third parties to take over more administration and monitoring of our funds • Problems with third party delivery agents could lead to a financial loss of 750.000 and increased scrutiny (AG, PAC and the media) and loss of public/political confidence	• Visits to Third Parties by Finance staff • Common guide to Best Practices • Pursuing harmonization of monitoring procedures with other funding agencies	7		

Project/Program Objective:

To achieve stated outcomes based upon a sound management control framework

Source – Risk Scorecard Toolkit (Appendix E)

- Upon completion of columns one and two, consider the impact and the likelihood of your concerns (column 1) materializing, given existing measures information (column 2). The resulting estimate of residual risk reflects a reduced level of risk impact and/or likelihood due to existing mitigation measures.

- The Risk Matrix, **Exhibit B3**, and the Risk Scorecard, **Exhibit B4**, are tools that can assist in estimating the level of residual risk.

- Having established the risk level, you would now use the Risk Scorecard to position the risk in square #7, the point of intersection for high likelihood and moderate impact. You will notice that the Scorecard (**Exhibit B4**) indicates that the risk falls into an "unacceptable" zone, which normally implies that, given existing measures, it is necessary to develop incremental strategies to reduce the residual risk further (NB: what is considered unacceptable will vary according to the risk propensity of the organization or program manager involved).

Exhibit B3: Risk Matrix ™
(Example Only - To be customized to the particular context)

Qualitative Measures of Impact

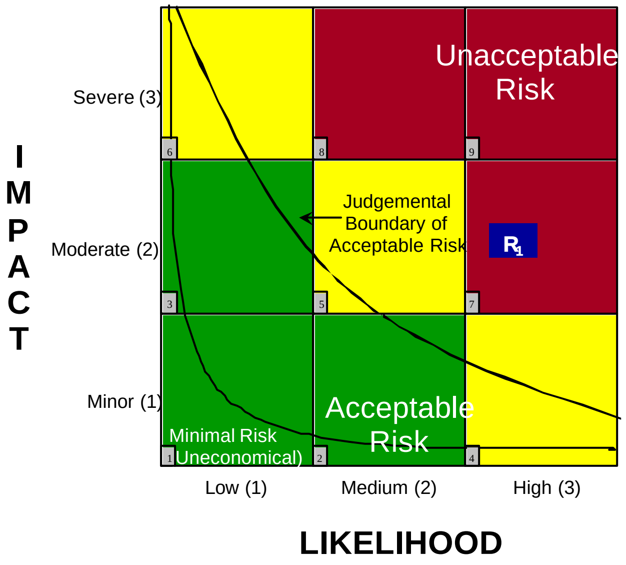
Level	Impact	Damage & Liability	Operational Effects	Reputational Loss
3	SEVERE	• Death • Loss of major asset(s) > $1M • Serious environmental damage	• Disruption of all essential programs/reviews > 7 days for large numbers ofclients	• Significant loss of client group trust • Public outcry for removal of Minister and/or departmental official
2	MODERATE	• Serious Injury • Loss of asset(s) $100K - $1M • Some environmental damage	• Disruption of some essential programs/services < 7 days	• Some loss of client group trust • Negative media attention
1	MINOR	• First Aid Treatment • Loss of asset(s) < $100K • Temporary environmental effect	• Schedule delays to minor projects	• Setback in building of client group trust • Some unfavourable media attention

Qualitative Measures of Likelihood (+24 Months Ti Horizon)

Level	Likelihood	Description
3	High	The event is expected to occur in most circumstances (+ 70%)
2	Medium	The event should occur at sometime (25 - 70%)
1	Low	The event occurring is unlikely (< 25%)

* The time horizon reflects the number of months before the expiration of the TBS authority which is, typically, 12 – 60 months.

Exhibit B4: Risk Scorecard Ò
(Example only)



Risk Areas	
R1	Cutbacks within our Third Party Delivery Agents
R2	
R3	

Source – Risk Scorecard Toolkit (Appendix E)

Step 4: Risk Response

- ❑ In the cases where the estimated residual level of risk is in the “unacceptable” zone (i.e. grid squares 7, 8 and 9), consideration should be given to developing incremental strategies to reduce the residual level of risk.

- ❑ Risk Response options could include a variety of strategies. You may choose to reduce impact by sharing the risk with delivery partners or avoiding the risk by not undertaking the activity that generates the risk. In situations where risk reduction options are not effective or available, risk avoidance may be your option of choice.

- ❑ Guidance on how to respond to a given level of assessed risk may be available if your organization has established a Risk Management Action (Tolerance) Model such as the sample shown in **Exhibit B6**.

Exhibit B5: Risk Analysis Worksheet

Name: Client Services Branch

Project/Program: ____________________

Date: ____________________

Risk Area (R): Cutbacks within our Third Party Delivery Agents

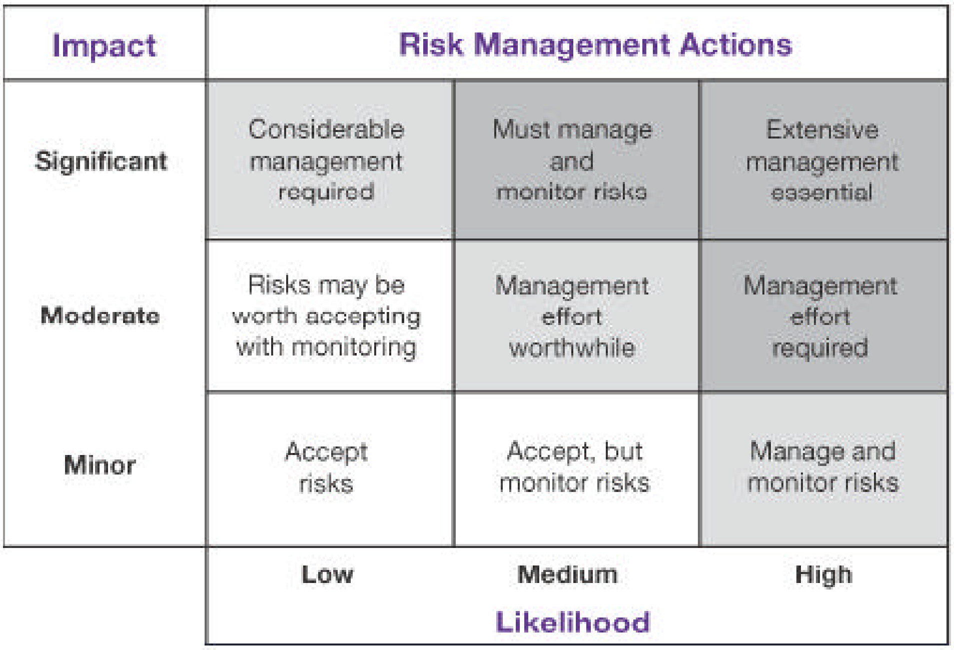
Risk Areas Particular Concerns (Damages & Liabilities, Op. Effects, Rep.)	Existing Approaches for Managing Risk Areas	Risk Assessment (1-9)	Incremental Risk Management Strategies	Risk Assessment (1-9)
• Third Party Delivery Agents are downsizing admin internal controls and management systems (external funding cuts) • We expect third parties to take over more administration and monitoring of our funds • Problems with third party delivery agents could lead to increased scrutiny (AG, PAC and the media) and loss of public/political confidence	• Visits to Third Parties by Finance staff • Common guide to Best Practices • Pursuing harmonization of monitoring procedures with other funding agencies	7	• **Continue to develop cooperative monitoring** • **A communications strategy to inform third parties of our requirements** • **Consider an audit of Branch Procedures for Monitoring Third Party spending**	

Project/Program Objective:

To achieve stated outcomes based upon a sound management control framework

Source – Risk Scorecard Toolkit (Appendix E)

Exhibit B6 Risk Management Action (Tolerance) Model



Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

Source – *Integrated Risk Management Framework*, TBS

- The degree of risk tolerance is based on the amount or level of risk that is generally acceptable to stakeholders. Organizations and stakeholders' tolerance levels vary in relation to the particular risk area being considered. For example, stakeholders may have a low tolerance for risks to health and safety and a higher tolerance for development project risk.

- Following the development of the incremental strategies, as illustrated in **Exhibit B5**, you could use a Risk Response Worksheet, like the one presented below, to review what has been done and to consider other management and communication strategies.

Exhibit B7: Risk Response Strategies Worksheet

- **Review**- Who should review this analysis to improve/strengthen its precision?
  - Departmental Security, MIS and Internal Audit groups

- **Communication/Reporting** - Who should be informed?
  - Branch Head

- **Implementation Plans** - What are the implications of the incremental risk management strategies (i.e. timeframe; assigned responsibility; cost-benefit?)
  - Minimal, except for the conduct of an audit, which will be paid by the Audit Branch

- **Monitoring Plan** - What information should be monitored? What is the Source?
  - The Branch Head will assign responsibility for implementing the incremental risk management strategies and follow-up as part of ongoing monthly management meetings

- **Surprise Events/Contingencies** - Consider what measures or contingency plans exist or should be established/enhanced
  - Discuss at monthly meetings and prepare a communication plan for managing a significant impact from a surprise event

- **Organizational Integration** - Who should be involved in future analysis?
  - Given that some Branch directorates were absent during this assessment, all directorates will be encouraged to attend

Source – Risk Scorecard Toolkit (Appendix E)

Step 5: Prepare Key Risk Summaries

- Prepare summaries of the particular concerns and existing measures for all of the risks that were analysed in detail.

- When many risk areas are subject to detailed analysis, risk summaries can be prepared for a representative sample of the risk areas analysed. Risk summaries can be presented in two groupings – “Key Risks” and “Other Risks”. For the most part, the “Key Risks” category includes risks rated as “medium and high” which usually have proposed incremental risk management strategies for reducing the level of risk. “Low” risk areas may be included as “Key Risks”, if you wish to highlight their importance in terms of the significant risk mitigation investments that have been made and that continued close monitoring is required;

- The description of “Other Risks”, which reflects the lower residual risks, contributes to a more complete understanding of the Risk Areas and residual risk levels facing the program, policy or initiative as well as the existing and incremental mitigation strategies.

- A sample Risk Summary for *a hypothetical transfer payment initiative* is presented below in **Exhibit B8**.

Exhibit B8: Sample Risk Summary

Key Risk #x
Cutbacks within Our Third Party Delivery Agents

Areas of Concern

The third party agents are experiencing cutbacks in their funding and are eliminating some of the resources and procedures that had provided control activities related to our transfer payments. Transferring more delivery responsibilities to third party agents may result in financial loss and increased scrutiny by oversight agencies.

Existing Measures

Third party activities are currently monitored through field visits conducted by our Finance Officers and provincial representatives who share information with us. In addition, third parties have been provided a best practice guide for administering our transfer payment.

Incremental Risk Management Strategy

A communication will be prepared to remind all third parties to follow the best practice guide. In addition, we will continue to develop information sharing practices with the provinces. Further, an audit of the monitoring practices of Finance Branch will be requested.

- Information on how key risks will be monitored should be explained, as part of overall program monitoring which is summarized in **Section 3.5**.

Appendix C - Process for Planning Recipient and Internal Audits

RECIPIENT AUDIT PLANNING

Management is responsible for determining which recipients and/or third parties should be audited, as well as the scope and timing of the audits. For example, if there are only a few contribution agreements that appear to be intuitively "high risk", management could simply audit all of them.

Collaboration between the manager and the internal auditor is desirable, as the internal auditor has the required audit expertise and may have special knowledge of the recipient(s).

Step 1 — Recipient Audit Objectives

The objectives for recipient audits involve the examination of whether there was compliance with terms and conditions and whether funds were used for the intended purposes.

Step 2 — Risk Factors Analysis Design

The process and methodology for determining risk, for recipient audit purposes, should be simply an extension of the exercise conducted in Section 3.4 and illustrated in Appendix B. It was described in Section 3.5 (b).

Those risk factors identified in Section 3.4, that pertain to recipients are brought forward and augmented by additional recipient-related factors that may be known to others (e.g. the Comptroller's, or Audit organization), but not to the program managers, and further augmented by audit risk (Internal Audit may help with these).

Exhibit C1 illustrates some risk factors (Impact, Likelihood and Audit Risk factors), along with sample criteria, that may be used to augment those carried forward from Section 3.4 (NB: the list of risk factors provided in Exhibit C should be considered as a sampling of factors that may be relevant in a given circumstance; in actual use, this list should be added to or subtracted from, as needed). Their assessment will be described in the next Step.

Step 3 – Recipient Audit Risk Factors Rating

As the recipient-related program risks would have already been rated, they don't have to be re-rated. They are simply carried forward. However the ratings carried forward, for those cases where the mitigation strategy is the implementation of controls, should be the rating before mitigation (to ensure that the rationale of testing the efficacy of controls, as part of the audit program, is preserved; i.e. to recognize that the efficacy of the mitigation measures that involve controls is dependent on the quality of their implementation and on their appropriate use).

Exhibit C1: Sample Recipient Audit Planning Worksheet

Recipient Audit Risk Factors	**Risk Rating Scale**		**Rating**	**Notes**
	Low	**High**		
Impact Factors				
▪ Materiality	<$xK - $1xxK	>$1xx K - $xM		
▪ Political Sensitivity	Not sensitive	Sensitive		
▪ Policy/Program Importance				
Likelihood/Probability Factors				
▪ Complexity of the Recipient Environment	Not Complex	Highly Complex		
▪ Systematic Risk Assessment	Recently (< 1yr)	Not Completed		
▪ Governance Risk	Few Concerns	Many Concerns		
▪ Control Risk Experience with Recipient	Few Concerns	Many Concerns		
▪ Recipient Experience with Contributions	Considerable	Little		
▪ Past Experience with Recipient	Few Issues	Many Issues		
▪ Past Audit Experience with Recipient	Few Issues	Many Issues/Not Audited		
Audit Risk				
▪ Risk of drawing the wrong audit conclusion				
- Impact	Low	High		
- Likelihood	Low	High		
NB: Some of these factors may have already been identified in the program risk assessment.				
Recipient Audit Risk Rating	**Low Risk**	**Medium Risk**	**High Risk**	
OVERALL RATING	⬬			

The sample Impact and Likelihood risk factors provided in Exhibit C1 are to be used in combinations, to obtain additional risk ratings for recipient audit purposes. In essence, using the same method used in Section 3.4 and the sample work instruments described in Appendix B, the risk profile developed for program risk can be recast for recipient risk by subtracting those risk factors that do not pertain to recipients, adding appropriate inherent risk factors from Exhibit C, conditioned by likelihood risk factors also from Exhibit C and similarly for the audit risk factors, ending up with a new risk profile for recipient audit purposes.

Once the rating of individual risk factors in the recipient risk profile has been completed, an overall risk rating is made (i.e. a composite rating) and the program manager is in a position to make recipient audit decisions.

Step 4 – Recipient Audit Planning Decisions

The recipient audit planning process entails establishing the objectives, scope, extent and timing of the audit, including a sampling strategy, where there are multiple recipients that are homogenous (if not homogenous, the risk profile could be used to decide which recipients to audit). This step may require assistance from an internal or external audit specialist.

The approach suggested as a general guide, below, could be adjusted due to numerous factors. For example, if the TBS terms and conditions require that a program audit be conducted during the timeframe of the funding authority, an audit would be conducted regardless of whether or not the risk was rated as high. However, if the risk is low, the audit may be less detailed than if the risk was high. Also, the audit program for intermediaries (sometimes called "third parties") will differ from that for the end recipient (e.g. the relationship between the program manager and the intermediary may be governed by a contract, while that with the end recipient will be governed by a contribution agreement).

Where the program manager relies on a recipient-initiated external audit (typically a financial audit), the manager will need to provide for compensatory monitoring/auditing to deal with those scope elements that might be covered in a broader-based recipient audit but not covered in the external financial audit.

As a general guide, one could consider the following audit approaches in relation to the levels of risk:

❑ LOW Risk – Conduct a minimum number of recipient audits.

  - Review a small sample (all if only a few) of client financial statements audits (prepared by recipient's external auditor) for anything unusual; the audit may also include lines of inquiry regarding whether the funds provided were used for the purpose intended.

  - Consider conducting at least a few recipient audits to signal that Canada will exercise its "right to audit" clause, as a matter of principle.

- ❑ MEDIUM Risk - Conduct a sample of recipient audits.

  - Review a larger sample (all if only a few) of client financial statements audits (prepared by recipient's external auditor) for anything unusual. Consider establishing the requirement for the recipient to include a schedule in their financial statements which details the expenditures of contribution funds as well as a request for the external auditor to include this schedule in their audit testing and audit opinion.

  - The sample of recipient audits should provide representative coverage according to the issues underlying the audit rating. For example, the recipients that are very inexperienced with contributions or have minimal business experience should be included in the audit coverage.

  - Consider inclusion of lines of inquiry regarding whether the funds provided were used for the purpose intended;

  - Consider possible improvements to the Management Control Framework that could be cost-effectively implemented to reduce the recipient audit risk.

- ❑ HIGH Risk - Conduct a larger sample of recipient audits.

  - Review a large sample (all if cost-effectively possible) of client financial statements audits (prepared by recipient's external auditor) for anything unusual. Consider establishing the requirement for the recipient to include a schedule in their financial statements which details the expenditures of contribution funds as well as a request for the external auditor to include this schedule in their audit testing and audit opinion;

  - The sample of recipient audits should give representative coverage according to the issues underlying the audit rating. For example, the recipients that are very inexperienced with contributions or have minimal business experience should be included in the audit coverage;

  - Consider inclusion of lines of inquiry regarding whether the funds provided were used for the purpose intended;

  - Consider possible improvements to the Management Control Framework that could be cost-effectively implemented to reduce the recipient audit risk;

INTERNAL AUDIT PLANNING

The process for internal audit planning is similar to that of planning for Recipient Audit, except that for internal audit planning, all of the risk factors identified for program management purposes is brought forward and augmented by risk factors not known to the program managers (e.g. those known to the Internal Audit, the Comptroller's organization and other stakeholders) and by audit risk factors.

As there is normally an ongoing Internal Audit Planning process, the risk profile developed here would be added the overall departmental risk profile and reassessed, to see whether the audit of the subject contribution program warrants displacement of other audits already planned.

Appendix D – Transfer Payment Accountability and Risk Management Environment

Exhibit D1: Transfer Payment Accountability and Risk Infrastructure

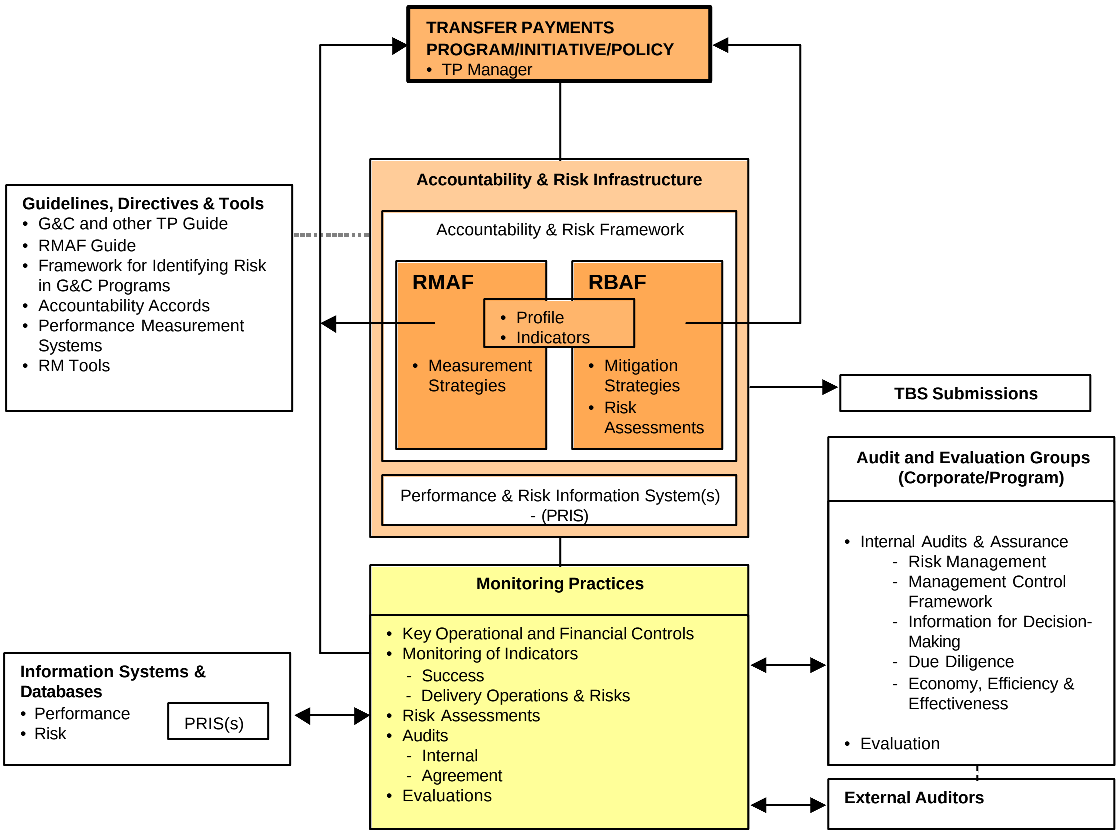
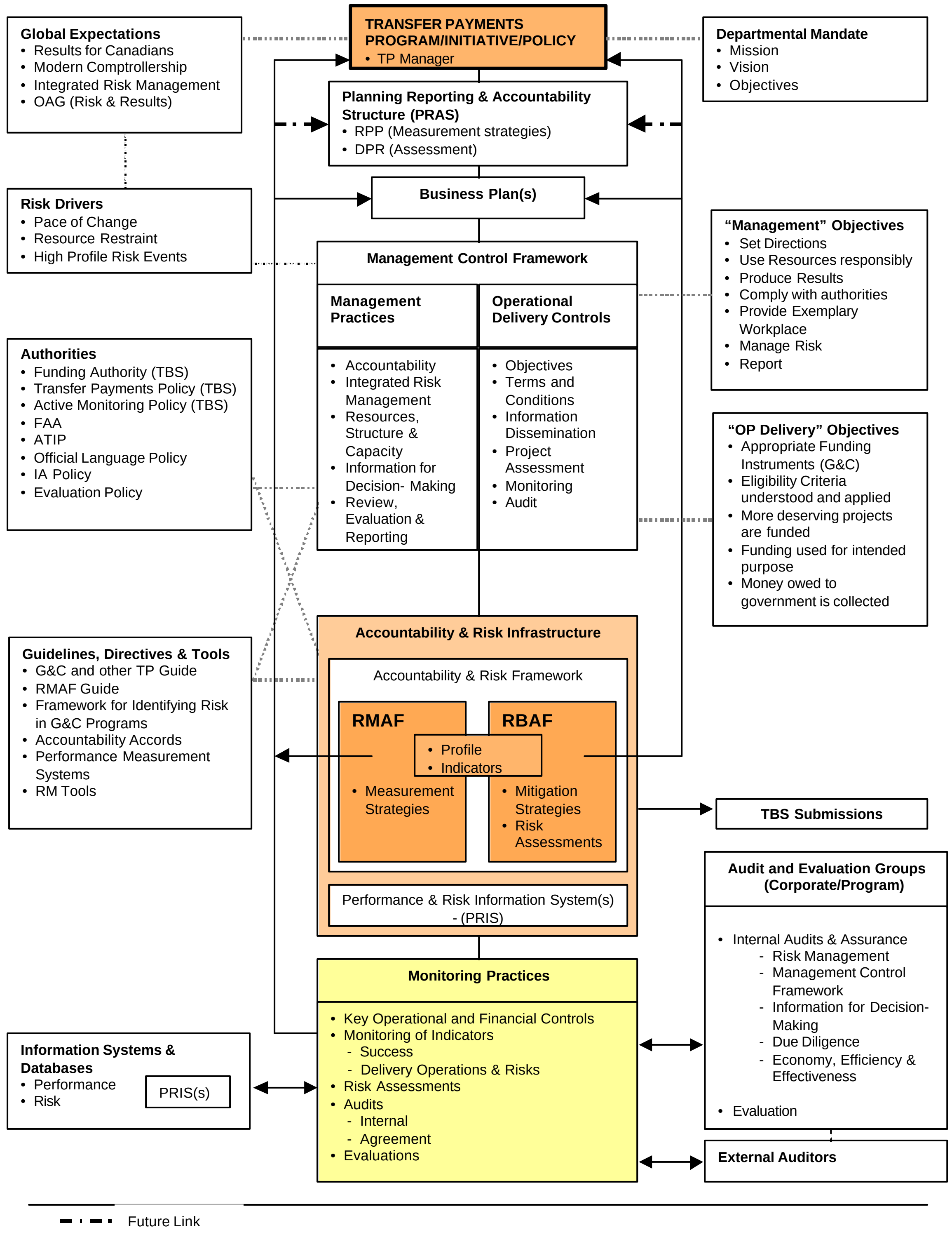

TRANSFER PAYMENTS PROGRAM/INITIATIVE/POLICY
• TP Manager
Guidelines, Directives & Tools
• G&C and other TP Guide
• RMAF Guide
• Framework for Identifying Risk in G&C Programs
• Accountability Accords
• Performance Measurement Systems
• RM Tools
Accountability & Risk Infrastructure
Accountability & Risk Framework
RMAF
RBAF
• Profile
• Indicators
• Measurement Strategies
• Mitigation Strategies
• Risk Assessments
Performance & Risk Information System(s) - (PRIS)
TBS Submissions
Audit and Evaluation Groups (Corporate/Program)
• Internal Audits & Assurance
- Risk Management
- Management Control Framework
- Information for Decision-Making
- Due Diligence
- Economy, Efficiency & Effectiveness
• Evaluation
Monitoring Practices
• Key Operational and Financial Controls
• Monitoring of Indicators
- Success
- Delivery Operations & Risks
• Risk Assessments
• Audits
- Internal
- Agreement
• Evaluations
Information Systems & Databases
• Performance
• Risk
PRIS(s)
External Auditors

Exhibit D2: Overall Transfer Payment Accountability and Risk Management Environment



Global Expectations
- Results for Canadians
- Modern Comptrollership
- Integrated Risk Management
- OAG (Risk & Results)

TRANSFER PAYMENTS PROGRAM/INITIATIVE/POLICY
- TP Manager

Departmental Mandate
- Mission
- Vision
- Objectives

Planning Reporting & Accountability Structure (PRAS)
- RPP (Measurement strategies)
- DPR (Assessment)

Business Plan(s)

Risk Drivers
- Pace of Change
- Resource Restraint
- High Profile Risk Events

Management Control Framework

Management Practices
- Accountability
- Integrated Risk Management
- Resources, Structure & Capacity
- Information for Decision- Making
- Review, Evaluation & Reporting

Operational Delivery Controls
- Objectives
- Terms and Conditions
- Information Dissemination
- Project Assessment
- Monitoring
- Audit

“Management” Objectives
- Set Directions
- Use Resources responsibly
- Produce Results
- Comply with authorities
- Provide Exemplary Workplace
- Manage Risk
- Report

Authorities
- Funding Authority (TBS)
- Transfer Payments Policy (TBS)
- Active Monitoring Policy (TBS)
- FAA
- ATIP
- Official Language Policy
- IA Policy
- Evaluation Policy

“OP Delivery” Objectives
- Appropriate Funding Instruments (G&C)
- Eligibility Criteria understood and applied
- More deserving projects are funded
- Funding used for intended purpose
- Money owed to government is collected

Accountability & Risk Infrastructure

Accountability & Risk Framework

RMAF
- Measurement Strategies

RBAF
- Mitigation Strategies
- Risk Assessments

- Profile
- Indicators

Performance & Risk Information System(s) - (PRIS)

Guidelines, Directives & Tools
- G&C and other TP Guide
- RMAF Guide
- Framework for Identifying Risk in G&C Programs
- Accountability Accords
- Performance Measurement Systems
- RM Tools

TBS Submissions

Audit and Evaluation Groups (Corporate/Program)
- Internal Audits & Assurance
  - Risk Management
  - Management Control Framework
  - Information for Decision-Making
  - Due Diligence
  - Economy, Efficiency & Effectiveness
- Evaluation

Monitoring Practices
- Key Operational and Financial Controls
- Monitoring of Indicators
  - Success
  - Delivery Operations & Risks
- Risk Assessments
- Audits
  - Internal
  - Agreement
- Evaluations

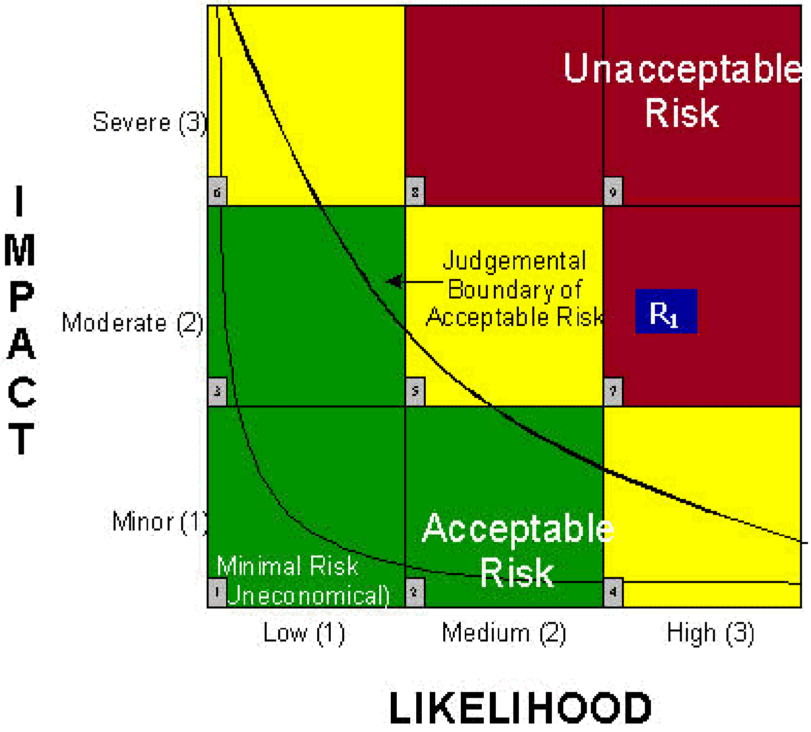
Information Systems & Databases
- Performance
- Risk

PRIS(s)

External Auditors

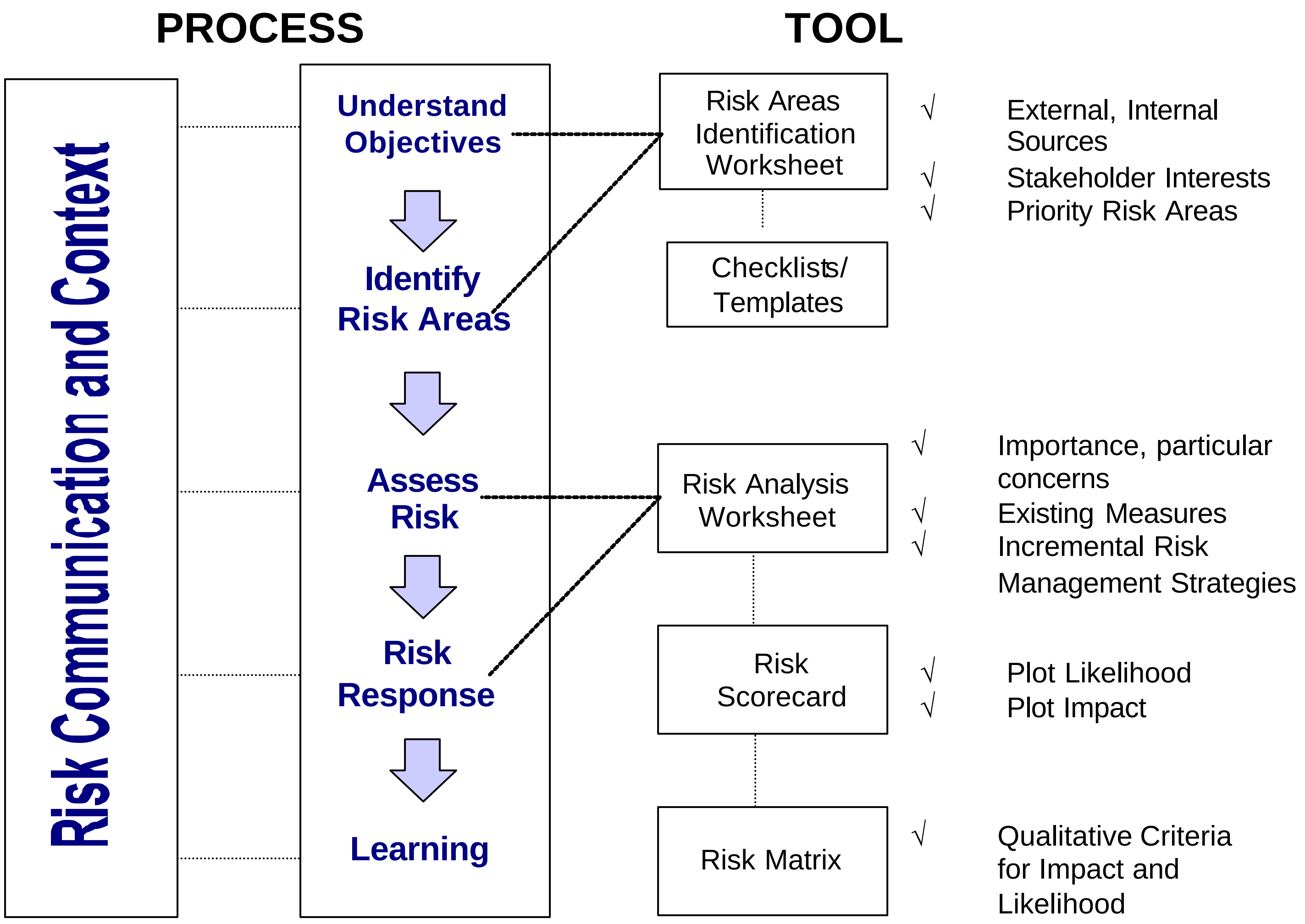
▬ · ▬ · Future Link

Appendix E – Risk ScorecardÒ[*] Toolkit



[*] “Risk Scorecard is a Registered Trade Mark of Wiltshire Consulting Inc. The Risk Scorecard Toolkit has been provided with the permission of Wiltshire Consulting Inc.”

Risk Scorecard^{Ò} Overview Process and Tools:



PROCESS

TOOL

Risk Communication and Context

Understand Objectives

Identify Risk Areas

Assess Risk

Risk Response

Learning

Risk Areas Identification Worksheet

Checklists/ Templates

√ External, Internal Sources

√ Stakeholder Interests

√ Priority Risk Areas

Risk Analysis Worksheet

√ Importance, particular concerns

√ Existing Measures

√ Incremental Risk

Management Strategies

Risk Scorecard

√ Plot Likelihood

√ Plot Impact

Risk Matrix

√ Qualitative Criteria for Impact and Likelihood

Qualitative Measures of Impact and Likelihood

Qualitative Measures of Impact

Level	Impact	Damage & Liability	Operational Effects	Reputational Loss
3	SEVERE	▪ Death ▪ Loss of major asset(s) > $1M ▪ Serious environmental damage	▪ Disruption of all essential programs/reviews > 7 days for large numbers of clients	▪ Significant loss of client group trust ▪ Public outcry for removal of Minister and/or departmental official
2	MODERATE	▪ Serious Injury ▪ Loss of asset(s) $100K - $1M ▪ Some environmental damage	▪ Disruption of some essential programs/services < 7 days	▪ Some loss of client group trust ▪ Negative media attention
1	MINOR	▪ First Aid Treatment ▪ Loss of asset(s) < $100K ▪ Temporary environmental effect	▪ Schedule delays to minor projects	▪ Setback in building of client group trust ▪ Some unfavourable media attention

Qualitative Measures of Likelihood (+24 Months Time Horizon)

Level	Likelihood	Description
3	High	The event is expected to occur in most circumstances
2	Medium	The event should occur at sometime
1	Low	The event occurring is unlikely

Risk Areas Identification Worksheet©

Project/Objective: ____________________			
Risk Areas *(Including estimate of surprise element)*			
	Preliminary Risk Assessment		
	High	**Med**	**Low**
1.			
2.			
3. 4.			
5.			
6.			
7.			
8.			
9.			
10. **Potential for Surprise**			

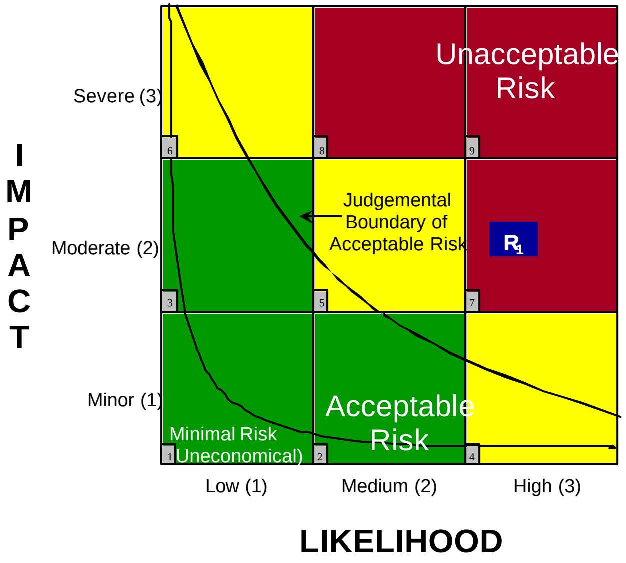
Risk Analysis Worksheet©

Name: ____. Project/Program: ______________________________________.

Date: ______________________________. Risk Area (R): ____.

Risk Areas Particular Concerns (Damages & Liabilities, Operational Effects, Reputation)	Existing Measures for Managing Risk Areas	Risk Assessment (1-9)	Incremental Risk Management Strategies	Risk after Incremental (1-9)
Project/Program Objective:				

Risk Scorecard Ò



Risk Areas	
R1	Cutbacks within our Third Party Delivery Agents
R2	
R3	

Source – Risk Scorecard Toolkit (Appendix E)

Note: Use attached Risk Matrix to assess impact and likelihood to assess (see page 6).

Risk Response Strategies Worksheet:

- **Review** - Who should review this analysis to improve/strengthen its precision?

- **Communication/Reporting** - Who should be informed?

- **Implementation Plans** - What are the implications of the incremental risk management strategies (i.e. timeframe; assigned responsibility; cost-benefit?)

- **Monitoring Plan** - What information should be monitored? What is the Source?

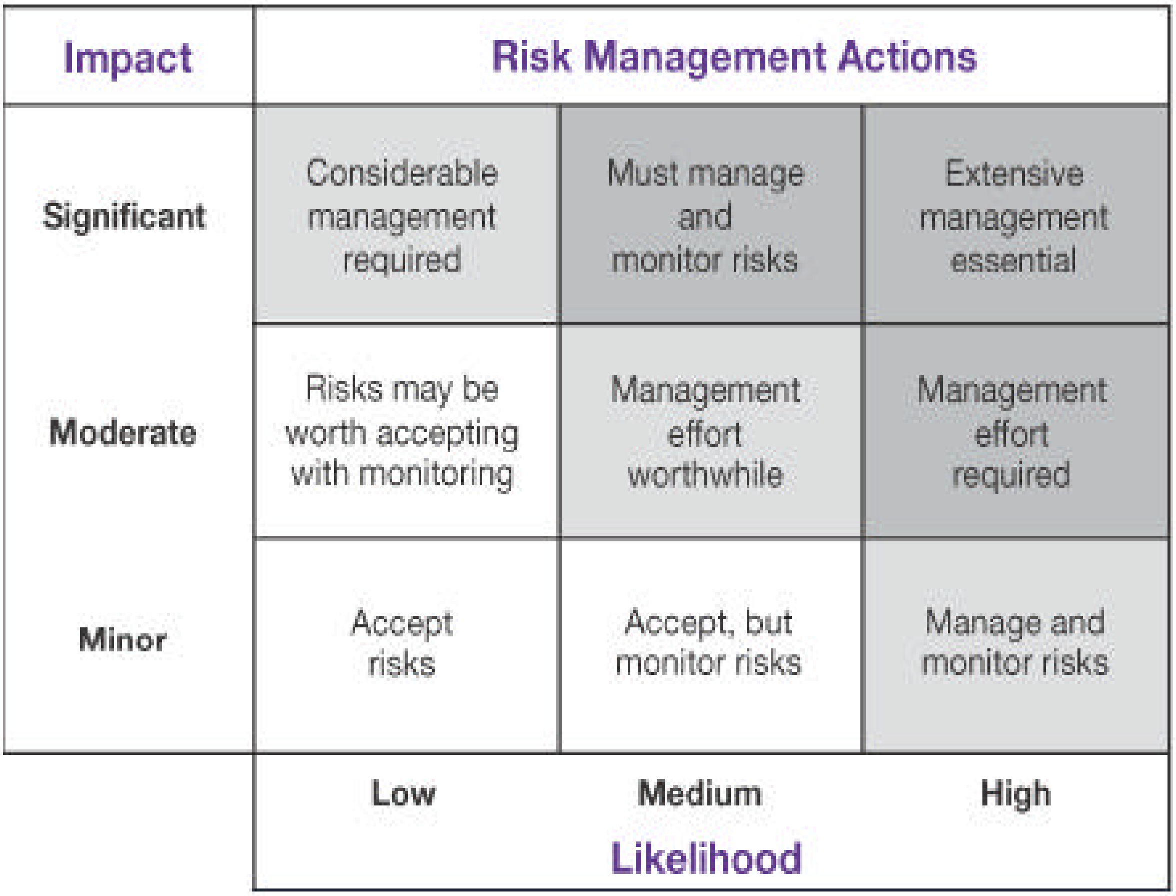
- **Surprise Events/Contingencies** - Consider what measures or contingency plans exist or should be established/enhanced

- **Organizational Integration** - Who should be involved in future analysis?

Appendix F – Sources of Risk Template

Strategic Risk Areas	Operational Risk Areas	Project Risk Areas
Highly Sensitive ⇒ Public/media opinion ⇒ Partnership – interaction ⇒ Safety and security ⇒ Sustainability of resource levels/service capacity ⇒ Human resource management ⇒ Management and accountability structures ⇒ Communications capacity ⇒ Information for decision making **Legal** ⇒ Actions to consider requirements of laws regulations and treaties **Political** ⇒ Media/public scrutiny ⇒ Loss of confidence of central agencies ⇒ Maintaining public service values, ethics, fairness and responsible spending ⇒ Program Objectives linked to government priorities **Performance Measurement** ⇒ Influence challenges ⇒ Measurement strategies ⇒ Reporting system ⇒ Evaluation strategy	**Contributions** ⇒ Selected recipients meet eligibility requirements ⇒ Funds used for appropriate purposes ⇒ Terms and conditions reflect nature complexity and materiality ⇒ Compliance with authorities **Process** ⇒ Efficient processes ⇒ Sufficient capacity ⇒ Timely processing **Integrity** ⇒ Fraud, illegal acts (employee, clients, suppliers) **Human Resources** ⇒ Loss of corporate memory ⇒ Resource allocation matched with workload ⇒ Capacity **Information Processing/ Technology** ⇒ Adequate infrastructure ⇒ Timely, relevant, reliable information **Financial** ⇒ Money owed is collected ⇒ Commitment ⇒ Monitoring ⇒ Third party payout for products and services	**Technical** ⇒ Defining requirements as technology changes ⇒ Advances in technology ⇒ User needs analysis **Development/ Implementation** ⇒ Developments/implementation process formality proportionate with the scope of project ⇒ Project size (large = Complex) ⇒ Dynamic business environment **Management** ⇒ Adequate business case for project ⇒ Project decisions are based on risk management ⇒ Experience of Project Managers matched to project magnitude/ complexity ⇒ Shared accountabilities between multiple stakeholders

Appendix G: Risk Management Action (Tolerance) Model



Impact	Risk Management Actions		
Significant	Considerable management required	Must manage and monitor risks	Extensive management essential
Moderate	Risks may be worth accepting with monitoring	Management effort worthwhile	Management effort required
Minor	Accept risks	Accept, but monitor risks	Manage and monitor risks
	Low	Medium	High
	Likelihood		

Source – *Integrated Risk Management Framework*, TBS