



## Reissue of Request for Supply Arrangement

**This Request for Supply Arrangement supersedes Request for Supply Arrangement number EN578-121746/A dated August 7, 2012 with a closing date of September 6, 2012 at 2 pm EDT.**

### **TABLE OF CONTENTS**

#### **PART 1 - GENERAL INFORMATION**

1. Introduction
2. Summary
3. Security Requirement
4. Canadian Content
5. Debriefings

#### **PART 2 - SUPPLIER INSTRUCTIONS**

1. Standard Instructions, Clauses and Conditions
2. Submission of Arrangements
3. Former Public Servant - Notification
4. Federal Contractors Program for Employment Equity - Notification
5. Enquiries - Request for Supply Arrangements
6. Applicable Laws

#### **PART 3 - ARRANGEMENT PREPARATION INSTRUCTIONS**

1. Arrangement Preparation Instructions

#### **PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION**

1. Evaluation Procedures
2. Basis of Selection
3. Security Requirement
4. Financial Viability

#### **PART 5 - CERTIFICATIONS**

1. Mandatory Certifications Required Precedent to Issuance of a Supply Arrangement

#### **PART 6 - SUPPLY ARRANGEMENT AND RESULTING CONTRACT CLAUSES**

##### **A. SUPPLY ARRANGEMENT**

1. Arrangement
2. Security Requirement
3. Standard Clauses and Conditions
4. Term of Supply Arrangement
5. Authorities
6. Identified Users
7. On-going Opportunity for Qualification

Solicitation No. - N° de l'invitation

EN578-121746/B

Client Ref. No. - N° de réf. du client

20121746

Amd. No. - N° de la modif.

File No. - N° du dossier

109zIEN578-121746

Buyer ID - Id de l'acheteur

109zI

CCC No./N° CCC - FMS No/ N° VME

- 
8. Priority of Documents
  9. Certifications
  10. Applicable Laws
  11. Insurance

**B. BID SOLICITATION**

1. Bid Solicitation Documents
2. Bid Solicitation Process

**C. RESULTING CONTRACT CLAUSES**

1. General

**List of Annexes:**

Annex A	Statement of Work
Annex B	Supply Arrangement Quarterly Usage Report
Annex C	Security Requirements for Information Technology
Annex D	Security Requirements Check List
Annex E	Risk Management Guide

## PART 1 - GENERAL INFORMATION

### 1. Introduction

The Request for Supply Arrangements (RFSA) is divided into six parts plus attachments and annexes, as follows:

- Part 1 General Information: provides a general description of the requirement;
- Part 2 Supplier Instructions: provides the instructions applicable to the clauses and conditions of the RFSA;
- Part 3 Arrangement Preparation Instructions: provides suppliers with instructions on how to prepare the arrangement to address the evaluation criteria specified;
- Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria which must be addressed in the arrangement, the security requirement, and the basis of selection;
- Part 5 Certifications: includes the certifications to be provided; and
- Part 6 6A, Supply Arrangement, 6B, Bid Solicitation, and 6C, Resulting Contract Clauses:
  - 6A, includes the Supply Arrangement (SA) with the applicable clauses and conditions;
  - 6B, includes the instructions for the bid solicitation process within the scope of the SA;
  - 6C, includes general information for the conditions which will apply to any contract entered into pursuant to the SA.

The Attachments include Technical Evaluation Criteria and Certifications Precedent to Contract Award.

The Annexes include the Statement of Work, Supply Arrangement Quarterly Usage Report, Security Requirements for Information Technology, the Security Requirements Check List, and the Risk Management Guide.

### 2. Summary

This solicitation is a Request for Supply Arrangement (RFSA) to provide Federal Government Departments, Agencies, and Corporations across Canada (as defined in Schedules I, I.1, II, III, IV, and V of the Financial Administration Act) with (1) Risk Management Process Services and/or, (2) Insurance and Risk Consulting Services, on an "as and when requested basis" in accordance with resulting contracts pursuant to this Supply Arrangement. The future intent is to migrate these services to the Task and Solutions Professional Services (TSPS) procurement tool, wherein this Supply Arrangement will be terminated.

A supply arrangement (SA) is an arrangement between Canada and pre-qualified suppliers that allows identified users to solicit bids from a pool of pre-qualified suppliers for specific requirements within the scope of a SA. A SA is not a contract for the provision of the goods and services described in it and neither party is legally bound as a result of signing a SA alone. The intent of a SA is to establish a

---

framework to permit expeditious processing of individual bid solicitations which result in legally binding contracts for the services described in those bid solicitations.

Suppliers who are interested in responding to individual bid solicitations issued under a SA framework are invited to submit an arrangement to become pre-qualified suppliers. The list of pre-qualified suppliers will be used as a source list for procurement within the scope of the SA and only suppliers who are pre-qualified at the time individual bid solicitations are issued will be eligible to bid. SAs include a set of predetermined conditions and mandatory requirements that will apply to subsequent bid solicitations and contracts.

SAs will not include any prices. Prices will be requested at the time of individual bid solicitations based on its specific scope of work. Each contract pursuant to these SAs will indicate the period of service during which the specified work will be performed.

This SA will cover the following streams/categories of services:

Stream 1: Risk Management Process Services:

Category 1: Procurement

Category 2: Real Property Management

Category 3: Corporate Management

Category 4: Delivery of public services to stakeholders external to the government.

Stream 2: Insurance and Risk Consulting Services.

In order to pre-qualify, Suppliers may submit an arrangement with separate projects for each category for which it wants to be considered:

Stream 1 - Category 1: Procurement; and/or

Stream 1 - Category 2: Real Property Management; and/or

Stream 1 - Category 3: Corporate Management; and/or

Stream 1 - Category 4: Delivery of public services to stakeholders external to the government; and/or

Stream 2 - Category 1: Insurance and Risk Consulting Services.

Following this RFSA process, new suppliers may submit arrangements to pre-qualify and be added to the list of suppliers pre-qualified to provide the services described in the SA. This process will also permit pre-qualified suppliers to qualify for work streams for which they are not already qualified. Canada may issue an unlimited number of SAs and may continue to issue SAs to new suppliers throughout the SA period.

The SA has no defined end-date and will remain valid until such time as Canada no longer considers it to be advantageous to do so.

It is estimated that the volume of work will be approximately \$1,000,000.00 per year total for the Risk Management Process streams and \$100,000.00 per year for Insurance and Risk Consulting Services.

There is a security requirement associated with this requirement.

The requirement is subject to the Agreement of Internal Trade (AIT).

---

The requirement covered by the bid solicitation of any resulting supply arrangement may be subject to a preference for Canadian goods and/or services or may be limited to Canadian goods and/or services.

### **3. Security Requirement**

There is a security requirement associated with the requirement of the Supply Arrangement. For additional information, see Part 4 - Evaluation Procedures and Basis of Selection, and Part 6 - Supply Arrangement and Resulting Contract Clauses.

### **4. Canadian Content**

The goods and/or services covered by the Supply Arrangement may be limited to Canadian goods and/or services as defined in clause A3050T.

SACC Manual clause A3050T (2010-01-11), Canadian Content Definition

### **5. Debriefings**

After issuance of a supply arrangement, suppliers may request a debriefing on the results of the request for supply arrangements process. Suppliers should make the request to the Supply Arrangement Authority within 15 working days of receipt of the results of the request for supply arrangements process. The debriefing may be in writing, by telephone or in person.

---

## PART 2 - SUPPLIER INSTRUCTIONS

### 1. Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the Request for Supply Arrangements (RFSA) by number, date and title are set out in the *Standard Acquisition Clauses and Conditions* (<http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp>) Manual issued by Public Works and Government Services Canada.

Suppliers who submit an arrangement agree to be bound by the instructions, clauses and conditions of the RFSA and accept the clauses and conditions of the Supply Arrangement and resulting contract(s).

The 2008 (2012-07-11), Standard Instructions - Request for Supply Arrangements - Goods or Services, are incorporated by reference into and form part of the RFSA.

Subsection 5.4 of 2008, Standard Instructions - Request for Supply Arrangements - Goods or Services, is amended as follows:

Delete: sixty (60) days  
Insert: ninety (90) days

### 2. Submission of Arrangements

Arrangements must be submitted only to Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and place indicated on page 1 of the Request for Supply Arrangements.

Due to the nature of the Request for Supply Arrangements, transmission of arrangements by facsimile to PWGSC will not be accepted.

### 3. Former Public Servant - Notification

Service contracts awarded to former public servants in receipt of a pension or a lump sum payment must bear the closest public scrutiny and reflect fairness in the spending of public funds. Therefore, the bid solicitation will require that you provide information that, were you to be the successful bidder, your status with respect to being a former public servant in receipt of a pension or a lump sum payment, will be required to report this information on the departmental websites as part of the published proactive disclosure reports generated in accordance with Treasury Board policies and directives on contracts with former public servants, Contracting Policy Notice 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

### 4. Federal Contractors Program for Employment Equity - Notification

The Federal Contractors Program (FCP) for employment equity requires that some contractors make a formal commitment to Human Resources and Skills Development Canada (HRSDC) - Labour to implement employment equity. In the event that this Supply Arrangement would lead to a contract subject to the Federal Contractors Program (FCP) for employment equity, the bid solicitation and resulting contract templates would include such specific requirements. Further information on the Federal Contractors Program (FCP) for employment equity can be found on HRDCS-Labour's website.

## 5. Enquiries - Request for Supply Arrangements

All enquiries must be submitted in writing to the Supply Arrangement Authority no later than 7 calendar days before the Request for Supply Arrangements (RFSA) closing date. Enquiries received after that time may not be answered.

Suppliers should reference as accurately as possible the numbered item of the RFSA to which the enquiry relates. Care should be taken by suppliers to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that suppliers do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all suppliers. Enquiries not submitted in a form that can be distributed to all suppliers may not be answered by Canada.

## 6. Applicable Laws

The Supply Arrangement (SA) and any contract awarded under the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Suppliers may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of the arrangement, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the suppliers.

---

## PART 3 - ARRANGEMENT PREPARATION INSTRUCTIONS

### 1. Arrangement Preparation Instructions

Canada requests that suppliers provide the arrangement in separately bound sections as follows:

Section I: Technical Arrangement (4 hard copies);  
Section II: Certifications (1 hard copy); and  
Section III: Additional Information (\_\_\_\_\_hard copies).

No prices must be indicated in any section of the arrangement.

The Supplier can submit more than one stream of work specified in the Statement of Work but must submit one project per category to be evaluated within their technical arrangement. Canada requests that the Supplier clearly identifies in the first pages of its technical arrangement for which categories of work it is submitting.

Canada requests that suppliers follow the format instructions described below in the preparation of the arrangement.

- (a) use 8.5 x 11 inch (216 mm x 279 mm) paper; and
- (b) use a numbering system that corresponds to that of the Request for Supply Arrangements.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement

(<http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html>).

To assist Canada in reaching its objectives, suppliers are encouraged to:

- 1) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing minimum 30% recycled content; and
- 2) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

Section I: Technical Arrangement

In the technical arrangement, suppliers should explain and demonstrate how they propose to meet the requirements and how they will carry out the Work.

Section II: Certifications

Suppliers must submit the certifications required under Part 5.

Solicitation No. - N° de l'invitation

EN578-121746/B

Amd. No. - N° de la modif.

File No. - N° du dossier

109z1EN578-121746

Buyer ID - Id de l'acheteur

109z1

Client Ref. No. - N° de réf. du client

20121746

CCC No./N° CCC - FMS No/ N° VME

---

### Section III: Additional Information

#### 1.1 Supplier's Proposed Site or Premises Requiring Safeguard Measures

As indicated in Part 4 under Security Requirement, the Supplier must provide the required information below, on the Supplier's proposed site or premises for which safeguard measures are required for Work Performance.

Address:

Street Number / Street Name, Unit / Suite / Apartment Number

City, Province, Territory / State

Postal Code / Zip Code

Country

## **PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION**

### **1. Evaluation Procedures**

- (a) Arrangements will be assessed in accordance with the entire requirement of the Request for Supply Arrangements including the technical evaluation criteria.
- (b) An evaluation team composed of representatives of Canada will evaluate the arrangements.

#### 1.1 Technical Evaluation

##### 1.1.1 Mandatory Technical Criteria

The arrangement must meet the mandatory technical criteria specified below. The Supplier must provide the necessary documentation to support compliance with this requirement.

Arrangements which fail to meet the mandatory technical criteria will be declared non-responsive. Each mandatory technical criterion should be addressed separately.

Table 1		
MT1 - Projects		
#	Mandatory Technical Criteria	Arrangement Preparation Instructions
MT1.1	The Supplier must have provided the services for Risk Management Process Services and/or Insurance and Risk Consulting Services, as defined in Annex A - Statement of Work, over the past 5 years from the RFSA closing date.	<p>In order to demonstrate compliance, the Supplier must submit the following information for each category that it wants to be considered for a Supply Arrangement:</p> <p>a) A description of 1 completed project per category that demonstrates its experience as defined in Annex A - Statement of Work, over the past 5 years from the RFSA closing date. Suppliers may submit a project for:</p> <ul style="list-style-type: none"> <li>i) Risk Management Process Services - Procurement;</li> <li>ii) Risk Management Process Services - Real Property Management;</li> <li>iii) Risk Management Process Services - Corporate Management;</li> <li>iv) Risk Management Process Services -Delivery of public services to stakeholders external to the government;</li> <li>v) Insurance and Risk Consulting Services;</li> </ul> <p>b) Start and end dates (month/year); c) Client organization name; d) Client representative name; and e) Client representative telephone number and e-mail address.</p>

Table 2

## MT2 - Fees

#	Mandatory Technical Criteria	Arrangement Preparation Instructions
MT2.1	<p>The Supplier must have billed, over the past 5 years from the RFSA closing date, a minimum cumulative total amount of \$250,000.00 in risk consulting fees (Canadian dollars, GST/HST excluded) relative to supplied Risk Management Process Services and/or Insurance and Risk Consulting Services.</p>	<p>In order to demonstrate compliance the Supplier must submit completed risk consulting projects that include the following:</p> <ul style="list-style-type: none"> <li>a) Name and overview of the project;</li> <li>b) Start and end dates (month/year);</li> <li>c) Amount billed for risk management consulting fees;</li> <li>d) Client organization name;</li> <li>e) Client representative name; and</li> <li>f) Client representative telephone number and e-mail address.</li> </ul> <p>There is no limit on the number of projects that a Supplier can submit in order to meet the Mandatory Technical Criteria.</p>

## **2. Basis of Selection**

2.1 To be declared responsive, an arrangement must:

- (a) comply with all the requirements of the Request for Supply Arrangements; and
- (b) meet all mandatory technical evaluation criteria.

2.2 Arrangements not meeting (a) or (b) above will be declared non-responsive.

## **3. Security Requirement**

3.1 Before issuance of a supply arrangement, the following conditions must be met:

- (a) the Supplier must hold a valid organization security clearance as indicated in Part 6A - Supply Arrangement;
- (b) the Supplier's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirement as indicated in Part 6A - Supply Arrangement;
- (c) the Supplier must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

3.2 Suppliers are reminded to obtain the required security clearance promptly. Any delay in the issuance of a supply arrangement to allow the successful supplier to obtain the required clearance will be at the entire discretion of the Supply Arrangement Authority.

3.3 For additional information on security requirements, suppliers should consult the "[Security Requirements for PWGSC Bid Solicitation - Instructions for Bidders](#)" (<http://www.tpsgc-pwgsc.gc.ca/app-acq/lc-pl/lc-pl-eng.html#a31>) document on the Departmental Standard Procurement Documents Web site.

## **4. Financial Viability**

SACC Manual clause S0030T (2011-05-16) Financial Viability

## **PART 5 - CERTIFICATIONS**

Suppliers must provide the required certifications and documentation to be issued a supply arrangement (SA).

The certifications provided by suppliers to Canada are subject to verification by Canada at all times. Canada will declare an arrangement non-responsive, or will declare a contractor in default, if any certification made by the Supplier is found to be untrue whether during the arrangement evaluation period, or during the period of any supply arrangement arising from this RFSA and any resulting contracts.

The Supply Arrangement Authority will have the right to ask for additional information to verify the Supplier's certifications. Failure to comply with this request will also render the arrangement non-responsive, or will constitute a default under the Contract.

### **1. Certifications Precedent to Contract Award**

#### **1.1 Code of Conduct and Certifications - Related documentation**

By submitting an arrangement, the Supplier certifies that the Supplier and its affiliates are in compliance with the Code of Conduct and Certifications - Arrangement in Section 01 of Standard Instructions 2008. The related documentation therein required will assist Canada in confirming that the certifications are true.

### **2. Additional Certifications Precedent to Issuance of a Supply Arrangement**

The certifications listed below should be completed and submitted with the arrangement, but may be submitted afterwards. If any of these required certifications is not completed and submitted as requested, the Supply Arrangement Authority will so inform the Supplier and provide the Supplier with a time frame within which to meet the requirement. Failure to comply with the request of the Supply Arrangement Authority and meet the requirements within that time period will render the arrangement non-responsive.

#### **2.1 Canadian Content Certification**

##### **2.1.1 SACC Manual clause A3050T (2010-01-11), Canadian Content Definition**

This procurement is limited to Canadian services.

The Offeror certifies that:

( ) the service offered is a Canadian service as defined in paragraph 2 of clause A3050T.

Certification

By submitting the arrangement, the Supplier certifies that the information submitted by the Supplier in response to the above requirements is accurate and complete.

## PART 6 - SUPPLY ARRANGEMENT AND RESULTING CONTRACT CLAUSES

### A. SUPPLY ARRANGEMENT

#### 1. Arrangement

The Supply Arrangement covers the Work described in the Statement of Work at Annex A.

#### 2. Security Requirement

2.1 The following security requirement (SRCL and related clauses) applies and form part of the Supply Arrangement.

2.2 Supplier's Site or Premises Requiring Safeguard Measures *(to be inserted at time of issuance)*.

The Supplier must diligently maintain up-to-date, the information related to the Supplier's site or premises, where safeguard measures are required in the performance of the Work, for the following addresses:

Address:

Street Number / Street Name, Unit / Suite / Apartment Number

City, Province, Territory / State

Postal Code / Zip Code

Country

2.3 There is a generic Security Requirements Check Lists (SRCL) attached to this Supply Arrangement (SA) (see Annex D), which PWGSC anticipates will satisfy most security requirements associated with individual bid solicitations. This generic SRCL may not meet the needs of some Clients for some requirements, in such cases, bid solicitation will include a unique SRCL that will apply to the resulting contract;

2.4 The Supplier must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of PROTECTED A, issued by the Canadian Industrial Security Directorate, Public Works and Government Services Canada.

2.5 The Supplier personnel requiring access to PROTECTED information, assets or work site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

2.6 The Supplier MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CISD/PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED A.

2.7 Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

2.8 The Supplier must comply with the provisions of the:

- (a) Security Requirements for Information Technology attached at Annex C;
- (b) Security Requirements Check List, attached at Annex D; and
- (c) Industrial Security Manual (Latest Edition).

### 3. Standard Clauses and Conditions

All clauses and conditions identified in the Supply Arrangement and resulting contract(s) by number, date and title are set out in the Standard Acquisition Clauses and Conditions (<http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp>) Manual issued by Public Works and Government Services Canada.

#### 3.1 General Conditions

2020 (2013-04-25), General Conditions - Supply Arrangement - Goods or Services, apply to and form part of the Supply Arrangement.

#### 3.2 Supply Arrangement Reporting

The Supplier must compile and maintain records on its provision of goods, services or both to the federal government under contracts resulting from the Supply Arrangement. This data must include all purchases paid for by a Government of Canada Acquisition Card.

The Supplier must provide this data in accordance with the reporting requirements detailed in Annex "C". If some data is not available, the reason must be indicated. If no goods or services are provided during a given period, the Supplier must still provide a "NIL" report.

The data must be submitted on a quarterly basis to the Supply Arrangement Authority.

The quarterly reporting periods are defined as follows:

- 1st quarter: April 1 to June 30;
- 2nd quarter: July 1 to September 30;
- 3rd quarter: October 1 to December 31;
- 4th quarter: January 1 to March 31.

The data must be submitted to the Supply Arrangement Authority no later than 15 calendar days after the end of the reporting period.

### 4. Term of Supply Arrangement

#### 4.1 Period of the Supply Arrangement

The Supply Arrangement has no defined end-date and will remain valid until such time as Canada no longer considers it to be advantageous to use it.

The period for awarding contracts under the Supply Arrangement begins\_\_\_\_\_. (to be determined at time of issuance)

## 5. Authorities

### 5.1 Supply Arrangement Authority

The Supply Arrangement Authority is:

Renee Stephen  
Supply Specialist  
Public Works and Government Services Canada  
Acquisitions Branch  
Project Delivery Services Division  
Place du Portage  
Phase III, 10C1  
11, rue Laurier, Gatineau (Quebec)  
K1A 0S5

Telephone: 819-956-6973

Facsimile: 819-956-2675

E-mail address: Renee.Stephen@tpsgc-pwgsc.gc.ca

The Supply Arrangement Authority is responsible for the issuance of the Supply Arrangement, its administration and its revision, if applicable.

### 5.2 Supplier's Representative

*(to be determined at time of issuance).*

## 6. Identified Users

The Identified Users include any government department, agency or Crown Corporation listed in Schedules I, I.1, II, III, of the *Financial Administration Act*, R.S., 1985, c. F-11.

## 7. On-going Opportunity for Qualification

A permanent Notice will be posted on the Government Electronic Tendering Service (GETS) to allow new suppliers to become qualified. Existing qualified suppliers, who have been issued a supply arrangement, will not be required to submit a new arrangement.

The process to qualify new suppliers will be at a minimum of once per year.

## 8. Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list.

- (a) the articles of the Supply Arrangement;
- (b) the general conditions 2020 (2013-04-25), General Conditions - Supply Arrangement - Goods or Services;

- 
- (c) Annex A, Statement of Work;
  - (d) Annex B, Supply Arrangement Quarterly Usage Report;
  - (e) Annex C, Security Requirements for Information Technology;
  - (f) Annex D, Security Requirements Check List;
  - (g) Annex E, Risk Management Guide; and
  - (h) the Supplier's arrangement dated \_\_\_\_\_ (to be inserted at time of issuance).

## 9. Certifications

### 9.1 Compliance

Compliance with the certifications and related documentation provided by the Supplier in the arrangement is a condition of the Supply Arrangement (SA) and subject to verification by Canada during the term of the SA and of any resulting contract that would continue beyond the period of the SA. If the Supplier does not comply with any certification, provide the related documentation or if it is determined that any certification made by the Supplier in the arrangement is untrue, whether made knowingly or unknowingly, Canada has the right to terminate any resulting contract for default and suspend or cancel the SA.

## 10. Applicable Laws

The Supply Arrangement (SA) and any contract resulting from the SA must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

## 11. Insurance

SACC Manual clause G1005C (2008-05-12) Insurance

## **B. BID SOLICITATION**

### **1. Bid Solicitation Documents**

Canada will use the bid solicitation template 2T-HIGH1 for all requirements, which is available in the [Standard Acquisition Clauses and Conditions](http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp) (<http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp>) Manual

based on the estimated dollar value and complexity of the requirement.

The bid solicitation will contain as a minimum the following:

- (a) security requirements;
- (b) a complete description of the Work to be performed;
- (c) 2003, Standard Instructions - Goods or Services - Competitive Requirements;
- (d) bid preparation instructions;
- (e) instructions for the submission of bids (address for submission of bids, bid closing date and time);
- (f) evaluation procedures and basis of selection;
- (g) financial capability;
- (h) certifications; and
- (i) conditions of the resulting contract.

### **2. Bid Solicitation Process**

- 2.1 Bids will be solicited for specific requirements within the scope of the Supply Arrangement (SA) from suppliers who have been issued a SA.
- 2.2 The bid solicitation will be sent directly to suppliers.
- 2.3 It is anticipated that the majority of bid solicitation process and award of contracts will be managed by identified users up to the \$2 million threshold. PWGSC, Acquisitions Branch will manage all requirements above the \$2 million threshold.
- 2.4 The following forms will be used for the first page of the bid solicitation document and the first page of the resulting contract document.

PWGSC-TPSGC 9400-3, Bid Solicitation  
PWGSC-TPSGC 9400-4, Contract.

These forms are available on the [Electronic Forms Catalogue](http://publiservice-app.tpsgc-pwgsc.gc.ca/forms/text/search_for_forms-e.html) ([http://publiservice-app.tpsgc-pwgsc.gc.ca/forms/text/search\\_for\\_forms-e.html](http://publiservice-app.tpsgc-pwgsc.gc.ca/forms/text/search_for_forms-e.html)) Web site.

## **C. RESULTING CONTRACT CLAUSES**

### **1. General**

The conditions of any contract awarded under the Supply Arrangement will be in accordance with the resulting contract clauses of the template used for the bid solicitation.

For any contract to be awarded using:

2T-HIGH1 (for higher complexity requirements), general conditions 2035 will apply to the resulting contract;

The above templates are set out in the *Standard Acquisition Clauses and Conditions* (<http://ccua-sacc.tpsgc-pwgsc.gc.ca/pub/acho-eng.jsp>) Manual issued by Public Works and Government Services Canada.

---

**ANNEX "A"****STATEMENT OF WORK****1. TITLE**

Risk Management Process Services / Insurance and Risk Consulting Services

**2. OBJECTIVE**

To provide Federal Government Departments, Agencies, and Corporations across Canada (as defined in Schedules I, I.1, II, III, IV, and V of the Financial Administration Act) with (1) Risk Management Process Services and/or, (2) Insurance and Risk Consulting Services, on an "as and when requested basis" in accordance with resulting contracts pursuant to this Supply Arrangement. The future intent is to migrate these services to the Task and Solutions Professional Services (TSPS) procurement tool, wherein this Supply Arrangement will be terminated.

**3. SCOPE OF WORK**

The related services for each Stream that may be required within this Supply Arrangement are as follows:

**3.1 Stream 1 - Risk Management Process Services**

Background:

The Contractor will be required to provide a full range of risk management process services (Establish Context; Risk assessment [Risk Identification, Risk Analysis, and Risk Evaluation]; Risk Response; Communication and Consultation; and Monitor and Review) for any or all phases of individual processes or projects or for programs, business lines, initiatives or key risks. The work performed must be conducted in accordance with:

- a) The principles and guidelines specified in ISO 31000:2009 and CSA Q31001:2011 regarding the risk management process.
- b) TBS Framework for the Management of Risk:  
<http://www.tbs-sct.gc.ca/pol/doc-eng>
- c) PWGSC Integrated Risk Management Policy.  
<http://publiservice.tpsgc-pwgsc.gc.ca/policy/text/p082-e.html>
- d) The Risk Management Guide attached at Annex E. Two notable features of the Risk Management Guide are information about positive risks, opportunities and the 5X5 grid for risks, which is the new PWGSC standard.

Appendix 1 to Annex A contains additional details regarding the requirement under this stream.

### 3.2 Stream 2 - Insurance and Risk Consulting Services

#### Background:

The Contractor will be required to provide professional advice on subjects related to insurance. Such services may include:

- a) review of insurance programs providing opinions on the effectiveness of the program;
- b) providing deductible amounts and costs of product;
- c) review of risk financing methods and which application may be the most advantageous for the Crown;
- d) conducting a gap review of risk management programs;
- e) providing advice and insight with respect to specialty insurance lines for large projects and whether or not other risk financing tools may be more fiscally prudent to the Crown;
- f) providing advice with respect to claims and financial recovery;
- g) providing options and applications of loss control programs; and
- h) providing any other requirements that may fall within the Insurance and Risk Consulting Services.

Note: The provision of advice or support for the following are specifically excluded from the scope of work:

- a) Insurance Broker services to procure and maintain insurance;
- b) Quantitative risk assessments; and
- c) Claim Adjustment and/or Claim Administration.

Appendix 2 to Annex A contains additional details regarding the requirement under this stream.

## 4. LANGUAGE REQUIREMENTS FOR ALL STREAMS

- 4.1 The Contractor's representatives must have the ability to provide services as well as the required reports and documents in both official languages i.e. English and French.
- 4.2 For general discussion and oral presentations, it is mandatory that at least one of the Contractor's representatives be bilingual in English and French. As well, documents related to various requirements may have to be submitted in both official languages.

## 5. SECURITY REQUIREMENTS FOR ALL STREAMS

The Contractor will be required to comply with the security requirements that will be specified in a Security Requirements Check List (SRCL) and will be required to ensure that any party that will receive information such as, but not limited to, other divisions within its company, will have the appropriate security clearances in place.

## 6. RESOURCE REQUIREMENTS FOR ALL STREAMS

Resources for Risk Management Process Services, Insurance and Risk Consulting Services, may include but are not limited to the following:

- a) Senior Consultant
- b) Consultant
- c) Account Assistant

Detailed task and education and experience requirements for resources in each stream can be found in Appendices 1 and 2 to Annex A.

Note: The categories described above are not intended to correspond to any one contractor's definition or categorization as such definitions or categorizations may vary between contractors.

## 7. PROBLEM ESCALATION MANAGEMENT PROCESS REQUIREMENTS FOR ALL STREAMS

This is a guideline that documents the process of raising concerns to higher authorities for timely resolution. Its intent is to ensure that the next level of management is informed within a specific period of time, if an issue cannot be resolved at the lower level.

1. Client department has an issue using with the service provider;
2. Complaint to be forwarded by e-mail to the Technical Authority (TA) and Supply Arrangement Authority (SAA);
3. TA and SAR propose resolution to Identified User;
4. If the Identified User accepts the resolution, TA and SAA document and archive the complaint and resolution;
5. Resolution is not accepted by the Identified User;
6. TA and SAA forward complaint to Contractor Senior Consultant, who will investigate the complaint and propose a resolution;
7. The resolution will be submitted to the Identified User through the TA and SAA;
8. If the Identified User accepts the resolution, TA and SAA document and archive the complaint and resolution;
9. Resolution is not accepted by the Identified User;
10. Complaint is escalated to Contractor National Practice Leader, who will propose a resolution through TA and SAA to the Identified User;
11. If the Identified User accepts the resolution, TA and SAA document and archive the complaint and resolution;
12. Resolution is not accepted by the Identified User ; and
13. TA and SAA will invite involved parties to participate in a resolution meeting.

Note: The categories described above are not intended to correspond to any one contractor's definition or categorization as such definitions or categorizations may vary between contractors.

## 8. INTERNAL CORPORATE MANAGEMENT APPROACH FOR ALL STREAMS

The Contractor should leverage risk management internally by building organizational capacity in risk management and embedding risk management into their internal management processes. Approaches to achieving this must include but are not limited to the following:

Solicitation No. - N° de l'invitation

EN578-121746/B

Amd. No. - N° de la modif.

File No. - N° du dossier

109zIEN578-121746

Buyer ID - Id de l'acheteur

109zI

Client Ref. No. - N° de réf. du client

20121746

CCC No./N° CCC - FMS No/ N° VME

- 
- a) The development of human resources and promulgation of tools and processes, to build its organizational capacity in risk management; and
  - b) The application of strategies to incorporate risk management into its internal management processes.

---

## **APPENDIX 1 TO ANNEX A RISK MANAGEMENT PROCESS SERVICES REQUIREMENTS**

### **STREAM 1**

#### **1. Required Services**

The Contractor must be able to provide Risk Management Process Services for the following elements:

- a) Establish Context;
- b) Risk assessment (consists of risk identification, risk analysis, and risk evaluation);
- c) Risk Response;
- d) Communication and Consultation; and
- e) Monitor and Review.

#### **2. Requirements**

##### **2.1 Risk Identification**

To identify risks, threats and vulnerabilities associated with those risks, for each organization, business line, program, project, process or initiative for which a risk assessment is being carried out, the Contractor must:

- 2.1.1 Identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and potential consequences. The output of this exercise must be a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. This list must form the basis for further analysis;
- 2.1.2 Identify risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident;
- 2.1.3 Identify the risks associated with not pursuing an opportunity;
- 2.1.4 Examine the immediate effects of particular consequences, cascade and cumulative effects, and consider a wide range of consequences even if the risk source or cause may not be evident;
- 2.1.5 Consider possible causes and scenarios that show what consequences can occur and in that regard must consider all significant causes and consequences;
- 2.1.6 Apply risk identification tools and techniques that are suited to the mandate, objectives, strategic outcomes, and risk assessment capabilities of the organization for which the risk assessment is being carried out, as well as the corporate risk profile. The Contractor must take into account the risk appetite of the organization when determining which risks are to be included in the risk identification process; and
- 2.1.7 Ensure that that relevant and up-to-date information is used in identifying risks, including appropriate background information where possible. The Contractor must ensure that key stakeholders within the organization with appropriate knowledge are involved in identifying risks.

---

## 2.2 Risk Analysis

To assess the level and nature of the risks, the Contractor must:

- 2.2.1 Analyze the risks identified in the risk identification stage to provide input to the Identified User's decision making in terms of whether risks need to be treated; the most appropriate risk treatment strategies and methods; and making decisions where choices must be made and the options involve different types and levels of risk;
- 2.2.2 Consider the causes and sources of risk, the positive and negative consequences, the likelihood that those consequences can occur, and other attributes of the risk;
- 2.2.3 Identify factors that affect consequences and likelihood, and take into consideration the multiple consequences and events can have and the multiple objectives that can be affected;
- 2.2.4 Take into account existing controls and their effectiveness and efficiency;
- 2.2.5 Ensure that the way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk, reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These must all be consistent with the risk criteria. The interdependence of different risks and their sources must be considered in the analysis. The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions must be considered in the analysis, and communicated effectively, within the organization, to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modeling must be stated and highlighted;
- 2.2.6 Consider the risk, the purpose of the analysis, and the information, data and resources available within the organization, in determining the degree of detail required to conduct the risk analysis. Analysis must be qualitative, quantitative or semi-quantitative, or a combination of these, depending on the circumstances;
- 2.2.7 Determine the consequences and their likelihood by modeling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data; and
- 2.2.8 Express the consequences in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor may be required to specify consequences and their likelihood for different times, places, groups or situations.

## 2.3 Risk Evaluation

To assist organizations in making decisions based on the outcomes of risk analysis, the Contractor must:

- 2.3.1 Compare the level of risk found during the analysis process with risk criteria established when the context was considered;
- 2.3.2 Take account of the wider context of the risk;
- 2.3.3 Consider the tolerance to the risks borne by parties other than the organization which benefits from the risk;

2.3.4 Make decisions in accordance with legal, regulatory, policy, and other requirements; and

2.3.5 Rank the risks.

2.4 Risk Response

Once the risks are evaluated by the Identified User, plans to respond to the risks must be selected and implemented. In consultation with the Identified User, the Contractor must:

2.4.1 Provide actions to mitigate the likelihood or the impact of a risk (or both);

2.4.2 Document control measures currently in place;

2.4.3 Document the implementation of mitigation strategies;

2.4.4 Ensure that the residual risk after response is tolerable;

2.4.5 Ensure that the costs of responding to the risks are in proportion to the costs of the impacts; and

2.4.6 Confirm resources are available to implement the response.

2.5 Communication and Consultation

Ongoing communication and consultation throughout the risk management process is critical as risks may change and may be perceived differently by stakeholders. In consultation with the Identified User, the Contractor must:

2.5.1 Develop plans for communication and consultation at an early stage in the risk management process;

2.5.2 Ensure communication with all key stakeholders. Risk practitioners or risk owners may want to consider identifying, recording, and taking into account stakeholders' perceptions in the decision-making process as these views may have a significant impact on the decisions taken

2.6 Monitor and Review

Monitoring and review should be included in all aspects of the risk management process. In consultation with the Identified User, the Contractor must:

2.6.1 Assess the effectiveness and efficiency of controls identified in a risk profile;

2.6.2 Ensure risks are still relevant with the internal and external contexts;

2.6.3 Identify when revisions to improve a risk profile are required;

2.6.4 Re-profile resources to higher priority risks; to analyze changes lessons learned, trends and changes to the context;

2.6.5 Identify emerging risks; and

2.6.6 Assess the progress of implementing a risk response plan.

---

**NOTE:**

The frequency for monitoring and review may be influenced by the likelihood and impact assessments of risks, the business planning cycle, a meeting of a specific committee to monitor and review risks and/or as determined by a group. Whenever possible, existing frameworks and committees should be used for monitoring and review activities. To ensure a risk profile or risk response plan is being monitored and reviewed as planned, roles and responsibilities should be assigned to stakeholders. Once the monitoring and review activities are complete, it is essential to communicate results to stakeholders within PWGSC who are accountable for the risks through the delegation of authority chain.

**3. Risk Reporting**

The Contractor must:

Provide risk reports that summarize and/or explain all the steps in the risk management process in the form of a written and/or oral presentation, as requested.

**4. Risk Management Methodology**

The Contractor must use a standard risk management approach when planning and performing its work that is in line with the Treasury Board's IRMF and ISO 31000 standards. The planning approach must include the following components:

1. Identified User requirement;
2. Proposed methodology;
3. Level of effort; and
4. Deliverables.

**5. Terminology Associated with Risk Management Process**

For terminology and associated definitions, please refer to Risk Management Guide.

**6. Risk Categories**

The Contractor must consider each task and activity performed in a risk assessment in the context of risk categories. Some of the most common risk categories are:

1. Compliance to Legislation, Regulations, and/or Policies;
2. Legal Liability;
3. Governance;
4. Capacity/Capability;
5. Environmental Concerns;
6. Threats and Hazards;
7. Reputation;
8. Ethics;
9. Participation/Stakeholder buy-in;
10. Market/Economy;
11. Jurisdiction;

12. Security; and
13. Technology.

## 7. Stream 1 Categories

When required, the Contractor must conduct risk assessments as defined in any one of the following categories :

- i) Category 1: Procurement
- ii) Category 2: Real Property Management
- iii) Category 3: Corporate Management
- iv) Category 4: Delivery of public services to stakeholders external to the government

### 7.1 Category 1: Procurement

This category specifically involves procurement activities, projects, processes, strategies and initiatives conducted pursuant to the Government Contracts Regulations and the Treasury Board (TB) Contracting Policy. It excludes leases and contracts for the fit-up of offices pursuant to the Federal Real Property and Federal Immovable Act; contracts related to the acquisition of land; grants and contributions; service level agreements between government departments; and memoranda of understanding with other governments or other levels of government.

This category is designed to be used for:

1. Project Risk Management pursuant to the TB Project Approval Policy and TB Policy on the Management of Projects, where the projects will result in Procurement contracts;
2. Application of the TB Policy on Decision Making in Limiting Contractor Liability in Crown Procurement Contracts;
3. The risk management component of:
  - a) Specific procurement actions, solicitations, or contracts for the acquisition of goods or services, and construction and architectural and engineering services;
  - b) Procurement processes; and
  - c) Commodity management and method of supply decision making; and Procurement transformation initiatives.

### 7.2 Category 2: Real Property Management

This category specifically involves real property projects, activities, strategies and initiatives, and acquisitions and dispositions pursuant to the Federal Real Property and Federal Immovables Act. This category is designed to be used for:

1. Project Risk Management pursuant to the TB Project Approval Policy and TB Policy on the Management of Projects;
2. Organizational Project Management Capacity Assessments pursuant to the TB Policy on the Management of Projects;
3. The risk management component of:

- a) Real Property acquisition strategy development. Acquisition includes purchase, lease, license, exchange, gift, easement, expropriation, transfer of administration from another department or agent Crown corporation or a transfer of administration and control from the provincial Crown;
- b) Real Property disposition strategy development. Disposition includes sale, lease, license, exchange, gift, easement, transfer of administration to another department or an agent Crown corporation, or transfer of administration and control to the provincial Crown;
- c) Management of Real Property (operation and maintenance); as defined in the Treasury Board Policy on Management of Real Property:

A project is an activity or series of activities that has a beginning and an end. A project is required to produce defined outputs and realize specific outcomes in support of a public policy objective, within a clear schedule and resource plan. A project is undertaken within specific time, cost and performance parameters.

- d) Development of business cases, including Real Property investment analyses and business strategies
- e) Real Property transformation initiatives;
- f) Environmental assessments; and
- g) Environmental performance improvement initiatives.

### 7.3. Category 3: Corporate Management

This category is designed to be used for activities associated with the management of organizational and strategic risks at the departmental or branch level, and more specifically, the risk management component associated with:

1. Accountability and decision-making structures;
2. Development of Integrated Risk Management frameworks;
3. Investment planning;
4. Business planning;
5. Delegation of financial authorities;
6. Organizational transition;
7. Development of human resources strategies;
8. Development of communications strategies; and
9. Emergency management planning.

### 7.4 Category 4: Delivery of public services to stakeholders external to the government

This category is designed to be used for activities associated with delivery of public services to stakeholders external to the government and more specifically, the risk management component associated with:

1. Accountability and decision-making structures;
2. Development of Integrated Risk Management frameworks;
3. Investment planning;
4. Business planning;
5. Delegation of financial authorities;
6. Development of human resources strategies; and
7. Development of communications strategies.

## **8. Resources for Risk Management Services**

The following categories of resources will be the only categories for Risk Management Services. The categories described below are not intended to correspond to any one contractor's definition or categorization as such definitions or categorizations may vary between contractors.

### **8.1 Senior Consultant**

A Senior Consultant has overall responsibility for overseeing the requested work. Tasks may include but are not limited to:

- i) Conducting the risk management process for major, complex projects, initiatives or programs;
- ii) Providing advice on the risk management methods, tools and techniques used;
- iii) Conducting quality assurance and providing direction and approving risk management related deliverables prior to submission to Identified Users ;
- iv) Managing the risk management project budget, schedule and resources, as applicable;
- v) Submitting progress reports to the Technical Authority;
- vi) Facilitating and maintaining open communication with the Technical Authority; and
- vii) Making presentations to senior management, on as requested basis.

#### **8.1.1 Minimum Educational/Experience:**

At a minimum the Senior Consultant must:

- a) Possess and currently maintain in good standing, a recognized risk management designation such as: Canadian Risk Management (CRM), Fellow in Risk Management (FRM), Certified in Risk and Information Systems Control (CRISC), Chartered Insurance Professional (CIP), Associate of the Insurance Institute of Canada (AIIC), Fellow of Chartered Insurance Practitioner (FCIP), Fellows of the Society of Actuaries (FSA), Professional Risk Manager (PRM), PMI Risk Management Professional (PMI-RMP), Chartered Accountant (CA), Certified Management Accountant (CMA), Certified General Accountant (CGA), Certified Internal Auditor (CIA), Certification in Control Self-Assessment (CCSA), Certified Information Systems Auditor (CISA), Chartered Enterprise Risk Analyst (CERA), and RIMS Fellow (RF);

#### **AND/OR**

Possess an undergraduate degree from a Canadian University or Canadian recognized University. The University degree must be from a recognized Canadian University, or if obtained

outside of Canada, be approved by a recognized Canadian academic credentials assessment Service i.e. identified at:

<http://www.cicic.ca/413/assessment-of-credentials-for-employment-in-canada.canada>; and

- b) Have 10 years of related work experience as a Senior Consultant within the past 15 years.

## 8.2 Consultant:

The Consultant is responsible for conducting services pertaining risk management process. For risk management process service, the tasks may include but are not limited to the following:

- i) Assist in conducting risk management process related activities for projects, initiatives or programs;
- ii) Providing advice on the risk management methods, tools and techniques used;
- iii) Developing interview guides and data collection instruments;
- iv) Liaising with and interviewing stakeholders as required to obtain, clarify and exchange information;
- v) Provide support in conducting risk management sessions in order to assess and prioritize risks;
- vi) Preparing briefing notes, presentations and papers.

### 8.2.1 Minimum Educational/Experience:

At a minimum the Consultant must:

- a) Must possess and currently maintain in good standing, a recognized risk management designation: Canadian Risk Management (CRM), Fellow in Risk Management (FRM), Certified in Risk and Information Systems Control (CRISC), Chartered Insurance Professional (CIP), Associate of the Insurance Institute of Canada (AIIC), Fellow of Chartered Insurance Practitioner (FCIP), Fellows of the Society of Actuaries (FSA), Professional Risk Manager (PRM), PMI Risk Management Professional (PMI-RMP), Chartered Accountant (CA), Certified Management Accountant (CMA), Certified General Accountant (CGA), Certified Internal Auditor (CIA), Certification in Control Self-Assessment (CCSA), Certified Information Systems Auditor (CISA), Chartered Enterprise Risk Analyst (CERA), and RIMS Fellow (RF);

### AND/OR

Possess an undergraduate degree from a Canadian University or Canadian recognized University. The University degree must be from a recognized Canadian University, or if obtained outside of Canada, be approved by a recognized Canadian academic credentials assessment Service i.e. identified at:

<http://www.cicic.ca/413/assessment-of-credentials-for-employment-in-canada.canada>; and

- b) Have 7 years of related work experience as a Consultant within the past 10 years.

## 8.3 Account Assistant

Under the direction of the Senior Consultant or the Consultant, as appropriate, the Account Assistant is responsible for providing assistance, as required, to the Senior Consultant and/or the Consultant. Tasks may include but are not limited to the following:

- i) Collecting and collating qualitative and quantitative data;
- ii) Conducting research;
- iii) Conducting preliminary analyses;
- iv) Compiling background documentation; and
- v) Providing assistance with the development of briefing notes, presentations, papers and reports.

### 8.3.1 Minimum Educational/Experience

At a minimum the Account Assistant must:

- a) Possess a secondary school diploma or General Education Development (GED) certificate; and
- b) Have 3 years of related work experience within the past 5 years.

## 9. Applicable Documents & References

### 9.1 Applicable Documents

The "Applicable Documents", listed below, contain methods, terminology and standards that are consistent with the manner in which Risk Assessments should be performed. In any case where there is doubt as to the meaning of the text contained in any of these documents, the service provider should consult the Project Authority. These documents are readily available and published by the named organizations

All risk assessments must be conducted in accordance with the applicable requirements set out in the following:

1. Treasury Board Integrated Risk Management Framework (IRMF) - (Effective August 27th, 2010 with an accompanying guide to follow);
2. ISO31000: 2009, Risk Management Principles and Guidelines is an International Standard which provides principles and generic guidelines on risk management. This Statement of Work (SOW) deals strictly with the risk assessment component of the Standard;
3. ISO Guide 73: 2009, Risk Management Vocabulary provides the definitions of generic terms related to risk management; and
4. Q850: 2009, Canadian Supplementary Standard on Risk Management is a companion document to the ISO31000, which ensures Canadian context for the implementation of the ISO standard.

### 9.2 Reference Documents

The following documents are for reference purposes only. These documents will enable the Contractor to develop a better understanding of the risk assessment process as it relates to the federal government.

1. Treasury Board Contracting Policy;
2. Treasury Board Policy on Management of Real Property;
3. Treasury Board Policy on Internal Control;
4. Treasury Board Policy on Government Security;
5. Treasury Board Project Approval Policy;
6. Treasury Board Policy on the Management of Projects;
7. Treasury Board Policy on Investment Planning - Assets and Acquired Services;
8. Treasury Board Policy on Decision Making in Limiting Contractor Liability in Crown Procurement Contracts;

Solicitation No. - N° de l'invitation

EN578-121746/B

Amd. No. - N° de la modif.

File No. - N° du dossier

109z1EN578-121746

Buyer ID - Id de l'acheteur

109z1

Client Ref. No. - N° de réf. du client

20121746

CCC No./N° CCC - FMS No/ N° VME

- 
9. Public Safety Canada's Emergency Management Planning Guide 2010-2011; and
  10. Individual departmental risk management policies, guides and tools.

In the event the Contractor requires access to any government reference documents not publicly available, the Project Authority will make the required documents available in the form of hard or soft copies, subject to availability. All reference documents will be provided in the latest available version.

## APPENDIX 2 TO ANNEX A INSURANCE AND RISK CONSULTING SERVICES

### STREAM 2

#### 1. Required Services

The Contractor's function will be to provide all requested advice and support pertaining to the identified areas of analysis.

The Contractor must have the capabilities to provide advice for:

- a) commercial insurance and surety markets including interpretation of insurance policy wordings;
- b) risk financing options and methodology;
- c) risk finance benchmarking and best practices;
- d) risk management information systems (RMIS);
- e) claim management practices and processes;
- f) loss prevention and reduction practices and processes;
- g) Comprehensive Insurance and Risk advice, including benchmarking and best practices;
- h) Detailed knowledge of risk financing models, including other options and methodology;
- i) Sound technical directives regarding the application of loss prevention methods; and
- j) Contractual risk analysis.

A detailed reporting mechanism is essential (as further described in Annex B) for all deliverables expected of the Contractor. It will be the Contractor's responsibility to ensure that its proposed reporting formats are compatible to the Technical Authority's own databases and that the Contractor's reporting is made readily available in current and easily adaptable electronic environment.

#### 2. Requirements

The Contractor must:

- 2.1 Analyze and report on the condition of, or trends in, Canadian and/or global insurance and surety markets;
- 2.2 Analyze and make recommendations pertaining to how the Government of Canada (GOC), through its various departments and agencies can finance their risks through the acquisition of commercial insurance, surety, or alternative risk financing measures;
- 2.3 Review and make recommendations on the GOC's existing insurance and/or self-insurance programs, their relevance and/or opportunities for improvement;
- 2.4 Analyze and report on the availability, efficacy and cost of RMIS applications. Note: This category does not permit the sale and/or licensing by the Contractor;
- 2.5 Analyze and report on current practices and processes in Claim Management (including best practices), as well as current state assessments of GOC practices and recommendations for improvement, excluding claim adjustments or claim administration services;
- 2.6 Analyze and make recommendations pertaining to engineering physical surveys and inspections used to identify property and liability loss exposures;

- 2.7 Analyze and report on loss forecasting and loss retention optimization analysis;
- 2.8 Analyze and make recommendations on contract documents, including procurement contracts, leases, lettings and licensing and the appropriate risk management clauses required to mitigate contractual risk; and
- 2.9 Review and make recommendations on PWGSC's standard insurance and surety clauses used in GOC procurement.

### 3. Resources for Insurance and Risk Consulting Services

For Insurance and Risk Consulting Services, the tasks to be provided by the following resources include but are not limited to the following:

- 3.1 Senior Consultant:
  - a) Reviewing of insurance programs providing opinions on the effectiveness of the program, deductible amounts and costs of product;
  - b) Reviewing of risk financing methods and which application may be the most advantageous for the Crown;
  - c) Conducting a gap analysis of risk management programs;
  - d) Providing advice and insight with respect to specialty insurance lines for large projects and whether or not other risk financing tools may be more fiscally prudent to the Crown;
  - e) Providing advice with respect to claims and financial recovery from other parties;
  - f) Providing options and applications of loss control programs;
  - g) Providing any other requirements that may fall within the Risk Management Services.
  - h) Conducting quality assurances on all deliverables;
  - i) Providing direction and approving deliverables prior to submission to clients;
  - j) Managing the risk assessment project budget, schedule and resources, as applicable;
  - k) Providing progress reports to the Technical Authority;
  - l) Facilitating and maintaining open communication with the Technical Authority; and
  - m) Making presentations to senior management

#### 3.1.1 Minimum Educational/Experience:

At a minimum the Senior Consultant must:

- a) Possess and currently maintain in good standing, a recognized risk management designation such as: Canadian Risk Management (CRM), Fellow in Risk Management (FRM), Certified in Risk and Information Systems Control (CRISC), Chartered Insurance Professional (CIP), Associate of the Insurance Institute of Canada (AIIC), Fellow of Chartered Insurance Practitioner (FCIP), Fellows of the Society of Actuaries (FSA), Professional Risk Manager (PRM), PMI Risk Management Professional (PMI-RMP), Chartered Accountant (CA), Certified Management Accountant (CMA), Certified General Accountant (CGA), Certified Internal Auditor (CIA), Certification in Control Self-Assessment (CCSA), Certified Information Systems Auditor (CISA), Chartered Enterprise Risk Analyst (CERA), and RIMS Fellow (RF); and
- b) Possess an undergraduate degree from a Canadian University or Canadian recognized University. The University degree must be from a recognized Canadian University, or if obtained outside of Canada, be approved by a recognized Canadian academic credentials assessment Service i.e. identified at:

<http://www.cicic.ca/413/assessment-of-credentials-for-employment-in-canada.canada>;and

Have 10 years of related work experience as a Senior Consultant within the past 15 years.

**OR**

Have 20 years of related work experience as a Senior Consultant within the past 25 years.

### 3.2 Consultant:

- a) Reviewing insurance portfolios and compare findings against insurance industry standards;
- b) Preparing various risk financing scenarios and illustrate the application to insurance program in question;
- c) Reviewing risks and provide methods of risk mitigation and provide a gap analysis;
- d) Providing clarification of insurance specialty lines and their application on specific projects;
- e) Reviewing claims processes and review claims settlements;
- f) Evaluating loss control programs and explain advantages and disadvantages of program application, including the impact on insurance premiums;
- g) Participating in sessions in order to provide expertise to special projects;
- h) Preparing reports; presentations and briefing notes.

#### 3.2.1 Minimum Educational/Experience

At a minimum the Consultant must:

- a) Must possess and currently maintain in good standing, a recognized risk management designation: Canadian Risk Management (CRM), Fellow in Risk Management (FRM), Certified in Risk and Information Systems Control (CRISC), Chartered Insurance Professional (CIP), Associate of the Insurance Institute of Canada (AIIC), Fellow of Chartered Insurance Practitioner (FCIP), Fellows of the Society of Actuaries (FSA), Professional Risk Manager (PRM), PMI Risk Management Professional (PMI-RMP), Chartered Accountant (CA), Certified Management Accountant (CMA), Certified General Accountant (CGA), Certified Internal Auditor (CIA), Certification in Control Self-Assessment (CCSA), Certified Information Systems Auditor (CISA), Chartered Enterprise Risk Analyst (CERA), and RIMS Fellow (RF); and
- b) Possess an undergraduate degree from a Canadian University or Canadian recognized University. The University degree must be from a recognized Canadian University, or if obtained outside of Canada, be approved by a recognized Canadian academic credentials assessment Service i.e. identified at:

<http://www.cicic.ca/413/assessment-of-credentials-for-employment-in-canada.canada>; and

Have 5 years of related work experience as a Consultant within the past 7 years.

**OR**

Have 10 years of related work experience as a Consultant within the past 15 years.

---

### 3.3 Account Assistant:

Under the direction of the Senior Consultant or the Consultant, as appropriate, the Account Assistant is responsible for providing assistance, as required, to the Senior Consultant and/or the Consultant. Tasks may include but are not limited to the following:

- a) Collecting and collating qualitative and quantitative data;
- b) Conducting research;
- c) Conducting preliminary analyses;
- d) Compiling background documentation; and
- e) Providing assistance with the development of briefing notes, presentations, papers and reports.

#### 3.3.1 Minimum Educational/Experience

At a minimum the Account Assistant must:

- a) Possess a secondary school diploma or General Education Development (GED) certificate; and
- b) Have 3 years of related work experience within the past 5 years.

## 4. Applicable Documents & References

The documents listed below will provide an understanding of methods, terminology and standards that are consistent with Risk Management applications used internally. The documents will enable the contractor to develop a better understanding of the risk management process as it relates to the federal government.

- a) Treasury Board Integrated Risk Management Framework (IRMF) - (Effective August 27th, 2010 with an accompanying guide to follow);
- b) Treasury Board Policy on Decision Making in Limiting Contractor Liability in Crown Procurement Contracts;
- c) PWGSC Risk Management Guide/Handbook; and
- d) Individual departmental risk management policies, guides and tools.

## **ANNEX "B"**

### **SUPPLY ARRANGEMENT QUARTERLY USAGE REPORT**

#### **1. Quarterly Reports**

At a minimum the quarterly report should contain:

- a) the supply arrangement number;
- b) the contract number;
- c) the client department name;
- d) a description of the requirement; and
- e) the total billed.

## **ANNEX "C"**

### **SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY**

#### **1. Security Requirements for Information Technology**

In regards to Security Requirements for Information Technology the Contractor must:

- a) have the ability to receive the client information via e-mail or facsimile;
- b) have the ability to receive the information in a word processor format e.g. Word, or a spreadsheet format e.g. Excel;
- c) retain electronically received information e.g. Word documents or Excel documents in password protected directories;
- d) ensure backup of information on a weekly basis; and
- e) ensure received hardcopy information is stored in locked file cabinets.

Solicitation No. - N° de l'invitation

EN578-121746/B

Amd. No. - N° de la modif.

File No. - N° du dossier

109zIEN578-121746

Buyer ID - Id de l'acheteur

109zI

Client Ref. No. - N° de réf. du client

20121746

CCC No./N° CCC - FMS No/ N° VME

---

**ANNEX "D"**

**SECURITY REQUIREMENTS CHECK LIST**

- Please see attached SRCL at end of document -

Solicitation No. - N° de l'invitation

EN578-121746/B

Client Ref. No. - N° de réf. du client

20121746

Amd. No. - N° de la modif.

File No. - N° du dossier

109z1EN578-121746

Buyer ID - Id de l'acheteur

109z1

CCC No./N° CCC - FMS No/ N° VME

---

**ANNEX "E"**

**RISK MANAGMENT GUIDE**

- Please see attachment 1 -



Contract Number / Numéro du contrat EN578-121746
Security Classification / Classification de sécurité UNCLASSIFIED

**SECURITY REQUIREMENTS CHECK LIST (SRCL)  
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)**

**PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE**

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine Public Works and Government Services Canada	2. Branch or Directorate / Direction générale ou Direction AB
---	--

3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant
--	---

4. Brief Description of Work / Brève description du travail  
To create a supply arrangement for risk management consulting services

5. a) Will the supplier require access to Controlled Goods? / Le fournisseur aura-t-il accès à des marchandises contrôlées?  No / Non  Yes / Oui

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? / Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?  No / Non  Yes / Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? / Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) / Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)  No / Non  Yes / Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. / Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.  No / Non  Yes / Oui

6. c) Is this a commercial courier or delivery requirement with no overnight storage? / S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?  No / Non  Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada <input checked="" type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	Foreign / Étranger <input type="checkbox"/>
--	--------------------------------------	---

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion <input checked="" type="checkbox"/>	All NATO countries / Tous les pays de l'OTAN <input type="checkbox"/>	No release restrictions / Aucune restriction relative à la diffusion <input type="checkbox"/>
Not releasable / À ne pas diffuser <input type="checkbox"/>		
Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>	Restricted to: / Limité à: <input type="checkbox"/>
Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:	Specify country(ies): / Préciser le(s) pays:

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A <input checked="" type="checkbox"/>	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A / PROTÉGÉ A <input type="checkbox"/>
PROTECTED B / PROTÉGÉ B <input type="checkbox"/>	NATO RESTRICTED / NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B / PROTÉGÉ B <input type="checkbox"/>
PROTECTED C / PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL / NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C / PROTÉGÉ C <input type="checkbox"/>
CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/>	NATO SECRET / NATO SECRET <input type="checkbox"/>	CONFIDENTIAL / CONFIDENTIEL <input type="checkbox"/>
SECRET / SECRET <input type="checkbox"/>	COSMIC TOP SECRET / COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET / SECRET <input type="checkbox"/>
TOP SECRET / TRÈS SECRET <input type="checkbox"/>		TOP SECRET / TRÈS SECRET <input type="checkbox"/>
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) <input type="checkbox"/>



Contract Number / Numéro du contrat EN578-121746
Security Classification / Classification de sécurité UNCLASSIFIED

**PART A (continued) / PARTIE A (suite)**

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?  
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?  No / Non  Yes / Oui  
If Yes, indicate the level of sensitivity:  
Dans l'affirmative, indiquer le niveau de sensibilité :
9. Will the supplier require access to extremely sensitive INFOSEC information or assets?  
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?  No / Non  Yes / Oui
- Short Title(s) of material / Titre(s) abrégé(s) du matériel :  
Document Number / Numéro du document :

**PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)**

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis
- |   |   |   |  |
|---|---|---|--|
| <input checked="" type="checkbox"/> RELIABILITY STATUS<br>COTE DE FIABILITÉ | <input type="checkbox"/> CONFIDENTIAL<br>CONFIDENTIEL           | <input type="checkbox"/> SECRET<br>SECRET           | <input type="checkbox"/> TOP SECRET<br>TRÈS SECRET               |
| <input type="checkbox"/> TOP SECRET - SIGINT<br>TRÈS SECRET - SIGINT        | <input type="checkbox"/> NATO CONFIDENTIAL<br>NATO CONFIDENTIEL | <input type="checkbox"/> NATO SECRET<br>NATO SECRET | <input type="checkbox"/> COSMIC TOP SECRET<br>COSMIC TRÈS SECRET |
| <input type="checkbox"/> SITE ACCESS<br>ACCÈS AUX EMPLACEMENTS              |   |   |  |
- Special comments:  
Commentaires spéciaux : \_\_\_\_\_

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.  
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?  
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?  No / Non  Yes / Oui  
If Yes, will unscreened personnel be escorted?  
Dans l'affirmative, le personnel en question sera-t-il escorté?  No / Non  Yes / Oui

**PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)**

**INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS**

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?  
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?  No / Non  Yes / Oui
11. b) Will the supplier be required to safeguard COMSEC information or assets?  
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?  No / Non  Yes / Oui

**PRODUCTION**

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?  
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?  No / Non  Yes / Oui

**INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)**

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?  
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?  No / Non  Yes / Oui
11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?  
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?  No / Non  Yes / Oui



**PART C - (continued) / PARTIE C - (suite)**

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.

Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

**SUMMARY CHART / TABLEAU RÉCAPITULATIF**

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL	SECRET	TOP SECRET	NATO RESTRICTED	NATO CONFIDENTIAL	NATO SECRET	COSMIC TOP SECRET	PROTECTED PROTÉGÉ			CONFIDENTIAL	SECRET	TOP SECRET
				CONFIDENTIEL		TRÈS SECRET	NATO DIFFUSION RESTREINTE	NATO CONFIDENTIEL		COSMIC COSMIC TRÈS SECRET	A	B	C	CONFIDENTIEL		TRÈS SECRET
Information / Assets Renseignements / Biens Production	✓															
IT Media / Support TI	✓															
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?  
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

No / Non  Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".  
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?  
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

No / Non  Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).  
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).



Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat EN578-121746
Security Classification / Classification de sécurité UNCLASSIFIED

**PART D - AUTHORIZATION / PARTIE D - AUTORISATION**

**13. Organization Project Authority / Chargé de projet de l'organisme**

Name (print) - Nom (en lettres moulées) Sewell, Malaika	Title - Titre jr analyst	Signature <i>M. Sewell</i>
Telephone No. - N° de téléphone 819-956-1727	Facsimile No. - N° de télécopieur 613-956-0400	E-mail address - Adresse courriel malaika.sewell@pwgsc.gc.ca
		Date 2011/11/17

**14. Organization Security Authority / Responsable de la sécurité de l'organisme**

Name (print) - Nom (en lettres moulées) Charron, Annick	Title - Titre SO	Signature <i>Annick Charron</i>
Telephone No. - N° de téléphone 819-956-0615	Facsimile No. - N° de télécopieur 819-934-1449	E-mail address - Adresse courriel annick.charron@tpsgo-pwgsc.gc.ca
		Date Nov 18, 2011

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? / Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

No / Non  Yes / Oui

**16. Procurement Officer / Agent d'approvisionnement**

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel
		Date

**17. Contracting Security Authority / Autorité contractante en matière de sécurité**

Name (print) - Nom (en lettres moulées) <i>Whitney Ball</i>	Title - Titre <i>AKSA</i>	Signature <i>[Signature]</i>
Telephone No. - N° de téléphone <i>613-948-1059</i>	Facsimile No. - N° de télécopieur <i>613-954-4171</i>	E-mail address - Adresse courriel <i>Whitney.Ball@pwgsc.gc.ca</i>
		Date <i>2011-11-21</i>



## RISK MANAGEMENT GUIDE

Developed by the Quality and Risk Management Directorate

Operational Integrity Sector

## TABLE OF CONTENTS

<b>1</b>	<b>INTRODUCTION</b> .....	<b>1</b>
1.1	PURPOSE .....	1
1.2	CONTEXT .....	1
1.3	TBS MANAGEMENT ACCOUNTABILITY FRAMEWORK: RISK MANAGEMENT EXPECTATIONS .....	2
<b>2</b>	<b>RISK MANAGEMENT AND BUSINESS PLANNING</b> .....	<b>3</b>
2.1	RISK MANAGEMENT AND RESOURCE ALLOCATION .....	4
2.2	THE LINK BETWEEN RISK AND PERFORMANCE .....	5
<b>3</b>	<b>UNDERSTANDING OPPORTUNITIES IN RISK</b> .....	<b>6</b>
<b>4</b>	<b>RISK MANAGEMENT PROCESS</b> .....	<b>7</b>
4.1	PROCESS .....	7
4.2	ESTABLISH CONTEXT .....	7
4.3	RISK ASSESSMENT .....	8
4.3.1	RISK IDENTIFICATION .....	8
4.3.2	RISK ANALYSIS .....	8
4.3.3	RISK EVALUATION .....	9
4.4	RISK RESPONSE .....	9
4.4.1	POSITIVE (OPPORTUNITY) RISK RESPONSE .....	10
4.4.2	NEGATIVE RISK (THREAT) RESPONSES .....	10
4.5	COMMUNICATION AND CONSULTATION .....	12
4.6	MONITOR AND REVIEW .....	12
5.0	SUMMARY: RISK PROCESS AND TOOLS .....	13
	<b>APPENDICES</b> .....	<b>14</b>
	<b>APPENDIX A: RISK MANAGEMENT TOOLS</b> .....	<b>15</b>
	<i>APPENDIX A1: POSITIVE (OPPORTUNITY) AND NEGATIVE (THREAT) RISK EXAMPLE SCENARIOS</i> .....	<i>15</i>
	<i>APPENDIX A2: RISK MANAGEMENT PROCESS GUIDANCE</i> .....	<i>16</i>
	ESTABLISH CONTEXT .....	16
	RISK IDENTIFICATION .....	16
	RISK ANALYSIS .....	19
	RISK RESPONSE .....	22
	COMMUNICATION AND CONSULTATION .....	25
	MONITOR AND REVIEW .....	25
	<i>APPENDIX A4: RISK INFORMATION SHEET</i> .....	<i>28</i>
	<b>APPENDIX B: GLOSSARY OF KEY RISK MANAGEMENT TERMS</b> .....	<b>29</b>
	<b>APPENDIX C: RISK MANAGEMENT REFERENCES AND LINKS</b> .....	<b>31</b>

## TABLE OF FIGURES

FIGURE 1:	MANAGEMENT ACCOUNTABILITY FRAMEWORK .....	2
FIGURE 2:	RISK AND BUSINESS PLANNING CONTINUUM .....	3
FIGURE 3:	RISK MANAGEMENT AND THE BUSINESS PLANNING CYCLE .....	5
FIGURE 4:	RISK MANAGEMENT PROCESS .....	7
FIGURE 5:	RISK RESPONSE PROCESS .....	10
FIGURE 6:	RISK MANAGEMENT PROCESS AND TOOLS .....	13



## TABLE OF TABLES

Table 1: Positive (Opportunity) Risk Responses .....	10
Table 2: Negative (Threat) Risk Responses .....	11
Table 3: Positive (Opportunity) and Negative (Threat) Risk Responses.....	11
Table 4: Example of a Risk Management Taxonomy.....	18
Table 5: Negative (Threat) Risk Analysis Heat Map .....	20
Table 6: Positive (Opportunity) Risk Analysis Heat Map.....	21
Table 7 – Management Areas of Oversight / Influence .....	24
Table 8: Influential Elements of a Risk Communication Plan.....	25



# 1 Introduction

Risks are not isolated events addressed by specialists; everyone, from senior-level management to employees, works with risk. A systematic risk management process and other tools are means by which risk is taken from a chance occurrence to a risk discipline that informs business planning and decision making and supports operational processes.

## 1.1 Purpose

This guide is a companion to the departmental [Integrated Risk Management \(IRM\) Policy](#) (DP082-2010). It is a “how to guide” for employing a consistent risk management process and indirectly establishing a risk framework for the Department. It also responds to the corporate risk management requirements set out in the Treasury Board Secretariat’s [Framework for the Management of Risk](#). This guide is for all employees in the Department who deal with risk – whether at the project level, the operational level or the corporate level.

This guide is divided into four sections. It is not imperative to read the guide sequentially, as each section has been written to stand alone from the others. It is important to note that the first three sections encompass the theoretical side of risk management, whereas the fourth section and the appendices encompass the practical side of risk management.

- Section 1 provides an introduction to risk management and explains the context for risk management across the global community, Canada and the federal public service, including the risk management expectations of the Treasury Board Secretariat (TBS) Management Accountability Framework (MAF).
- Section 2 provides a model risk management framework. It discusses the activities required to integrate risk management in an organization and positions risk management in the business planning cycle and performance measurement setting of PWGSC.
- Section 3 provides an explanation of risk as uncertainty with both positive and negative impacts.
- Section 4 focuses on the risk management process.
- Appendix A provides tools for the risk management process.
- Appendix B provides a glossary of key risk management terms.

## 1.2 Context

Several recent developments in the international and national risk management communities have led PWGSC to refresh its Integrated Risk Management policy and guide.

Recently, the ISO 31000 Standard in Risk Management has been redrafted. The standard, which embodies key principles in risk management, is a strong departure from its previous iteration in that it addresses risk as either a positive or negative outcome.<sup>1</sup> The international community has overwhelmingly approved the new standard and many countries are using it as a seminal document in the development of risk management.

Canada, which is a supporter of the ISO 31000 Standard, has developed a Canadian standard in risk management known as the CSA Q31001-11. The document embraces the concepts presented in the ISO 31000 standard, but incorporates a Canadian interpretation of risk management which emphasizes senior management involvement, the notion of public risks and demonstrable links between risk management and organizational performance and business planning.<sup>2</sup>

With respect to the federal government context, the TBS has released a new framework, called the Framework for the Management of Risk and an accompanying guide, the [Guide to Integrated Risk Management](#). PWGSC

<sup>1</sup> ISO GUIDE 73, 2009, pg 1.

<sup>2</sup> CAN/CSA Q31001-11 [Implementation to CSA –ISO31000](#), March 2011.

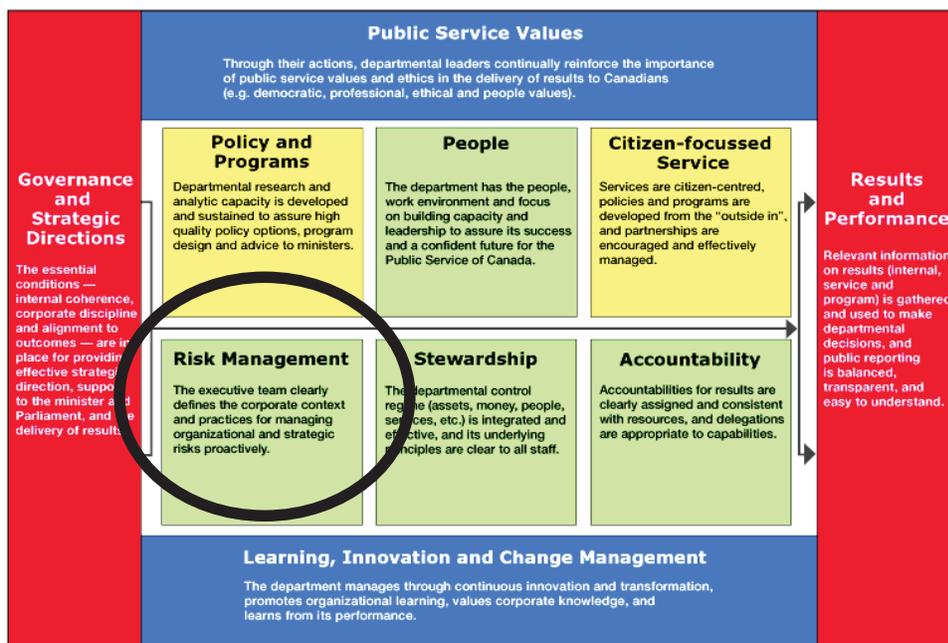
was an active participant in the development of the guide, by providing input, taking a lead role in coordinating comments from other government departments and assisting the TBS in organizing a critical drafting session.

Integrated risk management at PWGSC involves implementing a risk-smart culture in which risk management principles inform business planning, decision making and support operational process. Branches, Regions and staff are encouraged to engage in responsible decision-making by incorporating integrated risk management into their management framework.

### 1.3 TBS Management Accountability Framework: Risk Management Expectations

In 2003, the TBS introduced an accountability framework structured around ten key principles which define “good management” within a department or agency. This was called the [Management Accountability Framework](#) (MAF). The MAF consists of ten key elements followed by a series of indicators and associated measures. The focus of this guide is on Area of Management Nine (AoM 9): Corporate Risk Management which is shown in the green box in the bottom left hand corner of Figure 1.

Figure 1: Management Accountability Framework



Effective corporate risk management (identified by TBS in MAF as Area of Management 9), is in place when corporate decision-making, processes and management are informed in by appropriate risk management practices. Every year, the TBS develops lines of evidence for this area of management which are used to measure corporate effectiveness.

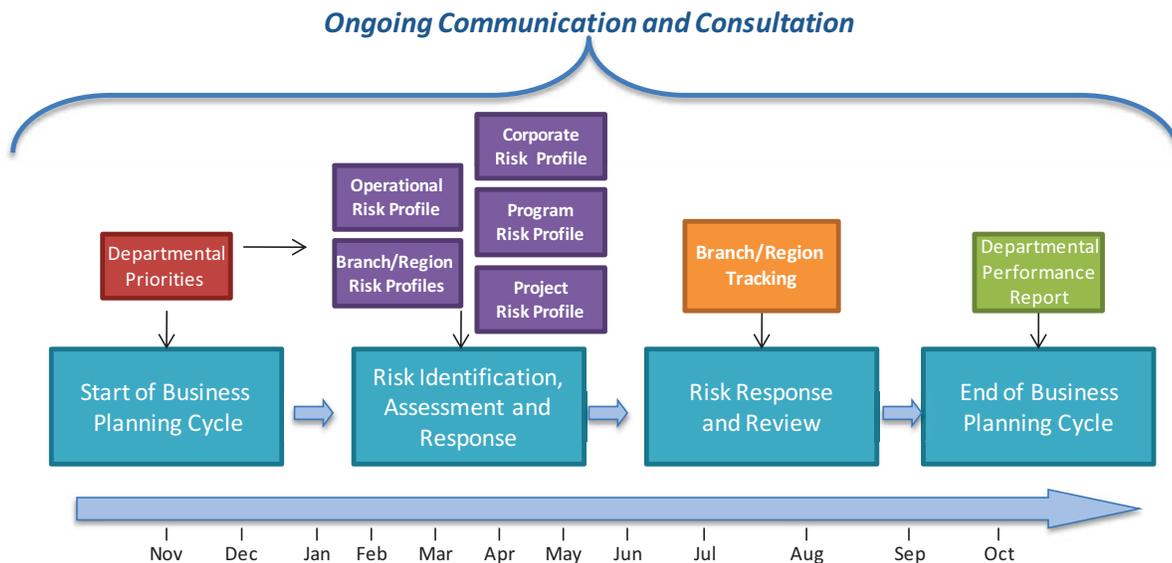
For each line of evidence there are several performance indicators. These are outcome based, which means outputs such as risk profiles or risk assessments are only part of the equation. PWGSC performance against these lines of evidence is assessed annually.

Note: For more information on the lines of evidence, please contact the [Director, Quality and Risk Management in the Operational Integrity Sector](#).

## 2 Risk Management and Business Planning

As per MAF AoM 9, senior management must manage operational and strategic risks. To facilitate this, risk management is embedded into the business planning cycle. Figure 2 provides a general view of the business planning continuum and its key outputs.

Figure 2: Risk and Business Planning Continuum



At the start of the business planning cycle, the department releases its Report on Plans and Priorities (RPP). The purpose of the RPP is to outline the departmental direction and to show how the department's key priorities will be achieved. The RPP includes a discussion on how the current challenges and risks can influence the current plans and priorities for the upcoming year.

Once the departmental priorities are confirmed, work begins on developing risk information that assists the organization in achieving its objectives. Examples of strategic or high-level operational risk information include an Operational, Branch, Regional and a Corporate risk profile. A description of each risk profile and its purpose is provided below.

- The Operational Risk Profile (ORP) is developed by identifying risks that may be associated with a lack of stewardship or non-compliance resultant from legislation, regulation, internal processes, people and systems or external events. Risks identified in the ORP can be horizontal, impacting more than one area. At PWGSC, these risks have only *negative* impacts, as they result from issues of non-compliance or lack of either stewardship or controls.
- The Branch Risk Profile (BRP) and the Regional Risk Profile (RRP) are developed by aggregating risks significant to the achievement of the branch/region commitments. Risks may be associated with commitments, and pertain only to functions within the Branch/Region. Branch/regional risks can be either positive or negative; that is, they can lead to either opportunities or unwanted results. Risks identified in the BRP and RRP may also have significant impact on other branches, regions or the Department as a whole. When this occurs, the most important risks are rolled up to the corporate level.
- The Corporate Risk Profile (CRP) is developed by identifying high level, strategic risks that can have an impact on the department's mandate, mission and/or vision. Risks identified in the CRP can be horizontal, with an impact on more than one area, or one or more highly significant risks that are

specific to a branch, a project or the department's operations. The risks identified in the CRP are neutral, and may have either positive or negative impacts. The CRP is updated annually to identify key corporate-level risks and record internal risk response strategies related to departmental initiatives.

- Program Risk Profiles are developed by OPIs using the risk management process to highlight risks related to specific programs within the organization. The risks identified in these profiles have an impact on the program only. These risks may be captured in a risk register or similar tool.
  - It is worth noting that when completing the Corporate and Operational Risk Profile exercises, the Operational Integrity Sector, along with the relevant stakeholders, uses Program Risk Profiles from major organizational programs as supporting evidence for the risks identified in the CRP and ORP.
  - For more information on the risk management process, see [Appendix A2: Process Guidance](#)
  - For information on a risk register, see [Appendix A3: Risk Register](#).
- Project Risk Profiles are developed by OPIs using the risk management process to highlight risks related to specific projects within the organization. The risks identified in these profiles have an impact on the project only. These risks may be captured in a risk register or similar tool.
  - It is worth noting that when completing the Corporate and Operational Risk Profile exercises, the Operational Integrity Sector, along with the relevant stakeholders, uses Program Risk Profiles from major organizational programs as supporting evidence for the risks identified in the CRP and ORP.
  - For more information on the risk management process, see [Appendix A2: Process Guidance](#)
  - For information on a risk register, see [Appendix A3: Risk Register](#).

After key risks have been identified, they are entered manually, as determined by each branch/region for regular monitoring and reviewing. The purpose of tracking the risks is to provide the Deputy Minister and senior level management with an overview of the top risks to the department's objectives, the risk responses used to manage them, and any changes that occur to the risks throughout the reporting period. Mid-year review is a significant marker in the business planning cycle as the identified risks and key risk profiles are reviewed and monitored at that time.

At the end of the business planning cycle, the Department reports on its performance in delivering on plans, addressing priorities and achieving results through the Departmental Performance Report (DPR). The DPR provides a discussion on the context, risks and operating environment in which results were achieved, as well as a specific section on lessons learned for each program activity. At this point in the cycle, consideration is given to which risks will remain as key risks for the next fiscal year.

## **2.1 Risk Management and Resource Allocation**

Risk management is a key element in business planning and achieving organizational priorities. At the beginning of the fiscal year, business commitments are identified. Risks are identified, analyzed and evaluated in relation to these commitments and risks are expressed in terms of their likelihood and impact on the achievement of the objectives. Once a risk has been assessed, management determines how to respond to and manage that risk. Resources are allocated accordingly. Risk information is communicated to staff at all levels as well as monitored and reviewed at regular intervals.

At mid-year these same priorities are re-examined, updated and / or re-confirmed. Risks are reassessed and responses are monitored. Resources are re-allocated accordingly to ensure the priorities and commitments have the best chance of being achieved.

At year-end, the same priorities, commitments and risks are reviewed to determine whether the organization was successful in achieving its objectives by realizing positive (opportunities) and managing negative (threats)

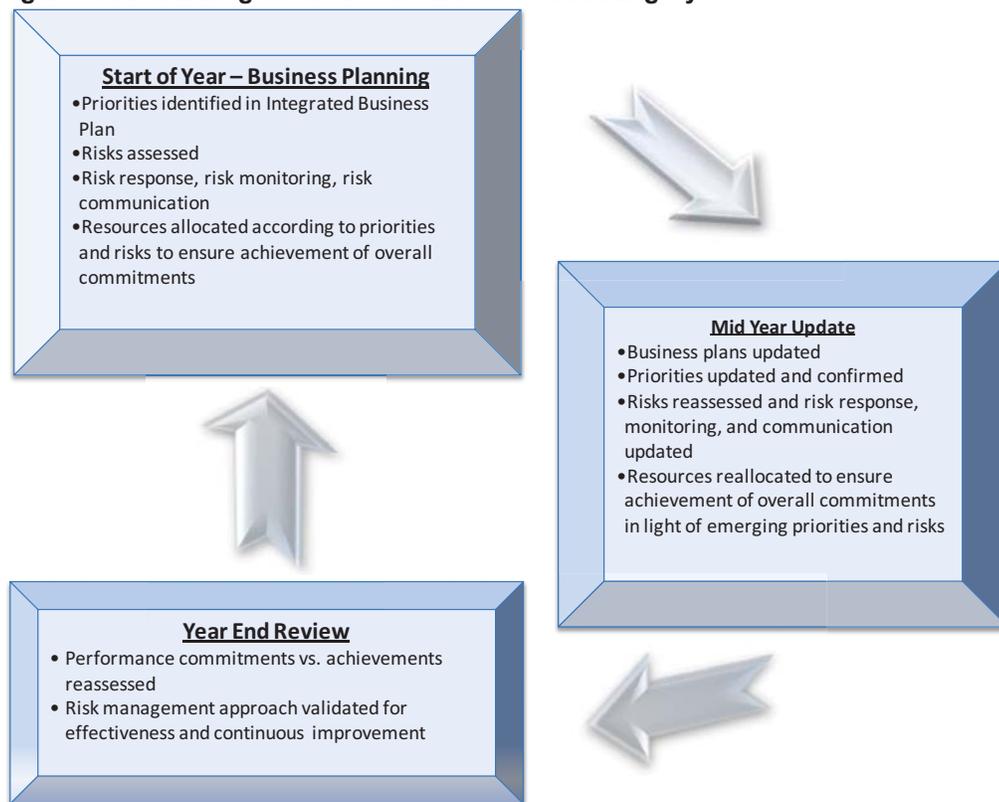
risks. This is also the time to determine whether a risk response was cost-effective and assisted the organization in achieving a desired result. At this point, a new business cycle begins. Management and staff review risks from the previous fiscal year and consider which risks are still relevant given the upcoming business priorities and commitments.

A risk-informed approach to business planning means that:

- It is acknowledged that uncertainties come and go and can change over time.
- The course of action taken is informed by an understanding of uncertainty at a specific point in time.
- Where efforts are focused, there is flexibility to ensure that the organization can always concentrate on the risks and opportunities that matter most to the achievement of its objectives.

Figure 3 is a rudimentary schematic indicating the key risk activities in the business planning cycle. The apex of the cycle – Start of Year – Business Planning – is the starting point of the cycle. The figure progresses clockwise to the Mid-Year Update and Year-End Review boxes.

**Figure 3: Risk Management and the Business Planning Cycle**



## 2.2 The Link between Risk and Performance

Expected results are generally reviewed as part of the annual business planning process; however, they are not likely to change significantly from year to year. They are linked to the Department's mandate and mission, internal and external factors that influence outcomes, and the performance results of prior periods. Expected results should be established at each of the departmental, branch/region and operational levels. All activities at each level should not only be linked to expected results, they should also directly lead to the achievement of expected results. Using targets and performance indicators can help make this link more explicit.

The goal of risk management is to manage those uncertainties that threaten or enhance the achievement of PWGSC priorities and expected results.

In prior years, it has been difficult to demonstrate how our actions have helped to manage specific risks, yet we know this occurred. Going forward, the link between major PWGSC risks and performance will be clear and monitored over time in the Integrated Business Plan (IBP).

To know if the Department is achieving its expected results and priorities, and is managing its risks effectively:

- Consider identifying key risks that could impact the achievement of priorities and expected results of each commitment in the Integrated Business Plan.
- With each risk, identify the potential consequences; along with the likelihood of the risk occurring and impact it may have (see [Appendix A2– Risk Management Process Guidance](#)).
- For each identified risk, consider how effective the existing risk response is. It may be beneficial to identify any planned risk responses that would enhance the management of the risk.
- As part of risk monitoring, review the performance measures for the business area and consider which one or two aligns best to the top risks for the business area and to the OPI responsible for those key risks. As part of the overall reporting approach in the business area, report on the progress made in responding to the key risks and any change in the risk itself.

### 3 Understanding Opportunities in Risk

In both ISO 31000 Standard in Risk Management and CSA Q31001-11, the risk management process is expanded to include both the negative (threat) and positive (opportunity) attributes of risk. Specifically, ISO 31000 and CSA Q31001-11 suggest that the organization should look at both the negative (threat) side of risk and the positive (opportunity) side of risk, as well as the risks associated with not pursuing an opportunity.<sup>3</sup> The newly released Treasury Board [Framework for the Management of Risk](#) supports this concept, moving the Federal Public Service away from viewing risk as having strictly negative attributes, and towards viewing risk as **neutral and uncertain** that can have either a positive or negative impact.

When positive, a risk can lead to the capacity and capability to exploit an opportunity. Opportunities can include savings (time and resources) from increased efficiency, performance enhancement and optimization of the relationship between your organization and its stakeholders. In the case of a positive risk (opportunity), the risk management process (see section 4 for more information) can be applied to capitalize on the opportunity (positive risk).

When negative, a risk can be perceived as a threat and if left untreated could lead to vulnerability, thus leaving the GoC, Department, project or program susceptible to a threat. Threats (negative risks) can include time delays, extra costs, performance shortfalls, reduced business benefits or strain on the relationship between the organization and its stakeholders. In the case of a negative risk (threat), the risk management process (see section 4 for more information) can be applied to protect against an exposure to a threat or vulnerability.

It is important to reiterate that because risk is neutral, the risk management process can be applied to both enable the realization of an opportunity (positive risk) and prevent the unwanted exposure of a threat (negative risk).

Tools for understanding positive and negative risk can be found in [Appendix A1: Positive \(Opportunity\) and Negative \(Threat\) Risk Example Scenarios](#)

---

<sup>3</sup> ISO GUIDE 73, 2009 and CAN/CSA Q31001-11 [Implementation to CSA –ISO31000](#), March 2011.

## 4 Risk Management Process

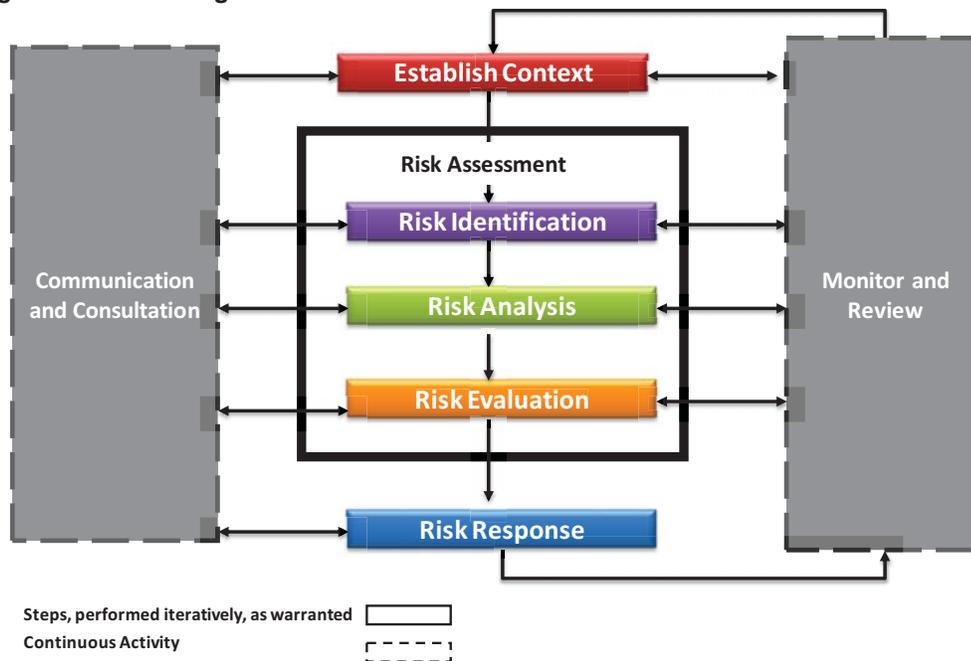
This section focuses on the risk management process. Throughout this section there are references to appendices. The appendices have been designed to provide assistance to users at each part of the process. They contain notes, guidance, questions and approaches that may be used when developing a risk register or similar tool.

### 4.1 Process

The risk management process is the cornerstone of risk management in the organization. By implementing a consistent risk management process, risk management supports operational processes, informs business planning, as well as decision making. Senior management must support the process and place emphasis on regularly monitoring, reviewing and communicating risks as well as consulting stakeholders.

The risk management process, which is captured in Figure 4, has seven components. The risk management process is used to assess and respond to both positive risks (opportunities) and negative risks (threats). The description of the process starts with the middle column - Establish Context, Risk Identification, Risk Analysis, Risk Evaluation and Risk Response – all the while ensuring that the left hand column – Communication and Consultation - is taking place and finishing with Monitor and Review.

Figure 4: Risk Management Process



### 4.2 Establish Context

Establishing a context provides a frame of reference against which risks are identified and assessed. As aspects of the context changes so too will the risks. By documenting the context, risk management practitioners leave a legacy document that provides information on a risk, decision or strategy that otherwise may appear inconsistent or out of place.

Generally, an environmental scan is the tool used to establish the context. It identifies a range of internal and / or external risks an organization may face. When examining the external context, stakeholders may refer to environmental, social, economic, political, industry, trade, legal, academic and other government department influences. As for the internal context, useful documents that may provide an organizational snapshot include policy, audits, the RPP, the DPR, budget statements, work plans and business plans. When establishing the context, it is important to think “what if...?” (i.e. what are the threats / opportunities to our organization should the risk materialize?)

When developing the context for the risk management process you will in effect be creating the risk criteria that you will be evaluating individual risks against later in the process. These criteria must respect and observe the legislative framework and be in compliance with the TBS policy framework and that of the Department.

Tools for establishing the context are available in [Appendix A2 – Risk Management Process Guidance](#).

## **4.3 Risk Assessment**

Risk assessment is the central risk management process. It consists of risk identification, risk analysis followed by risk evaluation. The outputs of the three components provide decision-makers with a clear understanding of those risks that could have a positive or negative impact on objectives. The process should be tailored to the organization’s context and inclusive of all relevant stakeholders.

### **4.3.1 Risk Identification**

Risk identification is the first step in managing risks. It involves recognizing the uncertainties that could impact the organization’s/branch’s/region’s/project’s/program’s ability to achieve its objectives.

The quality of risks collected during the risk identification stage is directly dependent on the stakeholders’ knowledge and experience and the approach used for collecting risks. Risk practitioners may want to consider stakeholders internal and external to their organization depending on the objective. It is also critical to select a methodology or a combination of methodologies to collect risks such as interviews, surveys, workshops and scenario analyses. This will ensure that all levels within the organization know the risk identification scope and approach and will help with buy-in.

It is important to capture and record all risks identified, even those that do not seem important, as risks that are discounted at this stage will not be considered in the later stages of the process. When listing risks, it may be helpful to use a risk taxonomy to group risks into possible categories, such as strategic, operational, and project. An example of a risk taxonomy can be found in [Appendix A2- Risk Management Process Tools](#). When identifying risks, it is important to keep in mind the positive (opportunity) and negative (threats) risks, as well as the risks associated with not pursuing an opportunity (positive risk). Once the list of risks is identified, develop risk statements, drivers, impacts (should the risk materialize) and timeframes (i.e. when the risk is expected to occur; how long the risk is expected to be managed) for each risk. The concepts and language used to define these items should represent the views of all stakeholders. Other considerations to take into account when identifying risks is whether a risk is meaningful to all stakeholders, as well as whether the risk is in fact a risk and not an issue. An issue is a final outcome, certain event and/or an ongoing concern that must be managed. A risk practitioner may choose to document this information in a risk register or template. An example of a risk register can be found in [Appendix A3 – Risk Register](#).

Tools for identifying risks are available in [Appendix A2– Risk Management Process Guidance](#).

### **4.3.2 Risk Analysis**

Risk analysis is about better understanding the importance of a risk. It takes into consideration the positive (opportunities) and negative (threats) impacts of a risk and the probability that a risk may occur. Risks are expressed in terms of their likelihood and the impact on the achievement of the organization's objectives if they should occur. It is important that both the worst-case and best-case scenarios are considered. Further analysis may be required should any factors concerning a risk change.

Information gathered through risk identification is assessed during the risk analysis stage. Some questions to consider are:

- What is the risk? Is it positive (opportunity) and/or negative (threat)?
- What are the positive and negative consequences to the objectives?
- What is the likelihood such consequences will take place?
- What is the impact on objectives should the risk take place?

The output of the risk analysis stage is a risk register / risk profile. A risk practitioner may use a risk register or a similar risk tool to document information collected during the risk analysis stage. A sample risk register is available in [Appendix A3 – Risk Register](#).

Tools for analyzing risks, including negative and positive risk heat maps, are available in [Appendix A2 – Risk Management Process Guidance](#).

### **4.3.3 Risk Evaluation**

In this stage, risk practitioners evaluate risks with respect to which risk requires a response and assigning a priority ranking for each response.

Risk evaluation involves comparing the level of risk determined in the analysis stage to the criteria established during the context stage. Based on the comparison, a response will be identified. Each response should be in compliance with legal, regulatory and policy requirements. It should also align with an organization's risk appetite and tolerance levels (see [Appendix B – Glossary of Key Risk Management Terms](#)) which will have been signaled in the development of the framework.

Once an initial evaluation is completed, it may be necessary to follow up with further analysis. It may also be decided at this stage that existing controls are sufficient or need improvement in order to respond to a risk.

### **4.4 Risk Response**

Once the risks are evaluated, the next step is to select and implement plans to respond to the risks. Risk response is a cyclical process (see Figure 5) that includes actions to mitigate the likelihood or the impact of a risk (or both), the documentation of control measures currently in place and implementation of mitigation strategies and checking that the residual risk after response is tolerable. The costs of responding to risks should be in proportion to the costs of the impacts. Responses will depend on the resources that are available.

**Figure 5: Risk Response Process**



There are several ways in which a risk practitioner or owner may respond to a risk. It is important to note that risk responses are neutral and as such can be applied to mitigate both positive (opportunity) and negative (threat) risks.

#### 4.4.1 Positive (Opportunity) Risk Response

There are several ways in which a risk practitioner or owner may respond to a positive risk (opportunity). Positive risk (opportunity) responses include capitalizing, enhancing, retaining, sharing or accepting the risk by conducting business as usual. Table 1 lists the most common positive risk (opportunity) response options.

**Table 1: Positive (Opportunity) Risk Responses**

Response Options	Definition
<b>Capitalize</b>	Opportunity is realized by taking explicit action. (e.g. making a conscious effort to realize an opportunity)
<b>Enhance</b>	Opportunity is realized by maximizing benefit and increasing the likelihood of an opportunity occurring (e.g. undertaking an activity that may result in realizing an opportunity)
<b>Retain</b>	Opportunity is realized by taking direct ownership (e.g. an opportunity that falls under a risk practitioners authority)
<b>Share</b>	Responsibilities and opportunities are shared by partners/collaborators. Parties are directly involved, and responsible for doing their parts to ensure that agreed-to objectives, results and/or outcomes are met.
<b>Accept</b>	Opportunities may be accepted for several reasons: Opportunity is unidentified, and therefore, unknown Response is not possible (opportunity accepted, then managed to best of our ability) Response is not practical or optional where response techniques are deemed not to be cost effective

#### 4.4.2 Negative Risk (Threat) Responses

There are several ways in which a risk practitioner or owner may respond to negative risk (threat). Negative risk (threat) responses include avoiding, mitigating, transferring, sharing and accepting the risk. A taxonomy of negative risk (threat) responses is displayed in Table 2.

**Table 2: Negative (Threat) Risk Responses**

Response Options	Definition
Avoid	Decision not to create a particular loss exposure or to eliminate completely any existing exposure. Such a decision reduces probability of loss to zero.
Mitigate by Segregation	Lessening exposure by separating or duplicating staff, units, activities, delivery mechanisms, etc., so that exposure to risk/loss is lessened or eliminated
Mitigate by Reducing Risk	Loss reduction measures lessen the severity of losses that do occur. There are two types of loss reduction measures: <ul style="list-style-type: none"> <li>• Pre-loss measures</li> <li>• Post-loss measures</li> </ul>
Mitigate by Prevention	Any measure that reduces the probability or likelihood of a particular loss but does not completely eliminate all possibility (i.e. immunization) Reduces loss frequency without necessarily having an effect on the likely severity of it.
Transfer Risk to Others	Risks are transferred to other parties who have agreed to accept them and the potential consequences. Those who accept the risk(s) are not directly involved in or responsible for the particular activity or project.
Share Risk with Others	Responsibilities and risks are shared by partners/collaborators. Parties are directly involved, and responsible for doing their parts to ensure that agreed-to objectives, results and/or outcomes are met. What is risked may be the same (e.g., shared financial loss) or different (individual responsibilities)
Accept the Risk	Risks may be accepted for several reasons: <ul style="list-style-type: none"> <li>• Risk is unidentified, and therefore, unknown</li> <li>• Mitigation is not possible (risk accepted, then managed to best of our ability)</li> <li>• Mitigation is not practical or optional where mitigation techniques are deemed not to be cost effective</li> <li>• Accepting a risk or set of risk may ensure than an important opportunity (positive risk) is NOT lost</li> </ul>

Table 3 shows a comparison of positive (opportunity) and negative (threat) risk responses.

**Table 3: Positive (Opportunity) and Negative (Threat) Risk Responses**

Negative Response	Generic Strategy	Positive Response
Avoid	Eliminate uncertainty	Capitalize
Mitigate (Prevent, Reduce)	Reduce possible threats/maximize benefits	Enhance
Transfer	Assign responsibility	Retain
Share	Develop horizontal linkages and synergies	Share
Accept	Business as usual	Accept

It is important to note that it may not be necessary to plan a response (positive or negative) for all risks. It may be acceptable based on an organization's tolerance levels (see [Appendix B – Glossary of Key Risk Management Terms](#)) to accept some low risks and perhaps some medium risks. Resources should be focused on situations that are medium to high risk as defined by the criteria set by senior management. When developing risk response strategies it is useful to ensure that risks are assigned to someone (consistent with PWGSC governance structure and delegated authority) and that performance indicators are established to measure progress.

Tools for risk response, including negative and positive risk heat maps: level of management, are available in [Appendix A2 – Risk Management Process Guidance](#).

#### **4.5 Communication and Consultation**

Ongoing communication and consultation throughout the risk management process is critical as risks may change and may be perceived differently by stakeholders. Plans for communication and consultation need to be developed at an early stage and should involve communication with all key stakeholders. Risk practitioners or risk owners may want to consider identifying, recording, and taking into account stakeholders' perceptions in the decision-making process as these views may have a significant impact on the decisions taken.

Tools for developing a risk communication plan are available in [Appendix A2– Risk Management Process Guidance](#).

#### **4.6 Monitor and Review**

Monitoring and review should be included in all aspects of the risk management process. The objective of monitoring and review is to:

- assess the effectiveness and efficiency of controls identified in a risk profile;
- ensure risks are still relevant with the internal and external contexts;
- identify when revisions to improve a risk profile are required;
- re-profile resources to higher priority risks; to analyze changes lessons learned, trends and changes to the context;
- identify emerging risks; and
- assess the progress of implementing a risk response plan.

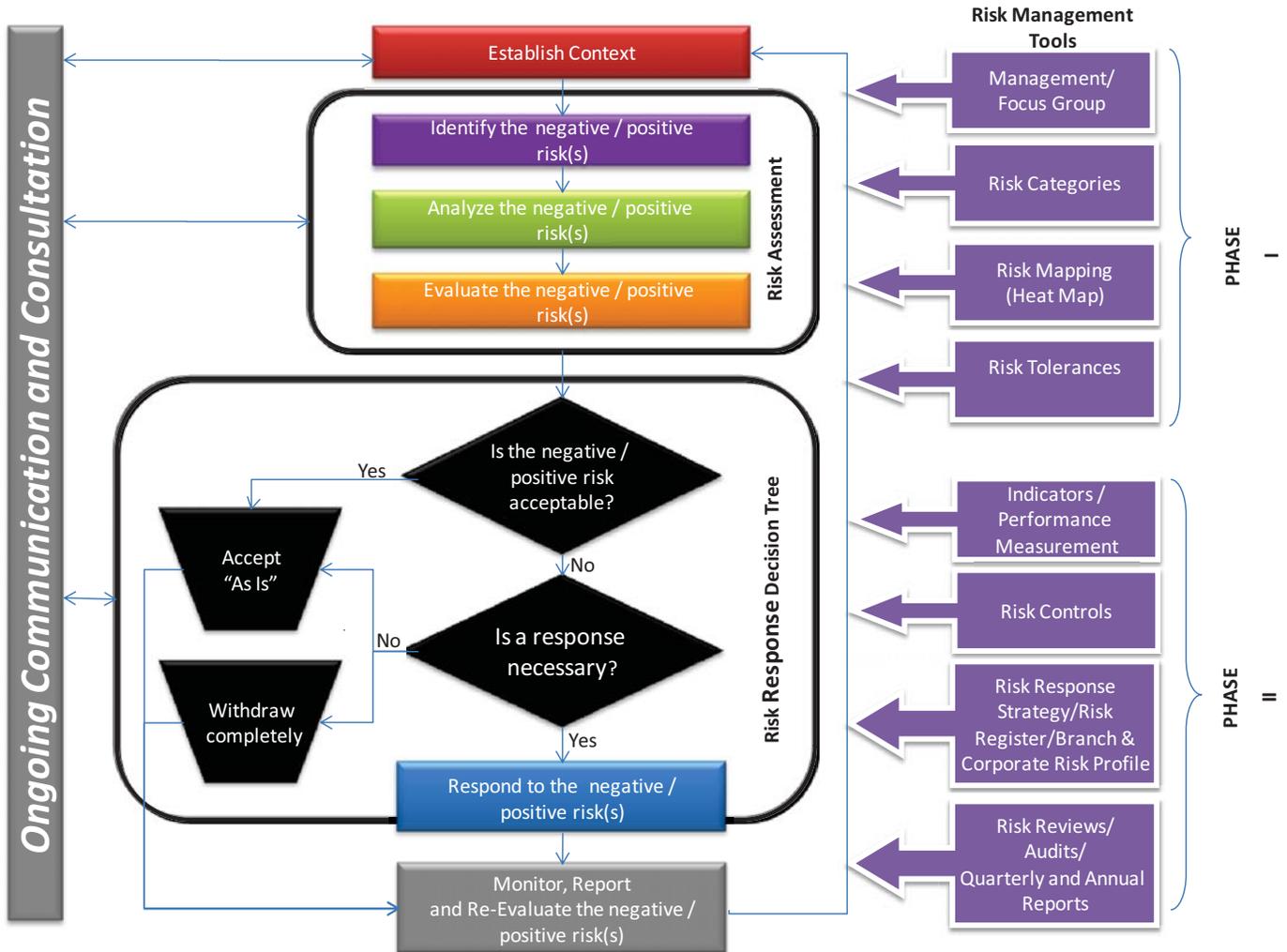
The frequency for monitoring and review may be influenced by the likelihood and impact assessments of risks, the business planning cycle, a meeting of a specific committee to monitor and review risks and/or as determined by a group. Whenever possible, existing frameworks and committees should be used for monitoring and review activities. To ensure a risk profile or risk response plan is being monitored and reviewed as planned, roles and responsibilities should be assigned to stakeholders. Once the monitoring and review activities are complete, it is essential to communicate results to stakeholders within PWGSC who are accountable for the risks through the delegation of authority chain.

Tools for developing a risk monitoring and review plan are available in [Appendix A2 – Risk Management Process Guidance](#)

## 5.0 Summary: Risk Process and Tools

The risk management process is rich with tools that assist in the development of a risk profile or risk register. Employing the right tools to the appropriate phase can lead to an effective risk management process. Figure 6 brings together the risk management process and the associated tools. The tools are aligned with the process in two distinct phases. Note: The risk tools and the risk management process depicted below can be utilized to manage both negative risks (threats) and positive risks (opportunities).

**Figure 6: Risk Management Process and Tools**





# APPENDICES

## Appendix A: Risk Management Tools

### Appendix A1: Positive (Opportunity) and Negative (Threat) Risk Example Scenarios

#### Scenario 1

**Risk:** Refitting an office in 90 days with an advanced refit technology.

**Positive Risk (Opportunity):** There is an opportunity that utilizing a new technology could enable the delivery of the project in 60 days instead of 90. There could be cost savings with less person hours being needed to refit the office space. The refit could lead to greater productivity if less time was needed to work in temporary office space.

**Negative Risk (Threat):** There is a risk that utilizing the new technology may impede your ability to deliver the project on time, due to an expertise and learning curve.

#### Scenario 2

**Risk:** Procurement of an advanced type of photocopier

**Positive Risk (Opportunity):** There is an opportunity that procuring the specific photocopier may attract positive media attention to highlight the fair and transparent procurement process employed by the Department. The procurement could lead to greater productivity, be easier to use, be more energy efficient, less maintenance needed, have fewer breakdowns, and have a lower cost per page.

**Negative Risk (Threat):** There is a risk that procuring this specific photocopier may attract negative media attention or a Canadian International Trade Tribunal or other complaint, due to potential allegations of unfair competition by Photocopier Company A against the incumbent Photocopier Company B who has won the contract.

#### Scenario 3

**Risk:** Strategic Review

**Positive Risk (Opportunity):** There is an opportunity that the implementation of the Strategic Review may streamline the Department's services and therefore enhance its ability to deliver quality services. Employees may be able to find their ideal type of jobs as they move to different positions within the Department. Resistance to change may lessen as employees are involved in initiating new work processes.

**Negative Risk (Threat):** There is a risk that the implementation of the Strategic Review may adversely affect the Department's ability to deliver on the quality of its services.

## Appendix A2: Risk Management Process Guidance

### Establish Context

#### Suggested sources for Environmental Scanning:

- in-house announcements of new policies and procedures;
- internal communications devices like the weekly Communiqué and items posted on the Source;
- interviews and conversations with subject matter experts;
- reports from newspaper articles, television, and the Internet;
- Regional Environmental Scan produced by Strategic Management in each region; and
- sources from Statistics Canada and World Trade Organization (WTO)

#### Key Questions to Consider in Environmental Scanning:

1. What trends in the internal or external environment could have an impact on a strategy/ initiative or objective?
2. What assumptions are you making in planning your strategy? Are they consistent with the internal and external environments?
3. Are there new policies on the horizon that could affect a program, initiative or process?
4. What keeps you awake at night?
5. Is the strategy/initiative dependent on other, already-existing strategies/initiatives?

### Risk Identification

#### Key Questions

##### *A. Departmental or Branch/Regional Level*

#### What are the department or Branches/Region's major priorities and expected results?

Each priority and expected result will have its own accompanying set of risks. At this level, it is important to keep the big picture and context in mind, and to consider whether the major priorities and expected results depend on initiatives within PWGSC or externally.

- How do PWGSC's priorities and expected results fit into the bigger picture / the government's priorities?
- Are these priorities and expected results dependent on other strategies or initiatives within the Branch/Regions or Department? If so, how?
- Which priorities and expected results are the most urgent or important?
- What are the potential advantages and disadvantages of the strategy/initiative?
- What activities are needed to accomplish priorities and expected results?
- Is the Department/Branch/Region the risk owner or is it an Agency risk?

#### How might the wider priorities and pressures of the Government of Canada affect a strategy/initiative?

- How might a new Parliament's priorities affect your strategies / initiatives?
- How might national and international pressures on a new government impact your ability to achieve expected results?

#### Can you identify risks that might threaten or enhance your ability to realize priorities and expected results based on the scenarios? (Concentrate on both worst-case and most likely scenarios)

- What is the most important project or initiative involved in delivering the priority and expected result?
- What adverse events have occurred recently that could have been avoided?

- What internal and external factors influence the achievement of the priority and expected result?

**Is the Department/Branch/Region capable of implementing the strategy/initiative? Does it have the capacity?**

- What are the main issues that may arise upon implementation?
- How will the current strategy/initiative accommodate internal and external changes in the future?
- What contingency/continuity plans exist or should exist to recover from failure/disaster?
- Do you have people to manage and implement the strategy/initiative?
- Do your people have the skills and abilities to manage the strategy/initiative?
- If the answer to the two previous questions is no, do you have a plan to either train employees or recruit others?

**Have you identified ethical risks / considerations that could arise as you move forward with the strategy / initiative?**

- Is there a risk that you or your team could enter into agreements with other organizations that have mandates, priorities or values that clash with those of the public service?
- Could the strategy / initiative give rise to situations that are inconsistent with the Values and Ethics Code for the Public Service or the PWGSC Statement of Values?

***B. Project Level***

Risks at the project level typically stem from the design of the project and the extent to which the project depends on manual or human elements. Controlling risks at the design stage of the project itself helps ensure that any remaining, residual risk will be small and acceptable. Therefore, the risk manager should be part of any design team.

**Key Questions**

1. Are the objectives of the project clearly defined?
2. Are there any unrealistic operational restraints (such as timeframes)?
3. Have all parameters (legal, proprietary, financial etc.) been fully addressed?
4. Are different versions of the same project being carried out in different locations/regions/offices?
5. Is the project dependent on other projects, or are other projects dependent on this process?
6. Where along the project have controls been placed? Are they directly aimed at risks?
7. At each decision point along the project, does the decision-maker have access to adequate information to make the decision with confidence? Could there be any internal or external pressures that would affect how a decision is made?
8. What effect could a new or changed project have on stakeholders?
9. Where in the project is there a chance that an unexpected event could occur to de-rail the process?
10. Does every employee involved in the project have a thorough understanding of how the project fits in with the Department's/Branches/Region's objectives?

**Table 4: Example of a Risk Management Taxonomy**

<b>Risk Category</b>	<b>Risk Sub-Categories</b>	<b>Examples</b>
<b>Strategic Risks</b>	<b>Reputation / Integrity Risk</b>	<ul style="list-style-type: none"> <li>▪ Impact of negative / positive media coverage</li> <li>▪ Delays in / accelerated processes and results</li> <li>▪ Loss of reputation/credibility / enhanced reputation/credibility</li> <li>▪ Existence of/lack of Fraud, illegal acts (employee, client, suppliers)</li> <li>▪ Ethical</li> <li>▪ Conflict of interest (e.g. employees handling public funds, contracts and the acquisition and disposal of assets)</li> </ul>
	<b>Culture Risk</b>	<ul style="list-style-type: none"> <li>▪ Failure / ability to set the tone for achieving objectives</li> <li>▪ Inability / ability to adapt to change in a timely manner</li> </ul>
	<b>External Risks</b>	<ul style="list-style-type: none"> <li>▪ Environment-related event difficult / easier to anticipate</li> <li>▪ Economic/social changes difficult / easier to anticipate</li> </ul>
	<b>Significant Horizontal Operational and Project Risks</b>	<ul style="list-style-type: none"> <li>▪ Knowledge management</li> <li>▪ Human resource turnover</li> <li>▪ Financial information strategy implications</li> </ul>
	<b>Financial Risks</b>	<ul style="list-style-type: none"> <li>▪ Settlements / court awards paid by PWGSC</li> <li>▪ Third party indemnification costs/savings</li> <li>▪ Economy</li> </ul>
<b>Operational Risks</b>	<b>Liability Risks</b>	<ul style="list-style-type: none"> <li>▪ Actions fail to consider requirements of laws (common law or jurisprudence) regulations and agreements</li> <li>▪ Health, safety and the environment not protected</li> </ul>
	<b>Process Risks</b>	<ul style="list-style-type: none"> <li>▪ Processes are inefficient/inefficient</li> <li>▪ Capacity and competencies available are insufficient/sufficient</li> <li>▪ Processing time too long/well delivered</li> </ul>
	<b>Human Resources Risks</b>	<ul style="list-style-type: none"> <li>▪ Loss/retention of corporate memory</li> <li>▪ Resource allocation not matched/matched to workload</li> </ul>
	<b>Information Processing / Technology Risks</b>	<ul style="list-style-type: none"> <li>▪ Infrastructure inadequate/adequate</li> <li>▪ Lack of timely, relevant, reliable information</li> </ul>
	<b>Financial Risks</b>	<ul style="list-style-type: none"> <li>▪ Day to day operations</li> </ul>
<b>Project Risks</b>	<b>Technical Risks</b>	<ul style="list-style-type: none"> <li>▪ Requirements change negatively/positively</li> <li>▪ Requirements are difficult / easier to meet</li> </ul>
	<b>Development / Implementation Risks</b>	<ul style="list-style-type: none"> <li>▪ Development / implementation process lacks/includes formality commensurate with the scope of project</li> </ul>
	<b>Management Risks</b>	<ul style="list-style-type: none"> <li>▪ Inadequate/adequate business case for project</li> <li>▪ Project decisions are not/ are based on risk management</li> </ul>
	<b>Financial Risks</b>	<ul style="list-style-type: none"> <li>▪ Cost overrun/</li> <li>▪ Too many/sufficient amendments to task authority</li> </ul>

## Risk Analysis

### Key Questions

#### *A. Likelihood (Probability)*

#### What criteria will you use to determine the likelihood of the risks you have identified?

- Is the risk internal or external?
- What is the history of occurrence? Has an event occurred recently?
- What are the predictions for occurrence in the future?
- If no additional action were taken, what would be the likelihood of the risk?

#### According to the responses to the questions, assess the likelihood of risk as:

- **High** (Almost certain); expected in almost all circumstances within a timeframe
- **Medium-High** (Likely); will probably occur
- **Medium** (Possible); could occur at some time
- **Medium-Low** (Unlikely); not expected to occur
- **Low** (Rare); exceptional circumstances only

#### *B. Impact*

#### What criteria will you use to determine the impact of the risks you have identified?

- What can go wrong? What could go right?
- What are the opportunities associated with the risk? What are the threats?
- Who will be affected? How will they be affected? How will they react (positive or negative)?
- Will the impact enhance the Department's/Branches/Region's ability to achieve its objectives?
- Will the impact threaten the Department's/Branches/Region's ability to achieve its objectives?

#### What controls are in place to prevent or minimize the risks?

- Are there too many controls for low risks?
- Are we maximizing on risks that could benefit the organization?
- Are there too few, or no, controls for high risks?
- Are we capitalizing on an opportunity (positive risk) to the maximum?

## Negative (Threat) Risk Heat Map

A negative (threat) risk heat map or matrix is the tool for assessing the likelihood and impact of a negative risk. Below is a 5x5 negative risk heat map for negative risks.

Table 5: Negative (Threat) Risk Analysis Heat Map

Likelihood	Impacts				
	Low	Medium-Low	Medium	Medium-High	High
High (Almost certain)	Yellow	Orange	Orange	Red	Red
Medium-High (Likely)	Yellow	Yellow	Orange	Orange	Red
Medium (Possible)	Light Green	Yellow	Yellow	Orange	Red
Medium-Low (Unlikely)	Light Green	Light Green	Yellow	Yellow	Yellow
Low (Rare)	Light Green	Light Green	Light Green	Yellow	Yellow

Source: CAN/ CSA Q31001-11 Risk Management: Implementation to CSA-ISO-31000

### Impact

5	<b>High (Severe):</b> would stop or accelerate achievement of functional goals/objectives
4	<b>Medium-High (Major):</b> would threaten or enable functional goals/objectives
3	<b>Medium (moderate):</b> necessitate significant adjustment to overall function
2	<b>Medium-Low (minor):</b> would inhibit or enable an element of the function
1	<b>Low (Negligible):</b> low consequence

### Likelihood

5	<b>High (almost certain):</b> expected in almost all circumstances
4	<b>Medium-High (Likely):</b> will probably occur
3	<b>Medium (Possible):</b> could occur at some time
2	<b>Medium-Low (Unlikely):</b> not expected to occur
1	<b>Low (Rare):</b> exceptional circumstances only

### Positive (Opportunity) Risk Heat Map

A positive (opportunity) risk heat map or matrix is the tool for assessing the likelihood and impact of a positive risk. Below is a 5x5 positive risk heat map.

**Table 6: Positive (Opportunity) Risk Analysis Heat Map**

Likelihood	Impact				
	Low	Medium-Low	Medium	Medium-High	High
High (Almost Certain)					
Medium-High (Likely)					
Medium (Possible)					
Medium-Low (Unlikely)					
Low (Rare)					

#### Impact

5	<b>High:</b> an opportunity with a high positive impact on the organization. Would accelerate achievement of objectives.
4	<b>Medium-High:</b> an opportunity that has a medium-high positive impact on the organization. Would enable functional goals / objectives.
3	<b>Medium:</b> an opportunity that has a medium positive impact on the organization. Would necessitate significant adjustment to overall organization.
2	<b>Medium-Low:</b> an opportunity that has a medium-low positive impact on the organization. Would enable the element of the function.
1	<b>Low:</b> an opportunity for the organization that has low impact on the organization.

#### Likelihood

5	<b>High (almost certain):</b> expected in almost all circumstances
4	<b>Medium-High (Likely):</b> will probably occur
3	<b>Medium (Possible):</b> could occur at some time
2	<b>Medium-Low (Unlikely):</b> not expected to occur
1	<b>Low (Rare):</b> exceptional circumstances only

## **Risk Response**

### **Selection of Risk Response Options**

An appropriate risk response involves balancing costs and efforts of implementation against benefits derived

- You must keep in mind legal, regulatory, social responsibility, protection of environment etc. when developing a risk response
- Identify the inherent risk (i.e. the risk that exists before any risk responses have been applied to respond to the risk) before developing risk response options. Knowing the inherent risk will help ensure that the risk response options are in line with the level of risk
- Response options may be applied individually or in combination – a combination option is normally of benefit to the organization
- Keep in mind stakeholders – some response options will be more acceptable than others to stakeholders, even if both are equally as effective
- Consider whether the response plans will impact other places within the organization / stakeholders
- Ensure on-going monitoring occurs while response happens. Ongoing monitoring allows for identification of risks throughout response process.
- Residual risks that need to be assessed, responded to, monitored and reviewed can be introduced through risk response.
- Residual risks must be incorporated into the same response plan. Link between risks (primary and secondary) should be identified and maintained.

### **Implementation of Risk Response Options**

- Purpose of Risk Response Plan: document how the chosen risk response options will be implemented.
- Information provided in plan should include:
  - Reasons for selection of response options, including expected benefits to be gained
  - Identification of those accountable for approving / implementing plan
  - Proposed action
  - Resource requirements, including contingencies
  - Performance measures and constraints
  - Reporting/monitoring requirements
  - Timing/schedule
- Be aware of the nature and extent of residual risk(s) that arise after risk response
- Residual risk(s) should be documented and subjected to monitoring, review and further response (if needed)

### **Key Questions**

#### **What is the risk tolerance?**

- Where can I find information on risk tolerance within the Department/ Branch/Region? (Sources include business plan, Directors, Director Generals, etc.)
- Does the risk lie within the risk tolerance or does it exceed it? What effect will the response have on likelihood and impact?

#### **What are the current responses in place to deal with the risk?**

- Are existing responses adequate?
- What can be done to improve the response?
- Are there any current initiatives which could be utilized to respond to the risk?

- What have other Branches/Region's done when faced with this same/similar risk?

**What threats or opportunities does the response create?**

- What are the consequences / benefits of implementing the response?
- How does it affect (positively/negatively) the risk?
- How does it affect (positively/negatively) stakeholders?

**What will the residual risk be after the response is implemented?**

- Is the residual risk within the Department's / Branches/Region's risk tolerance?
- Do you need to respond to the residual risk? If so, how and what is the cost?
- Do you need to find a different response (if the residual risk is too high)?

The negative (threat) risk heat map and positive (opportunity) risk heat map below indicate where resources should be focused and what level of management should be involved with respect to a low, medium-low, medium, medium-high and high negative (threat) and positive (opportunity) risk. The negative (threat) risk analysis heat map identifies four levels of oversight to ensure that the resources and oversight in place are commensurate with the level of negative risk. The positive (opportunity) risk analysis heat map identifies two levels of management to encourage flexibility in achieving the opportunity. The extent of management influence depends on the level of opportunity.

The area above the curve on the control framework shows the areas of oversight by management for high negative threat (risks). The area above the curve on the flexibility framework shows the area of influence by management for high positive (opportunity) risks.

Table 7: Management Areas of Oversight / Influence

Control Framework					Flexibility Framework					
Negative Impact					Positive Impact					
Low	Medium-Low	Medium	Medium-High	High	Likelihood (Negative and Positive)	High	Medium-High	Medium	Medium-Low	Low
Assign oversight/management responsibilities	Need senior management attention	Need senior management attention	Detailed management planning and attention is required	To be managed by senior management with a detailed management plan	High	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Regular monitoring/review by staff of opportunity as required
Assign oversight/management responsibilities	Assign oversight/management responsibilities	Need senior management attention	Need senior management attention	To be managed by senior management with a detailed management plan	Medium-High	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required
Manage by routine procedures	Assign oversight/management responsibilities	Assign oversight/management responsibilities	Need senior management attention	To be managed by senior management with a detailed management plan	Medium	Develop/implement plan, consult with stakeholders and senior management as required	Develop/implement plan, consult with stakeholders and senior management as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required
Manage by routine procedures	Manage by routine procedures	Assign oversight/management responsibilities	Assign oversight/management responsibilities	Assign oversight/management responsibilities	Medium-Low	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required
Manage by routine procedures	Manage by routine procedures	Manage by routine procedures	Assign oversight/management responsibilities	Assign oversight/management responsibilities	Low	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Regular monitoring/review by staff of opportunity as required	Monitoring/review by staff of opportunity as required

## Communication and Consultation

**Table 8: Influential Elements of a Risk Communication Plan**

Internal Elements	External Elements
PWGSC's mission, statement of values, and organizational culture	Past practices
Business strategies and planning priorities	Social and cultural changes flowing from the organizations behavior
Processes and operational functions	The credibility the organization has established with stakeholders in previous communications

Choosing the right communication channel is crucial to the success of the consultation and communication process with stakeholders to prevent stakeholder disengagement. It is important that the channel should fit with the language, culture, rights and expectations of the stakeholders, and should take into account their technological preference.

## Monitor and Review

### Key Questions

#### **Can risks be monitored on an ongoing basis or do they require separate evaluation?**

- Can this response be monitored as part of the process?
- What is the consequence of not identifying a deficiency immediately?
- What is the most cost-effective way to monitor response?

#### **How often should monitoring be done?**

Monitoring is costly in terms of financial and human resources. It is important not to err on the side of too much monitoring or too little.

- What are the consequences of identifying any deficiency?
- What are the costs/benefits of a particular frequency of monitoring?

#### **What should be done to address concerns identified through monitoring?**

Just as all risks are not equal, neither are deficiencies in responses. Once you have identified concerns regarding responses (for example, you have found a control that is not working as planned), it is important to consider the source, the nature, the problem and the consequences of the problem, and then develop a plan to correct the deficiency.

#### **What information should be reviewed and how often?**

Any information that aids in understanding the source, the nature, *and* the consequences of the deficiency should be reported so that action can be taken. To determine what information to report and how often, you should ask:

- What type of risk is being monitored?
- By how much does it deviate from the stated risk tolerance?
- What new responses should be used?
- How often must information be shared for management to respond to any new concerns?
- Has similar information been reported previously? Did the recipient consider the reports to be timely?
- How long will it take for the impact of the risk to be felt?

- 
- Review indicators, such as losses, complaints, etc.

## Appendix A3: Risk Register

Risk / Opportunity Statement	Consequences	Inherent Risk / Opportunity Score	Existing Risk / Opportunity Response	Planned Risk / Opportunity Response	Residual Risk / Opportunity Score
<i>Identify the risk and its triggers (causes)</i>	<i>Refers to the resulting impacts should the risk occur</i>	<i>The risk that exists before any risk responses have been applied to respond to the risk.</i>	<i>Refers to the risk measures or controls that have been developed and implemented to address an identified risk / opportunity.</i>	<i>Refers to the risk measures or controls that will be developed and implemented to address an identified risk / opportunity</i>	<i>The risk that exists after risk responses have been applied to respond to the risk.</i>
<p><b>EXAMPLE RISK:</b> High Level Operational and Management Priorities</p> <p>There is a risk that the organization may not meet its operational and management priorities for high level initiatives on time.</p>	<p>Organization would not meet client requirements</p> <p>Loss of reputation and credibility</p> <p>Organization would fail to realize the benefits that initiatives promise</p>	Medium-high	Engage senior management in regular meetings to oversee implementation	Ensure clear, risk-based decision making with identification of responsibilities, expectations and commitments	Low-medium
<p><b>EXAMPLE OPPORTUNITY:</b> High Level Operational and Management Priorities</p> <p>There is an opportunity that the organization could exceed its operational and management priorities.</p>	<p>Organization would exceed client requirements</p> <p>Enhanced reputation and credibility</p> <p>Organization would realize the benefits that initiatives promise</p>	Medium-high	Engage senior management in regular meetings to oversee implementation	Ensure clear, risk-based decision making with identification of responsibilities, expectations and commitments	High

## Appendix A4: Risk Information Sheet

Risk Management Process Step	How to Apply the Process Using The Risk Information Sheet	Risk Management Tools
<b>Phase I</b>		
<b>Identify the Risk</b>	<i>Establishing the Context</i>	Describe the decision to be made, the objectives it supports, time constraints for the decision, dependencies on other strategies or initiatives and key internal and external stakeholders
	Risk Name	Short title that provides a unique easy reference to the risk Example*: Human Resources
	Risk Statement	Description of the risk, including its drivers <b>Negative Risk (threat):</b> There is a risk that the organization may have a staffing shortage due to retirement and increased competition in the labour market. <b>Positive Risk (opportunity):</b> There is an opportunity that the organization may have the right staff in the right place at the right time in areas where there is a shortage in the Canadian labour market.
	Consequence Details	Refers to the resulting impacts should the risk occur: <b>Negative:</b> a) Inability to staff key functional areas. b) Excessive workload on remaining employees. <b>Positive:</b> c) The organization could become an employer of choice
<b>Risk Analysis</b>	Risk Controls (people, processes and systems already in place)	Refers to people, processes and systems currently in place to manage the risk. Where possible, the controls should be identified as a milestone, strategy or commitment to enable integration with the planned actions. Example*: To reduce the likelihood of staffing shortages, the organization has begun an aggressive recruiting campaign at various Canadian colleges and universities.
	Likelihood	Given the people, processes and systems in place, an estimate of the likelihood that the risk will occur. Values: High, Medium-High, Medium, Medium-Low, Low
	Impact	Given the people, processes and systems in place, an estimate of the potential impact to PWGSC objectives of the risk. Values: High, Medium-High, Medium, Medium-Low, Low
	Risk Level	A color rating based on the combined total value of risk impact multiplied by likelihood
<b>Evaluate the Risk</b>	Risk Decision	Based on the results of the analysis, determine whether or not a) The risk is acceptable. If yes, additional action may not be appropriate. If no, proceed to b) below and respond to the risk. b) Anything can be done to respond to the risk <i>Note: Consistent with PWGSC delegation of authority and executive accountability for risk tolerance and appetite, it is at the discretion of senior management to decide whether there is a need for a risk mitigation action plan.</i>
<b>Phase II</b>		
<b>Risk Response</b>	Risk Response & Implementation Date	Develop any additional risk response and include the date that the risk response strategy will be implemented
	Risk Owner (OPI)	The name of the resource that is responsible/accountable for the Risk
	Performance link	Should identify which of the existing performance indicators would most help your area to determine if progress was being made in managing this risk
<b>Communication</b>		Important: Consider the existing communication approach and requirements for your business area together with the risk information above: Who else needs to know about this risk? How will our internal and external stakeholders be consulted or informed?
<b>Monitoring and Review</b>		Monitor the most significant risks regularly in the same way and timing that organizational performance is also measured. See more at 'Monitoring and Review'.

\*Note: examples are fictitious

## **Appendix B: Glossary of Key Risk Management Terms**

**Ethical risks** (*risque éthique*) are events or situations that could affect the integrity, reputation, decision-making or stewardship of the department

**Impact** (*impact*) is an outcome of an event affecting objectives.

**Inherent Risk** is the risk that exists before any risk responses have been applied to respond to the risk

**Integrated risk management** (*gestion intégrée du risque*) is a systematic and continuous approach to understand, communicate and manage risk from an organization-wide perspective. It involves making strategic decisions that minimize negative consequences and maximize opportunities that contribute to the achievement of an organization's corporate objectives.

**Performance indicator** (*indicateur de performance*) is used to measure an organization's performance. These measures are usually established at the beginning of a process, cycle or project and are tracked at regular intervals to evaluate how successful an organization is in achieving results and/or the progress an organization has made in relation to its long-term goals.

**Issue** (*enjeu*) is a final outcome, certain event and/or an ongoing concern that must be proactively managed.

**Likelihood** (*probabilité*) refers to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and is described using either general terms or mathematically.

**Residual Risk** (*risque résiduel*) is the remaining risk after a risk response has been applied. It may contain unidentified risks.

**Risk** (*risque*) refers to the effect of uncertainty on objectives. It is the expression of the likelihood and impact of an event with the potential to influence positively or negatively an organization's achievement of objectives.

**Risk acceptance** (*acceptation des risques*) is an informed decision to accept a risk. Risk acceptance can occur without a risk response or during the risk response process and is subject to monitoring and review. Note: not addressing or identifying a risk is the default of acceptance.

**Risk appetite** (*appétit du risque*) refers to how much and the type of risk an organization is willing to pursue or take on to ensure it has ample opportunity to achieve its objectives.

**Risk assessment** (*évaluation des risques*) refers to assessing key risks, measuring their likelihood and impact, ranking the key risks, and implementing an appropriate response to them by considering the costs and benefits of measures for managing the risk and the needs, issues and concerns of stakeholders.

**Risk communication** (*divulgateion des risques*) is the transfer or exchange of information among stakeholders about the existence, nature, form, severity, or acceptability of risks. It also includes reporting and review.

**Risk management** (*gestion des risques*) is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, analyzing, evaluating, controlling, and communicating risks. Risk management involves the review and evaluation of strategies, policies and practices.

**Risk management plan** (*plan de gestion des risques*) is the document that specifies the approach, the management components and resources to be applied to the management of a risk.

**Risk mitigation** (*mitigation de risque*) is a risk response taken to reduce an undesired consequence.

**Risk of ethical reputation (risque d'atteinte à la réputation éthique)** refers to the potential outcomes and impacts related to making a decision without appropriate consideration of values and ethics. The impact of the risk when making an unethical decision is loss of public confidence and credibility; negative media coverage, loss of financial resources; delays in processes/results (e.g. if Treasury Board holds up approval of programs or projects); low employee morale and reduced productivity; and, in an extreme situation putting the future of PWGSC at risk.

**Risk perception (perception des risques)** is the value or concern with which stakeholders view a particular risk, irrespective of the expected or likely loss associated with the risk. Risk perception plays an important role in establishing risk tolerances and formulating/adopting risk management strategies.

**Risk profile** (*profil des risques*) is a description of a set of risks.

**Risk response** (*réponse au risque*) refers to the risk measures or controls that are developed and implemented to address an identified risk. It can include avoiding the risk, seeking an opportunity, removing the risk, changing the likelihood of a risk, changing the consequences associated with a risk, sharing the risk with another party, and or retaining the risk.

**Risk-smart culture** (*une culture sensibilisée au risque*) refers to building risk into existing governance and organizational structures, including business planning and decision-making and operational processes. It also ensures that the workplace has the tools to be innovative while protecting the public interest and maintaining public trust.

**Risk tolerance** (*tolérance à l'égard des risques*) is PWGSC's readiness to bear the residual risk after risk response has been applied.

**Uncertainty** (*incertitude*) is the state of having limited knowledge or understanding of an event and/or future outcome and its impact or likelihood.

**Values and Ethics Code for the Public Service** (*Code de valeurs et d'éthique de la fonction publique*) is the body of values and ethics to guide and support public servants in all their professional activities. It also serves to maintain and enhance public confidence in the integrity of the Public Service.

## Appendix C: Risk Management References and Links

### Risk Management References

#### **Treasury Board Publications:**

- [Framework for the Management of Risk](#);
- [Guide to Integrated Risk Management](#);
- [Management Accountability Framework](#);
- [Results for Canadians: A Management Framework for the Government of Canada](#);
- [Values and Ethics Code for the Public Service](#).

#### **PWGSC Publications:**

- [PWGSC Risk Management Guide](#);
- [Statement of Values](#).

#### **Other Publications:**

- CSA Q850 2010;
- Guide 73 Risk Management Terminology ISO;
- ISO 31000 2009.

### Risk Management Contact Information

#### **Operational Integrity Sector:**

- <http://source.tpsgc-pwgsc.gc.ca/dgs-dob/bapgr-ocro/gr-rm-eng.html>
  - *Please use the "Contact Us" link (under Benefits) for any risk management inquiries*
- Director, Quality and Risk Management: 819-956-5048