Emergency Management Planning Guide

2010–2011

Public Safety Canada Sécurité publique Canada

Canada

Cat. No.: PS4-87/2010E-PDF
ISBN: 978-1-100-16053-5

Printed in Canada

Preface

Threats and risks to Canadians and Canada are becoming increasingly complex due to the diversity of natural hazards affecting our country and the growth of transnational threats arising from the consequences of terrorism, globalized disease outbreaks, climate change, critical infrastructure interdependencies and cyber attacks. Emergencies can quickly escalate in scope and severity, cross jurisdictional lines, take on international dimensions and result in significant human and economic losses.

A key function of the Government of Canada is to protect the safety and security of Canadians. Federal government institutions are increasing their focus on emergency management (EM) activities, given the evolving risk environment in their areas of responsibility. EM can save lives, preserve the environment and protect property by raising the understanding of risks and by contributing to a safer, more prosperous and resilient Canada. EM planning, in particular, aims to strengthen resiliency by promoting an integrated and comprehensive approach that includes the four pillars of EM: prevention and mitigation, preparedness, response and recovery.

Effective EM results from a coordinated approach and a more uniform structure across federal government institutions. This is why Public Safety Canada has developed this Emergency Management Planning Guide, which is intended to assist all federal government institutions in developing their all-hazards Strategic Emergency Management Plans (SEMPs).

A SEMP establishes a federal government institution's objectives, approach and structure for protecting Canadians and Canada from threats and hazards in their areas of responsibility and sets out how the institution will assist the coordinated federal emergency response. EM plans, such as the SEMP, represent an institution's planning associated with its "external" environment. Business continuity plans (BCPs), by contrast, represent an institution's planning associated with its "internal" efforts to ensure the continued availability of critical services to Canadians in the event of an incident/emergency affecting the organization. Despite this general distinction between "external" and "internal," EM planning and business continuity planning are complementary, and EM planning builds on the BCP; for example, data used in business impact analysis helps define the risk environment for EM planning.

An effective SEMP does not need to be lengthy to be comprehensive; as is often the case with strategic, high-level documents, simplicity is a virtue—"less is more." The qualifier "strategic" is used to differentiate this high-level plan from other types of emergency management plans, including operational plans. Many federal government institutions already have specific planning documents or processes to deal with aspects of emergency management that relate to their particular mandates; many also have a long track record of preparing and refining BCPs.

The development and employment of a SEMP is an important complement to such existing plans, because it promotes an integrated and coordinated approach to emergency management planning within federal institutions and across the federal government. To promote a more uniform structure and approach across federal government institutions, these existing plans, procedures and internal processes are to be assessed, and modified or adapted as required, in order to take this Guide into account and to incorporate other resources such as the Federal Emergency Response Plan (e.g., emergency support functions) and other policy documents.

Federal government institutions in the early stages of developing a SEMP may find it useful to read the material in Sections One and Two, while other institutions with more established plans may wish to proceed directly to Section Three.

Supporting templates and tools can contribute to effective emergency management planning and are provided with this Guide. An All-Hazards Risk Assessment Framework and associated tools are also under development and will be included in a subsequent version of the Guide. In the meantime, questions related to the Guide and the All-Hazards Risk Assessment Framework may be addressed to Public Safety Canada, Emergency Management Planning Unit, at EMPlanning.Guide@ps-sp.gc.ca.

Amendments Record

The following is a list of amendments to the Emergency Management Planning Guide:

#	Date	Amended by	Comments

List of Acronyms

AAR	After Action Report
AER	After Event Report
AHRA	All-Hazards Risk Assessment
APP	Annual Priorities and Plans
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CAIP	Capability Improvement Process
CEMC	Canadian Emergency Management College
CIP	Critical Infrastructure Protection
CSA	Canadian Standards Association
EM	Emergency Management
EMA	*Emergency Management Act*
ESF	Emergency Support Function
FERMS	Federal Emergency Response Management System
FERP	Federal Emergency Response Plan
FPEM	Federal Policy for Emergency Management
FPT	Federal/Provincial/Territorial
GSP	Government Security Policy
GOC	Government Operations Centre
ICS	Incident Command System
ISO	International Organization for Standardization
ITAC	Integrated Threat Assessment Centre
MAF	Management Accountability Framework
MOU	Memorandum of Understanding
NERS	National Emergency Response System
PESTLE	Political, Economic, Social, Technological/Technical, Legal, Environmental
PMPRR	Prevention/Mitigation, Preparedness, Response, Recovery
PSRP	Public Service Readiness Plan
RCMP	Royal Canadian Mounted Police
SEMP	Strategic Emergency Management Plan
SLA	Service Level Agreement
SOPs	Standard Operating Procedures
SWOT	Strengths, Weaknesses, Opportunities, Threats
TBS	Treasury Board Secretariat
TOR	Terms of Reference
TRA	Threat Risk Assessment

Table of Contents

Annexes

List of Figures

List of Tables

How to Use this Guide

The *Emergency Management Planning Guide* uses a step-by-step approach and provides instructions that are supplemented by the Blueprint and the Strategic Emergency Management Plan (SEMP) template provided in Annexes A and B, respectively. The Guide is structured as follows:

Section One: Setting the Context – Explains the purpose of the Guide.

Section Two: Emergency Management Concepts and Premises – Contains a general overview of the concepts behind the step-by-step process.

Section Three: Developing the Strategic Emergency Management Plan – Provides the step-by-step process to develop a SEMP.

Section Four: Implementing and Maintaining the Strategic Emergency Management Plan – Provides key information on the steps required to implement and maintain the SEMP.

Maintaining this Guide

The Emergency Management Planning Unit, Public Safety Canada, is responsible for producing, revising and updating this Guide. As a matter of process, the *Emergency Management Planning Guide* will be reviewed annually or as the situation dictates, and amendments will be made at that time. The primary point of contact for any questions and comments, as well as any requests for further EM planning templates / tools not included in this Guide, including those related to after action reports (AARs), after event reports (AERs) and Capability Improvement Processes (CAIPs), is EMPlanning.Guide@ps-sp.gc.ca.

1

Section One: Setting the Context

Purpose

The purpose of this Guide is to assist federal officials, managers and coordinators responsible for emergency management (EM) planning. The Guide includes a Blueprint (see Annex A), a Strategic Emergency Management Plan (SEMP) template (see Annex B), and supporting step-by-step instructions, tools and tips to develop and maintain a comprehensive SEMP—an overarching plan that establishes a federal government institution's objectives, approach and structure, which generally sets out how the institution will assist with coordinated federal emergency management, including response.

Responsibilities

Section 6 of the *Emergency Management Act* (2007) (EMA) outlines the EM responsibilities of each minister accountable to Parliament for a government institution to identifiy risks that are within or related to his or her area of responsibility—including those related to critical infrastructure—and to prepare EM plans to address those risks.

To support these EMA responsibilities, the *Federal Policy for Emergency Management* (FPEM) provides all federal ministers who have such responsibilities with a framework for preparing mandate-specific EM plans that include a program, arrangement or other measure to address mitigation/prevention, preparedness, response and recovery. As such, federal institutions are to base EM plans on mandate-specific all-hazards risk assessments, as well as put in place institutional structures to provide governance for EM activities and align them with government-wide EM governance structures.

The EM plans of federal government institutions should address the risks to critical infrastructure within or related to the institution's areas of responsibility, as well as the measures for protecting this infrastructure. These EM plans are to include any program, arrangement or other measures to assist provincial/territorial institutions, and, through provincial/territorial governments, local authorities.

Context

This Guide provides overall advice on developing a SEMP. It reflects leading practices (such as those provided by the International Organization for Standardization (ISO) and Canadian Standards Association) and procedures within the Government of Canada, and should be read in conjunction with the *Federal Emergency Response Plan*, the *Emergency Management Framework for Canada* and the *Federal Policy for Emergency Management*. It does not lay out the requirements for preparing related EM protocols, processes, and standard operating procedures (SOPs) internal to the institution; however, these should be developed in support of the SEMP and related plans.

The SEMP is the overarching plan that provides a comprehensive and coordinated approach to EM activities. It should integrate and coordinate elements identified in operational plans and business continuity plans (BCPs). As outlined in the Preface, many federal government institutions already have specific plans or processes to deal with aspects of emergency management; many also have a long track record of preparing and refining BCPs, which endeavour to ensure the continued availability of critical services. In addition, there are other existing EM planning documents and initiatives that apply to a range of federal government institutions, such as the *Federal Emergency Response Plan* (FERP) and deliverables under the National Strategy for Critical Infrastructure.

Given this variety of EM planning documents, the distinctions between them are summarized in the following table.

Plan	Purpose and Overview
Strategic Emergency Management Plan (SEMP)	• A SEMP establishes a federal government institution's objectives, approach and structure for protecting Canadians and Canada from threats and hazards in their areas of responsibility, and sets out how the institution will assist the coordinated federal emergency response. • EM plans, such as the SEMP, represent an institution's planning associated with its "external" environment. • The qualifier "strategic" is used to differentiate this high-level plan from other types of EM plans, including operational plans. The development and employment of a SEMP is an important complement to other types of EM plans, because it promotes an integrated and coordinated approach to emergency management planning.

Plan	Purpose and Overview
Federal Emergency Response Plan (FERP)	• The FERP is the Government of Canada's all-hazards response plan. • It outlines the processes and mechanisms to facilitate an integrated Government of Canada response to an emergency and to eliminate the need for departments to coordinate a wider Government of Canada response. • It includes 13 emergency support functions that the federal government can implement in response to an emergency. Each of these functions addresses a need that may arise before or during an emergency.
Operational plans (including response and incident-specific)	• Operational plans are more geared to the "tactical" level and support the SEMP, but provide the detail required for a coordinated response to specific hazards identified through a formal risk assessment process. • Their purpose is to harmonize emergency response efforts by the federal and provincial/territorial governments, non-governmental organizations and the private sector. • Operational plans may be based on all four pillars of EM planning, or focus on the specific activities of a single pillar.
Business continuity plans (BCPs)	• BCPs help enable critical services or products to be continually delivered to Canadians in the event of an incident/emergency. • EM plans, such as the SEMP, represent an institution's planning associated with its "external" environment. BCPs, by contrast, represent an institution's planning associated with its "internal" efforts to ensure the continued availability of critical services in the event of an incident/emergency impacting the institution. • Despite this general distinction between "external" and "internal," EM planning and business continuity planning are complementary; for example, data used in business impact analysis helps define the risk environment for EM planning.
Deliverables under the National Strategy and Action Plan for Critical Infrastructure	• The National Strategy and Action Plan for Critical Infrastructure establishes a public-private sector approach to managing risks, responding effectively to disruptions, and recovering swiftly when incidents occur. • Implementation of the Strategy will feature targeted and accurate information products, such as security briefings for each critical infrastructure sector. It is intended that governments and industry partners will work together to assess risks to the sector, develop plans to address these risks, and conduct exercises to validate the plans. • Key outputs of this work include a sector risk profile and a sector work plan. This work at the sector level will inform, and will be informed by, work at the organizational level such as EM plans and their component parts.

2 Section Two: Emergency Management Concepts and Premises

Emergency management (EM) refers to the management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery. For the purpose of this Guide, an emergency refers to "an immediate event, including an IT incident, 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." The following diagram illustrates the EM continuum in the context of an effective EM system.

Emergency Management Continuum

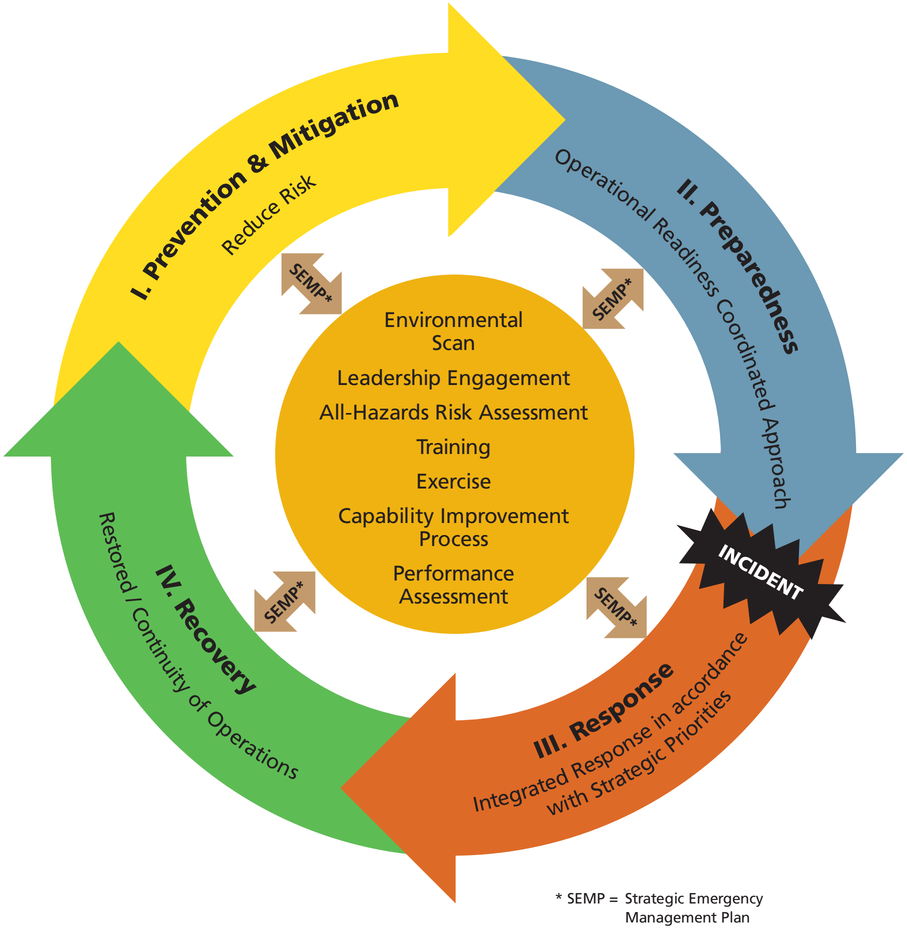

I. Prevention & Mitigation
Reduce Risk
II. Preparedness
Operational Readiness Coordinated Approach
III. Response
Integrated Response in accordance with Strategic Priorities
IV. Recovery
Restored / Continuity of Operations
INCIDENT
SEMP*
SEMP*
SEMP*
SEMP*
Environmental Scan
Leadership Engagement
All-Hazards Risk Assessment
Training
Exercise
Capability Improvement Process
Performance Assessment
* SEMP = Strategic Emergency Management Plan

Figure 1: Emergency Management Continuum

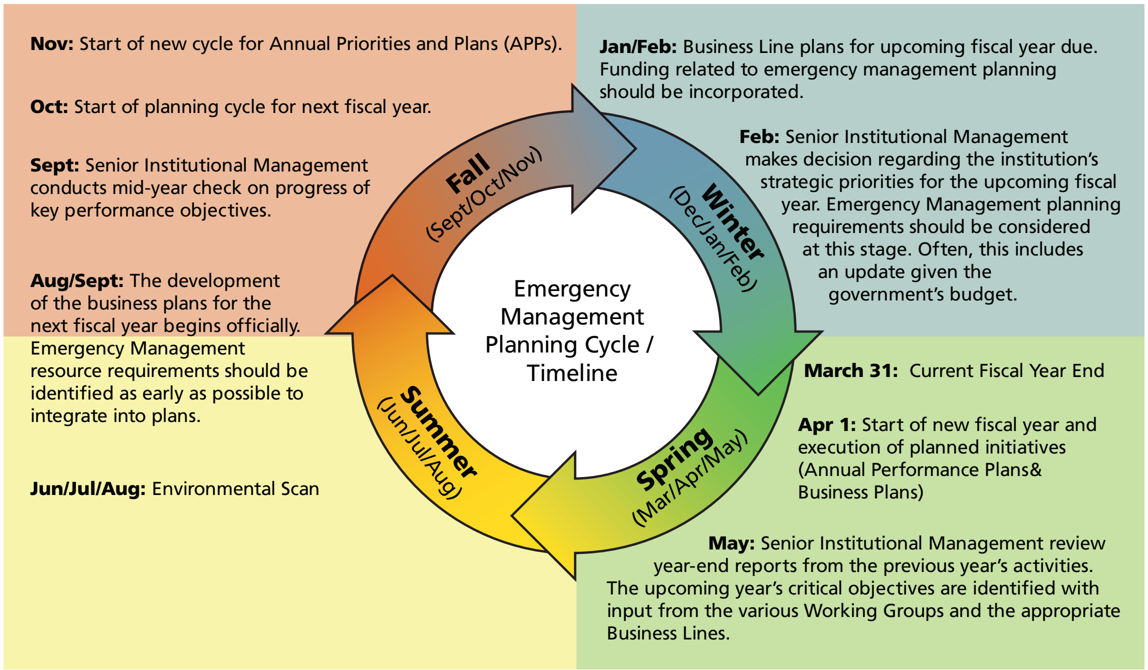
Figure 1 highlights the four interdependent risk-based functions of EM: prevention and mitigation of, preparedness for, response to, and recovery from emergencies. These functions can be undertaken sequentially or concurrently, and they are not independent of each other.

The inner circle includes all of the elements that influence the development of the SEMP, such as:

- updates of environmental scans;
- ongoing/regular all-hazards risk assessments;
- engaged leadership;
- regular training;
- regular exercises; and
- a Capability Improvement Process (CAIP)—the whole-of-government approach to the collection and analysis of government response for exercises and real events.

The figure also places the SEMP in the continuum as a living document that is continuously improved and adjusted, for instance, as lessons learned through responses/exercises or a changing risk environment are integrated.

The SEMP should ideally be reviewed on a cyclical basis as part of a federal government institution's planning cycle, as presented in Figure 2 below. Further guidance on the optimal planning cycle is provided in Section Four.



Nov: Start of new cycle for Annual Priorities and Plans (APPs).

Oct: Start of planning cycle for next fiscal year.

Sept: Senior Institutional Management conducts mid-year check on progress of key performance objectives.

Aug/Sept: The development of the business plans for the next fiscal year begins officially. Emergency Management resource requirements should be identified as early as possible to integrate into plans.

Jun/Jul/Aug: Environmental Scan

Jan/Feb: Business Line plans for upcoming fiscal year due. Funding related to emergency management planning should be incorporated.

Feb: Senior Institutional Management makes decision regarding the institution's strategic priorities for the upcoming fiscal year. Emergency Management planning requirements should be considered at this stage. Often, this includes an update given the government's budget.

March 31: Current Fiscal Year End

Apr 1: Start of new fiscal year and execution of planned initiatives (Annual Performance Plans& Business Plans)

May: Senior Institutional Management review year-end reports from the previous year's activities. The upcoming year's critical objectives are identified with input from the various Working Groups and the appropriate Business Lines.

Figure 2: Emergency Management Planning Cycle/Timeline is adapted from the Treasury Board Secretariat timelines for Annual Priorities and Plans (APPs).

3 Section Three: Developing the Strategic Emergency Management Plan

This section of the Guide outlines a recommended approach for developing a tailored SEMP and is supported by a blueprint and a SEMP template provided in Annexes A and B, respectively. The process comprises five comprehensive steps, as follows:

Step 1 – Initiate:

- Initiate the EM planning team:
  - identify team members and functional areas;
  - identify training and skill set requirements; and
  - establish authority and terms of reference.
- Confirm obligations and requirements:
  - review existing legislation and policies; and
  - review existing EM plans.
- Identify optimal planning cycle:
  - develop work plan.

Step 2 – Orientate:

- Complete/update environmental scan:
  - assess internal environment;
  - assess external environment;
  - identify existing plans and assess gaps in meeting institutional requirements; and
  - identify and review stakeholder positions and issues.
- Complete/update critical assets and services list:
  - update/conduct criticality assessment, including business impact analysis (BIA).
- Complete/update threats and hazards:
  - conduct/update all-hazards threat assessment.
- Identify vulnerabilities:
  - identify and assess current safeguards.
- Conduct all-hazards risk assessment:
  - identify risks:
    - establish a risk register.
  - analyze risks:
    - evaluate probability/likelihood of occurrence; and
    - analyze consequences/impact;
  - evaluate risks;
    - prioritize risks; and
  - identify risk prevention/mitigation options.

Step 3 – Develop SEMP building blocks:

- Develop SEMP building blocks:
  - establish EM governance structure;
  - confirm strategic priorities;
  - identify assumptions, constraints and limitations;
  - consider Prevention/Mitigation, Preparedness, Response and Recovery (PMPRR) requirements and opportunities; and
  - identify requirements for threat/hazard-specific plans, BCPs and other EM plans.

Step 4 – Write the SEMP and seek approval:

- Write the SEMP:
  - draft the SEMP;
  - engage internal/external stakeholders;
  - update/refine the SEMP;
  - consider optimal planning timeline; and
  - seek senior management approval.

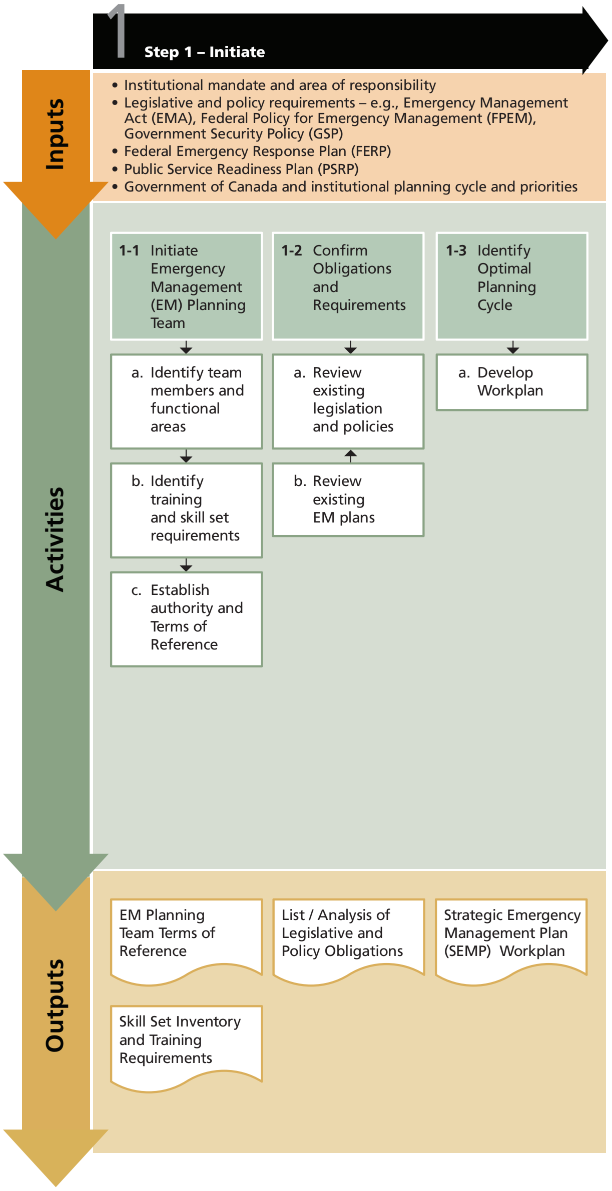
Step 5 – Implement, execute and maintain the SEMP:

- Implement the SEMP:
  - communicate the SEMP (internal/external);
  - secure resources;
  - train; and
  - exercise.
- Execute the SEMP (in response to triggers or an incident).
- Maintain/update the SEMP:
  - Continuous improvement.

Please note that Step 5 is presented under Section Four: Implementing and Maintaining the SEMP.

Each step identifies inputs or considerations at the outset and concludes with the associated outputs. Inputs should ideally be assembled, reviewed and well understood prior to engaging in each distinct planning activity as they form an important foundation for the work to be completed. Note that an input to a step/activity is often the output from a previous step/activity.

Step 1: Initiate


1
Step 1 – Initiate
Inputs
• Institutional mandate and area of responsibility
• Legislative and policy requirements – e.g., Emergency Management Act (EMA), Federal Policy for Emergency Management (FPEM), Government Security Policy (GSP)
• Federal Emergency Response Plan (FERP)
• Public Service Readiness Plan (PSRP)
• Government of Canada and institutional planning cycle and priorities
Activities
1-1 Initiate Emergency Management (EM) Planning Team
a. Identify team members and functional areas
b. Identify training and skill set requirements
c. Establish authority and Terms of Reference
1-2 Confirm Obligations and Requirements
a. Review existing legislation and policies
b. Review existing EM plans
1-3 Identify Optimal Planning Cycle
a. Develop Workplan
Outputs
EM Planning Team Terms of Reference
Skill Set Inventory and Training Requirements
List / Analysis of Legislative and Policy Obligations
Strategic Emergency Management Plan (SEMP) Workplan

This step involves starting the formal planning process in recognition of the responsibility to prepare a SEMP. The SEMP should be central to the federal government institution's EM activities and provide clear linkages for integrating and coordinating all other intra-departmental and inter-departmental emergency management plans. Planning can be triggered by the EM planning cycle or it can be initiated in preparation for, or in response to, an event that is induced either by nature or by human actions.

Inputs

The primary inputs or considerations for this step include:

- the federal government institution's mandate and area of responsibility;
- legislative responsibilities and policy requirements (e.g., discrete or departmental legislation, EMA, FPEM, GSP);
- the Federal Emergency Response Plan (FERP);
- the Public Service Readiness Plan (PSRP); and
- the Government of Canada and institutional planning cycle and priorities.

Activities

Activities Tip!

Consider having members of the EM planning team designated by your institution's senior management.

Activities Tip!

Consider including a member of your institution's corporate planning area on the EM planning team in order to help align the EM planning cycle with the institution's overall business planning cycle.

Activities Tip!

The team members should have the skills and training required to adequately carry out their assigned duties. Training is available to address EM requirements at the Canadian Emergency Management College (CEMC) and the Canada School of Public Service. The CEMC will begin offering a course on developing a SEMP in early 2011.

1-1 Initiate the EM planning team

The first activity is to form the EM planning team. The size and composition of the team may vary between federal government institutions; however, the planning team should ideally have the skill and experience necessary to develop the SEMP. The activities below can assist in the success of the planning team.

a. Identify team members and functional areas

One of the most crucial steps in the EM planning process is to identify appropriate members for the EM planning team. This team should be established under the authority of the institution's governance framework and have clear directions, including objectives. Consideration should be given to having representation from several program and corporate areas, including (if applicable) regional representation. The aim is to establish a multi-disciplinary planning team to provide optimal input.

b. Identify training and skill set requirements

Federal government institutions should consider identifying the range of experience and skill sets required in the EM planning team. In turn, institutions should provide training and education for the development of the SEMP.

c. Establish authority and terms of reference

The composition of the EM planning team will vary depending on institutional requirements; however, it is important that clear terms of reference (TOR) for the team be established and that individual assignments be clearly defined. These TOR can identify the responsibilities assigned to each team member and the requirements to allow that member to carry out the assigned function. A TOR template is provided in Annex C, Appendix 1.

1-2 Confirm obligations and requirements

a. Review existing legislation and policies

Activities Tip!

Consider giving a team member the responsibility of analyzing the legislative and policy obligations applicable to the development of the SEMP. Update the analysis regularly, as legislation and policies can change and have an influence on the scope of your SEMP.

After the EM planning team has clear authority and direction, the next step is to review any relevant existing legislation and policies. This is also an ideal time to involve institutional legal advisors to determine whether legislative requirements are being met.

b. Review existing EM plans

The next step is to review any existing EM plans (or other applicable documents). The review should ideally include any partner agency EM plans. Those federal government institutions that have mandated emergency support functions (ESFs) under the FERP should have these clearly identified.

1-3 Identify optimal planning cycle

Activities Tip!

Consider including EM planning requirements in the institution's annual business and strategic planning priorities to identify funding needs and to prompt appropriate actions/initiatives.

As noted in Section Two, the EM planning process should be carried out as part of an institution's overall strategic and business planning processes—this will support their alignment. Identify which team/sector in your institution is responsible for planning and determine what dates are milestones for developing the document. You may then wish to consider how best to align both processes.

a. Develop work plan

Developing the SEMP can be supported by a formal work or project plan to ensure that established timelines for plan development are met. After completing the above steps, the planning team should consider developing a detailed work plan that includes a schedule with realistic timelines, milestones that reflect the institutional planning cycle, and a responsibility assignment matrix with assigned tasks and deadlines. Specific timelines should be modified as priorities become more clearly defined. This is also an ideal time to develop an initial budget for such items as training, exercises, research, workshops and other expenses that may be necessary during the development and implementation of the SEMP.

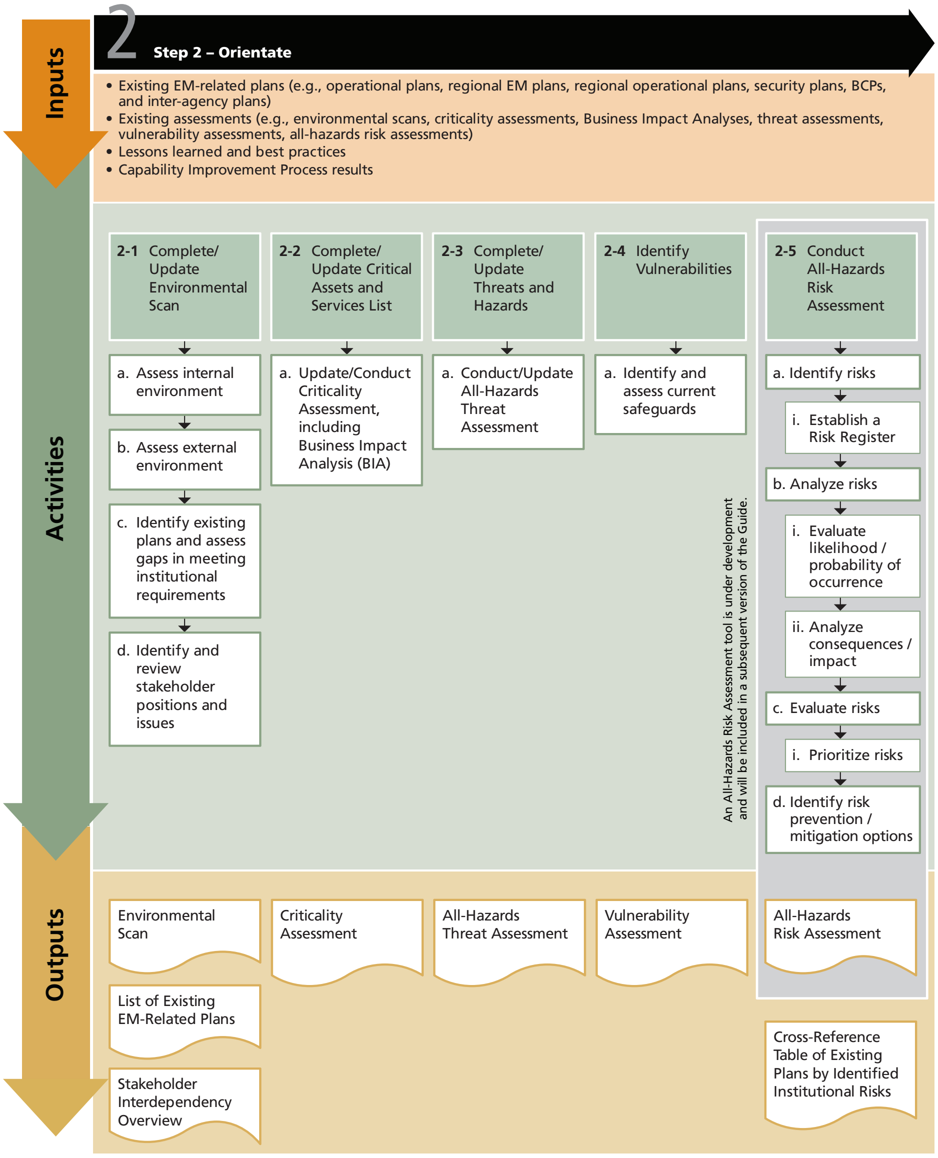
Outputs

Outputs

The outputs from the activities set out in Step 1 may include:

- an EM planning team terms of reference;
- an EM planning team skill set inventory and list of training requirements;
- a list/analysis of legislative and policy obligations; and
- a work plan for development, approval, and implementation of the SEMP.

Step 2: Orientate



- Existing EM-related plans (e.g., operational plans, regional EM plans, regional operational plans, security plans, BCPs, and inter-agency plans)
- Existing assessments (e.g., environmental scans, criticality assessments, Business Impact Analyses, threat assessments, vulnerability assessments, all-hazards risk assessments)
- Lessons learned and best practices
- Capability Improvement Process results

2-1 Complete/Update Environmental Scan

a. Assess internal environment

b. Assess external environment

c. Identify existing plans and assess gaps in meeting institutional requirements

d. Identify and review stakeholder positions and issues

2-2 Complete/Update Critical Assets and Services List

a. Update/Conduct Criticality Assessment, including Business Impact Analysis (BIA)

2-3 Complete/Update Threats and Hazards

a. Conduct/Update All-Hazards Threat Assessment

2-4 Identify Vulnerabilities

a. Identify and assess current safeguards

2-5 Conduct All-Hazards Risk Assessment

a. Identify risks

i. Establish a Risk Register

b. Analyze risks

i. Evaluate likelihood / probability of occurrence

ii. Analyze consequences / impact

c. Evaluate risks

i. Prioritize risks

d. Identify risk prevention / mitigation options

An All-Hazards Risk Assessment tool is under development and will be included in a subsequent version of the Guide.

Environmental Scan

List of Existing EM-Related Plans

Stakeholder Interdependency Overview

Criticality Assessment

All-Hazards Threat Assessment

Vulnerability Assessment

All-Hazards Risk Assessment

Cross-Reference Table of Existing Plans by Identified Institutional Risks

As a next step, federal government institutions should consider developing a comprehensive understanding of the planning context. This step is often the most comprehensive and complex. Notwithstanding the blueprint provided, this step is not proposed as a linear process, but rather as a set of related components and activities that can be undertaken in the sequence that best suits the institution.

Inputs

Inputs for this step may include existing documentation such as:

- EM-related plans (e.g., operational plans, regional EM plans, regional operational plans, security plans, BCPs and inter-agency plans);
- assessments (e.g., environmental scans, criticality assessments, business impact analyses, threat assessments, vulnerability assessments, risk assessments, all-hazards risk assessments);
- lessons learned and best practices; and
- Capability Improvement Process results.

Input Tip!

Additional supporting planning tools and templates as well as an EM glossary are provided in Annexes C and D, respectively.

Activities

2-1 Complete/update environmental scan

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 (see Figure 3: The Planning Context for additional information on the factors to consider). Scanning can be done on a regularly scheduled basis, such as annually, or on a continuous basis for environmental factors that are dynamic or that are of greatest interest to the institution.

As part of the environmental scan, the institution defines the internal and external parameters to be taken into account when managing the risk and setting the scope and risk criteria for the remaining risk assessment process. It sets the time, scope and scale and contributes to adopting an approach that is appropriate to the situation of the institution and to the risks affecting the achievement of its objectives.

Additionally, federal government institutions are responsible for conducting mandate-specific risk assessments, including risks to critical infrastructure. The key to any emergency planning is awareness of the potential situations that could impose risks on the organization and on Canadians and to assess those risks in terms of their impact and potential mitigation measures. The following diagram illustrates the external and internal environmental factors to consider.

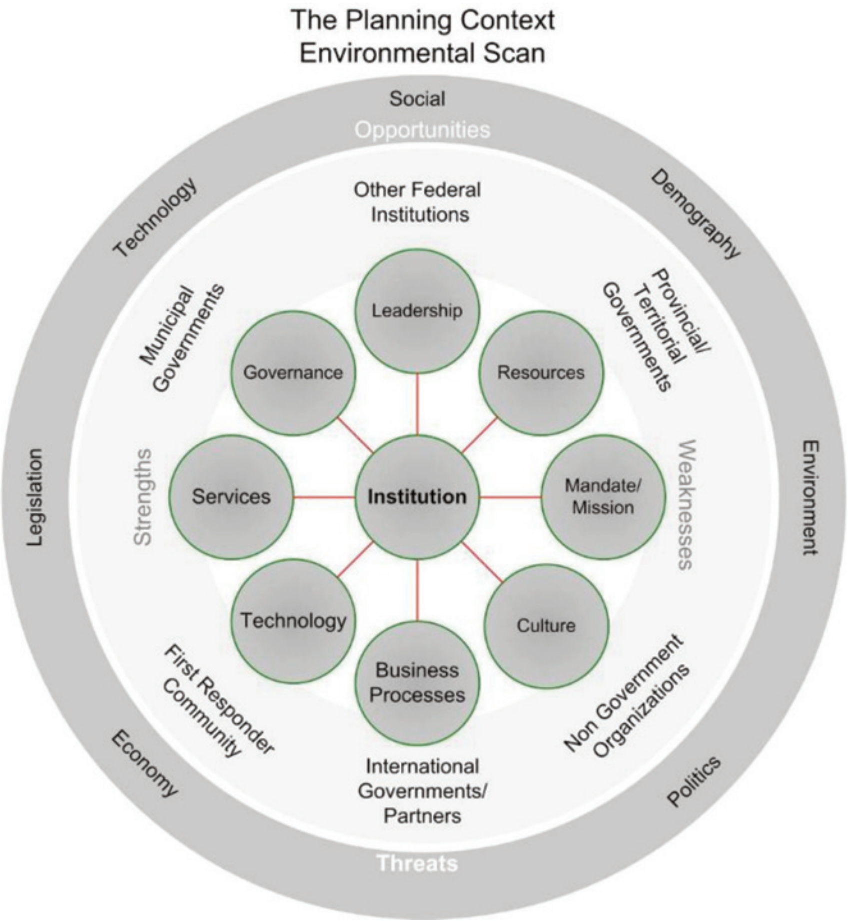


Figure 3: The Planning Context—Environmental Scan

a. Assess internal environment

Understanding the internal context is essential to confirm that the risk assessment approach meets the needs of the institution and of its internal stakeholders. It is the environment in which the institution operates to achieve its objectives and which can be influenced by the institution to manage risk. The internal context may include:

- the capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, technologies), including results from the Capability Improvement Process;
- information systems, information flows and decision making processes;
- internal stakeholders;
- the policies, objectives and strategies in place to achieve them;
- perceptions, values and culture;
- standards and reference models adopted by the institution; and
- structures (e.g., governance, roles and accountabilities).

b. Assess external environment

Understanding the external context is important to ensure that external stakeholders, their objectives and concerns are considered. The external context is the environment in which the institution seeks to achieve its objectives and may include:

- the cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having an impact on the institution's objectives; and
- the perceptions and values of external stakeholders.

Activities Tip!

Consider reviewing your federal government institution's most current environmental scan, as well as the most current RCMP Environmental Scan (which can be found on the RCMP Web site), in order to develop a better understanding of pressures and issues facing your institution.

There are several approaches to developing an institutional environmental scan. Samples of tools such as a SWOT (strengths, weaknesses, opportunities, threats) analysis and a PESTLE (Political, Economic, Social, Technological/Technical, Legal and Environmental) analysis are provided in Annex C, Appendix 2.

c. Identify existing plans and assess gaps in meeting institutional requirements

As part of assessing the internal environment of your institution, it is important to gather an inventory of existing EM plans and relevant assessments/analyses/scans such as:

EM-Related Plans

SEMP

Operational plans

Regional EM plans

Regional operational plans

Security plans

Business continuity plans

Inter-agency plans

Assessments

Environmental scans

Criticality assessments including data on critical infrastructure

Business impact analyses

Threat assessments

Vulnerability assessments

Risk assessments

All-hazards risk assessments

Once all documentation is identified, consider conducting a gap analysis to determine whether the institution is currently meeting its obligations as identified in Step 1. If gaps are identified, these should ideally be gathered and presented as part of Step 3 when developing the EM Planning Framework and confirming the institution's strategic EM priorities.

d. Identify and review stakeholder positions and issues

During this process, consider conducting a full review and analysis of stakeholder documentation and reports. Where possible, input from external partners should be sought. This process will add the extra assurance that your institution is linked in with partner agencies and others to assist in developing the broader environmental picture and in identifying EM-related interdependencies. Stakeholders may include First Nations, emergency first responders, the private sector (both business and industry), and volunteer and non-government organizations.

2-2 Complete/update critical assets and services list

An inventory of critical assets and services will assist the planning team in identifying the associated threats, hazards, vulnerabilities and risks unique to their institution. This activity may be accomplished as follows:

Activities Tip!

If a business impact analysis (BIA) has already been completed for your federal government institution's BCP, this analysis can greatly inform your criticality assessment.

a. Update/conduct criticality assessment, including business impact analysis

It is important to identify, appraise and prioritize all institutional assets. Assets can be both tangible and intangible and can be assessed in terms of importance, value and sensitivity. This assessment should ideally consider the entire institution (i.e., critical services and critical infrastructure, associated resource requirements and interdependencies).

Activities Tip!

When conducting a criticality assessment, it is important to be objective when prioritizing the importance of institutional assets, as not all assets are critical to an institution's operations.

2-3 Complete/update threats and hazards

Federal government institutions may wish to list potential "external" hazards and threats (i.e., threats to Canadians and Canada) that may fall within the institution's area of responsibility. All available threat assessments should ideally be reviewed by analyzing the assessment's evaluation of hostile capability, intentions and activity, the environment influencing hostile and potentially hostile groups, and environmental considerations, including natural, health and safety hazards.

A comprehensive but non-exhaustive list of hazards and threats relevant to the Canadian context can be found in Annex C, Appendix 3. For further information, you may wish to consult the Canadian Disaster Database, which contains detailed disaster information on over 900 natural, technological and conflict events (excluding war) that have directly affected Canadians over the past century. The database can help federal government institutions to better identify, assess and manage risks, and can be accessed by sending a request to Public Safety Canada at cdd-bdc@ps-sp.gc.ca.

Activities Tip!

Adopting the current Treasury Board Policy related to material and asset management and coding criteria will help structure an effective approach. For further information, consult TBITS 25: Material Coding Implementation Criteria.

Activities Tip!

Consider liaising with your security and/or intelligence staff to determine whether a threat assessment is available internally. As appropriate, more specific terrorist threat and hazard information can be obtained from ITAC. They can also add your federal government institution to a distribution list that contains unclassified information. ITAC can be contacted at itac1@smtp.gc.ca.

a. Conduct/update All-Hazards Threat Assessment

Traditionally, a threat assessment is an analysis of intent and capabilities in the occurrence of a threat. It should:

- focus on how the organization identifies those factors associated with indications and warnings of human-induced events (both intentional and unintentional) and naturally occurring hazards (geological, meteorological and biological);
- define liaison activities with other agencies; and
- assign organizations the task of collecting and reporting information.

The all-hazards risk assessment, presented below, can use information contained in institutional threat risk assessment (TRA) reports or information from other sources such as the Integrated Threat Assessment Centre (ITAC). A threat awareness collection process should ideally link to the federal institution's information requirements and available resources.

2-4 Identify vulnerabilities

A vulnerability assessment looks at an inadequacy or gap in the design, implementation or operation of an asset that could enable a threat or hazard to cause injury or disruption.

a. Identify and assess current safeguards

In order to identify vulnerabilities, an institution should first identify and assess existing safeguards associated with critical assets and activities. With respect to known threats and hazards, a vulnerability exists when there is a situation or circumstance that, if left unchanged, may result in loss of life or may affect the confidentiality, integrity or availability of other mission-critical assets. A vulnerability may also be described as the characteristics of a system that cause it to suffer a definite degradation (incapability to perform its designated function in support of the mission) as a result of having been subjected to the effects of a threat agent, hazard and/or hostile environment.

Examples of conditions that may be considered vulnerabilities include:

- personnel issues (e.g., high turnover, inadequately trained individuals);
- insufficient secondary or support processes; and
- existing EM plans that are immature and have not been tested.

2-5 Conduct All-Hazards Risk Assessment

Risk assessment is central to any risk management process as well as the EM planning cycle. It is a formal, systematic process for estimating the level of risk in terms of likelihood and consequences for the purpose of informing decision-making. Each institution has its own strategic and operational objectives, with each being exposed to its own unique risks, and each having its own information and resource limitations. Therefore, the risk assessment process is tailored to each institution. Institutions may choose to assess a portfolio of risks, as opposed to specific individual risks, which enables a holistic review of risk treatment decisions.

The output of the risk assessment process is a clear understanding of risks, their likelihood and potential impact on achieving objectives. It provides improved insight into the effectiveness of risk controls already in place and enables the analysis of additional risk mitigation measures. An all-hazards approach to risk management does not necessarily mean that all hazards will be assessed, evaluated and treated, but rather that all hazards will be considered. This part of the process consists of three main activities: risk identification, risk analysis and risk evaluation. The outputs of these three steps provide decision-makers with an improved understanding of the relevant risks that could affect objectives as well as the effectiveness of risk controls already in place. A risk assessment should generate a clear understanding of the risks, including their uncertainties, their likelihood and their potential impact on objectives.

The all-hazards risk assessment (AHRA) process should be open and transparent while respecting the federal institution’s context. It should be tailored to the institution’s needs and should identify any limitations such as insufficient information or resource constraints. Third-party review may be used to confirm the integrity of the AHRA process.

In this section, risks translate into events or circumstances that, if they materialize, could negatively affect the achievement of government objectives. The hazard risk domain is covered by the AHRA process. However, the strategic risk domain (e.g., political risks, reputational risks) and the operational risk domain (e.g., day-to-day issues confronting the institution) are not.

The hazard risk domain can be divided into three risk areas:

- natural hazards – the risks associated with natural (geological, meteorological or biological) hazards (e.g., earthquake, landslide, flood, drought, pandemic influenza, foot and mouth disease, insect infestation);
- intentional human actions – the risks associated with chemical, nuclear or other hazards, resulting from deliberate actions (e.g., terrorism, sabotage); and
- unintentional human actions – the risks associated with chemical, nuclear or other hazards resulting from accidents (e.g., hazardous material spill or release, explosion/fire, water control structure/dam/levee failure).

The AHRA process focuses on risks that may occur in the medium term (generally 1-3 years). It also encourages an all-hazards approach when considering risks to be assessed.

a. Identify risks

Once the institution’s context is clearly understood (refer to the environmental scan in Step 2-1), the next step is to find and recognize hazards, threats and possibly trends and drivers, and to describe them in risk statements. Risks should be described in a way that conveys their context, point of origin and potential impact. The aim is to generate a comprehensive list of risks based on those events that might prevent, degrade or delay the achievement of objectives. It involves the identification of risk sources, areas of impact, events and their causes, as well as potential consequences. Information can be gleaned from historical data, theoretical analyses, and informed and expert judgements.

Risks can be identified though several mechanisms: structured interviews, brainstorming, affinity grouping, risk source analysis, checklists and scenario analysis. Characterization of risks should use an appropriate breadth and scope; it can be difficult to establish a course of action to treat risks if the scope is too broad, while a scope that is too narrow will create too much information, thereby making it difficult to establish priorities. Risks should be realistic, based on drivers that exist in the institution’s operating environment. Risks are not to be confused with issues. Issues are events that may drive risks, but are not risks in themselves.

i. Establish a risk register

A risk register or log is used to record information about identified risks and to facilitate the monitoring and management of risks. A risk register will typically describe each risk, assess the likelihood that it will occur, list possible consequences if it does occur, provide a grading or prioritization for each risk, and identify proposed mitigation 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 prioritize groups of risks. The risk register will likely be adjusted as risk assessment results change.

b. Analyze risks

The objective of risk analysis is to understand the nature and level of each risk in terms of its impact and likelihood. It provides the basis for risk evaluation and decisions about risk treatment.

Activities Tip!

Consider consulting your institution's subject matter experts when evaluating quantitative likelihood through historical data, simulation models and other methods. Subject matter experts can also assist in evaluating likelihood from a qualitative perspective, for instance by using a Delphi technique (a group communication process for systematic forecasting).

i. Evaluate likelihood/probability of occurrence

The likelihood/probability of an event relates to evaluating factual data in order to better understand how identified threats and hazards can occur. Likelihood/probability can be estimated using quantitative techniques, qualitative techniques, or approaches that combine the two methods.

Likelihood/probability can be assessed quantitatively using deterministic methods (models and simulations) or probabilistic methods (calculating probabilities from historical data or expert views). 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, or where there is a lack of adequate information and the numerical data or resources necessary for a statistically significant quantitative approach. It is usually used for analyzing threats with less tangible intent (judgements on terrorism, sabotage, etc.). Descriptive scales can be formed or adjusted to suit the circumstances, and different descriptions can be used for different risks. Qualitative data can often be estimated from interviews with experts. Qualitative analysis is often simpler, but also results in high uncertainty in the results.

Activities Tip!

A number of algorithms and tools are already in use for consequence/impact assessments within Canada and globally for this purpose. Additional information on analyzing likelihood and impact is provided in the Treasury Board Integrated Risk Management Framework Guidelines.

ii. Analyze consequences/impacts

A risk can have many consequences/impacts and affect many objectives. Consequences/impacts can be expressed quantitatively through physical event modelling or extrapolation from experimental studies or past data, or qualitatively as a descriptive representation of the likely 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-US border?
- Does the risk have the potential to impact the environment in the long term?

Consequences can be expressed in terms of monetary, technical, operational, social or human impact criteria. They can be evaluated against predetermined segments of interest to the institutions (e.g., impact to critical infrastructure sectors such as food, water; impact on the population; national security and law enforcement; economy; environment).

c. Evaluate risks

The purpose of risk evaluation is to help make decisions about which risks need treatment and the priority for treatment implementation. This also provides a baseline as to risks without any management measures. Risk evaluation is the process of comparing the results of the risk analysis against risk criteria to determine whether the level of risk is acceptable or intolerable. Existing controls, the cost of further risk treatment and any policy requirement implications are considered when deciding on additional mitigation measures.

Risk criteria are based on internal and external contexts and reflect the institution's values, objectives, resources and risk appetite (over-arching expression of the amount and type of risk an institution is prepared to take).

i. Prioritize risks

Risks can be prioritized by comparing risks in terms of their individual likelihood and impact estimates. Prioritization can be shown graphically in a logarithmic risk diagram, risk-rating matrix or other forms of visual representations. The one most commonly used is the risk matrix (Figure 4), which normally plots the likelihood and impact on the x- and y-axes (the measured components of risks). Based on a risk diagram or rating matrix, a clustering of risks can be shown, leading to decisions on priorities. Such a plot can help establish acceptable or intolerable risk levels, and establish their respective actions.

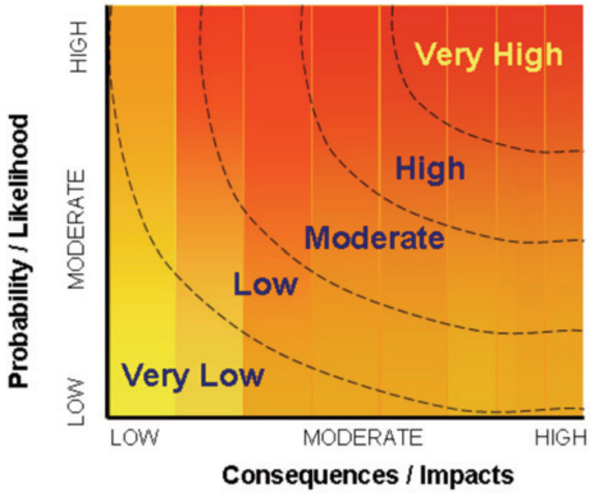


Figure 4: Example of a risk-rating matrix

Activities Tip!

Consider gathering a list of institutional risks and cross-referencing the existing plans (as identified in Step 2-1c) that address each risk. A sample cross-reference table of existing plans by identified institutional risks is provided in Annex C, Appendix 4.

d. Identify risk prevention/mitigation options

Risk treatment is the process of developing, selecting and implementing controls. 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;
- sharing the risk with another party; and
- retaining the risk by choice.

Risk treatment options can be prioritized by considering risk severity, effectiveness of risk controls, 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.

Outputs

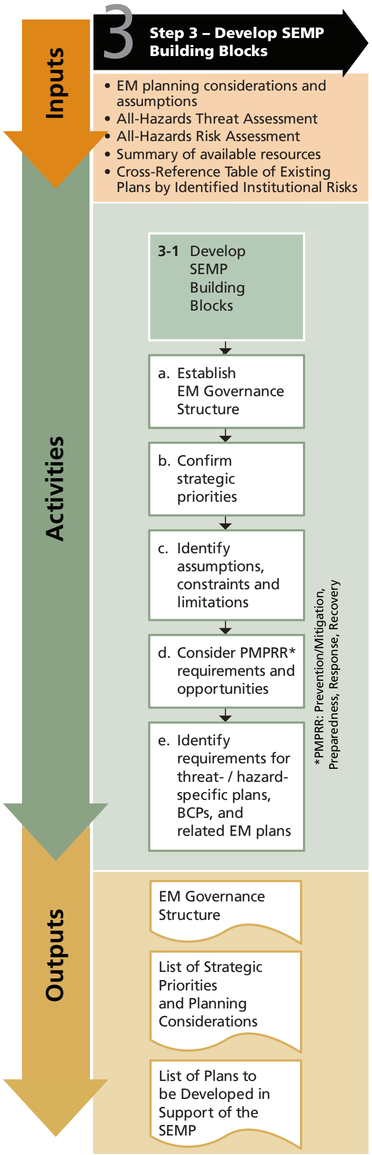
Outputs

The outputs from the activities associated with Step 2 contribute directly to the development of the SEMP building blocks, as well as the SEMP itself, and can include:

- an environmental scan;
- a list of existing EM-related plans;
- a stakeholder interdependency overview;
- a criticality assessment;
- a business impact analysis;
- an all-hazards threat assessment;
- a vulnerability assessment;
- an all-hazards risk assessment; and
- a cross-reference table of existing plans by identified institutional risks.

This step will contribute to the concept that sound EM decision-making can be based on an understanding and evaluation of hazards, vulnerabilities and related risks.

Step 3: Develop Strategic Emergency Management Plan (SEMP) building blocks


3
Step 3 – Develop SEMP Building Blocks
Inputs
• EM planning considerations and assumptions
• All-Hazards Threat Assessment
• All-Hazards Risk Assessment
• Summary of available resources
• Cross-Reference Table of Existing Plans by Identified Institutional Risks
Activities
3-1 Develop SEMP Building Blocks
a. Establish EM Governance Structure
b. Confirm strategic priorities
c. Identify assumptions, constraints and limitations
d. Consider PMPRR* requirements and opportunities
e. Identify requirements for threat- / hazard-specific plans, BCPs, and related EM plans
*PMPRR: Prevention/Mitigation, Preparedness, Response, Recovery
Outputs
EM Governance Structure
List of Strategic Priorities and Planning Considerations
List of Plans to be Developed in Support of the SEMP

This step focuses on developing an informed EM approach for your institution based on the four pillars of EM. The resulting SEMP building blocks will reflect strategic priorities—the desired balance between developing measures that respond to emergencies versus mitigating the risk. Often, the risk tolerance of an institution influences the direction of the SEMP. The aim is to develop a SEMP that integrates and coordinates elements identified in hazard-specific plans and BCPs.

Inputs

Inputs to the development of the SEMP building blocks should include senior management guidance as well as the following:

- EM planning considerations and assumptions
- all-hazards threat assessment
- all-hazards risk assessment
- summary of available resources (including personnel, facilities and EM capabilities)
- cross-reference table of existing plans by identified institutional risks

Activities

3-1 Develop SEMP building blocks

To help the planning team develop the SEMP building blocks, the following activities are suggested:

a. Establish an EM governance structure

Each institution should establish an EM governance structure to oversee the management of emergencies. The EM planning governance structure may include representatives of an institution's senior management team, from all functional areas (such as programs) and all corporate areas (including communications, legal services and security).

It is important to ensure that your institution's EM governance structure is aligned with other whole-of-government EM governance structures (e.g., as outlined in the FERP and PSRP). It is also crucial that roles and responsibilities, lines of accountability and decision-making processes be aligned and well understood by all concerned.

Activities Tip!

In identifying members of your institution's EM governance structure, keep in mind the relationship between your institution's mandate and the four pillars of EM.

b. Confirm strategic priorities

It is important that the planning team confirm the strategic priorities of the institution and of senior management so that they can be reflected in the SEMP.

Activities Tip!

Consider developing an overview of these priorities and identifying potential areas for attention given risk probabilities and vulnerabilities.

c. Identify assumptions, constraints and limitations

The planning team should aim to clearly identify the planning constraints and institutional limitations that will influence the SEMP building blocks and the subsequent development of the SEMP. For example, an institution can be constrained by the availability of training for EM planning team members and by the number of EM positions they have staffed. Similarly, certain assumptions will be made that influence the development of the SEMP building blocks. For example, an assumption might be made that the resources required to develop the SEMP will be paid out of the current fiscal year's budget.

d. Identify Prevention/Mitigation, Preparedness, Response and Recovery (PMPRR) requirements and opportunities

Each federal government institution is unique. When developing the SEMP, numerous planning considerations can be addressed. Although planning considerations will vary from institution to institution, the following identifies the most common planning considerations associated with the four pillars of EM planning. These are in large part taken from the Federal Policy for Emergency Management.

Prevention/mitigation

The objective of planning activities associated with prevention and mitigation efforts is to reduce risk. Accordingly, the planning team may wish to consider:

- conducting mandate-specific risk assessments, including those affecting critical infrastructure, within or related to their area of responsibility, based on all-hazards risk analysis and risk assessment methodology;
- using the common tools and leading practices, as may be provided by Public Safety Canada, to conduct risk assessments, while recognizing pertinent risks related to the individual institution;
- developing programs, arrangements or measures, where appropriate, aimed at mitigating risks from hazards relevant to institutional mandates; and
- applying and implementing changes, as well as collaborating with stakeholders to implement changes, based on lessons learned and best practices derived from training and exercises as well as from response and recovery experiences.

Activities Tip!

The cross-reference table of existing plans by identified institutional risks provided in Annex C, Appendix 4, can assist in cross-referencing your most prevalent risks and the tools in place to address them (such as existing plans). A further cross-referencing can then be undertaken with the four pillars of EM to help target specific activities in one or more of the following areas.

Activities Tip!

A SEMP should inform each federal government institution's overall priorities and tie into its business and strategic planning activities. This will allow greater integration of the SEMP into existing resource allocation mechanisms within federal government institutions.

Activities Tip!

Federal government institutions can perform a cost-benefit analysis of the prevention and mitigation options (e.g., is it cheaper to mitigate or to replace infrastructure and equipment?) in order to make policy recommendations for selecting the most feasible, cost-effective and beneficial options.

Preparedness

The objective of planning activities associated with preparedness is to have an effective and coordinated approach to EM and operational readiness. Accordingly, the planning team may wish to consider:

- maintaining a level of sustainable capacity to meet the goals outlined in individual EM plans, based on priorities, needs analysis and capability requirements;
- conducting or participating in exercises to test and implement EM plans and participate in training with respect to EM planning;
- incorporating lessons learned and best practices derived from actual events, training and exercises into the EM planning process;
- including any program, arrangements, or other measures to provide for the continuity of operations in the EM plans by using the guidelines and best practices provided by Public Safety Canada;
- providing the Government Operations Centre, based on criteria identified by Public Safety Canada, with information collected under the institution's authorities that affects or can affect Canada's national interests and contributes to national level situational awareness;
- providing post-exercise and post-event information related to whole-of-government response to Public Safety Canada in accordance with the Guidelines and improvement process provided to federal government institutions; and
- putting in place any required service level agreements (SLA), memoranda of understanding (MOU) and mutual assistance agreements with external stakeholders to ensure that services and/or facilities as well as equipment are secured in an emergency.

Activities Tip!

Federal government institutions should consider personnel surge capacity requirements in their plans to support sustained operations, as well as the ability to react to any additional hazard or event that may occur while the response and recovery operations are taking place. This capacity can be supported through a number of mechanisms, including mutual assistance agreements between jurisdictions and other pan-Canadian resources, such as professional associations, corporations and non-government organizations (e.g., Canadian Veterinary Medical Association to provide surge capacity in the case of a major animal disease outbreak in Canada).

Activities Tip!

Integrate the Incident Command System (ICS) into your response framework. The ICS helps to promote clear lines of authority, is scalable to large or small events, and is widely used by first responders such as police or fire departments in various jurisdictions. It is also the basis of the response framework for the FERP.

Activities Tip!

Think about engaging your communications branch so that they are aware of internal and external communications requirements. This will also help you target key message as appropriate.

Activities Tip!

Once the event is over and response operations are completed, federal institutions should participate in any whole-of-government reviews as appropriate. Federal institutions should also undertake their own internal reviews through meetings with all staff and stakeholders involved in the incident response to compare notes on the recovery operations, identify the lessons learned and best practices, and finalize the after event report (AER) and the Capability Improvement Process (CAIP) matrix.

Response

The objective of planning activities associated with institutional responses to changing threats, hazards or specific incidents is to have an effective and integrated response in accordance with established strategic priorities. Accordingly, the planning team may wish to:

- respond to emergencies, in a manner that is consistent with its areas of responsibility, the institutional response plan and existing arrangements;
- align event-specific and institutional response plans with the FERP in order to contribute, when requested, to an integrated Government of Canada response;
- support other federal government institutions, when requested, and take into account institutional capacity limitations to sustain their primary lead response capacity;
- undertake post-incident analysis and incorporate lessons learned and best practices into EM plans;
- provide the Government Operations Centre with information on updated institutional response activities (e.g., information requests, status of nationally coordinated response activities, emerging or changing threats, situational awareness products), in accordance with guidelines provided to federal government institutions; and
- take the necessary measures to confirm that trained and security-cleared liaison officers or subject matter experts are ready to be deployed and are provided, as required, by the Government Operations Centre to support an integrated response.

Recovery

The objective of planning activities associated with the recovery component of EM is to provide for the restoration and continuity of critical services and operations. Accordingly, the planning team may wish to consider:

- including arrangements or other measures for providing recovery assistance to provincial/territorial governments in support of the SEMP; and
- undertaking post-recovery analysis and incorporating lessons learned and best practices into regular reviews of the SEMP.

Activities Tip!

Consider developing an inventory of the plans that the institution currently has in place, and then "overlay" these plans with the risks that have been identified and the gaps requiring the attention of senior management, so that a decision can be made as to what other plans may need to be produced. The cross-reference table provided in Annex C, Appendix 5, as stated above, can serve as a tool to complete this task.

e. Identify requirements for threat/hazard-specific plans, business continuity plans and related EM plans

The information gathered to this point allows the EM planning team to identify specific requirements that will be useful for further planning related to developing threat/hazard-specific plans or BCPs.

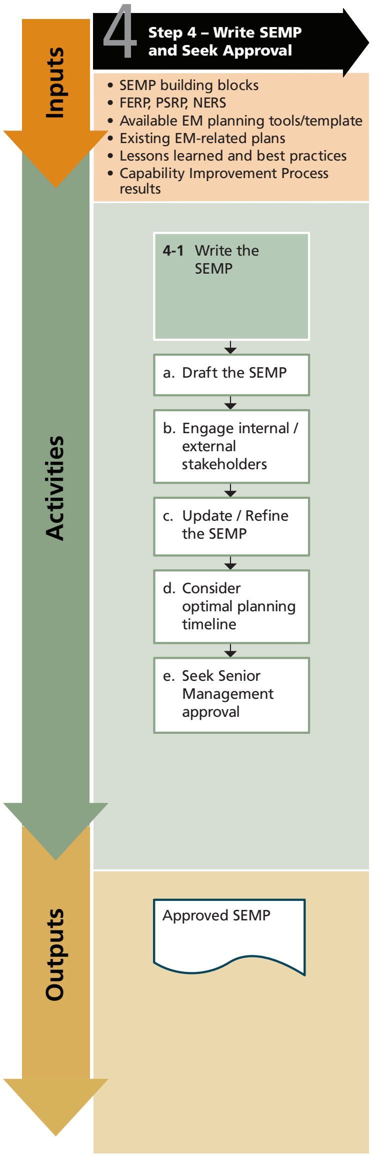
Outputs

Outputs

The outputs from the activities set out in Step 3 should include:

- an EM governance structure;
- a list of strategic priorities and planning considerations; and
- a list of plans to be developed in support of the SEMP (e.g., threat/hazard-specific plans, BCPs, related EM plans).

Step 4: Write the SEMP and seek approval


4
Step 4 – Write SEMP and Seek Approval
Inputs
• SEMP building blocks
• FERP, PSRP, NERS
• Available EM planning tools/template
• Existing EM-related plans
• Lessons learned and best practices
• Capability Improvement Process results
Activities
4-1 Write the SEMP
a. Draft the SEMP
b. Engage internal / external stakeholders
c. Update / Refine the SEMP
d. Consider optimal planning timeline
e. Seek Senior Management approval
Outputs
Approved SEMP

The SEMP establishes a federal government institution's objectives, approach and structure for protecting Canadians and Canada from threats and hazards in their areas of responsibility, and sets out how the institution will assist the coordinated federal emergency response. It should be strategic and be designed to have safeguards and processes to trigger appropriate actions in response to changing threats and hazards, as well as in response to specific incidents and events.

Inputs

Planning inputs into the development of the SEMP should include key linkages, including, but not limited, to:

- SEMP building blocks;
- the Federal Emergency Response Plan (FERP);
- the Public Service Readiness Plan (PSRP);
- the National Emergency Response System (NERS);
- available EM planning tools / templates;
- existing EM-related plans;
- lessons learned and best practices; and
- Capability Improvement Process results.

An effective SEMP is generally characterized in the following terms:

- *Comprehensive* – Considers and takes into account all hazards, all phases, all stakeholders and all impacts relevant to disasters
- *Progressive* – Anticipates future disasters and takes preventive and preparatory measures to build disaster-resistance and disaster-resiliency
- *Risk-Driven* – Uses sound risk management principles (hazard identification, risk analysis and impact analysis) in assigning priorities and resources
- *Integrated* – Helps ensure unity of effort among all levels of government and all elements of a community
- *Collaborative* – Creates and sustains broad and sincere relationships among individuals and organizations to encourage trust, advocate a team atmosphere, build consensus and facilitate communication
- *Coordinated* – Synchronizes the activities of all relevant stakeholders to achieve a common purpose
- *Flexible* – Uses creative and innovative approaches to solving challenges
- *Professional* – Values a science- and knowledge-based approach founded on education, training, experience, ethical practice, public stewardship and continuous improvement

Activities

4-1 Write the SEMP

In order to develop an effective SEMP, institutions are encouraged to consider the following activities:

a. Draft the SEMP

Activities Tip!

For plans that will not reside as an appendix to the SEMP, a consolidated list of plans can be provided in the SEMP. Include information on its owner and location.

To assist in this step, a template for a SEMP is provided in Annex B. The template serves as an outline that can be modified to meet institutional requirements and provides additional guidance on how to complete each section. The template comprises six parts:

Part I: Introduction – Provides general information about the institution's primary mandate/mission and clearly stated objectives, including the main goals of the plan and the method for attaining those goals. It should also provide an overview of any legislative requirements, limitations and authorities.

Part II: Risk Environment – Highlights the results of Step 2 – Orientate, including the environmental scan, criticality/threat/vulnerability assessments, the all-hazards risk assessment and the federal government institution's ability to respond.

Part III: Concept of Operations – Forms the main part of the plan, provides the details on the EM governance structure, and assigns specific tasks for each phase of the EM process.

Part IV: Roles and Responsibilities – Identifies the functional roles and responsibilities of internal and external agencies, organizations, departments/government institutions and those pre-determined areas of responsibility that support the SEMP. It also identifies lines of authority for internal and external agencies, organizations, departments/government institutions and positions.

Part V: Logistical Support and Resource Requirements – Identifies logistical support and resource requirements (annexes may be used to expand as required). It also details any financial management and administrative requirements.

Part VI: Plan Testing, Review and Maintenance – Outlines the procedures to be followed with regards to exercising and reviewing the SEMP, as well as the SEMP's "evergreening" process. It also describes how the SEMP will be updated based on after action reports and the Capabilities Improvement Process.

Appendices – Supporting plans (e.g., operational plans, regional EM plans, BCPs and communications/media plans) can be included as appendices to the SEMP or can be issued as separate and stand-alone plans.

b. Engage internal and external stakeholders

While writing the SEMP, it is important to once again engage internal and external stakeholders in order to have a comprehensive approach to plan development. This will also assist in open communications with key partners.

c. Update/refine the SEMP

Once stakeholder consultations are concluded, the final draft of the SEMP is prepared for review by senior management. Steps can include integration of comments from consultation.

d. Consider optimal planning timeline

In order to support the continued resourcing and relevance of the SEMP, federal government institutions should consider the optimal planning timeline for developing and reviewing the plan. It may be beneficial to align the EM planning cycle to the Government's business planning cycle, as demonstrated in Section Two.

e. Seek senior management approval

The final stage in developing the SEMP is to seek the approval of senior management. This will provide the authority for the SEMP to be implemented.

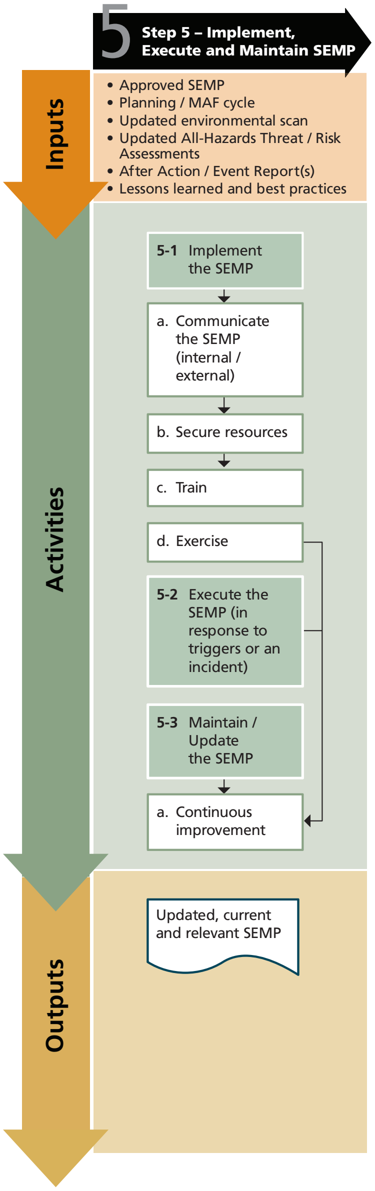
Outputs

Outputs

The output of Step 4 is an approved SEMP.

4 Section Four: Implementing and Maintaining the SEMP

Step 5: Implement, execute and maintain the SEMP



5 Step 5 – Implement, Execute and Maintain SEMP

Inputs

- Approved SEMP
- Planning / MAF cycle
- Updated environmental scan
- Updated All-Hazards Threat / Risk Assessments
- After Action / Event Report(s)
- Lessons learned and best practices

Activities

5-1 Implement the SEMP

a. Communicate the SEMP (internal / external)

b. Secure resources

c. Train

d. Exercise

5-2 Execute the SEMP (in response to triggers or an incident)

5-3 Maintain / Update the SEMP

a. Continuous improvement

Outputs

Updated, current and relevant SEMP

Inputs

The final step of the EM planning process is to implement and maintain the SEMP and, in response to trigger(s) or an incident, to execute the SEMP. The inputs that contribute to this step include:

- the approved SEMP;
- the planning/MAF cycle;
- an updated environmental scan;
- an updated all-hazards threat assessment;
- an updated all-hazards risk assessment;
- after action report(s) and after event report(s); and
- lessons learned and best practices.

Activities

5-1 Implement the SEMP

In order to implement the approved SEMP, the following activities are recommended:

a. Communicate the SEMP (internal and external)

The final and approved version of the institution's SEMP should be distributed to all members of the EM governance structure, the EM planning team, those employees who have key roles and responsibilities, and other stakeholders. This includes distribution to the communications branch to ensure that they have it readily available.

Activities Tip!

Blackberries are an excellent tool and can serve as a storage device for your SEMP. Ask your IT team how it can be uploaded to your device.

b. Secure resources

The SEMP must be resourced. This process involves assessing available resources including supporting departments' emergency support functions (ESFs) and their ability to respond. Key questions to consider include:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us as quickly as we may need them, or will they have other priority areas to serve?

If the answers are no, identify what can be done to correct the problem. For example, you may need to:

- develop additional emergency procedures;
- request resources through the business planning process;
- conduct additional training;
- acquire additional equipment;
- establish mutual assistance agreements; and
- reconsider the strategies that were developed.

Activities Tip!

Public Safety Canada's Canadian Emergency Management College (CEMC) can assist federal government institutions in bridging the knowledge gap for those involved in EM activities. The CEMC will offer a course on developing a SEMP in early 2011.

c. Train

During the development of the SEMP, an individual should be assigned responsibility for developing and supporting a training plan/schedule. The training plan should consider the training and information needs of employees, contractors, managers and those with an emergency response role identified in the SEMP. Over a 12-month period, the training plan should address the following questions:

- What will be the content and objectives of the training?
- Who will be trained?
- Who will do the training?
- What training activities will be used?
- When and where will each session take place?
- How will the session(s) be evaluated and documented?

d. Exercise

As set out in Section 6 of the EMA, federal institutions should develop and regularly conduct exercises to test their SEMP. An exercise is a focused practice activity that places the participants in a simulated situation requiring them to function in the capacity that would be expected of them in a real event. Its purpose is to promote preparedness by testing policies and plans and by training personnel.

There are a number of reasons for conducting exercises. Through exercises, organizations can:

- test and evaluate plans, policies and procedures;
- reveal planning weaknesses;
- reveal gaps in resources;
- improve organizational coordination and communications;
- clarify roles and responsibilities;
- improve individual performance; and
- satisfy regulatory requirements.

Exercises can be designed to test individual essential elements, interrelated elements, or the entire plan(s). They can take many forms, such as:

- drills;
- table top exercises;
- full-scale exercises; and
- functional exercises.

One objective of an exercise should ideally be to identify problem areas for resolution/ corrective action before an actual emergency occurs. It is important to keep records of events that occur throughout the exercise and to take note of what works, what does not work, and areas in need of improvement (e.g., clarity of roles and responsibilities).

After any exercise, consider completing an after activity report (AAR). The AAR should ideally recommend potential improvements to plans, policies, processes or procedures, closure of gaps or additional training required as best practices. The AAR should be accompanied by the CAIP matrix to track identified corrective actions. In addition, the SEMP should ideally be reviewed following any exercise, in order to incorporate lessons learned and best practices identified though the CAIP.

For further information, please contact EMPlanning.Guide@ps-sp.gc.ca.

5-2 Execute the SEMP

The SEMP should be executed in response to established triggers, an incident or a planned event. Institutions should consider developing concise SOPs to address how the relationship and interdependencies with other federal government institutions will be initiated when the SEMP needs to be executed.

The scale of the incident/event will dictate the response level and the degree to which all or part of the SEMP will be carried out. Once triggered, the SEMP will be executed in alignment with the FERP and in accordance with operational guidance provided by the federal government institution’s senior management responsible for EM or assigned lead. Operational guidance can include response and execution considerations such as an Incident Command System.

After any event/incident, consider completing an after event report (AER). The AER should ideally recommend potential improvements to plans, policies, processes or procedures, or additional training required.

5-3 Maintain/update the SEMP

The SEMP should be reviewed once every two years. In addition to periodic reviews, institutions are encouraged to maintain and update the SEMP through the following activities:

a. Continuous improvement

Continuous capability improvement, including incremental and transformational change, is undertaken systemically as an integral part of EM functions and practices at all levels, as appropriate, to minimize the recurrence of problems. Although reflected in Step 5 of the blueprint, capability improvement applies to all steps of the planning process.

A formal CAIP should be initiated under the following circumstances:

- after each training drill or exercise;
- after each emergency event / incident;
- when personnel or their responsibilities change;
- when there are changes in the institution’s mandate or mission; and
- when policies or procedures change.

As well, conducting an evaluation of the entire SEMP once every two years or as appropriate should be considered. The issues to be considered include the following:

- How can all levels of management be engaged in evaluating and updating the SEMP?
- Does the SEMP reflect lessons learned and best practices from exercises and actual events?
- Do members engaged in the EM process understand their respective responsibilities? Have new members been trained?
- Is the institution attaining its training objectives?
- Have the hazards affecting the institution changed?
- Are the names, titles and telephone numbers in the SEMP current?
- Have partner agencies and other federal government institutions been briefed on the plan? Are they involved in evaluating the SEMP?

Outputs

Output

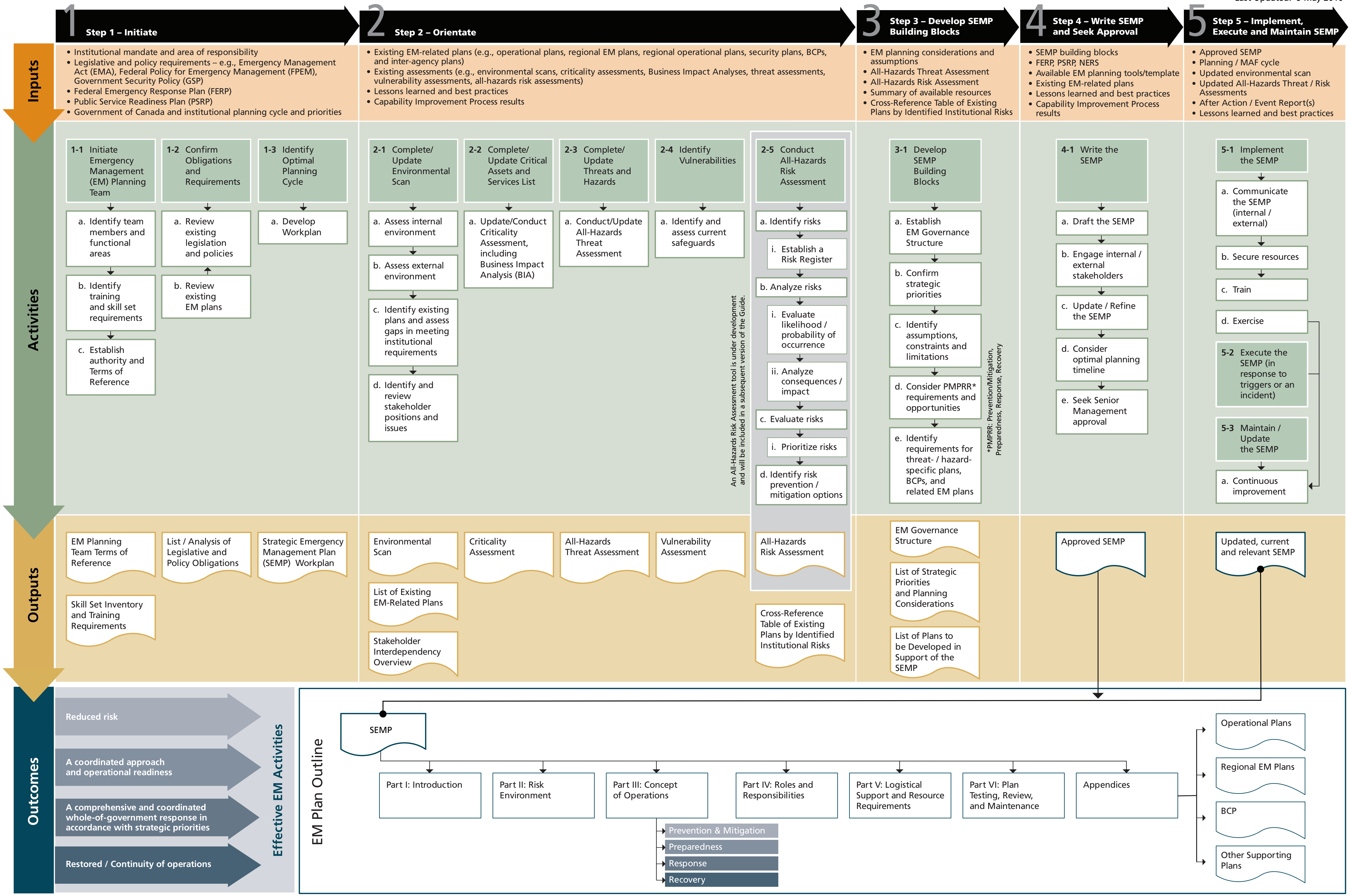
The output of Step 5, the final but continuous step in the EM planning process, is an updated, current and relevant SEMP.

A Annexes

Emergency Management Planning Guide Blueprint

Annex A – Emergency Management Planning Guide Blueprint

Last Updated: 5 May 2010



Inputs

Activities

Outputs

Outcomes

1 Step 1 – Initiate

Inputs

- Institutional mandate and area of responsibility
- Legislative and policy requirements – e.g., Emergency Management Act (EMA), Federal Policy for Emergency Management (FPEM), Government Security Policy (GSP)
- Federal Emergency Response Plan (FERP)
- Public Service Readiness Plan (PSRP)
- Government of Canada and institutional planning cycle and priorities

Activities

1-1 Initiate Emergency Management (EM) Planning Team

- a. Identify team members and functional areas
- b. Identify training and skill set requirements
- c. Establish authority and Terms of Reference

1-2 Confirm Obligations and Requirements

- a. Review existing legislation and policies
- b. Review existing EM plans

1-3 Identify Optimal Planning Cycle

- a. Develop Workplan

Outputs

- EM Planning Team Terms of Reference
- Skill Set Inventory and Training Requirements
- List / Analysis of Legislative and Policy Obligations
- Strategic Emergency Management Plan (SEMP) Workplan

2 Step 2 – Orientate

Inputs

- Existing EM-related plans (e.g., operational plans, regional EM plans, regional operational plans, security plans, BCPs, and inter-agency plans)
- Existing assessments (e.g., environmental scans, criticality assessments, Business Impact Analyses, threat assessments, vulnerability assessments, all-hazards risk assessments)
- Lessons learned and best practices
- Capability Improvement Process results

Activities

2-1 Complete/ Update Environmental Scan

- a. Assess internal environment
- b. Assess external environment
- c. Identify existing plans and assess gaps in meeting institutional requirements
- d. Identify and review stakeholder positions and issues

2-2 Complete/ Update Critical Assets and Services List

- a. Update/Conduct Criticality Assessment, including Business Impact Analysis (BIA)

2-3 Complete/ Update Threats and Hazards

- a. Conduct/Update All-Hazards Threat Assessment

2-4 Identify Vulnerabilities

- a. Identify and assess current safeguards

2-5 Conduct All-Hazards Risk Assessment

- a. Identify risks
  - i. Establish a Risk Register
- b. Analyze risks
  - i. Evaluate likelihood / probability of occurrence
  - ii. Analyze consequences / impact
- c. Evaluate risks
  - i. Prioritize risks
- d. Identify risk prevention / mitigation options

An All-Hazards Risk Assessment tool is under development and will be included in a subsequent version of the Guide.

Outputs

- Environmental Scan
- List of Existing EM-Related Plans
- Stakeholder Interdependency Overview
- Criticality Assessment
- All-Hazards Threat Assessment
- Vulnerability Assessment
- All-Hazards Risk Assessment
- Cross-Reference Table of Existing Plans by Identified Institutional Risks

3 Step 3 – Develop SEMP Building Blocks

Inputs

- EM planning considerations and assumptions
- All-Hazards Threat Assessment
- All-Hazards Risk Assessment
- Summary of available resources
- Cross-Reference Table of Existing Plans by Identified Institutional Risks

Activities

3-1 Develop SEMP Building Blocks

- a. Establish EM Governance Structure
- b. Confirm strategic priorities
- c. Identify assumptions, constraints and limitations
- d. Consider PMPRR* requirements and opportunities
- e. Identify requirements for threat- / hazard-specific plans, BCPs, and related EM plans

*PMPRR: Prevention/Mitigation, Preparedness, Response, Recovery

Outputs

- EM Governance Structure
- List of Strategic Priorities and Planning Considerations
- List of Plans to be Developed in Support of the SEMP

4 Step 4 – Write SEMP and Seek Approval

Inputs

- SEMP building blocks
- FERP, PSRP, NERS
- Available EM planning tools/template
- Existing EM-related plans
- Lessons learned and best practices
- Capability Improvement Process results

Activities

4-1 Write the SEMP

- a. Draft the SEMP
- b. Engage internal / external stakeholders
- c. Update / Refine the SEMP
- d. Consider optimal planning timeline
- e. Seek Senior Management approval

Outputs

- Approved SEMP

5 Step 5 – Implement, Execute and Maintain SEMP

Inputs

- Approved SEMP
- Planning / MAF cycle
- Updated environmental scan
- Updated All-Hazards Threat / Risk Assessments
- After Action / Event Report(s)
- Lessons learned and best practices

Activities

5-1 Implement the SEMP

- a. Communicate the SEMP (internal / external)
- b. Secure resources
- c. Train
- d. Exercise

5-2 Execute the SEMP (in response to triggers or an incident)

5-3 Maintain / Update the SEMP

- a. Continuous improvement

Outputs

- Updated, current and relevant SEMP

Outcomes

Effective EM Activities

- Reduced risk
- A coordinated approach and operational readiness
- A comprehensive and coordinated whole-of-government response in accordance with strategic priorities
- Restored / Continuity of operations

EM Plan Outline

SEMP

- Part I: Introduction
- Part II: Risk Environment
- Part III: Concept of Operations
  - Prevention & Mitigation
  - Preparedness
  - Response
  - Recovery
- Part IV: Roles and Responsibilities
- Part V: Logistical Support and Resource Requirements
- Part VI: Plan Testing, Review, and Maintenance
- Appendices
  - Operational Plans
  - Regional EM Plans
  - BCP
  - Other Supporting Plans

Annex B

Strategic Emergency Management Plan Template

Annex B – Strategic Emergency Management Plan Template

(Federal Institution Name)
Strategic Emergency Management Plan

(Month, Year)

Preface

This template was developed to assist federal government institutions in developing a Strategic Emergency Management Plan (SEMP). It will assist federal government institutions in meeting federal legislative requirements. This template serves as an outline that can be modified to meet institutional requirements and provides guidance on how to complete each section.

Text in black is proposed wording to complete a section that is more generic in nature; black text in brackets indicates sections to be customized. All text in blue italics serves as guidance on how to complete each section and should be deleted prior to finalizing the plan.

Table of Contents

1. Introduction

(Provide a general introduction to the SEMP and discuss the most common emergencies affecting the institution's area of responsibility.)

1.1 Purpose

The purpose of (institution name)'s Strategic Emergency Management Plan (SEMP) is to provide *(insert text)*.

(Clearly identify the intention of the plan as it relates to your organization. This should be one paragraph.)

1.2 Authorities and legislative requirements

The *Emergency Management Act 2007* (EMA) states that each federal minister is responsible for the identification of risks that are within or related to his or her area of responsibility, including those related to critical infrastructure. Under the EMA, ministers are required to prepare emergency management plans in respect of those risks; maintain, test and implement the plans; and conduct exercises and training in relation to the plans.

(Other relevant federal legislation should be identified. Specify areas of legislation that are specific to the institution and that were considered in preparation of the SEMP.)

This plan is consistent with the Federal Emergency Response Plan (FERP) and is an evergreen document that will evolve over time.

1.3 Scope

(This section should identify what the SEMP addresses and what it does not.)

1.4 Background

Comprehensive and integrated emergency management is a shared responsibility between all levels of governments, the private sector, non-governmental organizations and individual citizens. A key function for the Government of Canada is to promote the safety and security of Canada and Canadians. With respect to (institution name), the Minister is responsible for prevention/mitigation of, preparedness for, response to and recovery from emergencies *(indicate area of responsibility).*

(Include applicability of the SEMP to the institution and discuss historical data of relevance to understanding the current context.)

Four pillars of effective emergency management in Canada have been considered in all aspects of this plan and are described as follows:

Prevention and mitigation – Actions taken to identify and reduce the impacts and risks of hazards before an emergency or disaster occurs.

Preparedness – increases a community's ability to respond quickly and effectively to emergencies and to recover more quickly from their long-term effects, and involves actions taken prior to an event to ensure the capability and capacity to respond.

Response – actions taken during or immediately after an emergency or disaster to manage the consequences.

Recovery – actions taken after an emergency or disaster to re-establish or rebuild conditions and services to an acceptable level.

1.5 Objectives

(Identify the objectives of the SEMP. This can be informed by the SEMP building blocks developed in Step 3 of the Emergency Management Planning Guide.)

2. Risk Environment

(Define the institution's risk environment based on the outputs of Step 2 of the Emergency Management Planning Guide. These outputs include the environmental scan, the criticality assessment and the all-hazards risk assessment.)

3. Concept of operations

(This is the main part of the SEMP. It provides the details on the EM governance structure and details plans for each pillar of EM: Prevention/Mitigation, Preparedness, Response and Recovery. A diagram should be included to illustrate the institution's EM governance structure. The inter-relationships during an emergency between the institution in question and the rest of the Government of Canada, as well as provincial and territorial EM organizations and other key stakeholders, should also be described and possibly represented graphically. Response levels should also be defined.)

3.1 (Institution)'s emergency management governance structure

The *(institution)'s* emergency management governance structure is consistent with the structure of the Government of Canada as outlined in the FERP, which involves engaging existing governance structures to the greatest extent possible in responding to an emergency. The federal governance structure, which parallels the structures of most provincial/territorial counterparts, includes the Committee of Cabinet, the Deputy Ministers' Committee and the Assistant Deputy Ministers' Emergency Management Committee.

3.1.1 Minister

The (institution) Minister is the lead (complete as applicable).

3.1.2 Deputy Minister

The Deputy Minister of (*institution*) sits on the *(complete as applicable)***.**

3.1.3 Committee of Cabinet

3.1.4 (Other governance role, as applicable)

3.1.5 (Other governance role, as applicable)

3.1.6 Structure

(Insert a diagram of the governance structure and define the inter-relationships.)

4. Roles and responsibilities

4.1 Appointment or organization (as applicable)

(Identify the functional roles and responsibilities of internal and external agencies, organizations, departments/government institutions and positions. As well, identify the lines of authority for internal and external agencies, organizations, departments/government institutions and positions.)

5. Logistical support and resource requirements

(Describe logistics support and resource requirements. Appendices may be used to expand if required. Financial management requirements should also be identified in this section.)

6. Plan testing, review and maintenance

(Outline the procedures to be followed with regards to testing, exercising, maintaining and reviewing the SEMP. Refer to Step 5 of the Emergency Management Planning Guide for more details.)

7. Appendices

(Supporting plans – e.g., operational plans, regional EM plans, BCPs and communications/media plans – can be included as appendices to the SEMP or can be issued as separate, stand-alone plans. For plans that will not reside as an appendix to the SEMP, a consolidated list of plans can be provided in the SEMP. Include information on its owner and location.)

Possible appendices:

Appendix A: List of Existing EM-Related Plans (e.g., operational plans, regional EM plans, BCPs and communications/media plans)

Appendix B: Cross-Reference Table of Existing Plans by Identified Institutional Risks

Appendix C: Emergency Contact List

Appendix D: Glossary

Supporting Planning Tools and Templates

Annex C

Appendix 1: Emergency Management Planning Team – Terms of Reference Template

Background

A core responsibility of the Government of Canada is to promote the safety and security of Canada and Canadians. Emergencies, disruptions and other threats have the capacity to endanger life, personal health and safety and property, and to disrupt service delivery to Canadians. The Government of Canada has adopted an all-hazards approach to emergency management, encompassing four interdependent, but integrated functions: mitigation, preparedness, response and recovery.

Federal government institutions are responsible under the *Emergency Management Act* to identify the risks that are within or related to their area of responsibility, including those related to critical infrastructure, and to prepare emergency management plans in respect to those risks; maintain, test and implement those plans; and conduct exercises and training in relation to those plans.

The Federal Policy for Emergency Management requires government institutions to develop mandate-specific emergency management plans, based on an all-hazards risk assessment, that include a program, arrangement or other measure to address mitigation/prevention, preparedness, response and recovery. It also details the responsibilities of federal government institutions within each of the four integrated functions. This template provides further details on the responsibilities identified in the Federal Policy for Emergency Management to support senior departmental officials, managers and coordinators in meeting their integrated departmental emergency management planning requirements under the *Emergency Management Act*.

The *Emergency Management Planning Guide,* developed by Public Safety Canada, provides guidance to assist federal government institutions with the completion of their Strategic Emergency Management Plan (SEMP). It provides a comprehensive overview of the steps and process required to produce a SEMP. This Guide should serve as the primary resource for the planning team.

Team composition

The size of the planning team will depend on the federal government institution's scope of operations, requirements and resources. Regardless of the size of the core planning team, it should seek input from the following areas:
How can all levels of management be engaged in evaluating and updating the SEMP?
All functional program areas
Corporate Services, including Human Resources, Occupational Health and Safety, Communications, Security, Legal, and Finance, as well as regional offices.

Mandate

Mission statement

On authority of the federal government institution’s senior management, the planning team develops and issues a mission statement. The statement:

- defines the purpose of the plan and indicates that it will involve the entire organization; and
- defines the authority and structure of the planning group.

Schedule and budget

One of the first tasks of the planning team is to establish a work schedule and planning deadlines. Timelines can be modified as priorities become more clearly defined.
Develop an initial budget for such things as training, research, workshops and other expenses that may be necessary during the development process.

Governance

This section outlines the “governance structure” of the planning team and may involve expansion on separate terms of reference for key team members, such as the planning team leader. A sample individual TOR is attached to this document.

At a minimum, this section should outline the reporting chain for the planning team.

Meetings

This section outlines how many meeting that the planning team will undertake and can include a draft schedule for those meetings (e.g., “The planning team will meet every two weeks…”).

Work Plan

This section provides a high-level overview of the planning team’s work plan and should include the key initiatives, such as delivery of the draft emergency management plan to senior management.

Deliverable(s)

This section provides an outline of the key deliverables that the planning team is expected to provide and may include details on the format of those deliverables (e.g., PowerPoint presentation to senior management).

Resources and support

This section provides details on the resources and support that the planning team requires as well as information on how those assets/resources will be allocated.

Partner with your communications branch in the development of a communications plan to support internal notification and/or public emergency communications so that a protocol and approach is worked out prior to any situation.

Emergency Management Planning Team Leader—Terms of Reference

Responsibility: This position will primarily be responsible for leading the team that will develop the EM plan.

Activities may include:

- task management;
- facilitation of stakeholder meetings;
- data collection and analysis;
- development of concepts of operations;
- coordination of other integral planning documents; and
- oversight over the development of plan annexes to support communications and notification, emergency public information, and resource management and logistics.

Office of Primary Interest (OPI):
Effective Date:
Approved Version Number:
File Name:

Annex C

Appendix 2: SWOT and PESTLE Analysis

A **SWOT analysis** is a planning tool used to evaluate the **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats of an organization as they relate to a set outcome.

- **S**trengths — attributes of the organization that are helpful to achieving the objective(s)
- **W**eaknesses — attributes of the organization that are harmful to achieving the objective(s)
- **O**pportunities — *external* conditions that are helpful to achieving the objective(s)
- **T**hreats — *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 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 <1yr, medium 2-3 yrs, long term 3+ years)**	**Impact (low, medium, high) and relevance**	**Internal or external to institution**	**Action (if applicable)**

Annex C

Appendix 3: Hazards and Threats for the Canadian Context

Below is a comprehensive but non-exhaustive list of hazards and threats relevant to the Canadian context. For further information, you may wish to consult the Canadian Disaster Database, which contains detailed disaster information on over 900 natural, technological and conflict events (excluding war) that have directly affected Canadians over the past century. The database can help federal government institutions to better identify, assess and manage risks, and can be accessed by sending a request to Public Safety Canada email cdd-bdc@ps-sp.gc.ca.

Naturally occurring hazards		
Geological hazards	**Meteorological hazards**	**Biological hazards**
Earthquake	Flood, flash flood, seiche, tidal surge	Diseases that impact humans or animals (e.g., plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), influenza pandemic, bovine spongiform encephalopathy (BSE))
Tsunami	Drought	Animal or insect infestation or damage
Volcano	Fire (e.g., forest, range, urban, wildland, and urban interface)	
Landslide, mudslide, subsidence	Snow, ice, hail, sleet, avalanche	
Glacier, iceberg	Windstorm, tropical cyclone, hurricane, tornado, water spout, dust/sand storm	
	Extreme temperatures	
	Lightning strikes	
	Geomagnetic storm	

Human-induced events	
Unintentional events	**Intentional events**
Hazardous material spill or release (e.g., explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, radiological, corrosive)	Attacks (e.g., explosive, chemical, biological, radiological, nuclear, cyber)
Explosion/fire	Sabotage
Transportation accident	Civil disturbance, public unrest, mass hysteria, riot
Building/structure collapse	Enemy attack, war
Energy/power/utility failure	Insurrection
Fuel/resource shortage	Strike or labour dispute
Air/water pollution, contamination	Disinformation
Water control structure/dam/levee failure	Criminal activity (e.g., vandalism, arson, theft, fraud, embezzlement, data theft)
Financial issues, economic depression, inflation, financial system collapse	Electromagnetic pulse
Communications system interruptions	Physical or information security breach
Misinformation	
Critical infrastructure failure/disruption: structure/building failure	
Shortage/failure of critical services: telecommunication, electricity, fuel supply, information technology services and products, food safety, provision of government services, health services, manufacturing services, safety and emergency response services, transportation services, water service	

Annex C

Appendix 4: Cross-Reference Table of Existing Plans by Identified Institutional Risks

Risk	Prevention and mitigation	Preparedness	Response	Recovery
List all risks that could have an impact on your institution's operations/ environment (e.g., flood, acts of terrorism)	Identify the activity that would be enacted against the identified risk	Identify the plan that would be enacted against the identified risk	Identify the plan that would be enacted against the identified risk	Identify the plan that would be enacted against the identified risk
Example 1: Flood			National Flood Plan	
Example 2: Acts of terrorism		BCP	BCP	

Annex C

Appendix 5: References and Information Sources

Emergency Management Act (2007), Statutes of Canada (2007)

Emergency Management Framework for Canada (2008), Public Safety Canada

Federal Emergency Response Plan (2009), Public Safety Canada

Federal Policy for Emergency Management (2009), Public Safety Canada

National Emergency Response System, Public Safety Canada

Canada's National Disaster Mitigation Strategy, Public Safety Canada

Business Continuity Program Standard, Public Safety Canada

Policy on Evaluation (2009), Treasury Board Secretariat

Government Security Policy (2009), Treasury Board Secretariat

Communications Policy of the Government of Canada (2006), Treasury Board Secretariat

Canadian Standards Association, *Draft Standard CAN/CSA-Q850 – Risk Management: Implementation of CAN/CSA-ISO-31000* (2010)

International Organization for Standardization, *Draft International Standard ISO/DIS 31000 – Risk Management – Principles and Guidelines on Implementation* (2009)

International Organization for Standardization, *Draft Risk Management Vocabulary (2009), ISO/TMB WG on Risk Management N 066*

Treasury Board of Canada Secretariat, *Draft Risk Taxonomy* (2010), Centre of Excellence on Risk Management

Treasury Board of Canada Secretariat, *Draft Guide to Integrated Risk Management* (2010), Interdepartmental Working Group on Integrated Risk Management

Glossary

Annex D – Glossary

The following definitions* are provided to guide the reader and provide appropriate context. These definitions are to be used solely in the context of this planning guidance.

All-hazards emergency management planning

An approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the event, thereby permitting an optimization of scarce planning, response and support resources. The intention of all-hazards generic emergency planning is to employ generic methodologies, modified as necessary by particular circumstances.

All-hazards incorporates natural and man-made hazards threats including traditional emergency management events such as flooding and industrial accidents; as well as national security events such as acts of terrorism; and cyber events. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Asset

Any tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation. (*Government Security Policy* (2009). Treasury Board of Canada Secretariat).

Business continuity planning

An all-encompassing term that includes the development and timely execution of plans, measures, procedures, and arrangements to ensure minimal or no interruption to the availability of critical services and assets. (*Public Service Readiness Plan* (2008). Treasury Board of Canada Secretariat).

Business impact analysis

The process of determining the impact on an organization should a potential loss identified by the risk analysis actually occur. The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial, loss of life or other standpoint. (*Business Continuity Plan (BCP) Template*. Public Safety Canada).

Capability Improvement Process

The CAIP ensures that recommendations observed during real events and exercises are collected, appropriately stored and analyzed. This whole-of-government process provides the basis for recommended corrective actions and/or institutionalization of best practices aimed at improved capabilities across federal government institutions. (Public Safety Canada).

Critical service

Service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the effective functioning of the Government of Canada and must be continuously delivered (has no or very limited downtime). (Public Safety Canada).

Concept of operations

Concept of operations provides a framework to operationalize horizontal management and an effective governance structure and delineates clear roles and responsibilities of the principal committees and individuals central to each phase of the incident management process. (*Public Service Readiness Plan* (2008). Treasury Board of Canada Secretariat).

Critical infrastructure

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. (*National Strategy and Action Plan for Critical Infrastructure*. Public Safety Canada).

Emergency

A present or imminent event, including IT incidents, that requires prompt coordination of actions to protect the health, safety or welfare of people, or to limit damage to assets or the environment. **(***An Emergency Management Framework for Canada*. Public Safety Canada).

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. **(***An Emergency Management Framework for Canada*. Public Safety Canada).

***Emergency Management Act* (2007)**

The EMA sets out the responsibilities for all federal ministers regarding emergency management. (Public Safety Canada).

Emergency Management Framework for Canada

Sets out common principles that are at the heart of an emergency management framework in Canada. In essence, they reflect the key underlying beliefs and goals of emergency management. Their aim is to support the design, implementation and ongoing improvement of frameworks, programs, procedures, guidelines and activities that together comprise the emergency management system. (Public Safety Canada).

Emergency operations centre

A designated facility established by an agency or jurisdiction to coordinate the overall agency or jurisdictional response and support to an emergency. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Emergency support function

Emergency support functions are emergency response actions in support of the needs that are anticipated to arise prior to or during an emergency. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Environmental scan

The process by which key external and internal factors and risks influencing an organization's policy and management agenda are identified. (*Integrated Risk Management Framework*. Treasury Board of Canada Secretariat).

Federal government institution

Any department, branch, office, board, agency, commission, corporation or other body for the administration or affairs of which a minister of the Crown is accountable to Parliament. (*Emergency Management Act*, Public Safety Canada).

Federal Policy for Emergency Management (2009)

The FPEM policy promotes an integrated and resilient whole-of-government approach to emergency management planning, which includes better prevention/mitigation of, preparedness for, response to, and recovery from emergencies. (*Federal Policy for Emergency Management* (2009). Public Safety Canada).

Government Operations Centre

Canada's strategic-level operations centre that coordinates the activities of hub of a network of operations centres run by a variety of federal departments and agencies during emergencies. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Hazard

A hazard is 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. **(***An Emergency Management Framework for Canada*. Public Safety Canada).

Incident

An occurrence or event, sometimes comparatively, trivial in itself, which precipitates or could precipitate political unrest, open warfare, etc. (Oxford English Dictionary)

Incident Command System

A standardized on-scene emergency-management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Management Accountability Framework

The MAF provides deputy heads and all public service managers with a list of management expectations that reflect the different elements of current management responsibilities. (Treasury Board of Canada Secretariat).

Management by objectives

This is one of the principles of the Incident Command System. Personnel agree to the objectives and understand their overall direction. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Probability

The likelihood that is expressed as a number between 0 and 1, where 0 indicates that the occurrence is impossible and 1 indicates definite knowledge that the occurrence has happened or will happen, where the ratios between numbers reflect and maintain quantitative relationships. (*DHS Risk Lexicon*. Department of Homeland Security).

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. (*An Emergency Management Framework for Canada*. Public Safety Canada).

Risk assessment

The concept of risk is defined as a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. (*DHS Risk Lexicon*. Department of Homeland Security).

Risk based

The concept that sound emergency management decision-making will be based on an understanding and evaluation of hazards, risks and vulnerabilities. **(***An Emergency Management Framework for Canada*. Public Safety Canada).

Risk management

The use of policies, practices and resources to analyze, assess and control risks to health, safety, environment and the economy. (*An Emergency Management Frameworks for Canada*. Public Safety Canada).

Situational awareness

Situational awareness is having insight into one's environment and circumstances to understand how events and actions will affect business objectives, both now and in the near future. (*Government Security Policy* (2009). Treasury Board of Canada Secretariat).

Standard operating procedures

SOPs are a set of instructions constituting a directive, covering those features of operations which lend themselves to a definite, step-by-step process of accomplishment. SOPs constitute a complete reference document or an operations manual that provides the purpose, authorities, duration, and details for the preferred method of performing a single function or a number of interrelated functions in a uniform manner. (*Producing Emergency Plans: A Guide for All-Hazards Emergency Operations for State, Territorial, Local, and Tribal Governments*. Department of Homeland Security).

Threat

The presence of a hazard and an exposure pathway; threats may be natural or human-induced, either accidental or intentional. (*Federal Emergency Response Plan* (2009). Public Safety Canada).

Threat assessment

The process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations and/or property. (*DHS Risk Lexicon*. Department of Homeland Security).

Vulnerability

The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of an organization or community to the impact of hazards. **(***An Emergency Management Framework for Canada*. Public Safety Canada).

Vulnerability assessment

A process for identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards. (*DHS Risk Lexicon*. Department of Homeland Security).

*Definitions also include explanations of the purpose and scope of terms.