



Public Safety
Canada

Sécurité publique
Canada

BUILDING A **SAFE AND RESILIENT CANADA**



**All Hazards Risk Assessment
Methodology Guidelines**
2012–2013

Preface

This document has been developed by Public Safety Canada, in close partnership with Defence Research and Development Canada - Centre for Security Science, as part of the federal All Hazards Risk Assessment initiative endorsed by the Assistant Deputy Minister Emergency Management Committee in October 2009. The All Hazards Risk Assessment methodology and process, which are presented in these guidelines, have been developed in consultation with federal government institutions; Public Safety Canada would like to thank federal experts for their significant contribution to strengthening the principles, assumptions and application of the All Hazards Risk Assessment methodology. As well, other risk assessment stakeholders amongst key international government partners in the areas of risk assessment and emergency management in the United States, the United Kingdom and the Netherlands have provided valuable perspectives that have been incorporated into the methodology.

The All Hazards Risk Assessment methodology and process are the result of a pilot phase of the All Hazards Risk Assessment initiative, which concluded in October 2011. The information contained in this document is expected to evolve as the All Hazards Risk Assessment process is implemented on a cyclical basis every year and as best practices on risk assessment are established through international exchange and cooperation through organizations such as the Organisation for Economic Cooperation and Development, the World Economic Forum, the International Council on Risk Governance, the Canadian Standards Association, and the International Organization for Standardization.

The principal audience for the methodology guidelines is federal government institutions in Canada. The *All Hazards Risk Assessment Methodology Guidelines, 2012-2013* can be read on their own for those interested in conducting risk assessments. For readers interested in integrating risk assessment into emergency management planning, the methodology should be read in conjunction with Public Safety Canada's *Emergency Management Planning Guide, 2010-2011*, available at: http://www.publicsafety.gc.ca/prg/em/emp/_fl/emp-gd-2010-11-e.pdf.

Questions related to the All Hazards Risk Assessment and the current guidelines may be addressed to Public Safety Canada, Emergency Management Planning Division, at AHRA-ETR@ps-sp.gc.ca.

Amendments Record

The following is a list of amendments to the Federal All Hazards Risk Assessment Methodology Guidelines:

#	Date	Amended by	Comments
1.0	2011-12-01	Emergency Management Planning, Public Safety Canada	Initial version
2.0	2013-02-08	Emergency Management Planning, Public Safety Canada	Revised version to reflect 2012-2013

List of Acronyms and Abbreviations

AHRA	All Hazards Risk Assessment
BSE	Bovine Spongiform Encephalopathy
C3I	Communications, Command, Control and Intelligence
CDD	Canadian Disaster Database
CI	Critical Infrastructure
CSS	Centre for Security Science
DALY	Disability-Adjusted Life Year
DPR	Departmental Performance Report
DRDC	Defence Research and Development Canada
EM	Emergency Management
EMA	Emergency Management Act
ESF	Emergency Support Function
FERP	Federal Emergency Response Plan
FMD	Foot and Mouth Disease
FPEM	Federal Policy for Emergency Management
GC	Government of Canada
GTA	Greater Toronto Area
IRAWG	Interdepartmental Risk Assessment Working Group
ISO	International Organization for Standardization
NATO	North Atlantic Treaty Organization
NS	National Security
PESTLE	Political, Economic, Social, Technological/Technical, Legal and Environmental
PS	Public Safety Canada
RPP	Report on Plans and Priorities
SARS	Severe Acute Respiratory Syndrome
SME	Subject Matter Expert
StatCan	Statistics Canada
SWOT	Strengths, Weaknesses, Opportunities and Threats

Table of Contents

INTRODUCTION AND PURPOSE	1
BACKGROUND – AHRA IN EMERGENCY MANAGEMENT PLANNING	3
OVERVIEW OF THE AHRA PROCESS	4
FEDERAL AHRA BUSINESS CYCLE	7
STEP 1: SETTING THE CONTEXT	9
■ Objective of Setting the Context	9
■ Inputs Required	9
■ Tasks and Activities Expected in Setting the Context	11
Short-Term Threat/Hazards Analysis	11
Emerging and Future Risk Analysis	11
■ Outputs for Setting the Context	11
STEP 2: RISK IDENTIFICATION	12
■ Objective of Risk Identification	12
■ Inputs Required	12
■ Tasks and Activities Expected in Risk Identification	13
Initial Risk Identification	13
Risk Event Scenario Development	13
Use of Composite Risk Event Scenarios	16
■ Outputs for Risk Identification	19
STEP 3: RISK ANALYSIS	20
■ Objectives of Risk Analysis	20
■ Inputs Required	20
■ Tasks and Activities Expected in Risk Analysis	21
Likelihood Analysis	21
Impact/Consequence Analysis	22
Impact Categories	23
Approach for Impact Rating	23
AHRA Scoring Tool	24

Confidence Level and Justification for Likelihood Analysis and Impact/Consequence Analysis	24
■ Outputs for Risk Analysis	25
■ Impact Assessment Categories	25
People	26
Economy	27
Direct Economic Loss	28
Indirect Economic Loss	28
Environment	30
Magnitude of Response Required to Deal with an Event.....	31
Environmentally affected area	33
Magnitude of Damage Based on Environmental Adverse Effects	35
Modifier for Duration of Damage	36
Territorial Security	39
Modifiers for Duration of Disruption and Population Density.....	40
Canada’s Reputation and Influence	41
Society and Psycho-Social.....	43
■ Likelihood Assessment.....	45
Malicious Threats	45
Likelihood Rating for Malicious Scenarios.....	45
Non-Malicious Hazards	51
STEP 4: RISK EVALUATION.....	53
■ Objective of Risk Evaluation.....	53
■ Inputs Required	53
■ Tasks and Activities Expected in Risk Evaluation.....	53
■ Outputs for Risk Evaluation	55
STEP 5: RISK TREATMENT	56
■ Objective of Risk Treatment	56
■ Input Required	56
■ Tasks and Activities Expected in Risk Treatment	57
Scope of Risk Treatment.....	57
Recommending Risk Treatment Avenues to Senior Management.....	57
■ Outputs for Risk Treatment	58
DATA MANAGEMENT	59

■ General.....	59
■ AHRA Risk Register and Database.....	59
■ Data Management and Sensitivity.....	60
ACCUMULATING KNOWLEDGE AND CONTINUOUS IMPROVEMENT OF AHRA	61
ANNEX 1 – AHRA BUSINESS CYCLE.....	62
ANNEX 2 – SWOT AND PESTLE ANALYSIS.....	63
ANNEX 3 – AHRA RISK TAXONOMY.....	65
ANNEX 4 – RISK EVENT SCENARIO DESCRIPTION TEMPLATE.....	66
ANNEX 5 – RATING OF THE IMPACT ON CANADA’S REPUTATION AND INFLUENCE.....	70
ANNEX 6 – ECONOMIC CATEGORY ASSESSMENT TOOL – DIRECT AND INDIRECT ECONOMIC LOSS FOR REPAIR OR REPLACEMENT.....	72
ANNEX 7 – GLOSSARY.....	74

Introduction and Purpose

In today's world, a range of natural and health hazards, as well as man-made threats, are increasing in their frequency, complexity and interconnectedness as a result of globalization and natural and political forces. Pandemics, SARS, earthquakes in Japan and Haiti, and terrorism are examples of events that can impact Canada and Canadians. At home, floods, hurricanes, cyber attacks and forms of ideological radicalization are all recent threats and hazards that the Government of Canada (GC), often in collaboration with the provinces and territories, has taken a role in managing.

Threats and hazards vary in their likelihood and impact; an effective approach to managing them requires that the GC identify their risk. Increasingly, domestic governments and international organizations recognize that understanding risks through identifying, assessing and monitoring them is a key step to build the foundation for effective emergency management (EM) planning and a country's resilience. The Government of Canada has operated on similar principles by implementing controls in the form of legislation, regulations, policies and guidelines to address risk and assign risk responsibilities. In Canada, the overarching legislative umbrella in emergency management is the 2007 *Emergency Management Act* (EMA), which establishes the federal role in emergency management, and the role and responsibilities of the Minister of Public Safety as well as those of all Ministers.

In support of sound EM principles, the EMA stipulates that Ministers are responsible for identifying risks that are within or related to their mandate and to prepare EM plans to respond to those risks. It identifies the Minister of Public Safety as being responsible for providing leadership and guidance to federal government institutions, including in the preparation, maintenance, and testing of emergency management plans. The Act is articulated by the *Federal Policy for Emergency Management* (FPEM) and associated tools, such as the *Emergency Management Planning Guide, 2010-2011* (Guide).

The development of the All Hazards Risk Assessment (AHRA) methodology, led by Public Safety Canada (PS), in close partnership with Defence Research Development Canada (DRDC) – Centre for Security Science (CSS), supports all federal government institutions in fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for EM planning. As risks often cross boundaries and mandates, an effective means to deal with them is through a horizontal approach. In Canada, the approach to EM is based on four components: prevention/mitigation, preparedness, response and recovery. When viewed from this perspective, the ownership of risks is more often than not shared across the mandates of Ministers, or even across jurisdictions. Therefore, a coordinated approach is required to manage risks effectively by assessing them using the same methodology and then treating them through a collaborative approach that recognizes the interdependencies amongst ministerial mandates.

The AHRA process is premised on the assumption that risks are co-owned and co-managed. The intention of the process is therefore to produce a whole-of-government risk picture to support EM planning across federal government institutions and to ensure that interdependencies are recorded and managed. The risk picture provides an enhanced planning baseline for federal government institutions to support the development of EM plans, as outlined in the Guide, and future capacity and investment decisions in areas where attention may be required. As well, the methodology can be used by federal institutions to perform their own risk assessment and ensure integration and alignment with the whole-of-government process. Finally, this initiative provides a venue for the creation of a federal AHRA community of practice, and a forum for sharing risk information, tools and methodologies.

Risk assessment specific to the critical infrastructure (CI) sectors is beyond the scope of the federal AHRA methodology and would be carried out under the *National Strategy and Action Plan for Critical Infrastructure*. Going forward, the possibility of aligning these risk assessment activities will be examined.

The purpose of the present guidelines document is to describe the AHRA methodology and its process, which is primarily meant to support the EM process at the federal level.

Background – AHRA in Emergency Management Planning

The AHRA initiative incorporates expertise from a wide range of federal government institutions and applies an all hazards approach. It is a comprehensive and integrated means for assessing the impact and likelihood of both malicious and non-malicious hazards and threats that Canada could face over a five year period. By assessing the risks associated with all hazards in an integrated way, efforts may be broadly effective in reducing the vulnerability of people, property, the environment and the economy.

More specifically, the AHRA's objectives are to:

- Enable federal government institutions to perform AHRA consistently and efficiently as part of their risk management responsibilities under the EMA and other relevant legislation and policies.
- Address the interconnected nature of Canada's risk environment and provide a means to produce a collective judgment of risk assessments currently being carried out by different federal government institutions into a whole-of-government picture to inform future actions and initiatives.
- Support the relative ordering of risk events based on their ratings at a federal level, while enhancing decision-making processes within the GC.
- Capture risks that are significant and are of federal interest.
- Raise awareness of risks that may not be of federal concern at this time, but are likely to be elevated in the future.
- Raise awareness of risks that are not of federal concern, but ensure that these risks are monitored.
- Capture changes in risks over time.
- Help to foster an AHRA community of practice for the federal community.

Overview of the AHRA Process

The purpose of the federal AHRA process is to assess and view risks in a standardized fashion using a common set of principles and steps. The assessment of risks of a federal interest will be done on an annual basis, starting officially in June every year with the identification of priority threats and hazards. An AHRA business cycle is available at Annex 1.

In the context of the federal AHRA, an all hazards approach does not mean that all hazards will be assessed annually, but rather that all hazards will be considered at the beginning of each new cycle. The annual assessment will focus on the most probable and consequential risks. It is neither possible nor necessary to assess all risks within a given year; rather, a thorough risk picture will be built over several cycles under the guidance of federal experts.

The federal AHRA process is based on a methodology that comprises the following steps, as identified in ISO 31000, “Risk Management – Principles and Guidelines”:

1. **Setting the Context** – The process of articulating an institution’s objectives and defining its external and internal parameters to be taken into consideration when managing risks.
2. **Risk Identification** – The process of finding, recognizing, and recording risks.
3. **Risk Analysis** – The process of understanding the nature and level of risk, in terms of its impacts and likelihood.
4. **Risk Evaluation** – The process of comparing the results of Risk Analysis with risk criteria to determine whether a risk and/or its magnitude is acceptable or tolerable.
5. **Risk Treatment** – The process of identifying and recommending risk control or Risk Treatment options.

The AHRA process employs a scenario-based risk assessment approach. From a high-level perspective, the AHRA focuses on the five steps indicated above and is linked back to the overall emergency management approach, as illustrated in Figure 1.

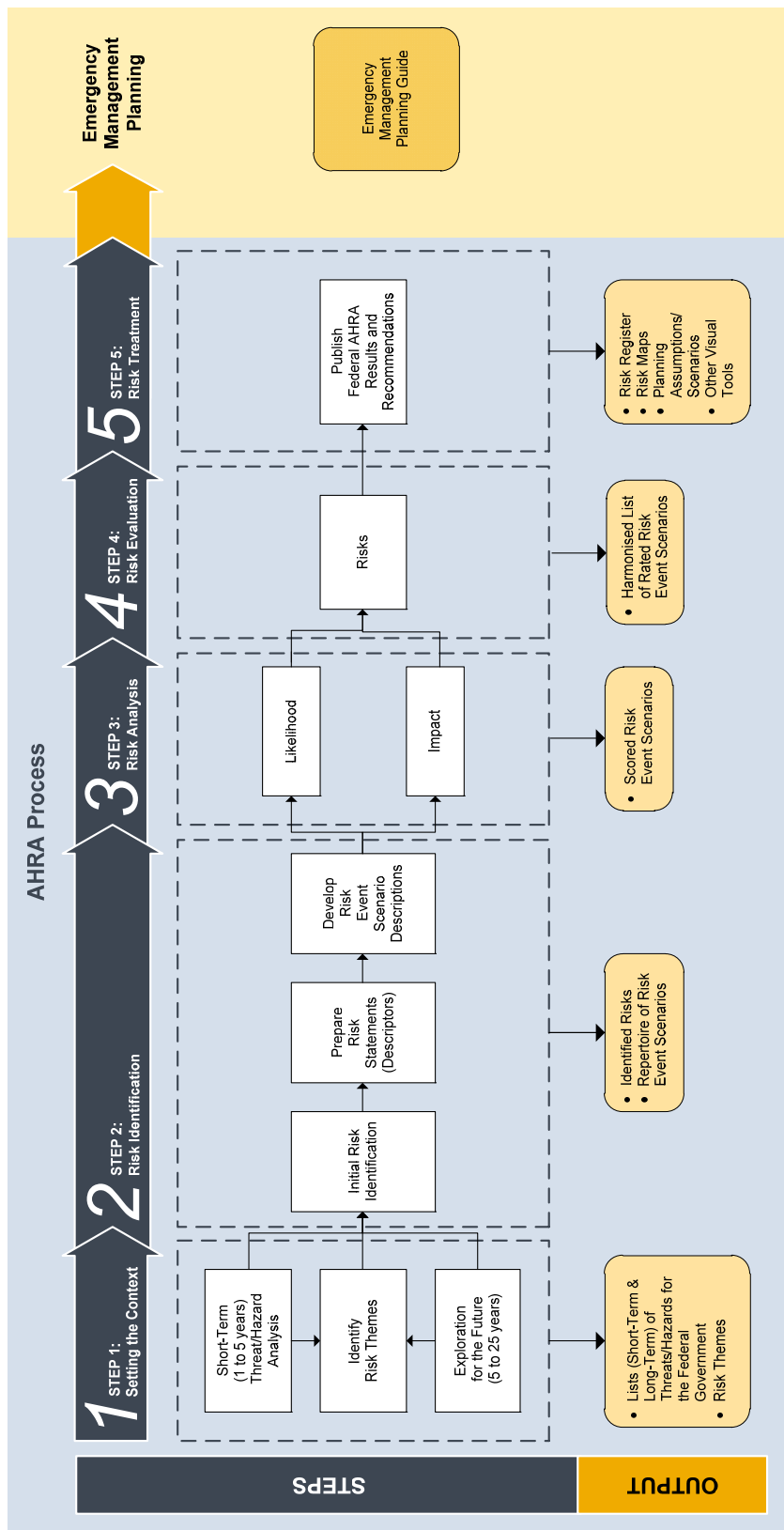


Figure 1 – AHRA Process and Linkage to EM Planning

The AHRA process is meant to create a multi-dimensional, high-level view of risks faced by Canadians, while bringing diverse risks from various sources into the same high-level view, as shown at Figure 2.

The outputs from the AHRA process should provide decision-makers with an improved understanding of the relevant risks – which is the combination of the likelihood and the consequence of a specified hazard or threat being realized – that could affect objectives as well as certain indicators of the effectiveness of Risk Treatment measures already in place, the potential effectiveness of additional Risk Treatment measures and an appreciation of the inherent uncertainties in all key aspects of the risk assessment process. Generally, risks translate into events or circumstances that, if they materialize, could negatively affect Canada and Canadians. The hazard risk domain is covered by the federal AHRA methodology. However, the operational risk domain (e.g., day-to-day issues confronting an institution) is not, although these aspects may be considered and factored in Setting the Context prior to identifying risks and assigning impact ratings during Risk Analysis.

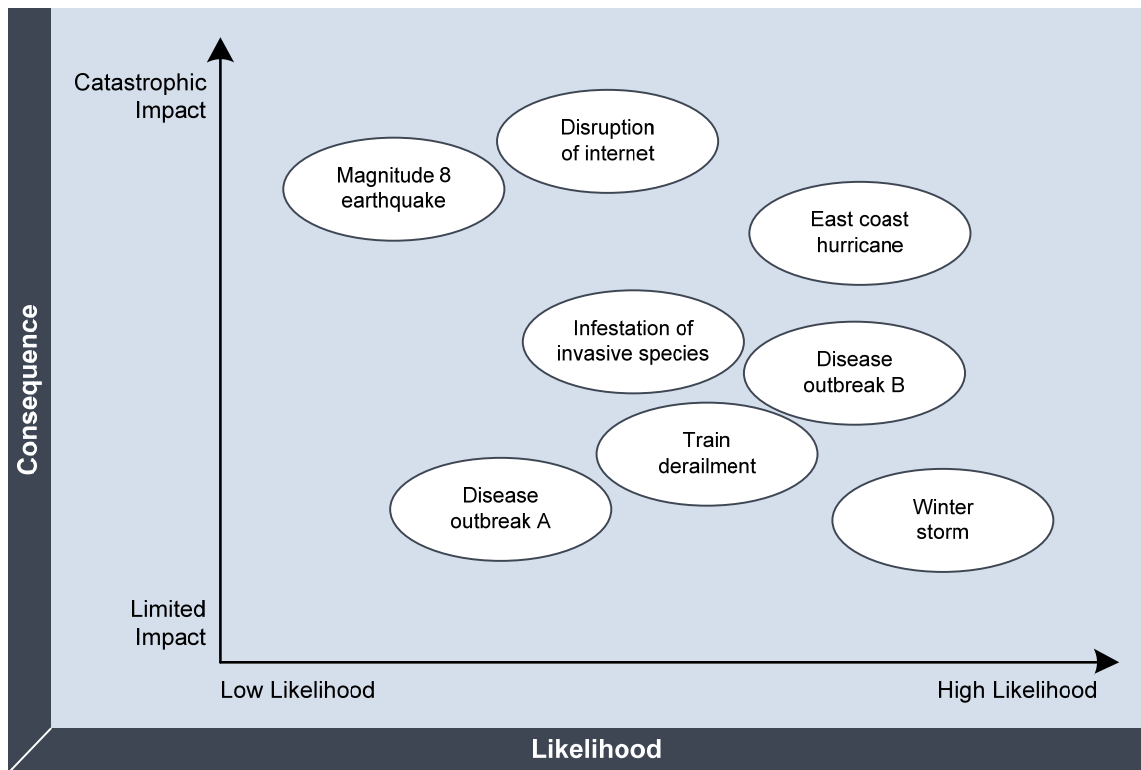


Figure 2. Example of Diverse Risk Event Scenarios Displayed on a Likelihood-Consequence Graph

Federal AHRA Business Cycle

In order to support federal institutions in aligning overall emergency management planning activities with departmental integrated corporate planning activities, PS has developed a specific business cycle for the AHRA. An overview of the cycle is provided in the following paragraphs.

As indicated in Figure 3 below, the cycle is initiated in the spring quarter, when PS evaluates risks that have been identified by federal institutions and prepares a report. These results will support federal institutions to identify threats and hazards, as well as strategic corporate directions that could become a priority in the context of a new fiscal year. Institutions should analyse these results to better understand their implications in terms of their organization's year-end review and emergency planning activities.

The summer quarter is used for assessing current business challenges, including the identification of priority threats and hazards (or risks) for federal institutions to be brought forward for the next federal AHRA cycle. This is the period during which AHRA results from the previous cycle will be reported out to senior management for decision (as necessary) and inform planning and priority setting exercises for the next AHRA and Emergency Management Planning cycles.

In the fall quarter, federal institutions launch departmental planning for the next fiscal year, including setting performance objectives, identifying resource needs and incorporating risk assessment results into revised EM plans. In September of each year, institutions should initiate the development of risk event scenarios for those risks that are retained as priorities by the federal community. Further guidance on risk event scenario development for the AHRA is available at the Risk Identification section.

During the winter quarter, experts from federal institutions are convened to conduct Risk Analysis based on the risk event scenarios developed during the fall quarter. This activity is the main objective of risk scoring workshops, which will be planned by PS. Initial results from the risk scoring workshops will support institutions in assessing their level of readiness against priority risks. PS will then plan the final AHRA step, in order to complete the process with Risk Evaluation during the spring and prepare final results in time for the next AHRA cycle.

In order to ensure a coordinated approach to the AHRA process, PS created an Interdepartmental Risk Assessment Working Group (IRAWG) representing federal institutions participating in the AHRA process. During the summer quarter, the IRAWG is responsible to choose, amongst the entire list of departmental priority threats and hazards, key risks that will be further assessed during each AHRA cycle. The working group is also responsible for providing PS with on-going and timely strategic safety and security advice related to the AHRA methodology and process.

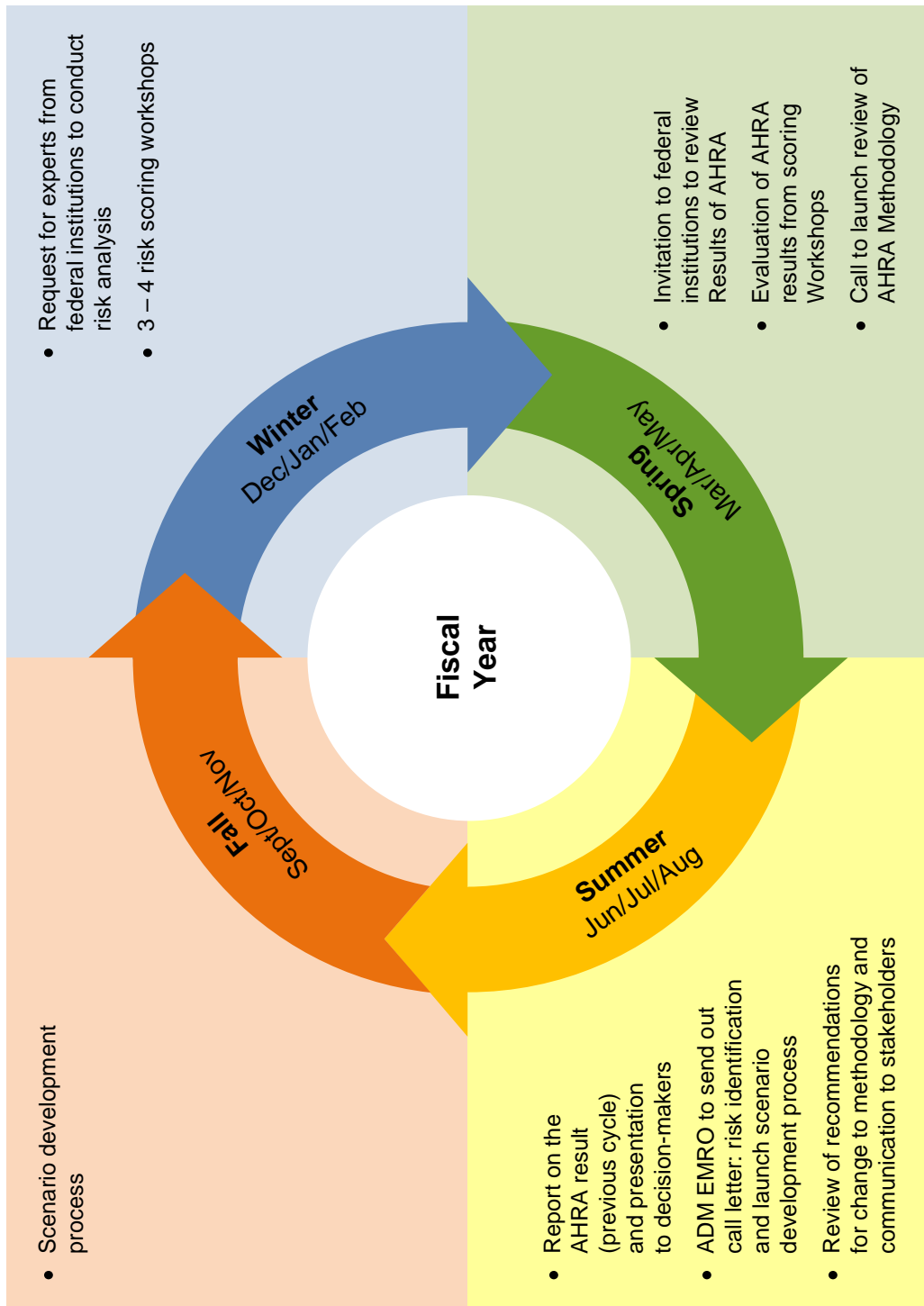


Figure 3. AHRA Business Cycle

1

Step 1: Setting the Context

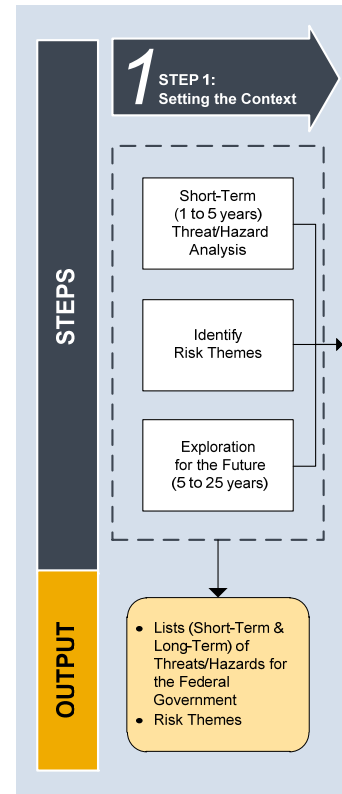
■ OBJECTIVE OF SETTING THE CONTEXT

The first step when initiating a formal AHRA is to develop a comprehensive understanding of the strategic and operating context of an organization. This is the main objective of Setting the Context. Each federal government institution is responsible to research, review and gather relevant data such as applicable legislation, reports on plans and priorities, departmental performance reports, etc. in order to enhance its understanding of its mandate, responsibilities, areas of interest and various information sources that would help inform the next AHRA process step: risk identification.

■ INPUTS REQUIRED

Many information sources may be reviewed when Setting the Context. The following are key data sources that may be considered during this process:

- **Departmental planning and reporting documentation.** Used to plan and report at the organizational level, departmental planning and reporting documents support every federal government institution's efforts to effectively plan and evaluate their performance, as well as the budgetary, appropriation and accountability responsibilities of parliament and the GC. Reports on Plans and Priorities (RPP) are annual expenditure plans that provide information on departmental strategic outcomes and program activities, plans and priorities, expected results, performance indicators and resource requirements on a three-year basis. Departmental Performance Reports (DPR) provide a strategic overview of every institution's performance and achievements in past fiscal years. They are primary instruments of transparency and accountability to Parliament and Canadians and are key documents in better evaluating an institution's risk environment.
- **Environmental scans.** An environmental scan involves being aware of the context in which an institution is operating so as to understand how it could be affected. It entails a process of gathering and analyzing information and typically considers both internal and external factors such as policies, capabilities and key societal drivers and trends (e.g. demography, economy, technology) at a local, national and international level. As part of the



environmental scan, the institution defines the internal and external parameters to be taken into account when managing risks and setting the scope and risk criteria for the remaining risk assessment process. There are several approaches to developing an institutional environmental scan. Samples of tools such as a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis and a PESTLE (Political, Economic, Social, Technological/Technical, Legal and Environmental) analysis are provided at Annex 2.

- **Historical Records.** Historical Records include any historical information relevant to the identification of risks within the domain of the federal government institution's mandate, responsibilities or interests. This will include past risk assessments and associated risk database or register information. The Canadian Disaster Database (CDD) contains detailed disaster information on over 900 natural, technological and conflicts events (excluding war) that have directly affected Canadians over the past century. This database helps citizens and governments to better assess and manage risks and also enhances the understanding of how risks have evolved over time: <http://www.publicsafety.gc.ca/prg/em/cdd/index-eng.aspx> In addition, statistical data such as census information (population density, profiles, etc) and special economic and infrastructure data and research literature published by Statistics Canada (<http://www.statcan.gc.ca>) or other research centres (e.g. National Research Council Canada – <http://www.nrc-cnrc.gc.ca/index.html>) may inform risks frequency of occurrence and consequences.
- **Intelligence Reports.** Intelligence reports are highly relevant to a range of risk types including rapidly time-varying or emerging phenomena and risks associated with malicious activities.
- **Other Information.** The Risk Assessment process should have access to any other information relevant to the identification of risks within the domain of the federal government institution's mandate, responsibilities or interests. For example, legislation applicable to a federal government institution may clearly indicate risks under the purview of an institution's mandate and may therefore be a reliable source for identifying potential risks of interest to an institution.

These information sources will support the identification of risk themes, defined as activities or phenomena of a particular interest to an institution with which significant risks might be associated. A list of themes may be developed, in order to focus the identification of particular risks of interest in preparation for the next AHRA process step. Finally, these sources will also help in understanding the level of tolerance of an institution towards certain risks.

Each federal government institution will determine what data and information inputs it requires according to its mandate, responsibilities or interests and information sources.

■ TASKS AND ACTIVITIES EXPECTED IN SETTING THE CONTEXT

Short-Term Threat/Hazards Analysis

Short-term threat/hazard analysis will identify, isolate and assess risk events that could logically and plausibly occur within the next five years and are under federal jurisdiction for at least one of the four components of emergency management (prevention and mitigation, preparedness, response, recovery). Even though some risk events retained may fall in part under provincial or municipal jurisdiction (e.g. floods, foodborne disease outbreak), their inclusion may be warranted because of authorities and responsibilities of the federal government for at least one of the four components of emergency management (e.g. Environment Canada provides scientific and technical advice and research regarding flooding, which are prevention and mitigation activities).

Emerging and Future Risk Analysis

Exploration for the future (or forecasting) will identify threats or hazards relevant to the period from 5 to 25 years into the future. Generally, the further into the future forecasts go, the more data deprived we are. To compensate for the lack of data, foresight practitioners and/or futurists resort to looking at trends, indicators etc. and use various techniques: Technology Mapping; Technology Road-Mapping; Expert Technical Panels, etc. These are alternate techniques that attempt to compensate for the uncertainty of the future and most often alternate futures will be explored. Federal risk experts can get emerging and future insights and trend indicators through community of practice networks such as the Policy Horizons Canada (<http://www.horizons.gc.ca>) environmental scanning practice group. Another source for emerging and future Risk Analysis is the PS-CSS produced Strategic Planning Guidance for the programs managed by CSS. Foresight activity and Risk Analysis play an integral role in this yearly process. For more information on Strategic Planning Guidance, federal institutions can contact PS Science, Technology and Interoperability Division, at S&T_Pol@ps-sp.gc.ca or CSS at css-info@drdc-rddc.gc.ca.

■ OUTPUTS FOR SETTING THE CONTEXT

The information outputs for Setting the Context are:

- Analysis of short-term (within the next 5 years) threats and hazards, accompanied with a certain level of comprehension regarding an institution's level of risk tolerance.
- Analysis of emerging and future (in 5 to 25 years) threats and hazards.
- Risk themes.

2

Step 2: Risk Identification

■ OBJECTIVE OF RISK IDENTIFICATION

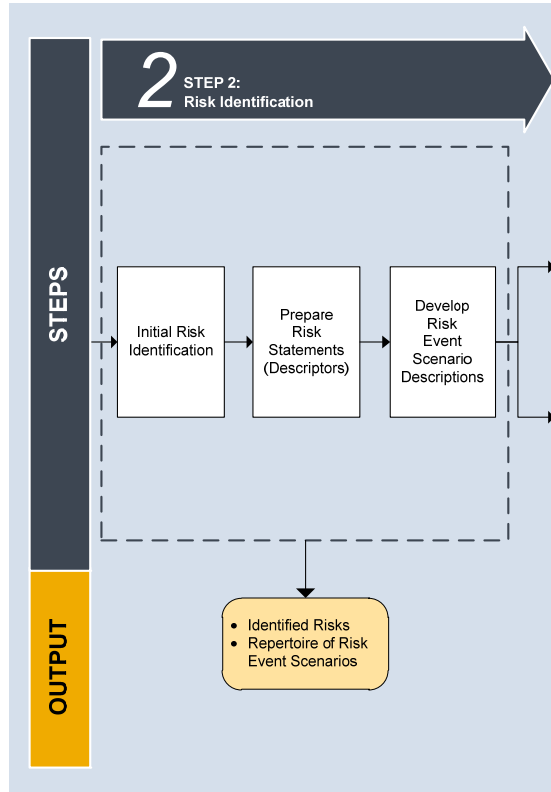
Risk identification is a key component of the risk assessment process. Risk identification is the process of finding, recognizing and recording risks. The objective of risk identification for the purpose of the AHRA is to identify key risks that have significant impact on Canada and/or Canadians, including Canadian federal institutions. Furthermore, the process assists each federal government institution in confirming risks according to its mandate and responsibilities and in developing plans or preparations necessary to reduce, mitigate or prevent these risks.

■ INPUTS REQUIRED

The following information input will help in identifying risks:

- Analysis of short-term (within the next 5 years) threats and hazards.
- Analysis of emerging and future (in 5 to 25 years) threats/hazards.
- Risk themes.

These inputs should be the outputs extracted from activities and tasks of the previous step, Setting the Context. Further input should be regularly sought from: historical data on relevant risk events, current and/or intelligence information, key policy documents and the Government of Canada's agenda.



■ TASKS AND ACTIVITIES EXPECTED IN RISK IDENTIFICATION

Initial Risk Identification

As per the AHRA business cycle (refer to Annex 1 for further details), federal government institutions should initiate the identification of top priority threats and hazards (or risks) which fall within their mandate by June of each year. Risks should be identified through the all hazards risk taxonomy (available at Annex 3). The taxonomy categorizes threats and hazards thus ensuring that a comprehensive span of risks is considered.

A departmental-wide environmental scan may be conducted to determine key risks. Environmental scanning may be performed by groups, by individuals or by a combination of groups and individuals. The following methods may be employed in the process of environmental scanning:

- Brainstorming
- Affinity grouping
- Risk source analysis
- Checklists
- Scenario analysis
- SWOT/PESTLE analysis
- Use of individual or group risk forms/identification sheets
- Surveys and questionnaires
- Interviews and focus groups
- Other methods as approved by the leader of the Risk Identification activity

Types of environmental scans may include: objective-based Risk Identification, scenario-based Risk Identification, taxonomy-based Risk Identification, common-risk checking and risk charting. An internal risk assessment process should be adopted, facilitating the process of ranking external threats and hazards.

Risk Event Scenario Development

Risks identified fall within the four component approach of emergency management planning. A risk event scenario template is available at Annex 4 and provides a detailed description of scenarios that seeks to limit assumptions and unknowns, which may interfere with the risk scoring process. The risk event scenario template describes relevant circumstances surrounding the event, provides context and information, mitigation strategies in place and/or data for experts to provide an accurate risk assessment.

Call for proposals for the risk event scenario development process will take place in the fall and the development of scenarios will continue up until the third quarter of the annual federal planning process (end of November). During the early portion of this phase (i.e. the summer), federal government institutions are to provide their highest ranking risks which will be utilized during the federal AHRA scoring process for the current year. From year to year, these risks may vary or remain the same. It is the responsibility of federal government institution to re-evaluate and determine top priority risks each year. Leads for specific risk event scenarios will be assigned depending on specific risks owned or led by federal government institutions. In all cases, PS will remain available to provide guidance and standardization to the process. Leads for risk event scenario development will have the following roles and responsibilities:

- Identify and contact relevant federal government institutions involved in the development of risk event scenario(s).
- Provide briefing or consultation if necessary on the risk event scenario development process.
- Organize and chair regular risk event scenario development working group meetings.
- Establish terms of reference if necessary.
- Develop a work plan and identify timelines to accomplish risk event scenario development.
- Identify and contact relevant federal government institutions involved in the validation of risk event scenario(s).
- Make the necessary revisions and organize meetings with subject matter experts (SME) to discuss conflicts, clarifications and inconsistencies in the risk event scenario.
- Hold the pen for the development of risk event scenarios.
- Finalize risk event scenarios in preparation for the risk scoring workshop. Key departments involved in the risk scoring process should be informed about adequately preparing research and/or data which will be used for the risk scoring process. This is to ensure that ratings are made in an efficient manner.

Risk event scenarios should be based on present day risk events and not on real past events. Historical events provide background and trends regarding hazards and threats, but are not applicable to current prevention, mitigation and preparedness activities in place, nor do they take into account present day infrastructure, technologies and institutional capabilities. Risk event scenarios should generate a “demand” picture rather than describing expected outcomes. A “risk event” is one or more inter-related events that have consequences for the safety and security of Canadians. A “risk event scenario” is a description of such an event in terms that allow for estimation of the likelihood and of the magnitude of the consequences.

The risk event scenario should:

- Include federal involvement.
- Be possible in principle, i.e. “it could happen”.

- Be a plausible story, with factual supporting information – or put another way: a report of events that could occur.
- Be so specific that it is possible to deduce which Risk Treatment capabilities will have to be brought to bear to satisfactorily address the risk.
- Include the information relevant to the representative description of a risk event.
- Describe the relevant circumstances surrounding the risk event.
- Provide the information required to be able to carry out a detailed assessment of likelihood and impacts/consequences.
- Indicate the capacity to respond e.g. mitigation strategies that are in place and its relative effectiveness.
- Signal key assumptions, unknowns and uncertainties.

For example, a risk event scenario involving an earthquake would be described with regard to the location, timing and magnitude of the earthquake, as well as the impacts that it can have on people (mortality, injury and displacement), the economy, the environment, territorial security, Canada's reputation and influence and society and psycho-social.

Preliminary assessment of likelihood and consequence is undertaken during the preparation of risk event scenarios. The risk event scenario should also include preliminary Risk Treatment planning information.

Mandated federal government institutions are responsible for leading the development of risk event scenarios; there will be a designated federal government institution with the legislated mandate related to a key element of an emergency for each risk event scenario. The designated Primary Department¹ will coordinate the development of the risk event scenario between all federal government institutions having responsibilities towards, or an interest in, the risk event.

Federal government institutions have discretion in how they choose to develop and coordinate the risk event scenario. Naturally, it will be important for Primary Departments to ensure that the risk event scenario is based on the best available information at the time and consequently, that all relevant information is researched and all relevant specialist judgement is sought. PS will provide guidance and coordinate assistance for the risk event scenario development. The selection of who to involve will be determined by the nature of the risk event scenario and the context, amongst other factors. As a best practice, workshops for risk event scenario development should be organized to facilitate the process and allow for multi-disciplinary contributions.

¹ According to the Federal Emergency Response Plan (FERP 2011), a Primary Department is a federal government institution with a mandate related to a key element of an emergency. Several federal government institutions may be designated as primary departments, depending on the nature of the emergency. A supporting department is a federal government institution that provides general or specialized assistance to a primary department in response to an emergency. PS is the federal coordinating department based on the legislated responsibility of the Minister of Public Safety under the EMA. As such, PS is responsible for engaging relevant federal government institutions.

Figure 4 below provides an illustration of the risk event scenario development process and mandatory fields for which information must be provided when developing a risk event scenario.

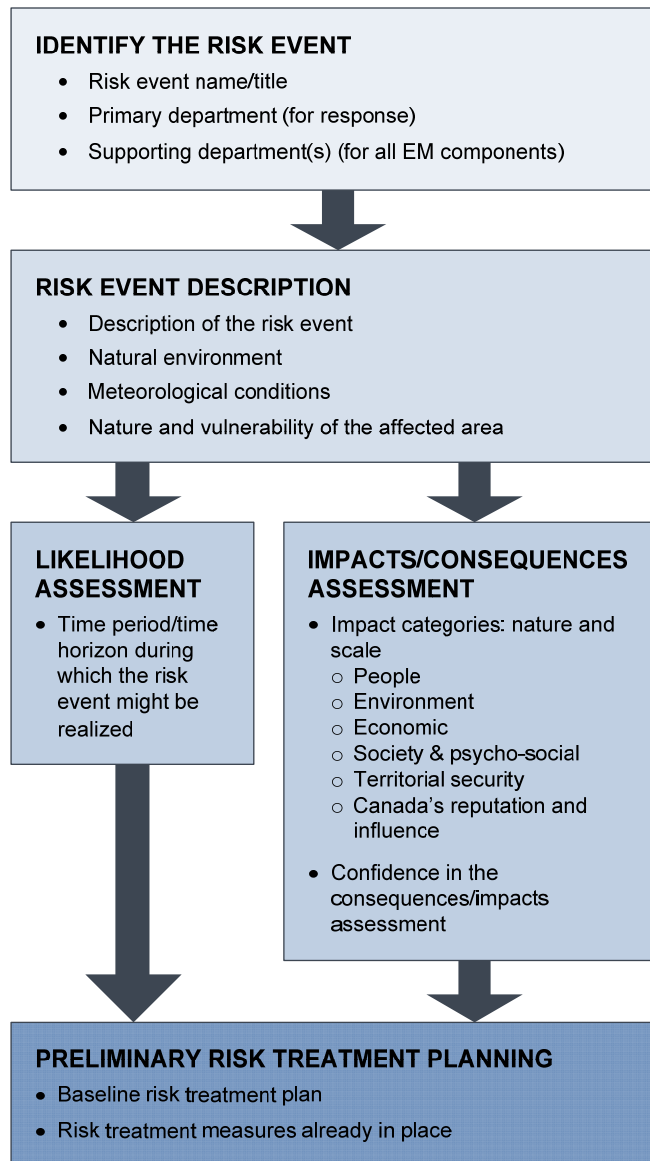


Figure 4 – Process for Developing a Risk Event Scenario

Use of Composite Risk Event Scenarios

One of the limitations to the scenario-based approach is that unless variations in risk event scenarios are introduced, a particular event, location or context is associated with that risk event. Therefore, a continuum of risk events can provide different consequences associated with different contexts for example, location, weather conditions, and size of population.

Nominal

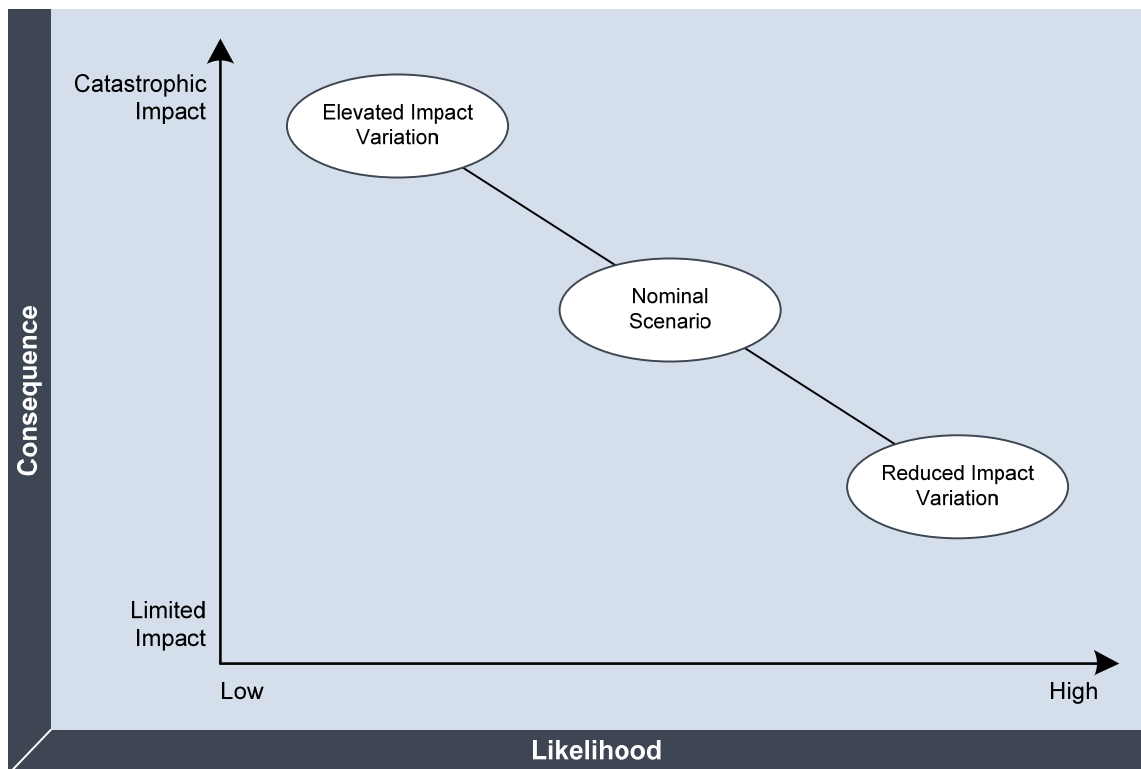
A nominal risk event scenario is considered the median event or a starting point from which risk event scenarios may continue to develop.

Reduced Impact Variation

A reduced impact variation includes reduced impacts and higher likelihoods. Reduced impacts may also be known as “best case” risk scenario events.

Elevated Impact Variation

A risk event scenario that involves an elevated impact represents a higher impact with lower likelihood in terms of outcome. Elevated impacts may also be known as “worst case” risk scenario events.



**Figure 5 – Three Variations of a Risk Event Scenario,
Displayed on a Likelihood-Consequence Graph**

Risk Event Scenarios for Non-Malicious Hazards

Natural disasters or hazards have historical links. Efforts should be made to develop risk event scenarios that would “challenge” the current approach to emergency planning capacity and/or management or be taken for future consideration. For natural disasters, nominal risk event scenarios coupled with variants is recommended in order determine best and worst case risk event scenarios. It is also recommended that risk event scenarios be developed for accidental hazards based on historical data and current non-compliance trends for regulated products, goods and services, which may be extracted from enforcement actions and results related, for instance, to the transportation of dangerous goods, the importation of products, etc. Enforcement actions may be taken after inspections, screenings and audits and may be recorded in, for example, an inspection report, including a blitz inspection report, a written non-compliance warning, detention or suspension notifications.

Risk Event Scenarios Pertaining to Malicious Threats (National Security)

Due to their sensitive level of classification, malicious threats/national security (NS) risk event scenarios will be led and held by primary security federal government institutions. Primary departments/agencies are to develop risk event scenarios based on availability to provide supporting evidence through intelligence information. In addition, subject matter experts (SMEs) are to provide specialist judgement which is essential to the process. Intelligence details relating to NS risk event scenarios should be identified within the scenario. Upon completion of the working draft of a risk event scenario, supporting and other federal government institutions will provide feedback and input in order to ensure that a four-component approach to emergency management is implemented.

Final drafts of the risk event scenarios are to be sent to supporting departments for review and analysis. The majority of the research and analysis should be completed prior to the risk scoring workshop. SMEs are strongly recommended to meet before the risk scoring workshops to agree on data scores and scores which will be decided on during the risk scoring workshop. Preparation for the risk scoring workshop is essential to ensure accuracy and efficiency in the process. During the risk scoring workshops, experts should provide their proposed score and supporting evidence.

Risk event scenarios should provide the following outcomes:

- Allow for experts to accurately assess risks.
- Allow for federal government institutions to develop EM plans.

■ OUTPUTS FOR RISK IDENTIFICATION

The information outputs for the Risk Identification process are:

- A list of identified top priority threats and hazards (or risks) by federal government institution.
- One or more risk event scenario(s) for each identified risk, contributing to a “repertoire” of risk event scenarios, to be utilized in the next step of the AHRA process.

3 Step 3: Risk Analysis²

■ OBJECTIVES OF RISK ANALYSIS

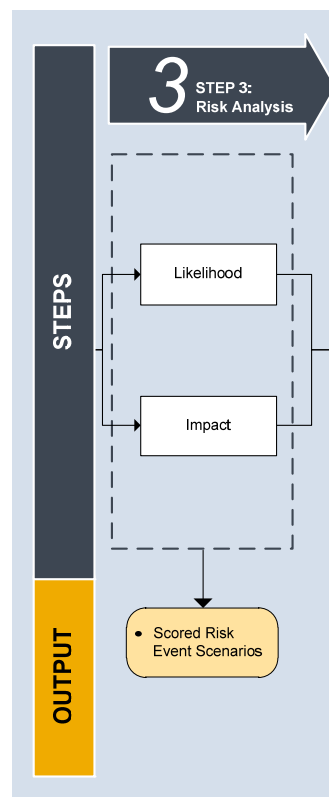
The objective of Risk Analysis is to understand the nature and level of each risk in terms of its likelihood and impact. It provides the basis for Risk Evaluation and decisions about Risk Treatment. Risk analysis is carried out by each federal government institution on the risks it has identified and retained for further analysis in terms of their frequency and overall consequence.

■ INPUTS REQUIRED

The information gathered during the Risk Identification process should be used as input for the Risk Analysis step. More specifically, risk event scenarios developed using the AHRA scenario template (at Annex 4) and supporting documentation will be required to develop sound estimates for retained risk likelihood and associated impacts.

Although not exhaustive, the list below provides the type of information required in order to estimate the likelihood of a risk scenario:

- Historical data on past events.
- Historical data on the frequency of contributing events (e.g. weather conditions).
- Simulation models of sequences of events, protective system failures, and the associated consequences.
- For malicious acts, intelligence judgements regarding intent, technical feasibility, including access to target, and enabling capabilities such as funding and logistics of adversaries.



² This section presents information at a high-level since subsequent sections provide detailed information on likelihood and impact assessments.

In addition, quantitative data extracted from past risk events or extrapolated from experiments or qualitative information derived from experts' judgement may support the estimation of the impacts for each of the following primary impact category:

- People
- Economy
- Environment
- Territorial Security
- Canada's Reputation and Influence
- Society and Psycho-Social

■ TASKS AND ACTIVITIES EXPECTED IN RISK ANALYSIS

There are two processes within Risk Analysis:

- Likelihood/probability analysis
- Impacts/consequences analysis

Likelihood Analysis

Likelihood is an estimate of the chance of an event or an incident happening, whether defined, measured or determined objectively or subjectively. It can be described using general terms or mathematical variables, such as a probability or a frequency over a time period. The term 'likelihood' will be retained for the AHRA process, regardless if the risk assessed is of natural causes, or results from an accidental or malicious source.

The assessment of the likelihood of a Risk Event being realized, or of "happening", relates to evaluating factual data in order to better understand how a Risk Event might occur. Likelihood can be estimated using either quantitative or qualitative techniques, or by using approaches that combine the two methods.

Likelihood can be assessed quantitatively using deterministic methods (models and simulations) or probabilistic methods (calculating probabilities from historical data or proxy indicators³). Probabilistic methods provide more information on the range of risks and can effectively capture uncertainty, but require more data and resources. Qualitative analysis is conducted where non-tangible aspects of risk are to be considered, such as the intent associated with terrorism or sabotage, or where there is a lack of adequate information and the numerical data or resources necessary for a statistically significant quantitative approach. Descriptive scales can be formed or adjusted to suit the circumstances, and different descriptions can be used for different risks.

³ In statistics, a proxy variable is something that might not in itself be of interest, but can represent a 'condition' for which there is no existing data.

Qualitative data can often be estimated from interviews with experts. Qualitative analysis is often simpler, but may result in higher uncertainty in the results.

More details on likelihood analysis for non-malicious risk events and malicious risk events can be found under the section on Likelihood Assessment.

Impact/Consequence Analysis

Risks can have many potential impacts/consequences which, by definition, can potentially affect many institutional objectives. Impacts/consequences can be expressed quantitatively through physical event modelling or extrapolation from experiments, studies or past data; or qualitatively as a descriptive representation of the likely potential outcome for each risk. For instance, a pre-determined set of impact questions can be used to better assess risk consequences, such as:

- Does the risk have the potential to impact a large geographic area?
- Does the risk have the potential to impact the health of the population?
- Does the risk have the potential to impact on the Canada-United States border?
- Does the risk have the potential to impact the environment in the long term?

Impacts can be expressed in terms of monetary, technical, operational, social or human criteria. They can be evaluated against predetermined segments of interest to institutions (e.g., impacts on people, the economy, the environment, national security and law enforcement).

The terms *impact* and *consequence* are sometimes used interchangeably. For the purpose of these guidelines, the term *impact* is used to estimate the extent of harm within each of the impact categories presented below. When describing a composite measure of impacts (considering more than one impact category), the term *consequence* is applied.

Impact Analysis generally comprises the following steps:

1. Identification of all individual impacts from all hazards and threats associated with the risk event.
2. Quantification of the impacts from all hazards and threats associated with the risk event, based on the six impact categories and their respective rating schemes as described in detail below.
3. Consolidation of all impacts into high-level impact dimensions.
4. Aggregation of the high-level impacts into an overall impact for the risk event, together with an expression of the level of confidence in the estimates.

Impact Categories

In the context of the AHRA, the primary impact categories are:

- People — which includes fatalities and injuries, including physical injuries, displacement, chronic diseases and mental illnesses.
- Economy — which encompasses direct and indirect losses on the Canadian economy.
- Environment — which captures the type of response, the geographical extent, magnitude and duration of damage.
- Territorial Security — which includes the disruption in the effective functioning of an area or a border, including the area affected, combined with duration and population density.
- Canada's Reputation and Influence — which are situations that would result in a shift in views towards the reputation and influence of Canada and actions taken by citizens and/or stakeholders as a consequence.
- Society and Psycho-Social — which captures the impact of widespread public anxiety and outrage.

Approach for Impact Rating

The proposed Impact Rating approach was designed with several considerations in mind, which include:

- The impact categories should be as “orthogonal”, or independent, as is possible, to avoid double counting of effects.
- The risk should be calculated explicitly for each impact category. This will provide a useful intermediate result for groups with a focused interest (e.g., the health sector might only be interested in “risk to people”).
- More details, through subordinate impact factors, can easily be added for each impact category without affecting the overall framework or interoperability with prior assessments. As is shown below, the “impact on people” is assessed through the three subordinate factors of “killed”, “injured” — including physical injuries, chronic and mental illnesses — and “displaced or lacking basic necessities of life”. This allows a more granular assessment that may be useful for the further development or refinement of detailed scenarios or might be of a particular interest to specific prevention and mitigation program areas for which that subordinate factor is important.
- Subordinate factors can be independent, and assessed as such — e.g., under the “People” factor, the number of killed, injured and displaced is independently assessed — or they can be additive, where multiplicative “dimensions” of impact are combined to produce one rating. For example, under the “Territorial Security” category, “modifiers” are used to change the rating for a base factor, “response magnitude”, to incorporate the population density of the affected area as well as the duration of disruption into the final rating. This will have the

benefit of not only taking into consideration factors that may increase the final rating for a particular impact category, but these factors may also have a positive impact on the final rating. In other words, some modifiers might “improve” the final rating by, for instance, considering subordinate factors that indicate a tolerable disruption because its duration may be minimal or under a certain pre-determined threshold.

More details are provided at the section on Impact Assessment Categories, when scoring tables for each impact category are discussed.

In order to ensure a consistent mathematical framework for the impact and risk scores, the impact category scores are defined as the “magnitude” of the severity associated with a loss for the category. This implies a constant ratio for the increase in severity from one level to the next. The proposed tables for each impact category use a logarithmic scale, with half scores for ratio increments of the square root of 10, used to increase the resolution of the assessment. Thus, the ratio for increased severity from one scoring level to the next is approximately 3.16 times (i.e., a severity of a “2.5” impact level is 3.16 times that of a “2” , and the severity of a “4” is also 3.16 times that of a “3.5”). You will note that the ratio for two levels (or one integer score) difference is 10 (3.16×3.16). This approach allows an easier comparison of values associated to each level, which cover a large range in terms of the severity magnitude.

AHRA Scoring Tool

An AHRA tool prototype was created to help users (generally risk analysts) define and score potential hazards and threats across the different categories of impacts and determine the likelihood of the risk event occurring within a five-year timeframe. The tool was built as a user-friendly Excel program with step-by-step prompts. The AHRA tool considers impacts to the following categories: people, economy, environment, territorial security, Canada’s reputation and influence and society and psycho-social as described earlier in the guidelines. Each impact category includes the option(s) to define assessors’ confidence level for the inputs as well as any justification they may wish to include. The tool can be demonstrated by contacting PS’s Emergency Management Planning Unit, at AHRA-ETR@ps-sp.gc.ca.

Confidence Level and Justification for Likelihood Analysis and Impact/Consequence Analysis

For each impact category, assessors must indicate their level of confidence in the estimates they have provided with respect to harm caused by the defined Risk Event Scenario. A confidence level from A to E is used to describe the confidence of assessors in the value they have defined or selected. The degree of confidence in the ratings produced will vary, depending on the availability of data, relevant experience and existing body of knowledge. Capturing the confidence level associated with each rating produced provides a crucial piece of information that helps complete the risk assessment picture. Confidence levels will be presented, along with final results, to indicate to decision makers where some low or very low confidence assessments may necessitate caution in interpretation. On the other hand, assessments accompanied with high or very high confidence levels will inspire trust in immediate actions required to treat pressing risks.

The following table presents definitions for confidence levels that must be used for each rating:

Confidence Level	Quantification
A	Very High confidence in the judgement based on a thorough knowledge of the issue, the very large quantity and quality of the relevant data and totally consistent relevant assessments.
B	High confidence in the judgement based on a very large body of knowledge on the issue, the large quantity and quality of the relevant data and very consistent relevant assessments.
C	Moderate confidence in the judgement based on a considerable body of knowledge on the issue, the considerable quantity and quality of relevant data and consistent relevant assessments.
D	Low confidence in the judgement based on a relatively small body of knowledge on the issue, the relatively small quantity and quality of relevant data and somewhat consistent relevant assessments.
E	Very Low confidence in the judgement based on small to insignificant body of knowledge on the issue, quantity and quality of relevant data and/or inconsistent relevant assessments

In addition, any justifications, assumptions and/or references for the various inputs defined by assessors during Risk Analysis should be recorded, along with the rating of each impact category.

■ OUTPUTS FOR RISK ANALYSIS

The information outputs related to the Risk Analysis process are:

- An assessment of the likelihood of the realisation of the hazards and threats associated with the risk event, with an associated confidence level.
- An assessment of the impact for the risk event in terms of each of the primary impact categories, with associated confidence levels.
- An assessment of the overall impact for the risk event, with an associated confidence level.
- Other information generated during the Risk Analysis Process, such as assumptions and justifications.

■ IMPACT ASSESSMENT CATEGORIES

In the AHRA process, each risk scenario is analyzed with respect to multiple impact categories. By consistently considering all of the possible dimensions of consequences, a whole-of-government view of risk can emerge.

The AHRA process uses the following impact categories, which are explained below:

- People
- Economy
- Environment
- Territorial Security
- Canada's Reputation and Influence
- Society and Psycho-Social

It is important to note that during the rating of each impact category, experts will provide their input for the various factors without actually relying on the quantitative scales (i.e. exact numbered rating) that are associated with their qualitative input, in order to avoid any distraction that could be caused by the actual numbered scales. Their input will be translated into a final rating in the scoring tool by the AHRA scoring tool itself at the end of the assessment exercise. The final score is made known after an entire Risk Event Scenario is scored, at the "Input Summary" sheet of the AHRA scoring tool.

People

A priority for the federal government is to protect the health and safety of Canadians. With that objective in mind, this category assesses the number of people killed, injured, and displaced or lacking the basic essentials of life following a given risk event. The focus of this impact category is to take into account the combined impact of various degrees of acute and chronic injury and the potential loss of life after the onset of a risk event.

To capture diverse health outcomes, analysts often use composite burden of disease measures. The Disability-Adjusted Life Years (DALY) is one such measure used to estimate health impacts by combining impacts from fatalities, non-fatal injuries and chronic diseases. The DALY measure for each injury type is composed of the product of the severity, the duration and the number of injuries. The severity scale ranges between 0 (perfect health) and 1 (death). The duration of the injury is represented in years. The DALY measure is also used to measure the impact of fatalities. The severity of a fatality is always equal to 1, while an estimate of the number of years of life-expectancy at the time of death is the appropriate measure of duration. This yields a higher estimate of impact for fatalities in children, as compared to fatalities among adults.

$DALYs \text{ by Injury Type} = \text{Number of Cases} \times \text{Severity} \times \text{Duration}$

$DALYs \text{ due to Fatalities} = \text{Number of Cases} \times \text{Years of Life Lost}$

$\text{Total DALYs} = \text{Sum of DALYs by Injury Type} + \text{DALYs due to Fatalities}$

The table below shows the conversion of the number of DALYs into an impact rating on a scale from 0 to 5. The conversion associated with the table below is generated by the AHRA scoring tool itself after assessors record their information into the People impact category Excel sheet.

Note that 0 on this impact rating scale is not the same as “No Impact.” Where a risk scenario results in no impact whatsoever for an impact category, this is not assigned a numerical score; it is captured as “No Impact.” The rightmost column is provided to show the linkage between fatalities and the overall People Impact rating. An adult fatality, on average, can be assigned a score of approximately 40 (for 40 years of lost life).

Magnitude of Impact Rating	Total DALYs Combining Injury and Fatality	Equivalent Number of Adult Fatalities
No Impact	0	0
0	40	1
0.5	120	3
1	400	10
1.5	1,200	30
2	4,000	100
2.5	12,000	300
3	40,000	1,000
3.5	120,000	3,000
4	400,000	10,000
4.5	1,200,000	30,000
5	4,000,000	100,000

Economy

The Economy impact category captures the dollar value following damage(s) or loss to economically productive assets and disruptions to the normal functioning of the Canadian economic system, which may result in the loss of service as a result of a risk event occurring. This loss is broken down into the following:

Direct Economic Loss

- Direct economic loss (stock losses) is the immediate economic damage generated by the disaster. These losses can be measured by the repair or replacement costs (at the pre-event price level) for assets that have been damaged or destroyed. In particular, this would include damage to:
 - Building construction: industrial, commercial, and institutional buildings (e.g. plants, offices, recreational facilities, hospitals, etc.).
 - Engineering construction: road infrastructure, water systems, marine construction (irrigation, docks, terminals, etc.), other transportation, electric power, and oil and gas engineering.
 - Machinery and equipment used in the production process (furniture, agricultural and industrial machinery, computers and software, telecommunication equipment, trucks, etc.).
 - Residential structures and content.
 - Raw materials: mineral fuels (coal, crude oil, natural gas), grains (crops ready to be harvested), animal and animal products (e.g. cattle and hogs-swine for slaughter, milk and eggs, fish), wood, ferrous and non-ferrous metals, non-metallic minerals, etc.

Two additional elements are “non-reproducible assets” (land, timber, subsoil resource stocks, etc.) and “human capital stock” (loss of lives and injuries). However, these, as well as other environmental, ecological, welfare and non-economic quality of life impacts will not be considered in the “economic loss” impact category thus avoiding the risk of “double counting”. This reflects the fact that these “nonmarket” impacts are difficult to translate into monetary terms. However, they should be taken into account in the People and Environment impact categories.

Indirect Economic Loss

- Indirect economic loss (flow losses) refers to the flows of goods and services which will not be produced due to damages to productive assets and economic infrastructure. This interruption or reduction in production should be measured in terms of **value-added** to avoid double-counting issues.⁴ For instance, this would include:
 - Production or service provision losses due to the full or partial paralysis of activities (e.g. losses in agricultural/industrial production due to damage to factories or shortages of raw materials/energy supplies)

⁴ In the case of production sectors, losses must be assessed at producer prices because they represent the value of what was not produced as a result of the disaster. In the case of interrupted service production (days or months of classes, the number of medical consultations, increased transportation costs due to detours, etc.), the most suitable approach is to value services not generated as a result of the event based on the prices or fares paid by the final consumer or end user.

- Higher operational costs due to the destruction of productive assets or losses to production and income (e.g. a ban on beef and cattle exports would first translate into higher maintenance cost due to rising inventory levels of live animals).
- Lost production due to linkages effects (e.g. the destruction of a factory reduces the economic activities of suppliers who have no alternative markets or of clients who have no other suppliers).
- Additional costs incurred due to the need to use alternative and potentially inferior means of production or provision of essential services (e.g. greater operating costs arising from reduced transportation or energy capacity).
- Costs of required government response (e.g. emergency and rescue operations).

Estimates of indirect losses should be undertaken with caution as some effects might be difficult to identify or quantify.⁵ It is suggested that only relevant external factors that significantly modify the estimate of the economic loss should be considered. Indirect losses should be made relative to the duration of the disruption. For instance, one could calculate how many days-worth of value-added in the transportation, financial, manufacturing, or tourism sector before a return to normal activities. Also, the assessment should ensure that no double-counting takes place: if effects are calculated on the production side, they must not be included again on the income side. For example, government compensation to farmers affected by an outbreak of foot and mouth disease (FMD) should not be included in addition to the associated production losses.

It is important to note that indirect losses can sometimes be counteracted by built-in mechanisms and behavioural changes, e.g. consumer-demand shift following a bovine spongiform encephalopathy (BSE) outbreak, substitution of inputs and/or reallocation of resources following a pandemic, use of alternative transportation means or production rescheduling following rail/airport closures, business relocations following an earthquake, etc. It is important to capture these “built-in counteractions” as assumptions, along with the rating of the Economic category. Finally, disasters sometimes produce benefits that can be estimated and must be deducted as well from the total losses estimate, e.g. a rise in land productivity following a flood.

Once all the contributions to the economic loss have been identified, all costs are added and the rating for this category is based on the final dollar figure.

⁵ For instance, indirect losses could also include the loss of income resulting from the non-provision of goods and services or from the destruction of previously used means of production. However, these are difficult to adequately quantify.

Magnitude of Impact Rating	Economic Loss
No impact	No impact
0	\$10M
0.5	\$30M
1	\$100M
1.5	\$300M
2	\$1B
2.5	\$3B
3	\$10B
3.5	\$30B
4	\$100B
4.5	\$300B
5	\$1,000B

It is important to note that macroeconomic studies provide a complementary way to assess the repercussions of direct and indirect economic losses. For instance, estimates of macroeconomic effects would take into account that some indirect effects could be exacerbated or mitigated in the aggregate by changes in prices or flexibility in the production process (e.g. through reallocations in spending/production across sectors or through the mobilization of production factors if production is not at full capacity). Estimates of high-order impacts require the use of more sophisticated economic models.

A table summarizing elements that should be considered in estimating economic losses can be found at Annex 6.

Environment

Another priority for the federal government is to protect the environment, as it recognizes that Canada's natural environment shapes our national identity, our health and our prosperity. In the area of the environment, the Government of Canada has a number of programs focused on conserving and restoring Canada's natural environment. Accordingly, this impact category relates to the preservation of specific components of the environment pertaining to air, water and soil ecosystems, including fauna and flora. The environment rating scale thus focuses on environmental damage caused by a risk event or an emergency. In the context of the AHRA, environmental damage refers to loss of environmental assets or environmental quality that

requires intervention⁶. This category will exclude assessing economic aspects created by such loss, as they should be captured under the Economy impact category in order to avoid double counting impacts.

The Environment impact category considers four elements that characterize the size and severity of environmental damage from a risk event or an emergency: 1) the principal element to factor in when rating environmental damage significance is the magnitude of a response required to deal with a situation, which involves the type of response required (local, regional, multi-jurisdictional, general, specialized, etc.); 2) the geographical extent of the damage; 3) the magnitude of damage based on adverse effects to different components of the environment; and 4) the duration of the damage including the level of recovery efforts.

Magnitude of Response Required to Deal with an Event

The magnitude refers to the type of response necessary when treating an event affecting the environment.

A **local** response will indicate that the damage and/or contamination is limited to a municipality or a region within a province, requiring a response from these authorities. In this instance, a federal surveillance and monitoring capacity from an institution may be required.

A **multi-regional** response will indicate that the extent of the damage and/or contamination is limited to two or more regions within a single province and response is expected by affected authorities. A multi-regional response may require some “for information” notification amongst federal government institutions about the incident, without a request for support. It may also involve some regional coordination activities amongst federal government institutions, with a possible request for support from regions affected.

A **multi-jurisdictional** extent and response will indicate that the extent of the damage and/or contamination affects an area comprised over two or more provinces and response is expected by affected jurisdictions. A multi-jurisdictional response will require mobilization from federal authorities in the form of some response capacity.

A **national and international** extent and response will indicate that leads are exclusively federal government institutions and that the extent of damage and/contamination crosses international borders. Rapid federal response capacity will be mobilized.

In essence, federal implication or assistance may be required, even if the type of response and extent of damage may be estimated to remain local (e.g. flood response is usually local, but surveillance and modelling capabilities may be shared with federal government institutions).

⁶ Adapted from: Glossary of Environment Statistics, Studies in Methods, Series F. No.67, United Nations, New York, 1997.

A response may require some intervention from general emergency response teams, such as workers from a fire or police department. Other emergencies may require specialized teams to contain and restore an affected area contaminated by a hazardous substance. In addition, a multi-functional response may be warranted depending on a risk event situation. A multi-functional response team is defined as a team of responders composed of police forces and emergency services, but also from community organizations and services, businesses and workplaces, and other members of an affected community or affected communities.

Base Rating	Response Magnitude
	Type of Response
No Impact	No Impact
0	Some local general response, but no specialized response
1	Some local specialized response, and surveillance and monitoring from federal authorities
2	Multi-regional general response, and notification from federal authorities
3	Multi-functional, multi-regional specialized response, and notification from federal authorities
4	Multi-functional, multi-jurisdictional specialized response, and mobilization from federal authorities
5	Multi-functional, national and international, specialized response, and rapid mobilization from federal authorities

Environmentally affected area

Localized damage may not be significant. Alternatively, widespread damage may be significant. The geographical extent of damage will be represented in terms of square kilometres of damage to the environment and will be applied as a modifier, in the sense that it will increase the overall rating of the magnitude of a response required to deal with a situation.

A baseline is proposed for environmentally affected area, which could be considered as the typical geographical extent for the respective response rating. A modifier is applied only if the size of the environmentally affected area is more than what is typically expected for that type of response.

The baseline associated with the size of the environmentally affected area will shift upwards as the environmental response magnitude rating increases, with modifiers added (or subtracted) for size greater than expected for that response level.

For example, the baseline (modifier value of 0) for the size of the environmentally affected area for local response with no federal monitoring (response rating of 0) would be 50 km² (anything below that size would barely raise any interest, considering the scope of AHRA). If the size is greater (size increasing threefold at each rating step, to be consistent with the overall approach), a modifier is added (in increments of 0.5):

Geographical Extent Modifier	Size of Damage (km ²)
0	Up to 50
+0.5	150
+1	500
+1.5	1500
+2	5000
+2.5	15000

Fact: The Greater Toronto Area (GTA) is about 7,200 km²

For a response level of 1 (local specialized with federal monitoring), the geographical extent baseline is considered to be 150 km², and a modifier is applied for a greater affected area:

Geographical Extent Modifier	Size of Damage (km ²)
0	150
0.5	500
1	1500
1.5	5000
2	15000

For a response level of 2 (multi-regional environmental response with notification from federal authorities), the geographical extent baseline is considered to be 500 km², and a modifier is applied for a greater affected area:

Geographical Extent Modifier	Size of Damage (km ²)
0	500
0.5	1500
1	5000
1.5	15000

For a response level of 3 (multi-regional, multi-functional environmental response with involvement from federal authorities), the geographical extent baseline is considered to be 1500 km², and a modifier is applied for a greater affected area:

Geographical Extent Modifier	Size of Damage (km ²)
0	1500
0.5	5000
1	15000

For a response level of 4 (multi-functional, multi-jurisdictional specialized environmental response, and mobilization from federal authorities), the geographical extent baseline is considered to be 5000 km², and a modifier is applied for a greater affected area:

Geographical Extent Modifier	Size of Damage (km ²)
0	5000
0.5	15000

For a response level of 5 (multi-functional, national and international specialized environmental response, and rapid mobilization from federal authorities), the geographical extent baseline is considered to be 15000 km², and there are no modifiers to be applied as this is already deemed the highest level.

Geographical Extent Modifier	Size of Damage (km ²)
0	15000

Magnitude of Damage Based on Environmental Adverse Effects

The magnitude refers to the severity of the adverse environmental effects, based on each criterion that applies to a risk event or an emergency and its associated severity value. This component will be applied as a modifier.

The following criteria and associated value can be used for determining the magnitude of damage based on adverse environmental effects:

- loss of rare or endangered species (value: 2)
- reductions in species diversity (value: 1)
- loss of critical/productive habitat (value: 2)
- transformation of natural landscapes (value: 0.5)
- loss of current use of lands resources (value: 1)
- loss of current use of water resources (value: 2)
 - loss of essential water resources
 - water-related environmental losses
- environmental losses from air pollution (value: 0.5)

As every criterion has its own value, the total value of the modifier will be reached by a simple addition of those applicable to a risk event.

Modifier	Sum of values associated with adverse environmental effects
0	3
0.5	9

Note, modifiers to the environmental impact assessment should only be used in exceptional cases, where the likely impacts of an event are beyond what would be captured by the primary indicator (environmental response). A given level of environmental response has certain implications in terms of size of the affected area, duration of environmental damage, and magnitude of environmental damage. Thus, the primary rating should only be augmented by modifiers if those components are greater than what would be typical for that level of environmental response.

Modifier for Duration of Damage

A modifier to increase or decrease the rating will be applied for the duration of damage.

When rating the magnitude of response required to deal with a risk event and the extent of the damage, the duration of the actual damage needs to be taken into account and reflected in the rating. In addition, recovery efforts will be factored in the rating of this modifier. If recovery efforts are made or positively expected to be made (recovery enforced by law, government or company commitment, etc.), the rating will be improved. The total rating will be reflected by adding the duration modifier with the recovery efforts, as described in the table below.

As in the case of the environmentally affected area, the environmental response magnitude already has some implications in terms of duration of environmental damage; a modifier is justified only if the duration is more than what is implied in the response.

A baseline is proposed for the duration of environmental damage, which could be considered as the typical duration for the respective response rating. A modifier is applied only if the duration is more than what is typically expected for that type of response.

The baseline associated with the duration will shift upwards as the environmental response magnitude rating increases, with modifiers added for duration longer than expected for that response level.

For example, the baseline (modifier value of 0) for the duration of environmental damage for local response with no federal monitoring (response rating of 0) would be 3 weeks (anything below that would barely raise any interest, considering the scope of AHRA). If the duration is longer

(duration increasing threefold at each rating step, to be consistent with the overall approach), a modifier is added (in increments of 0.5):

Duration modifier	Duration of environmental disruption
0	Up to 3 weeks (approx. 1 month)
0.5	10 weeks (approx. 2 months)
1	8 months
1.5	2 years
2	6 years
2.5	20 years

For a response level of 1 (local specialized with federal monitoring), the duration baseline is considered to be 10 weeks, and a modifier is applied for a longer duration:

Duration modifier	Duration of environmental disruption
0	10 weeks (approx. 2 months)
0.5	8 months
1	2 years
1.5	6 years
2	20 years

For a response level of 2 (multi-regional environmental response with notification from federal authorities), the duration baseline is considered to be 8 months, and a modifier is applied for a longer duration:

Duration modifier	Duration of environmental disruption
0	8 months
0.5	2 years
1	6 years
1.5	20 years

For a response level of 3 (multi-regional, multi-functional environmental response with involvement from federal authorities), the duration baseline is considered to be 2 years, and a modifier is applied for a longer duration:

Duration modifier	Duration of environmental disruption
0	2 years
0.5	6 years
1	20 years

For a response level of 4 (multi-functional, multi-jurisdictional specialized environmental response, and mobilization from federal authorities), the duration baseline is considered to be 6 years, and a modifier is applied for a longer duration:

Duration modifier	Duration of environmental disruption
0	6 years
0.5	20 years

For a response level of 5 (multi-functional, national and international specialized environmental response, and rapid mobilization from federal authorities), the duration baseline is considered to be 20 years, and there are no modifiers to be applied as this is already deemed the highest level.

Duration modifier	Duration of environmental disruption
0	20 years

While the expected recovery efforts can be captured, they should be factored in already in the expected duration of environmental disruption, not added separately through a modifier.

A cumulative factor will affect the final score for this category: the geographical extent of the damage, the magnitude of damage based on environmental adverse effects and the duration of the damage will be added to the base rating score as assessed by the magnitude of response, without exceeding 5.

Territorial Security

Territorial security is a core responsibility of the GC and provides the conditions permitting the free movement of Canadians, other people and legitimate goods within the country and across borders. It represents the effective functioning and control of international borders, and provides for the safety and security of Canadians to go about their lives in an ordinary fashion.

In a globalized society, there are an increasing number of challenges to the Government's ability to protect and maintain territorial security. Challenges can come from abroad (e.g. terrorist attacks, nuclear capability of adversarial states, challenges to Arctic sovereignty) or from natural disasters (e.g. hurricanes, earthquakes, infectious diseases). Ecological and/or geological loss in its strict sense will be captured under the environment category in order to avoid double counting impacts.

The Territorial Security impact category reflects losses in the ability of Canada to control its territory, either through annexation or invasion. This dimension captures conditions in which there is a loss in the ability of the Government of Canada to secure the territory or the border and to secure the safety of citizens. For this category, the baseline rating is rooted in geographical area of the country at risk or affected. The final score is determined by the area affected, with factors including the duration of disruption and population density.

Impact Score = (Area Affected) + (Duration Score) + (Population Density Modifier)

Fact: The *total* area of Canada (combines land and marine boundaries) is 9,984,670 km²

Base Rating for Area Affected	Size of Impact (km ²)
No impact	No impact
0	100
0.5	300
1	1,000
1.5	3,000
2	10,000
2.5	30,000
3	100,000
3.5	300,000
4	1,000,000
4.5	3,000,000
5	10,000,000

Modifiers for Duration of Disruption and Population Density

Modifiers to increase or decrease the rating will be applied for the duration of the disruption, as well as the population density of the area affected.

Duration of Disruption

Duration modifier	Duration of disruption
-2	1 hour
-1.5	3 hours
-1	10 hours (about ½ day)
-0.5	1 day
0	3 days (about ½ week)
+0.5	10 days
+1	1 month
+1.5	3 months

+2	1 year
+2.5	3 years
+3	10 years and over (not permanent)
+3.5	Permanent

Population Density of Area Affected

Density modifier	Density of area affected or at risk (People per km)
-1	0.1
-0.5	0.3
0	1
+0.5	3
+1	10
+1.5	30
+2	100

A cumulative factor will affect the final score for this category: the duration of disruption and population density modifiers will be added to the base rating score, with the total not exceeding 5.

Canada's Reputation and Influence

The interconnected nature of economies, societies, and governments means that the international reaction to an emergency event in Canada, or an event that involves Canadians abroad, can have widespread repercussions for the way foreign governments, populations, and organizations view Canada, and the influence Canada maintains on a global stage. Since the international reputation and influence of the GC and/or Canadians plays an important role in advancing Canada's interests and foreign relations, the potential of risk events to impact Canada's reputation and influence needs to be factored into the risk assessment in order to develop appropriate risk management strategies.

This category represents an expert assessment of the potential international reaction to an emergency event occurring in Canada, or involving Canadians abroad. Examples of potential triggers/events that can signal that an emergency has the potential to impact Canada's reputation and influence include damage or loss of control over Canada's embassies, suspension of international agreements, protests against Canada, imposition of travel restrictions to Canada, deterioration of bilateral political relations, etc. This category presents a non-exhaustive list of situations that would demonstrate a shift in views towards Canada's reputation and influence by

foreign governments, international actors and populations, and the types of responses that could arise from such a shift.

This assessment should be made based on reactions to similar emergency events previously experienced within Canada and/or in other countries. If such information is unavailable, departmental experts will provide a thoughtful assessment of potential outcomes.

As with other impact categories, the Canada's Reputation and Influence impact category is based on a 0-5 level log-scale. Half scales in this category are generally more difficult to determine due to the nature of potential actions, and political and non-political relations, but may still be assigned should experts feel it is appropriate. Aspects of an event situation to take into consideration when establishing an assessment could include the international consequences of a risk event, the extent and duration of people affected, the nature of the threat and its potential to spread across borders, the level of devastation experienced, among others.

Rating Level	Repercussions
0	No damage to Canada's reputation and influence
1	Insignificant damage to Canada's reputation and influence - <i>Minor, short term and localised reaction that is limited to small groups of individuals and has no repercussions for Canada or Canadians</i>
2	Minor damage to Canada's reputation and influence - <i>Minor, medium- to long-term, international reaction by groups of individuals that has a minor effect on Canada or Canadians</i>
3	Significant damage to Canada's reputation and influence - <i>Significant, short to medium-term, international reaction by groups of individuals, foreign governments and/or organizations that has a medium term effect on Canada and Canadians</i>
4	Major damage to Canada's reputation and influence - <i>Major, short- to medium-term, widespread reaction by large groups, foreign governments and/or organizations that has a long lasting effect on Canada and Canadians</i>
5	Severe damage to Canada's reputation and influence - <i>Major, long term, widespread reaction by large groups, foreign governments and/or organizations that has a lasting effect on Canada and Canadians</i>

There is a list at Annex 5 that includes possible examples of changes in international positions towards Canada, and ways the GC and/or Canadians may be impacted by a risk event that has international implications.

Society and Psycho-Social

Social actions, such as protests, civil disturbances or vandalism, can be provoked by an event and can impact response and recovery efforts. Social actions can be rooted in people's understanding and perception of the incident as well as their sense of control over the outcome. At the same time, even if people do not engage in social action following an event, they can nevertheless experience the psycho-social effects of disaster that can lead to changes in their individual pattern of behaviour over the short or long term. Psycho-social effects can also impact the effectiveness of the overall response and recovery efforts if they are not appropriately managed. Over the longer term, continued exposure to the source of stress or lack of support for the population may result in secondary disorders.

When scoring for this impact category, consideration should be provided to the dimension of public mood. The scoring of public mood is based on a subjective assessment that focuses on two criteria: public outrage and public anxiety. The descriptors for each of these attempt to capture how people's behaviour might be affected by an event and the score, although subjective, points to the possibility of short to long-term psycho-social impacts.

Impact Score	Public outrage descriptor	Public anxiety descriptor
No Impact	- No Impact	- No Impact
0	- Insignificant	- Insignificant: no changes in people's normal routine
0.5-1	<ul style="list-style-type: none"> - Minor - No authority or person perceived to be culpable or incompetent - Impact targeted on one particular group associated with the government (rather than being indiscriminate) - Little symbolic value 	<ul style="list-style-type: none"> - Minor anxiety but no change in people's behaviours - Short term avoidance of transport modes - Risk to children or future generations limited - Strong public familiarity with/understanding of the risk and its consequences - Less than a thousand people feel more vulnerable
1.5/2	<ul style="list-style-type: none"> - Significant but localized and temporary - Consequences are largely one-off - Public acceptance that the risk was a natural disaster or avoidable and largely not caused/exacerbated by human failure - Little symbolic value of site or target 	<ul style="list-style-type: none"> - Minor, localized and temporary changes in people's normal routines - Short to medium-term avoidance of transport modes - Good public understanding of the risk - Thousands of people feel more vulnerable (but less than 10,000 people)
2.5/3	<ul style="list-style-type: none"> - Serious, widespread - Consequences will not just be 	- Moderate anxiety leading to medium to short-term changes in peoples'

Impact Score	Public outrage descriptor	Public anxiety descriptor
	<ul style="list-style-type: none"> one-off, but still short-term - High impact on those perceived as vulnerable (i.e. elderly, women, children) - Public perception that the disruptive outcome was a result of someone/the government's failure - High symbolic value 	<ul style="list-style-type: none"> routines - Medium term avoidance of some modes of transport - Shortage of essential supplies due to panic-buying - Conceivable that the event could occur again - Impact was indiscriminate (as opposed to being focused on a specific group such as government officials or industrial workers) - Lack of control or helplessness - Some concern about potential health risk to future generations - Limited public understanding of the risk - Tens of thousands of people feel more vulnerable (but less than 100,000 people)
3.5/4	<ul style="list-style-type: none"> - Serious national-wide concern, with strong calls for government action - The adverse impact was intentional/ malicious - Domestic pressure for resignations; public perception that government/ person significantly failed - Risk results from human action rather than natural causes - Consequences will be medium-term rather than just one-off - Indiscriminate and very significant impact - Significant impact on those perceived as vulnerable (i.e. elderly, women, children) - Very high symbolic value 	<ul style="list-style-type: none"> - High levels of anxiety leading to sustained changes in people's normal routines - Intense and widespread information seeking by the public - High levels of concern about risks to children or future generations - High levels of concern that catastrophic event could occur again - Impact was indiscriminate and affected large (but less than 1,000,000) number of people (as opposed to being focused on a specific group such as government officials or industrial workers) - Significant sense of lack of control/helplessness - Lack of informed public knowledge or understanding of the risk - Millions of people feel more vulnerable
4.5/5	<ul style="list-style-type: none"> - Extreme, nation-wide, sustained - Widespread calls for severe governmental reprisal (i.e. the adverse impact was intentional/malicious) - Persistent domestic pressure for resignations at national/CEO level - Consequences will be long-term rather than one-off - Risk results from human action rather than natural causes 	<ul style="list-style-type: none"> - Extreme, widespread, prolonged - Widespread avoidance of an area - Social conflict and community tensions resulting from fear-induced behaviour - Severe loss of confidence in government's ability to protect citizens - Severe and prolonged loss of confidence in the financial markets - Significant concern about risks to children or future generations

Impact Score	Public outrage descriptor	Public anxiety descriptor
	<ul style="list-style-type: none"> - Indiscriminate and catastrophic impact - Severe impact on those perceived as vulnerable (i.e. elderly, women, children) - Very high symbolic value 	<ul style="list-style-type: none"> - Significant concern that catastrophic event could occur again - Severe sense of lack of control/helplessness - Impact was indiscriminate and directly affected very large (i.e., 10,000,000 or more) number of people; perception that the adverse consequences could happen to anyone - Very little informed public knowledge or understanding of the risk - Significant proportions of people feel more vulnerable

■ LIKELIHOOD ASSESSMENT

Likelihood assessment defines the chance of an event occurring in the next five years, whether it is a natural hazard or a malicious threat.

Malicious Threats

The malicious likelihood scale takes into consideration technical feasibility, enabling capability and intent. The overall likelihood score is based on the principle of the “weakest link”, meaning that if the capability is present but the intent is low, then the score for intent will take precedence.

A successful adversarial attack cannot occur if one of the elements is absent, lacking or unobtainable; in other words, an attack is assessed as impracticable if the level for one element of the overall capability is below a necessary level to being materialized. Risk scores associated with malicious risk events are based on an intelligent adversary. Therefore scores are decided upon by the intelligence community and/or organization’s estimate of technical feasibility, enabling capability and intent.

Likelihood Rating for Malicious Scenarios

Estimating the likelihood of malicious scenarios is considerably different than for other threats/hazards, as these estimates must take into account the determined and adaptive nature of an intelligent adversary. Such an adversary will make a choice to carry out an attack based, on the one hand, on the statement they want to make, in accordance with the individual’s or the organization’s ideology. To capture this dimension, the current approach relies on the intelligence community to provide expert judgment on an individual’s or organization’s *intent* to carry out an attack, as described in the scenario. On the other hand, the adversary’s choice of an attack is also based on considerations of whether mounting an attack is technically feasible, as well as whether they have adequate organizational and support means to carry it out. Again, the current approach relies on judgment from domain experts to assess various components of the *technical feasibility* of a malicious attack scenario, and on the intelligence community to provide

expert judgment on whether an individual or organization has sufficient *capability* to carry it out. The combined assessments of feasibility, capability, and intent are used to generate an overall assessment or composite judgment of likelihood.

Technical Feasibility

The Technical Feasibility is rated across a number of components or indicators:

- Materials
- Equipment
- Access to target
- Technical expertise
- Access to critical information

Each component can be seen as a hurdle on the path to a successful scenario or event (see diagram below). The Technical Feasibility Score is determined by selecting the lowest component rating, across all components, thus reflecting the highest hurdle or biggest constraint on the feasibility of the given scenario or event; the lower the feasibility, the higher the hurdle.

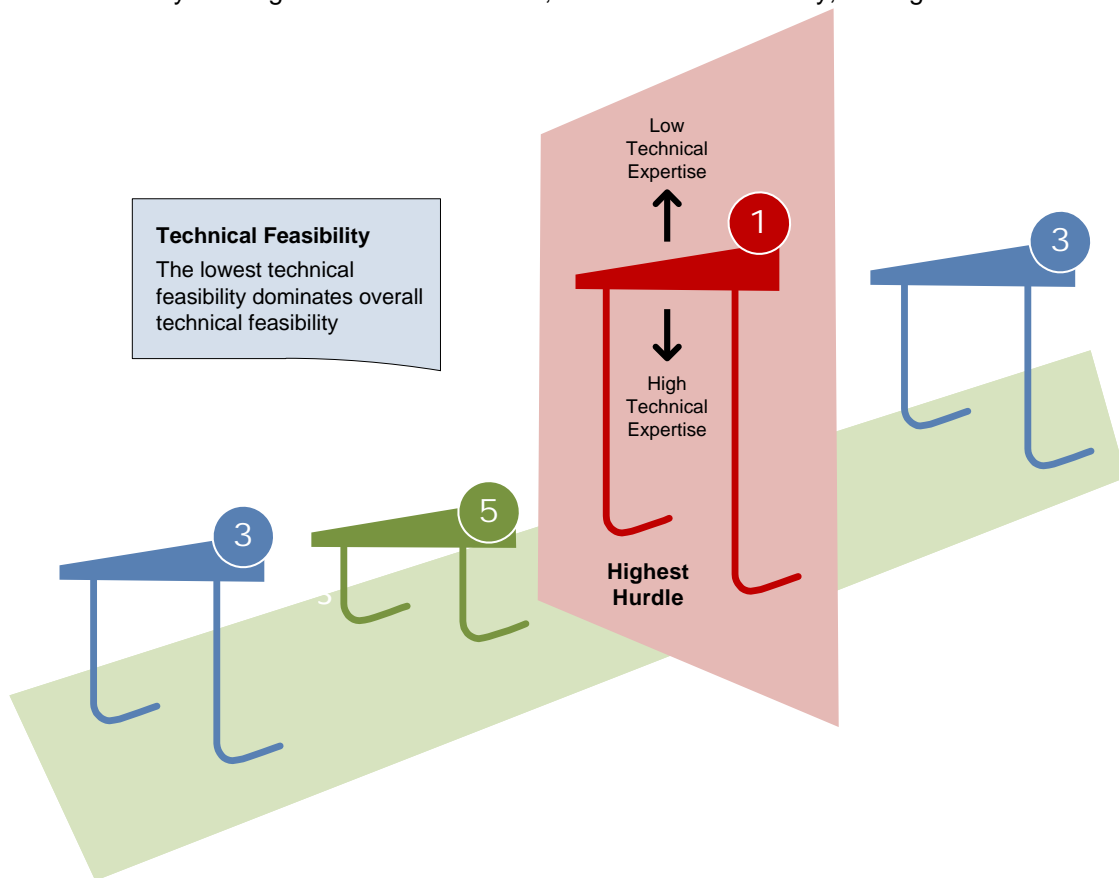


Figure 6. Technical Feasibility

The same principle applies when comparing the overall capability rating to the intent rating. Again, the lower of the overall capability and intent ratings would determine the overall likelihood.

Each of these feasibility components is rated based on a “verbal descriptor scale”, as shown in the table below:

Feasibility					
Scoring:	Material	Equipment	Access to the Target or System	Technical Expertise	Access to Critical Information
0	Almost impossible to produce or acquire	Requires custom designed and/or state of the art manufactured equipment	Almost impossible	Requires controlled advanced specialized technical training	Almost impossible
0.5-1	Extremely difficult to produce or acquire	Requires custom designed and/or controlled manufactured equipment	Extremely difficult	Requires advanced specialized technical training	Extremely difficult
1.5-2	Very difficult to produce or acquire	Requires specialized equipment	Very difficult	Requires advanced technical training	Very difficult
2.5-3	Difficult to produce or acquire	Requires some specialized equipment components	Difficult	Requires some advanced technical training	Difficult
3.5-4	Easily produced or acquired	Requires standard laboratory and/or manufacturing equipment	Accessible	Requires minimal technical training	Easily accessible
4.5-5	Readily available	Requires no specialized equipment	Very accessible	Requires very low technical training	Readily accessible
Ratings:					

Minimum Feasibility Score:

The technical feasibility score is given by the lowest rating across the various components, which is a reflection of the feasibility within a given scenario.

Enabling Capability

Once the technical feasibility has been assessed, the organizational and support capabilities of various malicious actors are assessed relative to whether they are sufficient to enable the level of technical feasibility assessed for the malicious scenario, as shown in the table below:

Scenario-Specific Enabling Capabilities		
Scoring:	Organization / Command, Control and Communications Intelligence (C3I) (organizational structure and ability, human resources, C3I functions)	Support & Logistics (funding, infrastructure)
0	Organization or individual has little-to-no organizational/C3I capability, only sufficient to enable a much lower level of technical feasibility than the one assessed for this scenario.	Organization or individual has little-to-no support & logistics capability, only sufficient to enable a much lower level of technical feasibility than the one assessed for this scenario.
0.5-1	Organization or individual has limited organizational/C3I capability, only sufficient to enable a lower level of technical feasibility than the one assessed for this scenario.	Organization or individual has limited support & logistics capability, only sufficient to enable a lower level of technical feasibility than the one assessed for this scenario.
1.5-2	Organization or individual has some organizational/C3I capability to enable the level of technical feasibility assessed for this scenario.	Organization or individual has some support & logistics capability to enable the level of technical feasibility assessed for this scenario.
2.5-3	Organization or individual has demonstrated organizational/C3I capability to enable the level of technical feasibility assessed for this scenario.	Organization or individual has demonstrated support & logistics capability to enable the level of technical feasibility assessed for this scenario.
3.5-4	Organization or individual has demonstrated organizational/C3I capability to enable a higher level of technical feasibility than the one assessed for this scenario.	Organization or individual has demonstrated support & logistics capability, sufficient to enable a higher level of technical feasibility than the one assessed for this scenario.

4.5-5	Organization or individual has demonstrated organizational/C3I capability to enable a much higher level of technical feasibility than the one assessed for this scenario.	Organization or individual has demonstrated support & logistics capability, sufficient to enable a much higher level of technical feasibility than the one assessed for this scenario.
Ratings:		

Minimum Enabling Capability Score:

Once again, the minimum scoring across the two enabling capability components is retained. This rating is used further to determine an overall capability score, together with the technical feasibility rating. The technical feasibility rating will be adjusted based on the assessed level of enabling capability. This will reflect whether any malicious actors potentially behind an attack such as the one described in the scenario have adequate organizational and support capability components to enable the technical capability requirements to carry it out. The adjustment will consider a “baseline” or threshold level of enabling capability required to carry out the scenario, given the assessed technical feasibility, and will modify the feasibility assessment negatively, if the enabling capability level is found insufficient compared to the baseline, or positively, if the enabling capability level is found more than sufficient compared to the baseline. An example of modifier values associated with the various enabling capability levels is shown below:

Combined Capability Rating ($\min(C_{org/C3I}, C_{support/logistics})$)	Associated modifier applied to Feasibility Rating
0	-3
0.5	-2.5
1	-2
1.5	-1.5
2	-1
2.5	-0.5
3	0
3.5	0.5
4	1
4.5	1.5
5	2

Overall Capability Score

The overall capability score is obtained by combining the technical feasibility score with the enabling capability score, as described in the paragraph above.

Intent

The intent judgment is meant to provide an indication of an individual's or group's motivation to carry out the scenario being assessed. The intent is rated using the following table:

Scoring	Intent
0	There is little to no evidence of an individual's or a group's intention .
0.5-1	There is limited evidence of an individual's or a group's intention .
1.5-2	There is at least some evidence of an individual's or a group's demonstrated intention .
2.5-3	There is at least one documented case of evidence of an individual's or a group's demonstrated intention .
3.5-4	There are several documented cases of evidence of an individual's or a group's demonstrated intention .
4.5-5	There are ample documented cases of evidence of an individual's or a group's demonstrated intention .

	Intent Rating
--	----------------------

Overall Likelihood for Malicious Threats

The overall Likelihood assessment will reflect the lowest of the ratings for Intent and Capability, following again the "weakest link" principle.

Calibration of malicious and non-malicious likelihood assessments

A calibration process was developed following the 2010-2011 AHRA cycle that sought to establish a correspondence between the likelihood of malicious events and the non-malicious frequency scale. The process sought to make the likelihood assessment for malicious events compatible with frequency-based estimates such as: "once every 10 years", or equivalently,

“10-1 times per year”. This was accomplished via a set of hypothetical “reference” scenarios that, by design, were intended to describe events ranging from very frequent (such as once per year) to very rare (once per 100,000 years). Nine reference scenarios were developed, to fit into three broad categories: high, medium and low likelihood. Each likelihood category was represented by a “triplet” of three reference scenarios, which were ranked relative to each other by doing a pair-wise comparison within the triplet. The likelihood estimate, on the non-malicious scale, of at least one of the hypothetical reference scenarios in the triplet was required, which was accomplished through consensus among a group of intelligence experts, given assumptions about the feasibility and capability components, and the intent. Once one scenario was “pinned” to the frequency scale, the other two followed, by virtue of their relative position within the triplet. The process was repeated for each of the three “triplets” of reference scenarios covering the same likelihood category; at the end, all nine reference scenarios were positioned on the frequency scale, in other words, their likelihood was described in terms that are compatible with frequency-based estimates. The set of nine hypothetical scenarios served as reference points by which the likelihood of actual malicious scenarios was then estimated, by assessing their likelihood relative to the likelihood of one or more of the scenarios in the reference set. The process was piloted during the 2011-2012 AHRA cycle and proved successful.

Non-Malicious Hazards

Likelihood estimates for non-malicious hazards can be based either on historical frequencies, predictive models, or expert judgment. When using historical frequencies, the likelihood estimate can be modified if an increasing or decreasing trend is expected compared to historical conditions.

Table 1, below, represents the level of detail expected in likelihood estimates. Within the scoring approach, all likelihood estimates are converted to a five-year timeframe for occurrence.

It is important to consider that global climate change has created conditions where natural disasters are changing in frequency and magnitude. While some natural events may not have been experienced in the past, they may be more common today or in five years. An approach that takes into consideration differing situations and foresight will allow for a more robust assessment of non-malicious likelihood.

Similarly, for health-related matters, as global trade and tourism continue to expand, increased numbers of Canadians and Canadian products will have the potential to be exposed to unfamiliar or uncommon diseases. International travel and commerce will also help spread disease more quickly than historically encountered creating a situation that must also be considered for accurate assessment.

Estimated frequency, once every X years, where X is:
100,000 (years)
30,000
10,000
3,000
1,000
300
100
30
10
3
1

4

Step 4: Risk Evaluation

■ OBJECTIVE OF RISK EVALUATION

Risk Evaluation is the process of comparing the results of Risk Analysis with risk criteria to determine whether a risk and/or its magnitude is/are acceptable or tolerable. The purpose of Risk Evaluation is to support the development of sound recommendations about risks that may need treatment or may be identified as priority for treatment. Risk Evaluation also provides a baseline of the risks without any management measures.

■ INPUTS REQUIRED

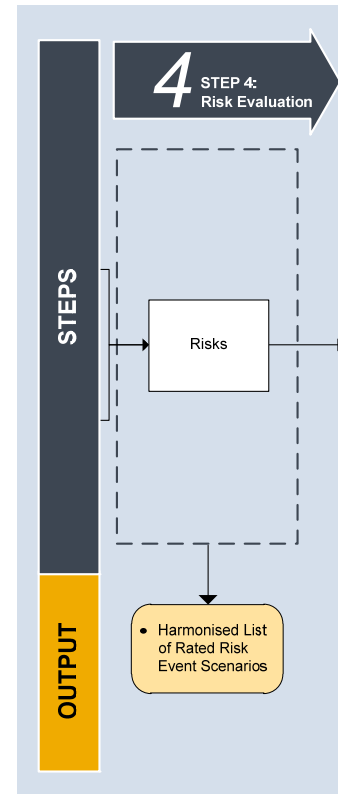
The information inputs for the Risk Evaluation process are:

- The likelihood of the realisation of the hazards/threats associated with the risk event, with an associated confidence level and assumptions and/or justifications, as applicable.
- Assessments of the impact for the risk event in terms of each of the primary impact categories, with associated confidence levels and assumptions and/or justifications, as applicable.
- The total impact for the risk event, with an associated confidence level and assumptions and/or justifications, as applicable.
- Other information from the Risk Analysis Process, as supporting or background information.

■ TASKS AND ACTIVITIES EXPECTED IN RISK EVALUATION

The Risk Evaluation generally comprises the following steps:

- a. Determination of the risk magnitude (i.e. likelihood and impact) for the risk.
- b. Aggregation and consolidation of risk assessment results for all federal government risks into a whole-of-government AHRA.



- c. Production of selected AHRA information products and/or graphical representations of results.

As previously stated, Risk Evaluation is the process of comparing the results of the Risk Analysis against risk criteria to determine whether the level of risk requires further study. Existing controls, Risk Treatment and policies are considered when recommending mitigation measures/options. Risk criteria are based on internal and external contexts and can reflect the institution's values, objectives, resources and risk appetite (i.e. an over-arching expression of the amount and type of risk an institution is prepared to take or tolerate).

Risks can be ranked by comparing them in terms of their individual likelihood and impact estimates. The relative ordering of risk events based on their ratings can be shown graphically in a logarithmic risk diagram, risk-rating matrix or other forms of tabular or visual representations. The one most commonly used is the risk matrix which normally plots the likelihood and impact on the x- and y-axes (the measured components of risks). The three figures below provide examples of options for visualizing the Risk Analysis results.

In a risk diagram such as Figure 7, a clustering of risks can be shown. Such a plot can help risk managers and decision-makers establish acceptable or intolerable risk levels, and identify their respective courses of action.

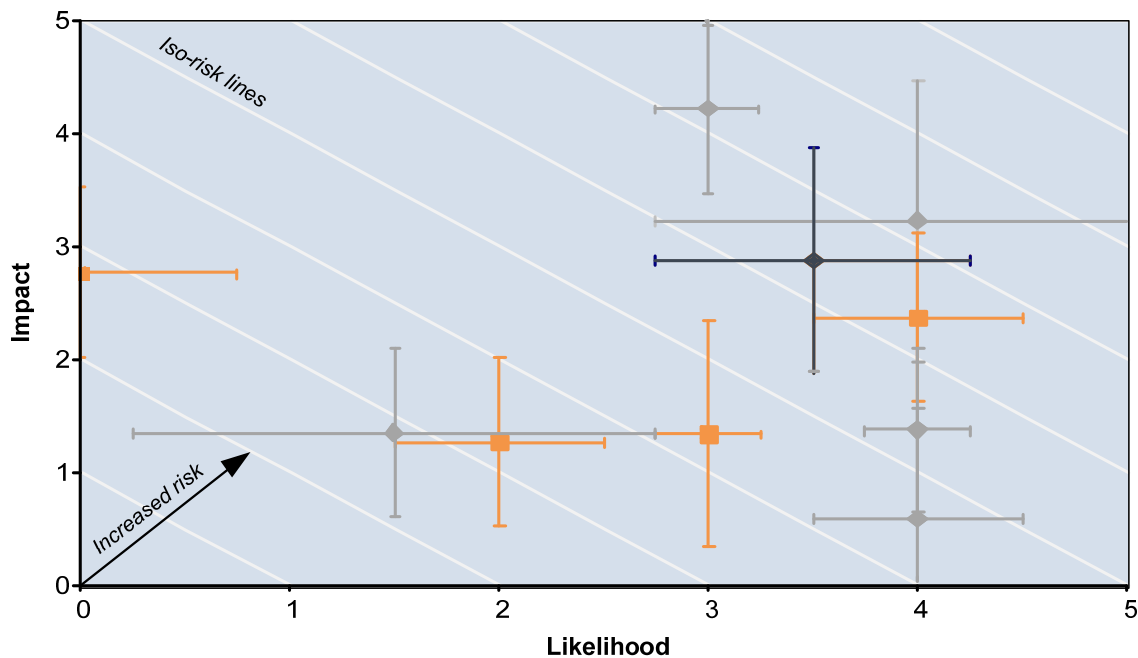


Figure 7. Example of a Risk Event Rating Scatter Plot

Figure 8 shows an example of how multiple scenarios or scenario variants can be compared across impact categories, which provides a picture of the areas most affected by the risk scenario being studied.

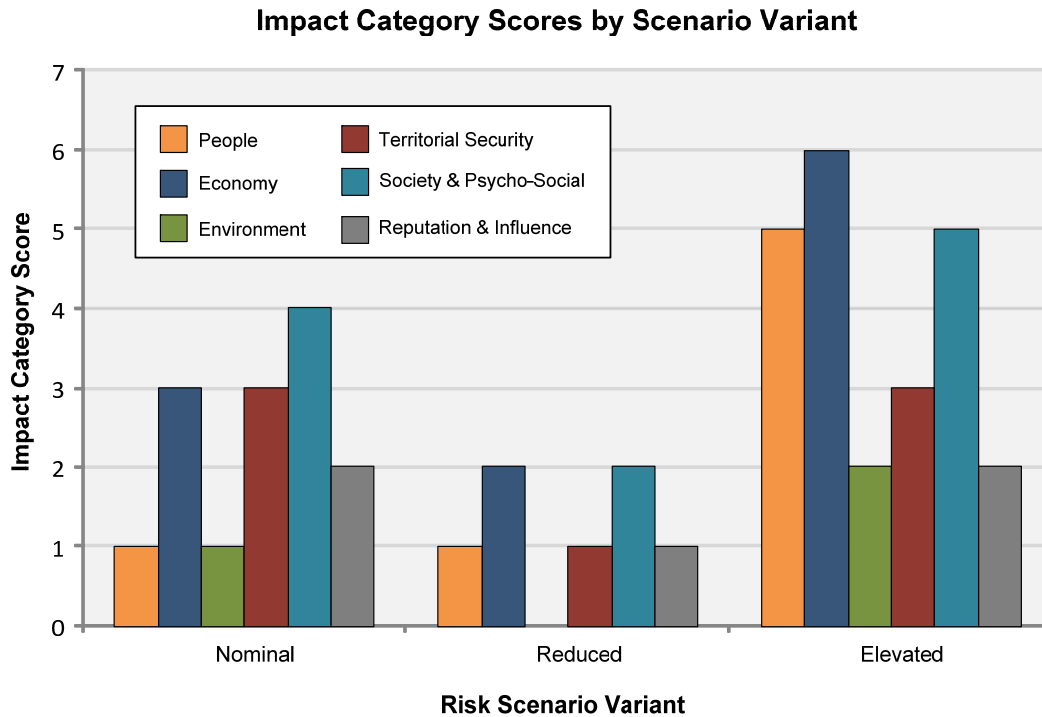


Figure 8. Example of an Impact Rating Plot by Impact Category and Risk Scenario Variant

Based on a risk diagram or rating matrix, a clustering of risks can be shown, leading to recommendations and/or decisions on the relative ordering of risk events based on their ratings. Such a plot can help risk managers and decision-makers establish acceptable or intolerable risk levels, and identify their respective courses of action. Risk mitigation options (risk reduction) and even risk tolerance levels could also be represented graphically to enhance risk communication.

■ OUTPUTS FOR RISK EVALUATION

The information outputs from the Risk Evaluation process are:

- Risk Evaluation results or list of rated risk event scenarios (in the form of a report and/or a presentation).
- Various AHRA information products and graphical representations of the analysis and evaluation data (AHRA information products could include the consolidated likelihood and impact data for each scenario in a risk fiche).
- Various risk indicators such as whole-of-government or institutional thresholds for risk aversion and/or risk acceptance may be derived from the outputs of Risk Evaluation.

5

Step 5: Risk Treatment

■ OBJECTIVE OF RISK TREATMENT

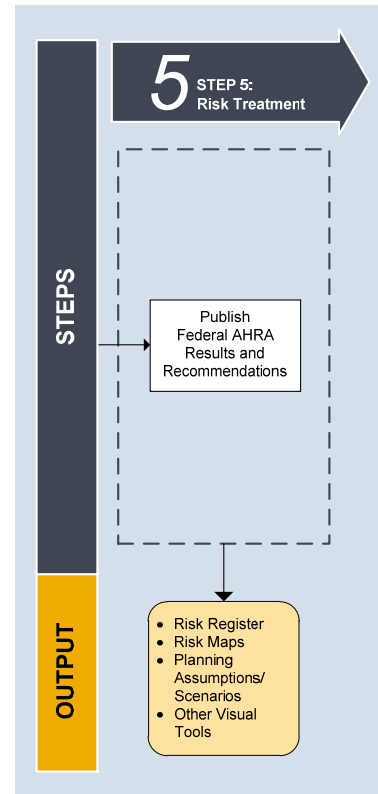
Risk Treatment is the process of developing, selecting and implementing risk controls measures.

Step 5 of the AHRA methodology is the development of recommendations for Risk Treatment options, from a risk analyst perspective, based on the results of the Risk Evaluation and other considerations. These recommendations are meant to inform risk managers and decision-makers in their formulation of Risk Treatment options.

■ INPUT REQUIRED

The information inputs to Risk Treatment are the outputs of the Risk Evaluation:

- Risk Evaluation results or list of rated risk event scenarios (in the form of a report and/or a presentation).
- Various AHRA information products and graphical representations of the analysis and evaluation data (AHRA information products could include the consolidated likelihood and impact data for each scenario in a risk fiche).
- Various risk indicators such as whole-of-government or institutional thresholds for risk aversion and/or risk acceptance may be derived from the outputs of Risk Evaluation.



■ TASKS AND ACTIVITIES EXPECTED IN RISK TREATMENT

Scope of Risk Treatment

As previously stated, Risk Treatment is the process of developing, selecting and implementing risk control measures. Treatments that deal with negative consequences are also referred to as risk mitigation, risk elimination, risk prevention, risk reduction, risk repression and risk correction. Treatment options can include, but are not limited, to:

- Avoiding the risk by deciding not to continue with the activity that gives rise to the risk.
- Removing the source of the risk.
- Changing the nature or magnitude of the likelihood.
- Changing the consequences.
- Reducing exposures or vulnerabilities.
- Sharing the risk with another party.
- Retaining the risk by choice.

Risk Treatment options can be prioritized by considering a number of factors, including institutional obligations, political impetus, humanitarian grounds, cost, etc. and by considering risk severity, risk tolerance, effectiveness of Risk Treatment measures, cost and benefits, the horizontal nature of the risk, and existing constraints. These treatment options, forming recommendations, would be used to develop the Risk Treatment step in the risk management or emergency management cycle.

Risk Treatment options should be assessed, to better understand if residual risk levels are tolerable to an institution. If they are not, a new Risk Treatment should be considered and its effectiveness, assessed. Risk tolerance levels within an institution should be promptly identified during the AHRA process, as early as when Setting the Context.

Recommending Risk Treatment Avenues to Senior Management

In recommending Risk Treatment options, the risk analyst must do so based on the results of the Risk Analysis and Risk Evaluation at hand, and be mindful of the level of inherent uncertainty and reliability of the treated data. In certain risk areas that are data deprived (e.g., low frequency and potentially high consequence events), qualitative judgements will likely be the source of data, with their own associated uncertainty and reliability. It remains important to qualify any recommendation with a clear statement on those aspects, including the source of the data, the reliability of the data, and the uncertainty.

Another aspect, in formulating recommendations, is the notion of risk reduction and the ability to demonstrate the potential for risk reduction. This is particularly difficult due to the fact that risk reduction metrics are very difficult to isolate and measure. This is especially true for speculative cases where there is no case history.

In most cases, the risk analyst should endeavour to communicate (verbally, in text and in graphics) the results of the Risk Analysis and Risk Evaluation in a way that will help risk managers and decision-makers isolate their own options. By using a framework process that is repeatable and offers the ability to consider additional elements (i.e., new impact categories and factors), it will open the possibilities for further exploration and analysis; and possibly address issues such as uncertainty.

As recommendations form part of the overall risk assessment, they must be captured in such a way as to facilitate tracking throughout successive iterations of the risk assessment process. The following section will discuss the aspect of data management.

■ OUTPUTS FOR RISK TREATMENT

The information output from Risk Treatment is a set of recommendations for Risk Treatment options, from a risk analyst perspective, based on the results of the Risk Evaluation and other considerations. These recommendations are meant to inform risk managers and decision-makers in their formulation of Risk Treatment options.

Data Management

■ GENERAL

A major shortfall in many risk assessment processes is the lack of adequate data management capability and associated resources. Since risk assessments are conducted periodically and across many federal government institutions, domains and entities, the satisfactory management of the related data over time becomes crucial. It is particularly so when trying to establish the effectiveness of risk reduction measures and their impact over time. In the case of the AHRA, each federal government institution is encouraged to strive for the implementation of a number of data management options ranging from a formatted spreadsheet to allow for the capture of risk ratings, all the way to a risk register to capture all the information meaning from each risk assessment steps taken to fully understand risks. It is understood that these techniques and tools will evolve over time through exploration and implementation of the federal AHRA every year. Simplicity will be crucial in ensuring that the data management principles and practices can be universally applied.

It is important to note that these data management tools, their relative configuration and the software programs which will be employed to implement them are subject to change as the AHRA methodology and the understanding of optimal means for its implementation also evolve over a period of time.

Other data management tools will be explored to enhance the accessibility to, analysis and visualization of risk data. These may include the use of geo-referenced risk maps and other graphical options.

■ AHRA RISK REGISTER AND DATABASE

The results of the AHRA will be compiled by PS in a report and inventoried in an electronic risk register, using Excel or a similar software program. The AHRA risk register will inventory the pertinent information linked to each assessed risk. The risk register will typically describe each risk event, capture the likelihood that it may occur, list possible consequences if it does occur, provide a relative ordering of risk events based on their ratings, and identify proposed treatment strategies. It can be a useful tool for managing and addressing risks, as well as facilitating risk communication to stakeholders. A risk portfolio or profile can be created from the register, helping to compile common risks in order to assess interdependencies and to provide a relative order of risk events based on their ratings by groups. The risk register is meant to provide a lasting record and will be adjusted as risk assessment results change.

This register will be maintained by PS with data from each successive cycle of risk assessment. The register will permit easy access to the risk data for analysts and decision-makers.

The AHRA register will catalogue the data relevant to the current AHRA cycle and will also hold the data from previous AHRA cycles, to be used for:

- Tracking the progress of risks and risk assessments over time.
- Analysis of trends in emerging risks.
- Lessons-Learned analyses.
- Information on the AHRA Community of Practice for the federal community.

■ DATA MANAGEMENT AND SENSITIVITY

Data will be managed in accordance with its sensitivity and classification, as established by an injury test. It will also be handled according to applicable legislation and policies relating to security and information management, including the GC security policy and the information management policy.

Data will be retained and maintained for historical value, for government archives, for trend analysis and to support risk management activities.

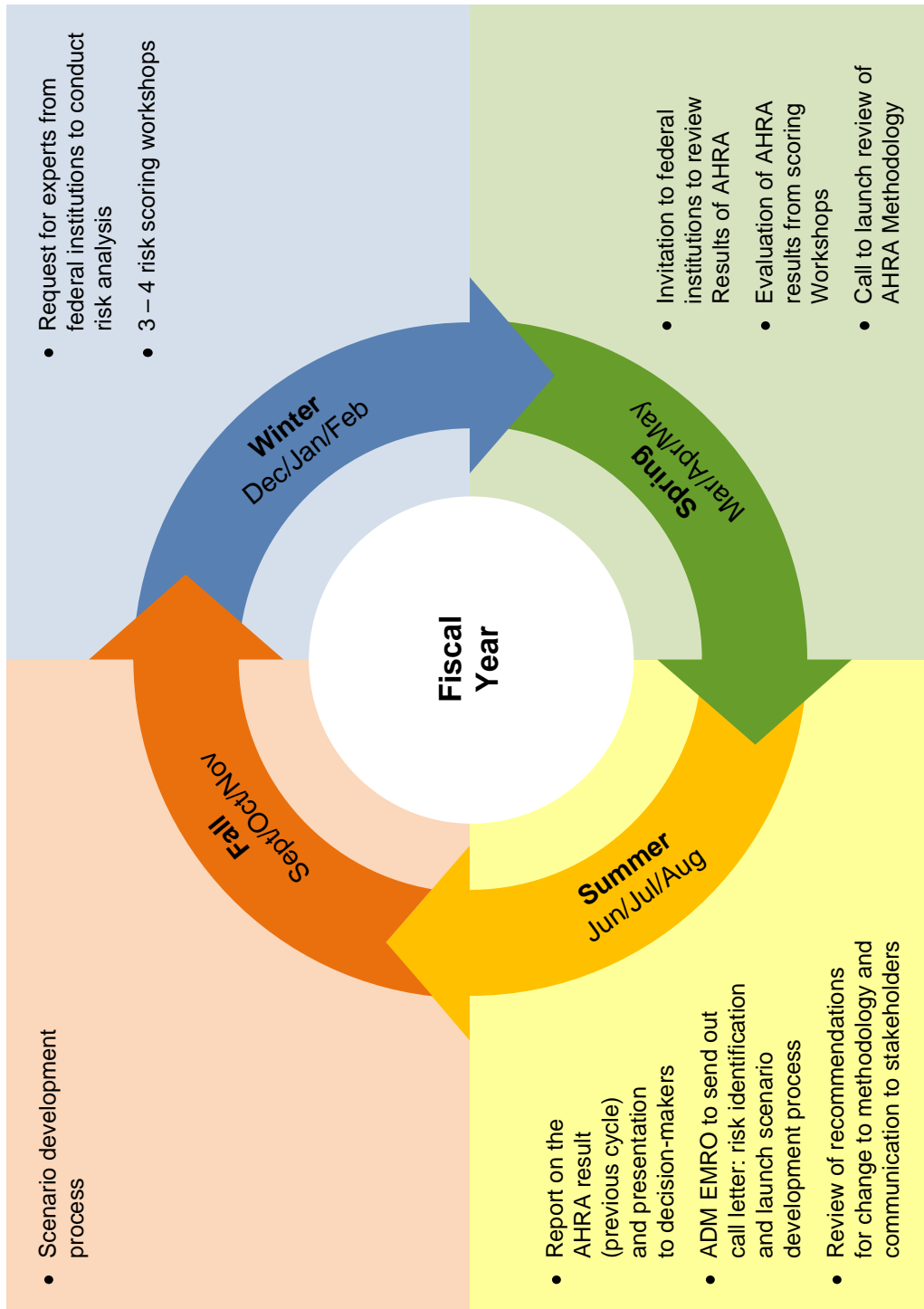
Accumulating Knowledge and Continuous Improvement of AHRA

The AHRA process will be iterative, in recognition of the fact that the array of risks facing Canada as well as our level of knowledge about these risks is constantly changing. For example, development along rivers can increase the potential impact of flooding, the introduction of a vaccination program may decrease the impact of an infectious disease outbreak scenario, and surveillance activities may identify an emerging source of malicious activity. These changing conditions can prompt updated risk assessments, and the evolving risk picture can be tracked over time.

Once the standardized methodology has been applied by the various federal government institutions, regular updating of the outputs based on changing conditions would be a relatively less intensive undertaking. In addition, as new information becomes available, it is expected that each round of risk assessment will be improved by incorporation of more accurate data, expertise and experience gained during previous iterations of the assessment process.

Finally, international work performed by the GC in relation to the sharing of leading risk assessment and risk management practices will continue to make the AHRA methodology and its process evolve, emphasizing on the federal government's commitment towards continuous improvement of the AHRA.

Annex 1 – AHRA Business Cycle



Annex 2 – SWOT and PESTLE Analysis

A **SWOT analysis** is a planning tool used to evaluate the Strengths, Weaknesses, Opportunities and Threats of an organization as they relate to a set outcome.

- **Strengths** — attributes of the organization that are helpful to achieving the objective(s).
- **Weaknesses** — attributes of the organization that are harmful to achieving the objective(s)
- **Opportunities** — *external* conditions that are helpful to achieving the objective(s)
- **Threats** — *external* conditions which could do damage to the objective(s)

The analysis involves specifying the objectives of the initiative and identifying the internal and external factors that are favourable and unfavourable to achieving them. The first step to a SWOT analysis is therefore to define the desired “end state” or goal. In the case of emergency management planning, this “end state” is to have an effective institutional emergency management program.

Below are simple rules for a successful SWOT analysis:

- Be realistic about the strengths and weaknesses of the organization.
- Distinguish between where your organization is today and where it could be in the future.
- Be specific.
- Keep it short and simple.

Table 1: Sample SWOT table

	Helpful (to achieve the goals)	Harmful (to achieve the goals)
Internal Origin (attributes of the organization)	Strengths • • • • •	Weaknesses • • • • •
External Origin (attributes of the environment)	Opportunities • • • • •	Threats • • • • •

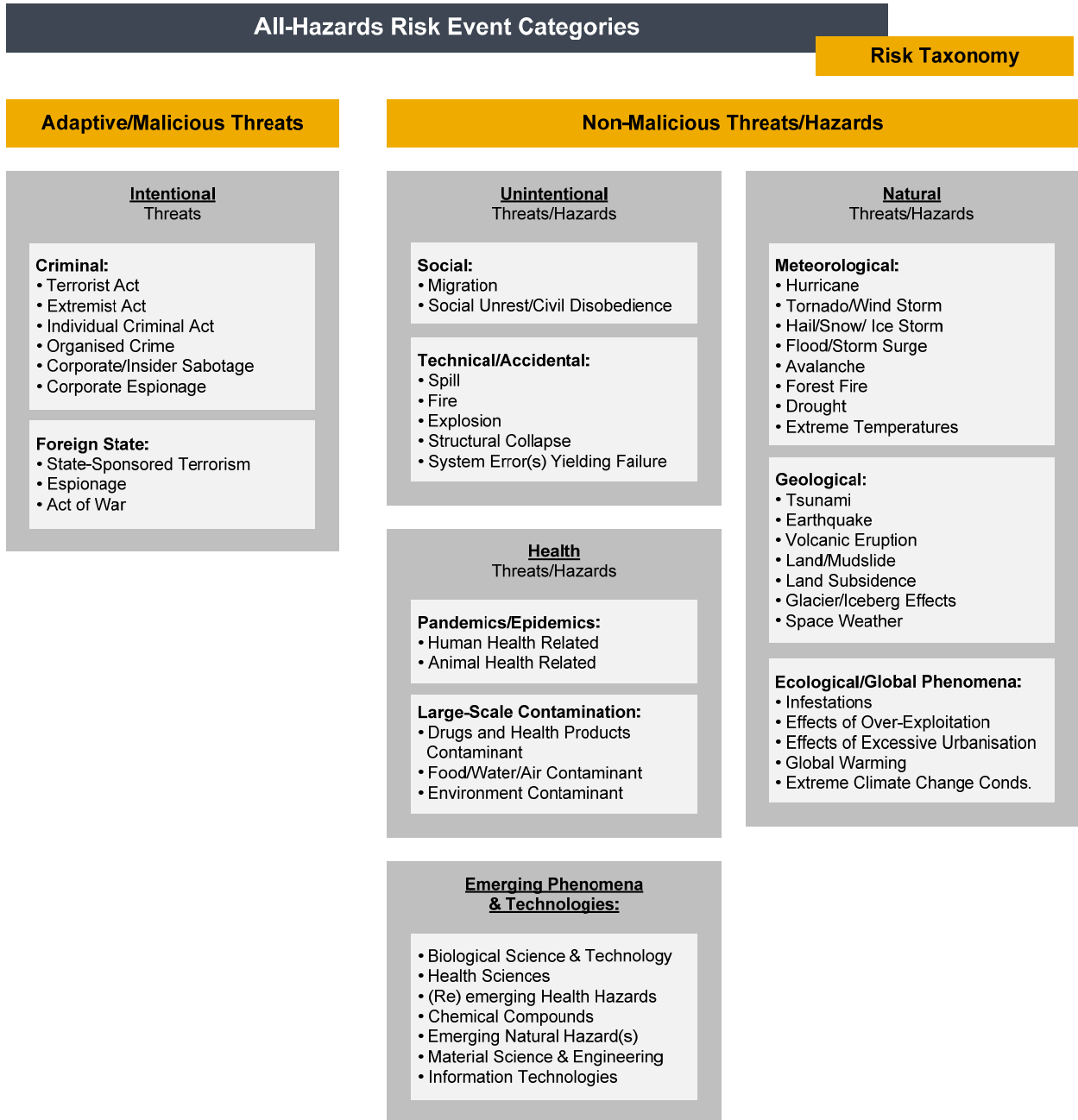
In conducting a PESTLE (Political, Economic, Social, Technological/Technical, Legal, Environmental) analysis, first list external PESTLE factors that may impact on an institution. This may require brainstorming and expert advice. Then identify the implications of each PESTLE factor for an institution. Lastly, decide on the importance of the implications of the external factors—rank or rate them.

Table 2: Sample PESTLE analysis table

(PESTLE = Political, Economic, Social, Technological/Technical, Legal, Environmental)

PESTLE element that may impact EM planning	Timeline (short < 1 yr, medium 2-3 yrs, long term 3+ years)	Impact (low, medium and high) and relevance	Internal or external to institution	Action (if applicable)

Annex 3 – AHRA Risk Taxonomy



Please indicate the level of CLASSIFICATION of the scenario here

Annex 4 – Risk Event Scenario Description Template

RISK EVENT SCENARIO DESCRIPTION	
Risk event name/title:	<p><i>Baseline description used to evaluate both likelihood and impact.</i></p> <p><i>In areas where likelihood and impact should be considered and scored, text should be marked with (L) for likelihood and (I) for impact. This is suggested for text that is embedded in descriptions and not obvious to the reader.</i></p>
Applicable risk code(s) for the principal constituent threat or hazard (including the category(ies) of the standard AHRA risk taxonomy affected):	<i>Please refer to the AHRA taxonomy, Annex 3.</i>
Applicable risk code(s) for the secondary threat(s) or hazards (s) (including the category(ies) of the standard AHRA risk taxonomy affected):	<i>This field is optional and related to risks that have secondary effects, such as floods that occur after a hurricane.</i>
Primary department (for response):	<i>The Federal Emergency Response Plan (2011) describes the primary department as a federal government institution with a mandate related to a key element of an emergency. Several federal government institutions may be designated as primary departments, depending on the nature or severity of the emergency.</i>
Supporting department (for all EM components):	<i>According to the Federal Emergency Response Plan (2011), a supporting department is a federal government institution that provides general or specialized assistance to a primary department in response to an emergency.</i>
Key information sources for the risk event scenario description - please tag the information as <u>Unclassified</u> (U) or <u>Classified</u> (C; S; TS; TS SA):	<p><i>Identification of supporting documentation is important, especially in cases where qualitative and/or quantitative data supports scores decided upon during the risk scoring workshop. This ensures credibility and legitimacy of risk scores. In addition, reference can be made back to decision points at any point in time and by anyone.</i></p> <p><i>Clearly identify unclassified and classified information, for ease of reference when assessing likelihood components for malicious threats.</i></p>

RISK EVENT DESCRIPTION	
Description (context, setting, cause, source, nature, scale), of the risk event:	<p><i>The description entered here must be plausible in that factual information would support such an occurrence. The considered time-frame from which events are considered in the AHRA process is short-term (within the next 5 years) threats/hazards. Long-term threats/hazards (that span 5 – 25 years into the future) are not currently considered in the AHRA.</i></p> <p><i>Background information leading up to the risk event provides context to the scenario without making broad assumptions which may skew results during the risk scoring workshop. Information inserted in this area should take into consideration the assessment of the following impact categories: People, Environment, Economic, Territorial Security, Canada's Reputation and Influence and Society and Psycho-Social.</i></p>
Description of the lead-up to the incident, consisting of the (underlying) cause and any underlying insidious process:	<i>This section is optional.</i>
Geographical considerations (location, geographical extent, region):	<i>This section is optional. Geographical coordinate system (latitudinal and longitudinal lines), country, province, territory or region is to be included in this section.</i>
Natural environment:	<i>Relevant physical or environmental characteristics are inserted in this area facilitating the assessment of the Environmental impact category.</i>
Meteorological conditions:	<i>Relevant meteorological condition(s) that influence the outcome of the scenario should be inserted in this area. If applicable variants may be inserted in this area.</i>
Seasonal:	<i>This section is optional and left to the discretion of the scenario developers. Dependant on the scenario, seasonal changes may influence the outcome of assessment of a particular risk.</i>
Hazard characteristics:	<i>Characteristics of chemical, biological, radiological and/or nuclear agent(s) involved in the scenario are inserted in this area. Elements captured should relate to: toxicity, transmissibility, behaviour, fate and persistency to indicate a hazard severity and duration.</i>

<p>Nature and vulnerability of the affected area (context, population density, degree of urbanisation, key infrastructure, economic considerations, political considerations, etc.):</p>	<p><i>This area is important to note as it provides relevant information from which subject matter experts score risks. Population density, degree of urbanisation and key infrastructure influence the People and possibly the Society and Psycho-Social impact category.</i></p> <p><i>Economic considerations affect the Economic impact category.</i></p> <p><i>Political, geographical and territorial considerations influence Canada's Reputation and Influence and Territorial Security impact categories.</i></p>
<p>Any other relevant assumptions made in describing the risk event scenario:</p>	<p><i>If assumptions relating to the risk event description can be identified or isolated they should be inserted in this area.</i></p> <p><i>Although this field is considered optional, the information may still be required in the risk scoring tool.</i></p>
<p>Uncertainty or variability in the risk event description:</p>	<p><i>If there are areas of uncertainty or unpredictability, it should be inserted in this area.</i></p> <p><i>Although this field is considered optional, information may be required in the risk scoring tool.</i></p>
<p>Other relevant information, notes or comments:</p>	<p><i>Any other relevant information relating to the risk event description should be identified in this area.</i></p>
<p>LIKELIHOOD ASSESSMENT</p>	
<p>Time period/time horizon during which the risk event might be realised:</p>	<p><i>The translation of the data in likelihood of occurrence on a yearly basis will be done in the risk scoring tool.</i></p>
<p>Uncertainty in the likelihood assessment:</p>	<p><i>Unknown factors which would influence the likelihood assessment should be inserted in this area.</i></p>
<p>Other relevant information, notes or comments:</p>	<p><i>Any other relevant information relating to the primary likelihood assessment should be inserted in this area.</i></p>
<p>IMPACTS/CONSEQUENCES ASSESSMENT</p>	
<p><u>Impact categories: nature and scale</u></p>	
<p>1. People:</p>	<p><i>Specific indicators have been selected to evaluate the effect of hazards and threats on people. Estimated figures should be inserted in this box e.g. the number of fatalities, serious injuries, etc.</i></p>
<p>2. Economy:</p>	<p><i>Based on the Department of Finance Canada's criteria of risks and hazards on the economy. This impact category captures direct and indirect losses. Direct losses are immediate economic damage as a result of a risk event. Losses are measured based on repair or replacement costs. Indirect losses refer to the flow of goods and services which will not be produced as a result of damage to productive assets and infrastructure.</i></p>

3. Environment:	<i>Based on the indicators developed by Public Safety Canada, in close collaboration with Environment Canada, on the effects of hazards and threats on the environment.</i>
4. Territorial security:	<i>Based on indicators that capture conditions in which there is a loss in the ability of the Government of Canada to secure the territory or the border and to secure the safety of citizens.</i>
5. Canada's reputation and influence:	<i>Based on expert assessment of the potential international reaction to an emergency event occurring in Canada, or involving Canadians abroad.</i>
6. Society and psychosocial:	<i>Based on indicators regarding public outrage and public anxiety, as well as social actions, such as protests, civil disturbances or vandalism, can be provoked by a risk event.</i>
Uncertainty in the impacts/consequences assessment:	<i>Uncertainty, unpredictability or areas of doubts relating to the impacts/consequences assessment should be inserted in this area.</i>
Other relevant information, notes or comments:	<i>Other relevant information relating to the impacts/consequences assessment should be inserted in this area.</i>
PRELIMINARY RISK TREATMENT PLANNING	
Baseline risk treatment plan (treatment actions, timeframe(s), readiness, etc.):	<i>This area is optional. Federal institutions may choose to fill it out after the completion of the risk scoring workshop. This area would assess the capacity of the Emergency Support Functions (ESF).</i>
Risk treatment measures already in place	<i>As the AHRA takes into consideration mitigation measures in place when assessing the likelihood of occurrence and the impacts of a risk, (all or some of) these measures should be clearly captured somewhere in the risk event scenario template. This will force divisions which "own" mitigation measures (usually Program divisions) to share their information with EM divisions (usually under GOC, Operations or Corporate Branches).</i>
Degree to which the risk (likelihood, impacts) can be reduced by Risk Treatment.	<i>This area may be completed by departments and agencies. This area would assess the capacity of the ESF.</i>
Additional risk treatment resources required.	<i>Additional information relating to risk treatment may be inserted in this area.</i>
Other relevant information, notes or comments:	<i>Other relevant information relating to the impacts/consequences assessment should be inserted in this area.</i>

Annex 5 – Rating of the Impact on Canada’s Reputation and Influence

Level	Actions	Political Relations	Non-Political Relations
0 – 1.0 Insignificant	<ul style="list-style-type: none"> - Canadian missions abroad are not affected. - Concentrated and short-lived condemnation of Canada/Government of Canada. - Canadians abroad are not affected. 	<ul style="list-style-type: none"> - Trade regulations slow Canadian exports into some minor foreign markets but are not stopped. - Canadian mission staff are not affected. - Bilateral trade agreements are temporarily suspended. - International working level meetings are delayed. 	<ul style="list-style-type: none"> - No effect on international events. - International travel is discouraged to one region within Canada by foreign governments.
1.0 – 2.0 Minor damage to Canadian reputation/prestige	<ul style="list-style-type: none"> - Canadian missions abroad receive threats but none materialise. - Short-lived condemnation of Canada internationally. - Threats issued to Canadians abroad but are unlikely. 	<ul style="list-style-type: none"> - Temporary trade bans and/or sanctions are imposed by a few minor trading partners. - Canadian mission staff exercises increased levels of vigilance. - Canadians delayed at border crossings but visas are not imposed. - Cancellation of meetings with minor international partners. - Minor trade agreements are temporarily suspended. 	<ul style="list-style-type: none"> - International conferences see fewer participants. - International travel is discouraged to several regions within Canada by foreign governments.
2.0 – 3.0 Significant damage to Canadian reputation/prestige	<ul style="list-style-type: none"> - Canadian missions abroad receive serious threats and are forced to close. - Significant condemnation of Canada and/or the Government of Canada internationally. - The Government of Canada encourages citizens not to travel due to threats abroad. 	<ul style="list-style-type: none"> - Trade bans and/or sanctions imposed by a few major and minor trading partners and trading blocs (United States, Japan, United Kingdom, China not included). - Canadian mission staff leaves host country due to insecurity. - Entry visa requirement imposed on Canadians travelling abroad. - Cancellation of bilateral meetings with major and minor international partners. - Minor trade agreements are cancelled. 	<ul style="list-style-type: none"> - International events are forced to reschedule. - International travel to Canada is discouraged by foreign governments.

Level	Actions	Political Relations	Non-Political Relations
<p>3.0 – 4.0</p> <p>Major damage to Canadian reputation/prestige</p>	<ul style="list-style-type: none"> - Attempted invasion, occupation, and/or destruction of Canadian missions abroad. - Wide-spread condemnation of Canada and/or the Government of Canada nationally and internationally. - Persistent threats to Canadians abroad. 	<ul style="list-style-type: none"> - Trade bans, embargoes, blockades and regulations imposed by some major and minor trading partners and trading blocs (United States not included). - Forced deportation of Canadian mission staff. - Denial of entry Visas to a number of countries or the imposition of extreme fees (e.g. United Arab Emirates Visa). - Temporary suspension of trade agreements such as the North American Free Trade Agreement. - Cancellation of major and minor international delegations to Canada or the rejection of Canadian delegations to other countries. 	<ul style="list-style-type: none"> - Significant international events are cancelled. - International travel to Canada is discouraged by international organizations such as the World Health Organization, the United Nations, American Government, etc.
<p>4.0 – 5.0</p> <p>Severe damage to Canadian reputation/prestige</p>	<ul style="list-style-type: none"> - Invasion, occupation, and/or destruction of Canadian missions abroad. - Wide-spread and continuous condemnation of Canada and/or the Government of Canada nationally and internationally. - Threats to Canadians abroad materialise. 	<ul style="list-style-type: none"> - Trade bans, embargoes, blockades and regulations imposed by major and minor trading partners and trading blocs (ex: United States, Japan, United Kingdom, China, etc.). - Deportation, arrest and/or killing of Canadian mission staff. - Denial of entry Visas to many countries. - Cancellation of Canadian trade agreements such as the North American Free Trade Agreement. - Canada is expelled from major security organizations such as the North Atlantic Treaty Organization. - Relations between the Government of Canada and foreign governments cease. - Public cancellation of major international visits (ex: State Visit by the President). 	<ul style="list-style-type: none"> - Refusal by major and minor Canadian partners to attend significant international events, such as the G8/20, Olympics, etc. - Cancellation of major international events in Canada by event organizers (ex: International Olympic Committee, International Federation of Association Football, la Francophonie, the Commonwealth, etc.). - Ban on international travel to Canada. - Ban on Canadians travelling overseas.

Annex 6 – Economic Category Assessment Tool – Direct and Indirect Economic Loss for Repair or Replacement

Direct Economic Loss (those involving damages to stock and assets occurring at the time of the disaster or soon after)

Buildings: e.g. industrial, commercial, institutional (plants, offices, recreational facilities, hospitals).	
Infrastructure: e.g. roads, water systems, irrigation, docks, terminals, other transportation, electric power, oil and gas engineering.	
Machinery and equipment: e.g. computers and software, agricultural and industrial machinery, furniture, trucks, etc.	
Residential housing and contents.	
Raw materials: e.g. coal, crude oil, natural gas, grains, animals and animal products, wood, ferrous, non-ferrous, non-metallic.	

Indirect Economic Loss (those involving a loss in the flow of production of goods and services which begin after the disaster and may extend through the reconstruction period)

Production or service provision losses due to the full or partial paralysis of productive activities: e.g. loss in industrial production due to damage to factories or shortages of raw materials/energy supplies, loss in agricultural production due to flooding or prolonged drought, loss of profits in the fishing and tourism industry following an oil spill, loss of production due to illness following a pandemic or listeriosis outbreak, etc.	
Higher operational costs due to destruction of physical infrastructure and inventories or losses to production or income: e.g. a ban on beef and cattle exports would first translate into higher maintenance costs due to rising inventory of live animals.	
Lost production due to linkage effects: e.g. destruction of a factory reduces the economic activities of suppliers who have no alternative markets.	
Additional costs incurred due to the need to use alternative means of production or provision of essential services: e.g. costs arising out of need to use alternative roads or transportation means due to damage to principal routes and critical infrastructures.	
Costs of required government response due to emergency and rescue operations: e.g. overtime payments to provide emergency assistance and repair critical infrastructure, additional expenses incurred to accommodate evacuees or for investigation, productivity loss induced from distortion of government resources and time allocation, etc.	

Mitigating Factors, if applicable (disasters sometimes involve indirect benefits or adjustments over the short-medium term which we may want to flag)

<p><i>Shift in consumer demand/spending:</i> e.g. following a BSE outbreak, demand for other types of meat may increase.</p>	
<p><i>Change in the productivity of assets:</i> e.g. following a flood, land productivity sometimes rises.</p>	
<p><i>Labour reallocation:</i> e.g. some workers could work longer or harder to make up for the shortfall in labour supply due to a pandemic outbreak.</p>	
<p><i>Reconstruction activity:</i> e.g. rebuilding activities after a hurricane.</p>	

Annex 7 – Glossary

Term	EM Vocabulary Approved Terms ⁷
Accident	<p>An unintended, unplanned and unexpected event that interrupts an activity and sometimes causes injury or damage.</p> <p>Note: Examples of accidents include transportation accidents, hazardous material spills or releases, fire and accidental explosions.</p>
All Hazards	<p>Referring to the entire spectrum of hazards, whether they are natural or human-induced.</p> <p>Note: For example, hazards can stem from industrial accidents, national security events or cyber events.</p>
All Hazards Approach	<p>An emergency management approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the incident, thereby permitting an optimization of planning, response and support resources.</p> <p>Note: The intention of an all-hazards approach is to employ generic emergency planning methodologies, modified as necessary according to the circumstances.</p>
All Hazards Risk Assessment	<p>The process of identifying, analyzing and evaluating risks using an all-hazards approach.</p>
Disaster	<p>An event that results when a hazard impacts a vulnerable community in a way that exceeds or overwhelms the community's ability to cope and may cause serious harm to the safety, health or welfare of people, or damage to property or the environment.</p> <p>Note: A disaster may be triggered by a naturally occurring phenomenon that has its origins within the geophysical or biological environment or by human action or error, whether malicious or unintentional, including technological failures and terrorist acts.</p>

⁷ In January 2011, PS initiated a project to standardize terminology used for emergency management, in partnership with terminologists from the Translation Bureau, Public Works and Government Services Canada (PWGSC). An EM vocabulary working group was created, to provide a departmental forum for standardization of key terms and their definitions in emergency management. Over 230 bilingual EM terms and associated definitions were standardized through the publication of the Emergency Management Vocabulary whose contents will become accessible in *TERMIUM Plus* (<http://btb.termiumpius.gc.ca/tpv2alpha/alpha-eng.html?lang=eng>). Only risk-related terms and definitions from this project are provided in the current annex.

Emergency	A present or imminent event that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment.
Emergency Management	The management of emergencies concerning all-hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery.
Frequency	The number of occurrences of an event in a defined period of time.
Hazard	A potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation.
Hazard Analysis	<i>To be defined.</i>
Hazard Identification	The process of identifying, characterizing and validating hazards. Note: Hazard identification looks at the type, the properties and the potential effects of hazards and is part of hazard assessment.
Likelihood	The chance of an event or an incident happening, whether defined, measured or determined objectively or subjectively.
Mitigation	Actions taken to reduce the impact of disasters in order to protect lives, property and the environment, and to reduce economic disruption. Note: Mitigation includes structural mitigative measures (e.g. construction of floodways and dykes) and non-structural mitigative measures (e.g. building codes, land-use planning and insurance incentives). Prevention and mitigation may be considered independently or one may include the other.
Natural Hazards	A source of potential harm originating from a meteorological, environmental, geological or biological event. Note: Examples of natural hazards include tornadoes, floods, glacial melt, extreme weather, forest and urban fires, earthquakes, insect infestations, infectious diseases
Probability	In statistics, a measure of the chance of an event or an incident happening.
Qualitative Assessment	A risk assessment method that assigns non-statistical values to risks. Note: A qualitative assessment produces narrative, descriptive or comparative information about risks. It can be based on limited information, numerically incomparable data or complex non-linear relationships.

Quantitative Assessment	A risk assessment method that assigns statistical values to risks.
Residual Risk	Risk that remains after implementing risk mitigation measures.
Resilience	<p>The capacity of a system, community or society to adapt to disruptions resulting from hazards by persevering, recuperating or changing to reach and maintain an acceptable level of functioning.</p> <p>Note: Resilience is built through a process of empowering citizens, responders, organizations, communities, governments, systems and society to share the responsibility to keep hazards from becoming disasters.</p>
Risk	The combination of the likelihood and the consequence of a specified hazard being realized; refers to the vulnerability, proximity or exposure to hazards, which affects the likelihood of adverse impact.
Risk Analysis	<p>A process to comprehend the nature of a risk and to determine its level.</p> <p>Note: Risk Analysis provides the basis for Risk Evaluation and decisions about Risk Treatment.</p>
Risk Assessment	The overall process of Risk Identification, Risk Analysis and Risk Evaluation.
Risk Avoidance	An informed decision to avert or to withdraw from, an activity in order not to be exposed to a particular risk.
Risk Communication	<p>The imparting, exchanging and/or receiving of clear, credible and timely information about the existence, nature, form, likelihood, severity, acceptability, treatment or other aspects of risk to improve decision-making in risk management.</p> <p>Note: Risk communication is carried out among public authorities, risk assessors, risk managers, the public and all other interested parties. It is intended to achieve a better understanding of risks and risk management.</p>
Risk Identification	The process of finding, recognizing and recording risks.
Risk Management	The use of policies, practices and resources to analyze, assess and control risks to health, safety, environment and the economy.
Risk Perception	<p>A stakeholder's view on a risk.</p> <p>Note: Risk perception reflects the stakeholder's needs, issues, knowledge, beliefs and values.</p>
Risk Profile	A description of an entity's existing management practices, common vulnerabilities, tolerance and key interdependencies concerning its particular risks, as well as an assessment of their relative likelihood, consequences and priority.

Risk Register	<p>A register that contains a list of identified risks and related information used to facilitate the monitoring and management of risks.</p> <p>Note: The risk register is generally in the form of a table, spreadsheet or database and may contain the following information: statement or description of the risk, source of risk, areas of impact, cause of the risk, status or action of sector network, existing controls, risk assessment information and any other relevant information.</p>
Risk Taxonomy	<p>A comprehensive and common set of risk categories that is used within an organization.</p>
Risk Tolerance	<p>The willingness of an organization to accept or reject a given level of residual risk.</p> <p>Note: Risk tolerance may differ across an organization, but must be clearly understood by those making risk-related decisions.</p>
Threat	<p>The presence of a hazard and an exposure pathway.</p> <p>Note: A threat may be natural or human-induced, accidental or intentional.</p>
Threat Assessment	<p>A process consisting of the identification, analysis and evaluation of threats.</p>
Vulnerability	<p>A condition or set of conditions determined by physical, social, economic and environmental factors or processes that increases the susceptibility of a community to the impact of hazards.</p> <p>Note: Vulnerability is a measure of how well prepared and equipped a community is to minimize the impact of or cope with hazards.</p>
Vulnerability Assessment	<p>The process of identifying and evaluating vulnerabilities, describing all protective measures in place to reduce them and estimating the likelihood of consequences.</p>