Risk Management Guide for Critical Infrastructure Sectors

Public Safety Canada
Sécurité publique Canada

Foreword

Managing risk is a shared responsibility among all critical infrastructure stakeholders, including governments, industry partners, first responders and non-government organizations. While partnerships and information sharing represent the building blocks of the Canadian approach to enhancing the resiliency of critical infrastructure, these cannot be undertaken in isolation of risk management and the development of plans and exercises to address these risks.

Recognizing that the impacts of disruptions can cascade across sectors and jurisdictions, the purpose of this document is to provide practical guidance for implementing a coordinated, all-hazards approach to critical infrastructure risk management. Moving forward with this comprehensive risk management process requires federal departments and agencies to collaborate with their critical infrastructure partners, including industry stakeholders and other levels of government. While this guidance document promotes a common approach to critical infrastructure risk management, owners and operators and each jurisdiction are ultimately responsible for implementing a risk management approach appropriate to their situation.

This guide is adapted from the ISO 31000 International Standard: “Risk Management – Principles and guidelines on implementation”, and includes the following sections:

1. Overview, Principles and Process
2. Sector Networks: Communication and consultation
3. Sector Overviews: Part 1 – Sector Operations
4. Sector Overviews: Part 2 – Sector Risk Profile
5. Sector Overviews: Part 3 – Sector Workplan
6. Ongoing improvement and feedback

Sections 2 through 6 focus on implementation and contain the following sub-sections:

Key Elements: The inputs and expected deliverables.
Implementation: Recommended approaches to implementation.
Considerations: Questions, issues and challenges to consider.

One of the underlying principles of sound risk management is that of continuous improvement. To that end, this guide will be updated periodically based on lessons learned through the application of the process. The most recent guide, tools and other information to support an all-hazard risk management approach to critical infrastructure are being developed on an ongoing basis and can be found at the Public Safety Canada website at:
http://www.publicsafety.gc.ca/prg/em/ci/index-eng.aspx

Amendments Record

The following is a list of amendments to this guide:

#	Date	Amended By	Comments
1.0	2010 07 01	Critical Infrastructure Policy, Public Safety Canada	Initial version

FOREWORD 2

AMENDMENTS RECORD 3

1. OVERVIEW, PRINCIPLES AND PROCESS 6

1.1 THE VALUE OF MANAGING RISKS COLLECTIVELY 6
1.2 PRINCIPLES 7
1.3 PROCESS 9

2. SECTOR NETWORKS: COMMUNICATE AND CONSULT 11

2.1. KEY ELEMENTS 11
2.2. IMPLEMENTATION 11
2.3. CONSIDERATIONS 12

3. PART I – SECTOR OPERATIONS 14

3.1. KEY ELEMENTS 14
3.2. IMPLEMENTATION 14
3.3. CONSIDERATIONS 16

4. PART II – SECTOR RISK PROFILES 18

4.1 IDENTIFY RISKS 19
4.1.1 KEY ELEMENTS 19
4.1.2 IMPLEMENTATION 19
4.1.3 CONSIDERATIONS 21
4.2. ANALYZE RISKS 21
4.2.1 KEY ELEMENTS 21
4.2.2. IMPLEMENTATION 22
4.2.3 CONSIDERATIONS 22
4.3 EVALUATE RISKS 23
4.3.1 KEY ELEMENTS 23
4.3.2 IMPLEMENTATION 23
4.3.2 CONSIDERATIONS 24

5. PART III – SECTOR WORKPLAN 25

5.1 KEY ELEMENTS 25
5.2 IMPLEMENTATION 26
5.2.1 DEVELOP MITIGATION GOALS AND OBJECTIVES 26
5.2.2. DEVELOP AN IMPLEMENTATION PLAN 26
5.3 DEVELOP AN EXERCISE PLAN 29

5.4 CONSIDERATIONS 30

6. ONGOING IMPROVEMENT AND FEEDBACK 32

6.1 KEY ELEMENTS 32
6.2 IMPLEMENTATION 32
6.3 CONSIDERATIONS 33

ANNEX A: TERMS AND GLOSSARY 34

ANNEX B: LIST OF HAZARDS AND THREATS 36

1. Overview, Principles and Process

> *The practice of risk management is well-developed within the insurance, engineering, finance, and political risk industries. It is clear, however, that risk management remains relatively immature in its application to the homeland security field. Some might argue that the implementation of risk assessment and management in the homeland security and counterterrorism fields may be more complex than in its industrial application where the primary objective is to protect against financial loss.*
>
> - "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress", Congressional Research Service, February 2007

1.1 The value of managing risks collectively

Organizations undertake a number of activities to mitigate risks to their operations through a combination of:

- Strategic planning to set objectives, determine actions, allocate resources and measure progress;
- Risk assessments to identify, assess and evaluate risks to the organization;
- Emergency management planning to integrate and coordinate an approach to identify and minimize the impact of risks relating to all operations of an institution;
- Business continuity practices to deal with disruptions and ensure the continuation of essential services;
- Security measures to address threats; and
- Emergency planning to ensure adequate response procedures are in place to deal in the case of emergencies.

Despite these actions, significant gaps remain. Some risks may be poorly addressed because their causes or effects are poorly understood, they are new, or because there is a lack of information on how to address them. Others may be outside of the organization's sphere of influence, such as vulnerabilities due to dependencies, vulnerabilities in the supply chain or in cyber networks. Accountabilities for addressing risks may be misunderstood, unclear or shared – leading to inaction. Finally, some risks may be too rare to justify resources or the consequences too large for any organization to address by itself.

Sector Networks, the National Cross-Sector Forum, the Federal-Provincial-Territorial Critical Infrastructure Working Group, and other mechanisms established by the Strategy are designed to complement risk management activities at the organizational and regional level and address these gaps.

Through participation in Sector Networks, public and private sector partners can better respond in emergencies, better identify vulnerabilities due to interdependencies, collectively allocate their resources towards priority areas and develop more appropriate measures to mitigate risks that reflect a better understanding of sector-wide operations and requirements.

Governments and private-public sector partners will work together to clarify and define roles and responsibilities, where needed, and to build trusted partnerships within the sector and across sectors. Collective risk management activities will enable the Government to:

- Identify and address legislative and policy gaps;
- Provide owners and operators with more timely, accurate and useful analysis and information on threats and risks;
- Work with owners and operators to emphasize the benefits of investing in security measures and enhancing resiliency;
- Provide tools, best practices and other guidance to support risk management activities within critical infrastructure sectors; and
- Strengthen time-sensitive information sharing during emerging threat and incident management situations.

Collective risk management activities lead to benefits for the entire critical infrastructure community, including:

- Identifying and addressing strategic, systemic or national risks;
- Identifying and addressing risks due to dependencies;
- Faster and more effective response to attacks and disruptions;
- Swift recovery of vital assets and essential services when disruptions occur;
- Leveraging collective public-private sector expertise and resources to confront existing and emerging threats; and
- Strengthened resiliency of Canada's critical infrastructure, thereby building a safer, more secure Canada.

1.2 Principles

Based on lessons learned and best practices from international allies, provinces and territories and within the federal government, the following principles apply to the risk management process described herein:

> **Strategic level:** The scope of this process is at the sector level – that is systemic, strategic, or national risks. It is intended to complement risk management activities at the organizational and regional level. Specifically:

- Risks that have been identified as strategic priorities by the Sector Network, or governments;
- Risks that may have systemic, sector-wide or multi-sector effects – this could include risks that are common to many stakeholders, risks that are uncommon but have high consequences to the sector; and/or
- Risks to the national interest.

Complement organizational processes: To the extent possible, the process and approach should build on, and complement existing mechanisms, as well as threat, vulnerability, and risk assessments undertaken at the organizational and sector level. Likewise, strategic planning, business continuity planning, emergency management planning, emergency response planning and other relevant activities should be considered and leveraged when undertaking critical infrastructure activities at the industry and sector level.

Common framework: Critical infrastructure draws together many different disciplines, industries and organizations – all of which may have different approaches and interpretations of risk and risk management, as well as different needs. To bridge these gaps, a common framework has been developed which allows flexible inputs from different organizations within a sector that may be combined in a way that allows risks to be identified, assessed and compared across sectors, so that they may be combined into a National Cross-Sector Profile.

Iterative and incremental process: The approach to describing the operations of the sectors, the interdependencies within and among sectors, assessing and evaluating risks and taking actions to mitigate these risks will evolve over time as lessons learned are incorporated, the risk environment changes and as sectors innovate and change. The process described herein builds on discrete and achievable objectives and deliverables and incorporates feedback and improvement to the process itself at every stage.

Future iterations and products may focus on specific high priority threats, impacts, and vulnerabilities; drill down as appropriate into sector operations such as technical operational requirements, specific asset types, regional operating environments and other details, as needed.

1.3 Process

The risk management process advanced in International Organization for Standardization's ISO 31000 provides a flexible and generic approach to risk management that can be tailored to the needs of individual sectors and sub-sectors. When implemented, it enables:

- Proactive, rather than reactive risk management;
- Improved identification of threats;
- Identification of vulnerabilities due to interdependencies;
- Compliance with international norms;
- Improved stakeholder confidence and trust;
- A reliable basis for decision making and planning;
- Effective allocation of resources for risk treatment;
- Improved incident management and prevention while minimizing loss;
- Improved organizational and sectoral learning; and
- Improved resilience.

The process of managing risks will help Sector Networks start and sustain a dialogue on critical infrastructure issues among the security and intelligence community, risk experts, the lead sector departments, governments, critical infrastructure associations and the owners and operators of critical infrastructure.

Aside from building trusted relationships, through dialogue and information sharing, the process is envisioned to have as output three separate but interlocking documents:

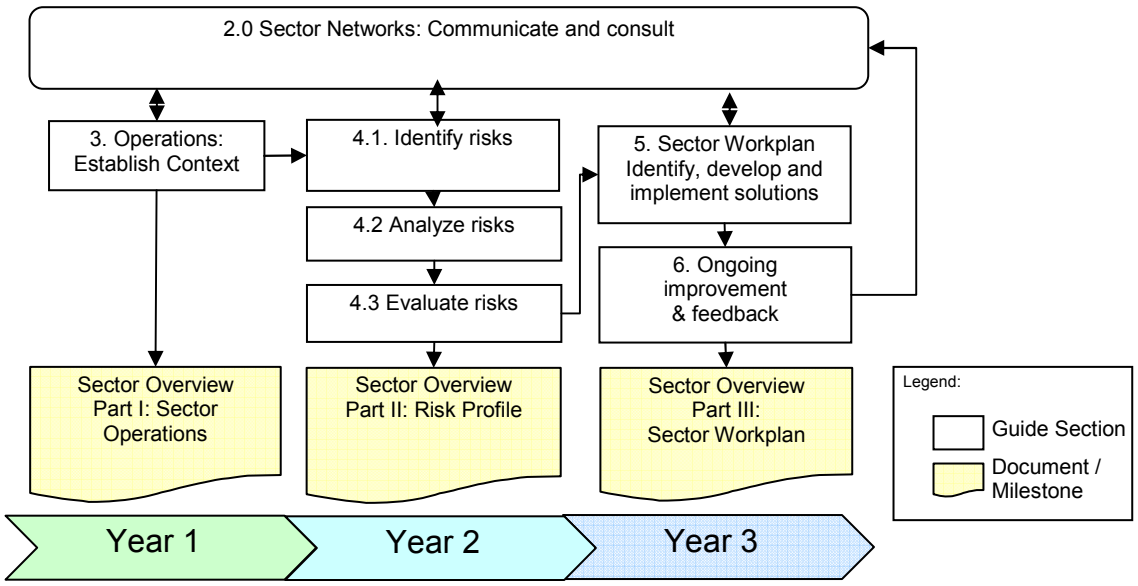
- Sector Operations: the sector and its operations;
- Sector Risk Profile: the risks to the sector; and
- Sector Workplan: the sector's future activities and its plan for addressing priority risks.

These documents may be combined into a Sector Overview. The information contained in the Sector Overviews will be combined into a National Cross-Sector Profile that identifies the key risks to critical infrastructure in Canada, outlines the key interdependencies within and across sectors and provides a roadmap for improving resiliency nation-wide.

The ISO process for managing risks has been adapted for the *National Strategy and Action Plan* and the context of Sector Networks and involves the following:

- Communication and consultation throughout the process;
- Establishing the context;
- Identifying, analyzing, evaluating risk;
- Identifying, developing and implementing actions to mitigate risk; and
- Monitoring, reviewing and continually improving risk mitigation actions, as well as risk management processes and practices.

The diagram below illustrates the risk management process, the relationship between the main deliverables (the Sector Overviews Parts I, II and III) and the sections of this guidance document.



2. Sector Networks: Communicate and Consult

> *"Analyzing homeland security risks is an especially "wicked" problem. Such problems are not amenable to solutions based on simple risk formulas, but rather require discourse-based, multi-party, conflict resolution techniques."*
>
> - Strategic Risk Management in Government: A Look at Homeland Security Schanzer, Eyerman, de Rugy

Communication and consultation allows trusted relationships to form – which is particularly important in the area of managing risks to critical infrastructure. It is an iterative exchange of information and opinion with the objectives of:

- Building trusted relationships;
- Building a shared awareness and common understanding of risks and the risk management process;
- Building a shared awareness and common understanding of the roles, responsibilities and capabilities of different stakeholders;
- Ensuring varied views are considered; and
- Learning from each other.

2.1. Key Elements

The key element of this step is to establish a consultative team in order to communicate and consult with internal and external stakeholders, and to ensure broad and diverse perceptions of risk are taken into account. Sector Networks and their members fulfill this role.

2.2. Implementation

Sector Networks provide standing fora for discussion and information exchange among sector-specific industry stakeholders and governments. They reflect a partnership model that enables governments and critical infrastructure sectors to undertake a range of activities (e.g. risk assessments, plans to address risks, exercises) unique to each sector. These Sector Networks also enable improved collaboration among critical infrastructure partners and information sharing activities both within and across interdependent Sector Networks.

Sector Networks, to the extent possible, are based on existing mechanisms. For this reason, many of the stakeholders have already been identified – they are the members of the Sector Network, and/or the organizations represented by the members of the Sector Network.

A terms of reference or other form of mutual understanding for the operation of Sector Networks provides a starting point to define how the network operates, what its goals are, and the resources that may be required to participate. It will

also help define how the Sector Network will communicate and consult with the broader critical infrastructure stakeholder community.

Given the potential sensitivity of discussing threats, vulnerabilities, operations, capabilities and other related information, one of the first deliverables under the *Action Plan*, after the establishment of the Sector Network, is the development, adoption and implementation of an information sharing and protection protocol to allow the open discussion of risks, vulnerabilities and other issues.

2.3. Considerations

Information Sharing
Not all of the stakeholders affected by a risk to a sector are members of the Sector Network. Consideration should be given to whom, how and through what channels relevant information can be provided to all affected stakeholders. This includes interdependent stakeholders and organizations.

Likewise, consideration should be given to how best to exchange information on cross-sector risks and issues identified and addressed in the National Cross-Sector Forum, as well as the Federal, Provincial and Territorial Critical Infrastructure Working Group.

Information Protection
The protection of information is a key concern for both government and private sector organizations, however, this must find a balance with sharing of information – which is required to advance overall critical infrastructure resiliency.

Several issues should be considered when sharing and protecting information:

> **Protection of information under the federal *Access to Information Act:*** The legal framework provided by the *Emergency Management Act*, recognizes that the ability to exchange specific and reliable information in a timely manner with the private sector is essential to the government's role in providing national leadership in critical infrastructure. This Act includes a consequential amendment to the *Access to Information Act* that allows the Government of Canada to protect critical infrastructure information supplied in confidence to the government by third parties, subject to criteria laid out in the Act.
>
> **Classification of material:** Unclassified information or open source information allows the freest flow of information. Classified information or other sensitive information (e.g., trade secrets, operational information, intellectual property) is subject to legal, physical and procedural protection. Whenever possible, parties should consider developing an unclassified or high-level version of the sensitive or classified information so that it can be shared (subject to the information sharing and protection

protocols of the Sector Networks).

Constraints on actions and information sharing: Federal, provincial and territorial departments and agencies are subject to laws, regulations, and procedures that they and their representatives are expected to follow. The private sector may also have constraints and limitations on how they can operate within the Sector Network from issues such as serving as boards of directors, company policies, grant restrictions, and legal regulations. Small businesses may be limited in the amount of resources they can contribute and the amount of time they can devote to the partnership. Recognizing and understanding the constraints and limitations of all sides and developing strategies to address the issues will enable the network to function more effectively.

Use of expertise outside of Sector Networks

Depending on the nature of the communication, others may be invited for specific agenda items, such as:

- Departments and agencies with related and/or intersecting mandates;
- Specialists and experts;
- Stakeholders from other sectors (including interdependent sectors);
- Customers;
- Regulatory agencies and departments;
- Organizations and entities who may be affected by the operations and activities of the sector;
- Special interest groups;
- Contractors, suppliers and other elements of the sector's supply chain;
- Emergency services organizations;
- Applicable not-for-profit organizations; and
- Security and intelligence agencies and departments.

3. Part I – Sector Operations

"Risk comes from not knowing what you are doing"
- Warren Buffet

Risk refers to the uncertainty that surrounds future incidents and their outcomes. It is the chance of something happening that will have an impact on objectives.

The potential consequences of a disruption of a critical service or product can only be assessed and addressed if the service or product is identified; threats and hazards can only be identified in relation to the systems and assets they threaten; and cascading effects due to dependencies can only be addressed to the extent they are known. Therefore, in order to assess the significant risks to a sector, it is necessary to identify the objectives and functions of the sector, as well as its services and products, and to understand its supply chain and operations.

3.1. Key Elements

The key deliverable of this stage of the risk management process is "Sector Overview Part I – Sector Operations". It is a document that is to capture the context of the sector, the sector's critical services and products and the dependencies of the sector.

3.2. Implementation

The most important part of this step is to capture why the sector is critical. Different sectors operate in different contexts, have different expectations placed on them, different requirements in terms of continuity of service delivery, and different cultures. There is no one size fits all approach to determining what is critical about a sector. Sectors may use a number of methods and approaches* to determine what is critical. At a minimum, the Sector Operations document should include:

✓	A description of the **critical services and products** - the outputs of critical infrastructure – those services and products whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-	*Note: The results of organizational business impact analyses and criticality assessments can provide insight as to what is critical at a sector level.*

* See Tools & Information

	being of Canadians, and/or to the effective functioning of the government.	
✓	Identify the **dependencies** of the sector – that is the services and products within the sector and from other sectors that are needed to produce or deliver the sectors' critical services and products	*Note: a **dependency** is a service or product requirement that is necessary to ensure the delivery of a "critical service or product".*
✓	An outline of the **sector supply chain and supporting operations** – highlighting how the critical services and products are created, produced, transmitted and distributed. This includes the goods and services provides by both private sector partners as well as public sector.	*Note: The appropriate level of detail is for the Sector Network and/or lead sector department to determine.* *Sector Networks may wish to describe only the key systems and features of the supply chain, others may describe the supply chain in more detail – providing the sub-systems, networks, and the types of assets required to produce and deliver critical services and products.* *These descriptions should not provide information on specific vulnerabilities, the location and characteristics of specific assets or other sensitive information.*

This document can also:

- Highlight why the sector is important to Canada and Canadians, and to North America – this could include contribution to GDP, number of people employed, value of imports and exports and other key statistics;
- Provide an overview of the key trends affecting the sector – such as technological, social, economic, geographic, environmental or political trends. Business drivers, business opportunities and business risks may also be included, if applicable;
- Outline the capabilities of the sector in an emergency;
- Describe the organization of the sector including roles and responsibilities of various levels of government, key players, controlling legislation, regulation and/or international agreements; and
- Highlight any international and regional considerations.

Lead sector departments may wish to hold workshop(s), conduct surveys or other consultative methods to identify critical services, products, systems and dependencies.

3.3. Considerations

Most business continuity planning processes consider the critical services and products as well as the interdependencies of an organization. This information, when aggregated to the sector level can provide insight as to what may be considered critical at the sector level.

It is anticipated that as the risk management process advances, the view of what is critical, what are the dependencies and how the supply chain operates will evolve. The first iteration will set a baseline, providing a way to measure progress over time.

Including the appropriate level of detail requires an understanding of what is important to the sector and what will best enable the identification of risks and risk mitigation measures. Some sectors may wish to have a very detailed description of the sector, others a simplified one, still others may wish to have both.

Describing the critical products and services, the supply chain, and dependencies of a sector provide a common baseline to discuss risks. The purpose is **not** to determine relative worth of any asset, system, service or product. A system may have a high replacement value, but not be critical in terms of providing a critical service or product.

Determining what is critical will depend on a number of factors, such as:

- **Risk tolerance:** The criticality of a service or product may depend on willingness to accept a risk to that service or product. This risk tolerance may depend on the context of the service or product in question, how the service or product may be disrupted, and the expectations of the population and stakeholders. For example, the risk tolerance of short term disruptions to landline telecommunications in a storm may be different than failures in the food safety for baby food.
- **Scope and Concentration:** Some systems and assets may be more critical if they account for a large percentage of the critical service or product, represent a significant portion of a region's economy or are only located in a certain region.
- **Substitutability:** Some systems, assets, services and products may be more critical if they are not easily substituted or replaced.
- **Perspective:** Criticality can depend on where you sit – what an organization produces or delivers is critical to that organization, and may be critical to the area or region where the organization operates, but less

critical at the systemic, strategic and national level. Sector Networks should keep in mind that the intent and scope is at the strategic level, rather than the organizational or regional level.

4. Part II – Sector Risk Profiles

The second module of the Sector Overview concerns risks. The process is to identify those hazards and threats – natural or human induced which are most likely to affect the sector, to assess their relative likelihood and consequences and to evaluate them. The output of this module is to create a Sector Risk Profile – a description of the risks to the sector, as well as their relative priority.

An all-hazards approach to risk management does not mean that all hazards will be assessed, evaluated and treated, rather that all hazards will be considered. Those threats and hazards which could disrupt sectors at a strategic, systemic or national level should be assessed and evaluated in depth. This includes natural hazards, threats and accidents. Annex B provides a list of threats and hazards to be considered, although the sector may have additional input.

The following are outside the current scope of this risk management process:

- Longer term or broader global issues such as climate change or competition for energy;
- Everyday occurrences – like street crime – that can cause extended misery and damage over a long period of time, but are not emergencies that would require direct Federal or Provincial emergency response, or that do not have the potential to disrupt critical services or products are also not to be considered; and
- "Positive risks" (e.g., business opportunities) or risks associated with not pursuing an opportunity.

It should be noted that risks due to external factors, such as disruptions of interdependent goods and services, and intentional, but non-malicious acts such as border closures **are** included in the scope of this process.

Note: A risk assessment method has been developed by Defence Research and Development Canada for use by Sector Networks. Lead sector departments can obtain this method from Critical Infrastructure Policy, Public Safety Canada.

4.1 Identify Risks

4.1.1 Key Elements

This step in the risk assessment process seeks to identify those threats and hazards which could disrupt the critical services and products identified by the Sector Networks. It takes, as input, the sector's collective knowledge of its risks – based on the Sector Operations document, organizational threat, vulnerability, and risk assessments; any sector level threat and risk assessments; and any other relevant information (e.g., policy documents, criticality assessments). The output of this step is to:

- Develop a list (or "register") of risks that may, or are expected to, affect the sector; and, based on this list
- Identify priority risks for further evaluation.

4.1.2 Implementation

The aim of this step is to generate a clear, concise and comprehensive list of potential risks (sometimes referred to as a "risk register") based on those events that might prevent, degrade or delay the provision of critical goods and services.

The risk register is generally in the form of a table, spreadsheet or database, and may contain the following information:

- **Statement or description of the risk:** A phrase that describes the risk;
- **Source of risk:** The threat or hazard that is the source of the risk;
- **Areas of impact:** The part of the sector that is affected;
- **Cause of the risk:** Why the threat or hazard is a risk to the sector;
- **Status / action of Sector Network:** The relative priority of the risk, and the action (if any) taken by the Sector Network;
- **Existing controls:** What is currently in place, or the known controls for the risk;
- **Sources of information:** For further reference;
- **Risk assessment information:** such the assessed likelihood and consequences from risk assessments undertaken at the sector level, organizational level or other risk information; and
- Other information such as related threat, criticality or vulnerability assessments, the degree of uncertainty of the information on the risk, regions likely to be affected, and trends – whether the risk is increasing or decreasing, may also be noted.

Only threats and hazards which have a potential impact on the sector should be considered. A list of threats and hazards may be found at **Annex B** of this document. This provides a starting point - other sources of information to further develop the list include:

- Past risk, threat and vulnerability assessments;
- Historical records of natural hazards, accidents and attacks;
- Scientific models and theory;
- Local or overseas experience;
- Expert judgement;
- Structured interviews;
- Focus group discussions;
- Strategic and business plans;
- Insurance claims; and
- Past organizational / sector experience.

The reliability and availability of information should be considered in creating the scenarios and determining their relative importance. **If there are gaps in information, this should also be recorded and provided in the risk register.**

It is anticipated that the number of potential risks to a sector would be very large. It is not feasible to assess all of them. The next step is for the Sector Network to determine what should be assessed in further detail.

The factors in making this determination should be recorded and provided in the risk register. There are a number of criteria that can be considered, including:

- High risk (based on an initial assessment of likelihood and consequence);
- High vulnerability;
- Anticipated increases in consequences and/or likelihood;
- Critical to the interests or mandate of the sector;
- Risks due to complex interactions and dependencies within and among sectors;
- Common to many owners and operators and where it is felt that a better understanding of the risk could lead to better mitigation strategies;
- Threats and hazards whose likelihood and/or consequences are poorly understood; and
- Where there are feasible and cost-effective risk mitigation strategies.

It should be noted that the priority threats and hazards for further evaluation in this process may not necessarily be the same priorities as determined by other risk assessments, even if these are all-hazards risk assessments.

4.1.3 Considerations

It is important to develop as comprehensive a list as possible. What is not identified at this stage will not be included in further analysis.

Threats and hazards identified at this stage may be outside the scope of the process described here (i.e., climate change). They should still be recorded in the register, as it may be that future risk assessment processes will consider these threats, or that the Sector Network may choose to take action to mitigate the associated risk even though it was not formally assessed.

A risk register is a living document that provides continuity on the issue of threat identification and risk assessment in between assessment periods. It allows the prioritization of action, and ensures that all known threats and hazards are considered – even if they are not formally assessed.

From the risk register and the assessment and evaluation process a Sector Risk Profile will be produced. Section 4.3 of this document discusses the Sector Risk Profile in depth.

4.2. Analyze Risks

Risk analysis is the assessment of the consequences and their likelihood, and other attributes of the risk.

The analysis of risks allows:

- Better understanding of the vulnerabilities of the sector;
- More information about consequences or likelihood to inform decision making;
- Better understanding of the risk to guide mitigation plans;
- Better understanding of the gaps in knowledge;
- Better understanding of the residual risk (the risk that is left over after risk mitigation efforts); and
- Better understanding of the tolerance to accept this risk.

4.2.1 Key Elements

The inputs are the potential threats and hazards that have been identified as higher priority, the outputs are a ranked list of risks based on likelihood and consequences of the incident in question.

4.2.2. Implementation

At a minimum, the risk assessment should:

1) Assess the disruption to the critical services and products provided by the sector.
2) Assess the risk
    a. Determine the likelihood of the threat or hazard; and
    b. Determine the consequences of the threat or hazard, taking into account the disruption of the critical services and products.

There are many techniques to undertake this analysis:

- Use of multi-disciplinary groups of experts;
- Structured interviews with experts in the area of interest; and/or
- Questionnaires and surveys.

Assumptions made in the analysis should be recorded. Factors that affect consequences and likelihood should be identified and recorded.

4.2.3 Considerations

There is no single way to assess risks – the method and best practices to assess risks will evolve. No matter what technique is used to assess the risks, lessons learned and recommendations for improvement should be captured.

An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account.

The consequences are to be considered from a system and sector level – not from an organizational or asset-specific level, unless the effects on an organization or to an asset are of national, systemic, and sectoral significance.

Recognizing and taking into account the varying interests of the parties assessing the risk at the sector level will allow common ground to found and trusted partnerships to develop. Considerations should be given to the different interests: private sector organizations would be concerned with the costs associated with the risk such as lost revenue, damage to reputation and other concerns to the organization; whereas public sector organizations may focus on public safety and security issues.

Tip: Risk assessments are more consistent across sectors and inter-sector understanding is accelerated if peers from other sectors (especially interdependent ones) are a part of the risk assessment process.

4.3 Evaluate Risks

The evaluation of risks should lead to a discussion on:

- The level of risk tolerance or acceptance;
- Priorities for risk prevention and mitigation action; and
- Priorities for other action.

4.3.1 Key Elements

The inputs to this step are the assessed risks; these risks are to be evaluated to create a Sector Risk Profile that includes:

- A prioritization of the risks;
- Information gaps; and
- Lessons learned.

Part II of the Sector Overview: Sector Risk Profile, is to be an unclassified version of the Sector Risk Profile, if the Profile, or a portion thereof, is classified.

4.3.2 Implementation

Risks may be evaluated by dividing them into three bands:

- Those risks that are intolerable and risk reduction, prevention and/or mitigation measures are essential;
- Those risks where the benefits and costs of risk prevention and mitigation activities should be balanced against adverse consequences; and
- The risks are negligible – the consequences are very low, the likelihood remote, or the risk is accepted or tolerated. No risk reduction measures are recommended.

The criteria for evaluation should be based on:

- Consequences;
- Likelihoods;
- How and to what extent the critical services and products of the sector may be disrupted; and
- Range of uncertainty in the consequence or likelihoods of incidents;

As risks are evaluated, the risk register should be updated with some of the following information from the assessment and evaluation, including:

- Insights on the threat or hazard and its causes;
- A description of the scenario(s) used in the assessment, including any assumptions;
- The results of the assessment; and
- Recommendations for when (and if) the assessment of the risk should be re-visited.

4.3.3 Considerations

As the understanding of the risks evolve, it may be worthwhile to revisit and update the risk register.

Other considerations in evaluating the risks include:

- The source of each threat or hazard;
- When, where, how and why the threat or hazard is likely to occur;
- Roles, responsibilities and mandates;
- Who is affected;
- Who might be involved in risk reduction measures;
- What controls presently exist to treat this risk;
- Whether certain actions mitigate multiple risks; and
- Cumulative effects of multiple events.

5. Part III – Sector Workplan

"The time to repair the roof is when the sun is shinning."
- John F. Kennedy

By Year 3 of the Action Plan, Sector Networks are to have developed Sector Specific Workplans to reduce risks and undertake other critical infrastructure activities. It is anticipated that the Sector Specific Workplans will continue to evolve as the critical infrastructure, threats against them, and strategies for protecting against and responding to these threats and incidents evolve.

Workplans should be:

- **Comprehensive:** They should address the physical, cyber and human elements of critical infrastructure. Workplans should be all-hazards and should identify and address interdependencies within and across sectors.
- **Integrated:** Sector Workplans need to be complementary across federal, provincial and territorial governments and sectors.
- **Risk-based:** Sector-specific work plans should be based on an understanding of the risk environment and designed to allow measurement, evaluation and feedback on the effectiveness of mitigation efforts. This allows owners, operators and governments to re-evaluate risk levels after the plan has been implemented.

5.1 Key Elements

This stage of the process involves identifying options to address the risks, evaluating the options and producing a plan to implement and monitor the selected options.

The key deliverable is a Sector Workplan that outlines the activities of the Sector Network to reduce risk, which should include:

1) Goals and objectives;
2) Mitigation Actions - the specific actions to achieve the goals and objectives and the risks they address;
3) An Implementation Plan that includes a plan to monitor and track results; and
4) An Exercise Plan to test and validate actions taken.

5.2 Implementation

The process used to develop a successful risk mitigation plan is just as important as the plan itself. The steps below provide a generic approach to developing the risk mitigation plan - it may be necessary to alter the sequence of steps or tasks below to fit the needs of the sector.

5.2.1 Develop Mitigation Goals and Objectives

Developing clear goals and objectives improves focus and clarifies solutions to problems and issues as they arise. Well articulated goals and objectives provide the necessary framework by which decisions on mitigation actions will be based.

Goals are broad, forward-looking statements that succinctly describe the aim of the risk mitigation process and what the Sector Network wants to achieve. These should not identify specific mitigation actions (those will be developed later), but identify the overall improvements desired.

Objectives define strategies or implementation steps to attain the identified goals. Unlike goals, objectives are specific and measurable. They expand on the goals and provide more detail on the ways to accomplish them. It is important to have measurable objectives because they provide a roadmap for successfully implementing the strategy.

The formulation of risk mitigation goals and objectives should be based on the review and analysis of the risk assessment.

5.2.2. Develop an Implementation Plan

Once goals and objectives have been identified, actions to accomplish the objectives should be identified, evaluated and prioritized.

5.2.2.1 Developing an Implementation Plan: Step 1- Identify Options

The starting point for identifying options is often a review of existing domestic and international measures, best practices and lessons learned for reducing that type of risk.

The options for mitigating risks may seek to:

- Avoid the risk by stopping, or not starting activities that give rise to the risk;
- Reduce the likelihood of the threat or hazard;
- Reduce the consequences of the threat or hazard;
- Change the consequences of the threat or hazard;

- Share the risk (i.e. through insurance, joint ventures, partnerships); and/or
- Retain the risk.

The analysis of the risks should provide a comprehensive understanding of its underlying causes, sources, chain of events leading to the incidents, consequences and other facets, including:

- The causal factors which can help determine what type of actions can be taken to prevent future harm;
- Immediate causes and any underlying factors, the likely chain of events leading to the event, the potential consequences and the likely actual consequences;
- The range of potential consequences, and the most likely consequences; and
- The range of likelihoods and the confidence in these estimations.

Business continuity planning, consequence management, emergency management, disaster mitigation, vulnerability assessment, insurance and other related disciplines all provide a wealth of possible actions. These disciplines are well-developed and will not be treated in this document.

Scientists and hazard experts (e.g., geologists, seismologists, hydrologists, etc.), as well as floodplain managers, emergency managers, fire marshals, public works engineers, transportation engineers, and civil engineers who are expert in applying mitigation and emergency management principles all have valuable experience in knowing what works to mitigate hazards.

Some potential alternative actions may require additional study before a solution or alternative mitigation action can be identified.

5.2.2.2 Developing an Implementation Plan: Step 2 - Identify and analyze federal, provincial, territorial and local mitigation capabilities

Understanding what capabilities are available to mitigate risks will help determine which actions are most likely to yield positive results. This analysis could list local government agencies, departments, and offices with responsibility for planning, building code enforcement, mapping, building, and/or managing physical assets, as well as for emergency management functions. Not-for-profit (e.g., Red Cross Society of Canada) and for-profit organizations (e.g., private security firms) may also have applicable capabilities, as well as other departments or agencies that do not appear to have a direct impact on mitigation but could have an indirect effect on the overall mitigation program.

5.2.2.3 Developing an Implementation Plan: Step3 - Evaluate and prioritize mitigation actions

The evaluation should determine whether the action would work for the specific mitigation goals and objectives formulated by the Sector Network.

Once options for reducing risk have been developed, they should be evaluated and prioritized. The following are possible considerations:

- Ease of implementation and cost-effectiveness;
- Whether the action creates new risks and/or unintended consequences;
- Environmental impacts (positive and negative);
- Multi-objective actions;
- Long term or short term results;
- Effectiveness;
- Direct and indirect benefits;
- Legal, regulatory, social and moral obligations;
- Efficiency;
- Equity and acceptability; and
- Timing and duration.

5.2.2.4. Developing an Implementation Plan: Step 4 – Write the Plan

Once actions have been identified, an implementation plan should be developed and agreed to. The plan should include target dates, responsibilities, and key milestones.

Potential partners in developing and implementing the workplan could include local, provincial, territorial and federal governments, private sector organizations and businesses, academic institutions and upstream and downstream organizations and interdependent sectors.

Sector Networks should incorporate the principles of results based management into the implementation plan - this could include a logic model, performance indicators and expected results and outcomes.

The manner in which implementation will be monitored should also be developed. Key aspects of monitoring implementation may include:

- Confirming and clarifying roles and responsibilities;
- Integration of mitigation actions throughout operations;
- Determining mechanisms and frequency of monitoring implementation and progress;
- Establishing indicators of effectiveness or success; and
- Documenting and sharing successes (and failures) and lessons learned.

The Sector Workplan should also take into consideration that the risk environment, the sector's operating environment and other factors change. The Workplan should also monitor and track:

- High risks;
- Experience of other countries, sectors and organizations with risk reduction strategies including their potential failures as well as progress on the most promising strategies;

- Changes in risk tolerance; and/or
- Technological advances that may change the context.

To maintain support throughout the implementation process, stakeholders should be kept informed about the incremental progress and success of the program. The findings of progress reports, key activities, can be distributed or posted on the Public Safety Critical Infrastructure Website to keep stakeholders up-to-date on accomplishments and possible setbacks.

If applicable, it may be worthwhile to integrate the monitoring of implementation into already existing processes, such as budget cycles and other reporting cycles.

5.3 Develop an Exercise Plan

One of the key mechanisms to validate and test risk mitigation actions, plans and systems is through exercises. Exercises serve to:

- Encourage the building of relationships across and between industries and disciplines;
- Clarify roles and responsibilities as well as capabilities;
- Identify and address dependencies and interdependencies of critical infrastructure;
- Raise awareness of the risks to critical infrastructure;
- Provide personnel with an opportunity to practice assigned roles;
- Determine the state of readiness for a particular incident; and
- Identify gaps in communication protocols, operating procedures and emergency response procedures.

Sector Networks should include a plan and timeline to undertake exercises in order to test and validate the risk mitigation actions taken.

Tip: Including interdependent sectors and organizations, as well as emergency management / response personnel, as both exercise design partners and players in the exercise increases resiliency.

Exercises may range from simple tabletop exercises, to fully operational simulations.

Tabletop exercise	A method of exercising plans in which participants review and discuss the actions they would take in response to a specific scenario, as presented by a facilitator. Specific actions are not performed.
Functional	A method of exercising plans in which participants perform

exercise	some or all of the actions they would take in the event of plan activation to respond to a specific scenario.
Full operational exercise	A method of exercising plans in which the participants suspend normal operation and activate the plans as if the event were real.

The results of an exercise should capture any gaps and limitations in current actions.

Departments and agencies with responsibility for supporting Sector Networks should, to the extent possible, adapt the lessons learned for general sector-wide use and distribute these generic lessons learned throughout the sector's stakeholders.

Exercises should be planned and conducted taking the following into consideration:

- The scenario should reflect reality as far as is practicable;
- The scenario should be based on the risk assessment;
- Key stakeholders should participate and roles and responsibilities should be clearly defined;
- Resources can be deployed or simulated;
- The emergency operation centres can be activated;
- Equipment and procedures identified in the emergency plan can be used;
- Linkages with other organizations and agencies can be included;
- Debriefing sessions should be included at the end of the exercise; and
- Lessons learned should be documented.

5.4 Considerations

Decisions surrounding rare but severe risks require careful consideration as the legal, moral and social responsibilities may override the economic considerations. These low likelihood, but high consequence risks are less likely to be on the radar than high likelihood, but low consequence risks. It may very well be that these low likelihood but high consequence risks are more important as sectors are less likely to be resilient to these types of incidents.

Any gaps in information, resources, or capabilities should be noted and included in the Sector Workplan.

Special scheduling needs, such as seasonal climate conditions, funding cycles, agency work plans, and budgets should be considered in any resource requirements.

Not adequately incorporating lessons learned from an exercise into operations is an all too common in emergency management and critical infrastructure

activities. The lessons learned should be documented and used to improve and revise operations, risk mitigation actions and other plans, and an organizations senior management should monitor and track this implementation.

6. Ongoing improvement and feedback

The risk environment is not static – the implementation of the risk mitigation plan, and experience gained dealing with incidents lowers risk. On the other hand, new threats emerge, new goods and services and the new entrants to the sectors change the context and operations, innovation spurs new technologies – all of which introduces new risks and vulnerabilities. Sector Networks provide a lasting forum to monitor and respond to this changing risk environment.

6.1 Key Elements

Ongoing improvement and feedback should be incorporated into every aspect of the risk management process.

Sector Networks should continually capture and share lessons learned and best practices to improve the resilience of sectors, the operations of the Sector Network, other Sector Networks, the actions of governments at all levels, the processes, methods and tools used to manage risks – this includes during normal operations and after an incident.

6.2 Implementation

Lessons learned can and should be captured during sector operations, after an incident occurred and during and after an exercise.

Post-incident analysis, in particular, provides useful insight into improving the risk management process. This analysis could include:

- A comparison of the actual event to the risk assessment: Did the risk identification process identify the risks from the incident? Was the risk properly assessed? Is there additional data? Is there new data on vulnerabilities, root causes or other aspects of the threat or hazard?
- Evaluation of the implemented risk mitigation actions: How well did they perform? Were emergency plans and business continuity practices sufficient? Where they well executed? Did the mitigation action have an effect?
- Revisit the list of mitigation actions in light of the recent incident: If new infrastructure is to be built – should it incorporate features to make it more resilient? Should it be built in a new location, or to a different plan? Should the priority of mitigation actions be modified?
- Evaluate deficiencies in the response and identify improvements to emergency response plans, business continuity plans, training, etc…
- Evaluate any new equipment required or modifications to facilities.

6.3 Considerations

Sector Networks should capture what worked well and what did not work well throughout the risk management process and share these insights with sector stakeholders as well as lead sector departments, other Sector Networks, the National Cross Sector Forum and Public Safety Canada, in accordance with the information sharing and protection protocol.

Annex A: Terms and Glossary

It should be noted that these terms are not intended to define how the various elements interact and/or are assessed, nor is it a Government of Canada standard. Rather, they are common definitions chosen for clarity in order to provide a common language across diverse disciplines.

It is recognized that these terms may be applied differently within different disciplines and sectors. It is anticipated that this lexicon will evolve as the critical infrastructure stakeholder community evolves.

This has been developed in consultation with Public Safety Canada, the Integrated Threat Assessment Centre, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and Defence Research and Development Canada.

All-hazards: The Strategy sets out an all-hazards risk management approach – under which the full range of sources and causes of potentially harmful or dangerous incidents are considered. All-hazards incorporates traditional emergency management events such as flooding and industrial accidents; as well as national security events such as acts of terrorism; and cyber events. *(source: adapted from Federal Emergency Response Plan (2009). Public Safety Canada)*

Asset: Any person, personal capability, facility, material, information, or activity that contributes to the accomplishment of an objective. *(source: adapted from DHS Risk Lexicon)*

Consequences: results or effects of an incident. *(source: Oxford English Dictionary)*

> *Note: The type of incident, its magnitude, and the vulnerabilities, value and functions of the assets affected determine the consequences.*

Critical infrastructure refers to the 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. *(source: National Strategy and Action Plan for Critical Infrastructure)*

Critical services and products: the outputs of critical infrastructure – those services and products 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. (*source: Policy on Government Security*)

Dependency: one-directional reliance of an asset, system, network, or collection thereof, within and/or across sectors, on input, interaction, or other requirement from other sources in order to function properly[1]. *(source: new)*

Incident: Occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action. *(source: DHS Risk Lexicon)*

Interdependency: mutual, shared or reciprocal dependencies. *(source: new)*

Likelihood: Probability of an incident occurring. *(source: new)*

Risk refers to the uncertainty that surrounds future incidents and outcomes. It is a function of the likelihood and consequences of an incident - the higher the likelihood and/or the greater the consequences, the greater the risk. *(source: TBS Integrated Risk Management Framework)*

Risk management is systematically setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues. *(source: TBS Integrated Risk Management Framework)*

System: A set of assets, resources, or elements that work together as a mechanism or interconnecting network. *(source: adapted from Oxford Dictionary)*

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

> *Note: The threat may be assessed to determine the likelihood of hostile or harmful actions. To do so, the actor's intent and capability to undertake such actions may be assessed. The assessment may also consider specific targets (such as specific persons or assets), generic targets (such as sectors, categories of targets, or regions), attack methods, vulnerabilities, as well as provide recommendations to mitigate or eliminate the threat.*

Vulnerability: a characteristic or attribute of an asset which renders it susceptible to effects of an incident. Vulnerability informs both the likelihood and consequence of an incident. *(source: SARMA consensus definition)*

---

[1] Dependencies may be:

- Physical: dependency on products, services and resources for continued operation.
- Informational: dependency on information for continued operation.
- Geographic: dependency due to the geographic proximity of the infrastructures.
- Logical: dependency due to economic, political, or management factors (i.e., effects of markets and prices of inputs, command and control of large organizations, border effects on flow of goods and people, and others.)

Annex B: List of Hazards and Threats

Note: No list of threats and hazards is ever complete. Below is a list of common threats and hazards that could affect critical infrastructure. It is anticipated that this list will evolve.

Natural Hazards	

Meteorological:
- Windstorm, tropical cyclone, hurricane, tornado
- Thunderstorm
- Snow, ice, hail, sleet storm
- Flood
- Storm surge
- Extreme weather
  - Heat wave
  - Cold wave
  - Drought
Glacier, iceberg
	Geophysical:
	- Earthquakes
	- Tsunami
	- Volcanic eruptions
	- Landslide, mudslide, subsidence
	- Geomagnetic storm
	Fire:
	- Forest, wildland
	- Urban
	- Fire following earthquake
	Biological:
	- Diseases that affect humans
	- Diseases that affect animals
	- Diseases that affect plants
	- Animal or insect infestation or damage

Intentional / Deliberate threats	

Attacks:
- Chemical attack
- Biological attack
- Radiological attack
- Nuclear attack
- Explosive attack
- Cyber attack
- Conventional arms attack
Enemy attack / war
Electromagnetic pulse
	- Sabotage
	- Espionage (industrial and otherwise)
	- Crimes (e.g., theft, kidnapping, arson, extortion)
	- Social unrest (riot, lawful / unlawful protest, disruption)
	- Strike or labour disruption
	- Other intentional actions that can affect critical infrastructure (non-malicious):
	  ○ Border closure
	  ○ Regulation change

Accidental / Technical Hazards	

Accident
- Transportation accident
- Hazardous material spill or release (explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, biological, radiological)
- Fire
  ○ Urban fire
  ○ Industrial fire
  ○ Chemical fire
- Accidental explosion
 	
Failure / Technical
- Technical failure
- Mechanical failure
- Software failure
- Operator error
- Process / procedure failure
- Structural failure (e.g., Bridge collapse, Mine collapse, Dam collapse / failure, Water main failure)
	- Dependent CI disruption / failure (i.e. failure in provision of critical services or products in the information & communication technology, finance, energy, food, safety, government, health, manufacturing, transportation or water sectors)