Public Safety and Emergency Preparedness Canada
Critical Infrastructure Protection and Emergency Preparedness

Sécurité publique et Protection civile Canada
Protection des infrastructures essentielles et Protection civile

Selection Criteria to Identify and Rank Critical Infrastructure Assets

20 January 2004

Public Safety and Emergency Preparedness Canada
Critical Infrastructure Protection and Emergency Preparedness

Sécurité publique et Protection civile Canada
Protection des infrastructures essentielles et Protection civile

Selection Criteria to Identify and Rank Critical Infrastructure Assets

20 January 2004

TABLE OF CONTENTS

List of Figures and Tables

Foreword

This document has been prepared with the expectation that the critical infrastructure owners, operators and stakeholders will contribute to the development of the overall national criteria for identifying and ranking national critical infrastructure under the National Critical Infrastructure Assurance Program (NCIAP). PSEPC will meet with interested stakeholders by spring 2004 to review the application of the proposed criteria from this paper in the context of the NCIAP Position Paper.

1. INTRODUCTION

1.1 BACKGROUND

The Critical Infrastructure Protection and Emergency Preparedness section of Public Safety and Emergency Preparedness Canada (PSEPC) has been established to provide national leadership in the protection of Canada's critical infrastructure and in the enhancement of emergency management in Canada. It is also the government's primary agency for ensuring national civil emergency preparedness.

PSEPC has been discussing with partners the feasibility of developing a program to provide appropriate assurance for critical infrastructure (CI); those systems, assets and network elements that would have national impacts should they be unavailable due to an emergency situation. These discussions have led to a proposal for a National Critical Infrastructure Assurance Program (NCIAP) with the goal of the continued availability of essential services to Canadians. A draft NCIAP Discussion Paper was issued November 1, 2002 to stimulate a productive dialogue with principal stakeholders on key concepts and issues. An updated NCIAP Position Paper will be issued in the winter of 2004.

This paper builds on the work done in the draft document *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets* released on December 19, 2002 by OCIPEP and the consultations with and feedback from stakeholders on that document. The material from consultations, conferences, studies, workshops and available literature on Critical Infrastructure Protection displayed increasing congruence of the various models in use; for example, many jurisdictions have looked at and supported the National Contingency Planning Group March 2000 report and supporting material *Canadian Infrastructures and their Dependencies* which provided a detailed reference for modeling criticality and interdependencies of Canada's infrastructures.

This paper does not supercede the *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets* which remains a valid reference document as it and other existing asset identification models can be used as complementary tools to this paper. For example, owners, operators and critical infrastructure stakeholders may use the approach in this paper to either validate an existing list or to develop an initial list of critical assets. There is significant benefit in validating a critical assets list against other models.

1.2 OBJECTIVES

Within the context of the NCIAP, one of the objectives of this paper is to further develop criteria to assist owners and operators of critical infrastructure in identifying assets and establishing their relative criticality or priority as part of an integrated risk management process to protect critical assets and assure critical services. As critical infrastructure owners and operators undertake these exercises, assurance and/or protection strategies

can be developed or upgraded. A second objective is to work with owners, operators and CI stakeholders to develop national criteria and/or an overall model to be used to identify national critical infrastructure (NCI) assets.

One proposal for consideration is that CI stakeholders tie their individual organization or sector ratings into the CI Priority Assessment Screening Model grid shown at the end of this paper until the overall model is developed. This screening model reflects the risk management approach upon which the NCIAP is based. Many CI owners use risk management during their normal business practices and the use of consistent, proven, risk management principles (as presented in this paper and in the NCIAP Position Paper) will contribute to the uniform use of the overall model developed. It is also proposed that if CI owners, operators and stakeholders need assistance with Vulnerability Assessments, Threat and Risk Assessments or funding, that they must illustrate their requirements with the eventual model.

PSEPC will meet with interested stakeholders by spring 2004 to review the application of the proposed criteria in the context of the NCIAP Position Paper.

2. RISK MANAGEMENT APPROACH

The identification and rating of CI assets fits squarely within the risk management process. Because assets have differing values, an assessment is required to determine the investment to properly secure them. Some assets are indispensible to the continuity of a service and will require significant resources to provide for their security. As 100% protection is neither affordable nor feasible, the assuring of CI services against disruption or failure is ultimately a risk management process.

A risk management framework, such as the one issued by the Treasury Board of Canada Secretariat for the Government of Canada (GOC), provides an organization with a mechanism to develop an overall approach to manage strategic risks by creating the means to discuss, compare and evaluate substantially different risks on the same page. It applies to an entire organization and covers all types of risks faced by that organization (e.g. policy, operational, human resources, financial, legal, health and safety, environment and reputational). Implementation of a risk management framework will support governance responsibilities, improve results through more informed decision-making, strengthen accountability and enhance stewardship[1].

---

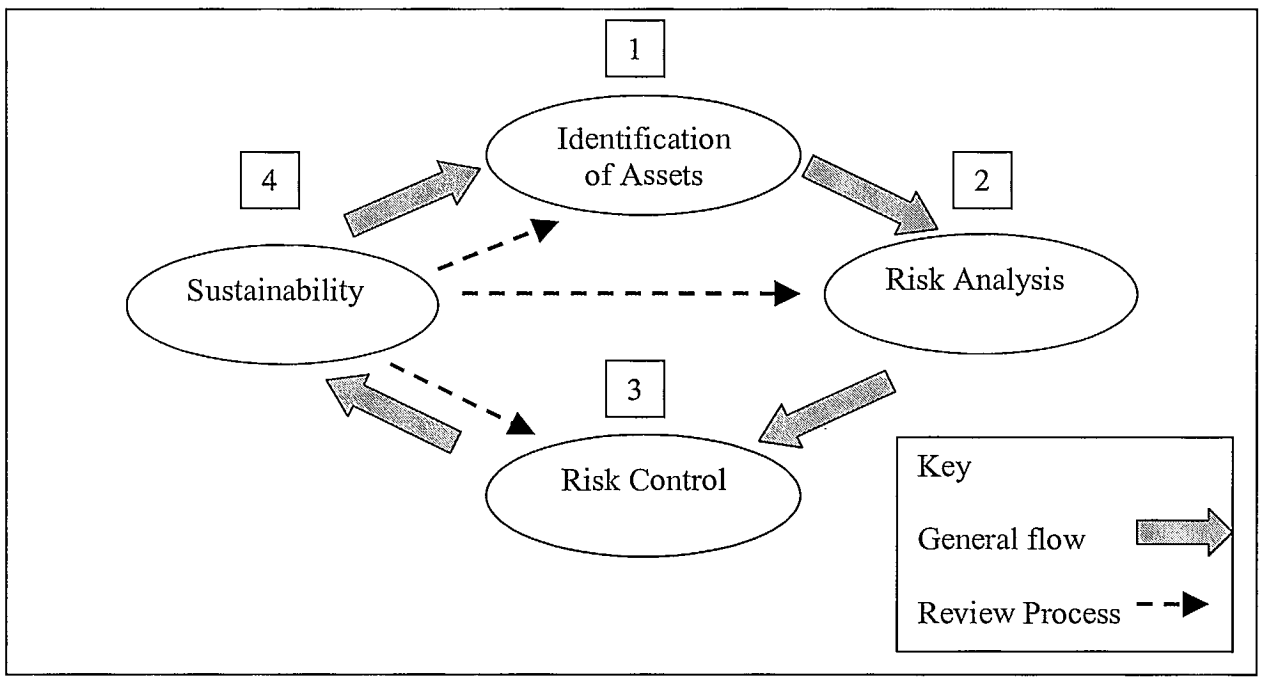
[1] The Treasury Board Secretariat's Integrated Risk Management Framework anticipates that the GOC's implementation of the framework will:

- support the government's governance responsibilities by ensuring that significant risk areas associated with policies, plans, programs and operations are identified and assessed, and that appropriate measures are in place to address unfavourable impacts and to benefit from opportunities;
- improve results through more informed decision-making, by ensuring that values, competencies, tools and a supportive environment form the foundation for innovation and responsible risk-taking, and by encouraging learning from experience while respecting parliamentary controls;

The challenge for all partners is to develop a common risk management framework. Critical infrastructure owners and operators use a variety of risk management processes. Some manage this process formally; many others do it informally. The consistent identification of CI should form part of a continuous risk management process for CI owners and operators.

For the NCIAP, reference to a common risk management process will encourage partners and CI sectors to address identified CI consistently within a common risk management process. For the purposes of this paper, Figure 1 below illustrates a risk management model based on widely-accepted business continuity practices. The following model uses four stages as the basis of an ongoing, iterative risk management process. Other models use additional stages, but all start with the identification of assets (and/or associated services) and the associated impact assessments relating to loss or damage of each asset (and/or service) as the starting point. Using this information, the assets (and/or services) are prioritized based on the potential consequences of their loss.

Figure 1 – Risk Management Model



- strengthen accountability by demonstrating that levels of risks associated with policies, plans, programs and operations are explicitly understood, and that investment in risk management measures and stakeholder interests are optimally balanced; and
- enhance stewardship by strengthening public service capacity to safeguard people, government property and interests.

See Treasury Board of Canada Secretariat (TBS), *Integrated Risk Management Framework*, March 2000, available on-line at: www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp.

As this paper deals with only the first stage of the risk management model – Identification of Assets – a description of the other stages, additional possible phases and their relationship is not covered in any detail[2].

Stage 2 requires the use of an all hazards approach to prepare assessments of vulnerabilities and threats to an asset (and/or associated service). Combining these assessments with the impact assessments and consequences from stage 1 comprises the risk analysis. (It is suggested that the discretion of senior managers or team leaders should be used when briefing the assessment teams prior to the conduct of the CI assessments in the risk analysis stage.)

Stage 3 involves the activities undertaken to control the risks to the service and calls upon the discretion and accountability of the executive level of the organization. The risk control stage is a consideration of possible measures to be taken to minimize threats and to reduce the vulnerabilities of and the impacts to the asset from the hazard.

The stage 4 level is reached when there is an acceptable level of risk for each asset. Stage 4 also involves an ongoing assessment of each new asset and changing threat and vulnerability information to determine the requirement to re-allocate scarce resources. Under the NCIAP, information sharing is recognized as fundamental to cooperative efforts in protecting critical infrastructures. Incorporating information sharing solutions into the regular business processes of stakeholders will facilitate the review process. In addition, the criteria (used in stage 1) for determining what might be critical assets have changed and expanded over time and will likely continue to do so[3].

---

[2] For examples of a full iterative risk management cycle see the TBS' *Integrated Risk Management Framework*, March 2000 available on-line at: www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/rmf-cgr01-1_e.asp; the Deloitte & Touche report prepared for the Office of Critical Infrastructure Protection and Emergency Preparedness, *National Critical Infrastructure Evaluation Criteria*, March 5, 2002; U.S. National Infrastructure Protection Centre, *Risk Management : An Essential Guide to Protecting Critical Assets*, November 2002, available on-line at : www.nipc.gov/publications ; National Defence - National Contingency Planning Group, *Risk Assessment Methodology, National Infrastructure Risk Assessment,* March 2000, www.oag-bvg.gc.ca/domino/reports.nsf/html ; Government of Alberta Municipal Affairs Crisis Management, www.aepp.ab.ca/files/crisis ; and Sandia National Laboratories, www.sandia.gov/CIS/capability.htm

[3] Without a standard or agreed upon definition, the concept of infrastructure in policy terms has been fluid in the past and as it appears to be today. Comments made by John Moteff, Claudia Copeland, and John Fischer, Resources, Science and Industry Division, Report for Congress, Congressional Research Service, The Library of Congress, Critical Infrastructures: What Makes an Infrastructure Critical?, August 30, 2002.

3. ASSET SELECTION CRITERIA

3.1 CHARACTERIZE OR STANDARDIZE ASSETS

The potential list of assets is huge and diverse. In order to develop an inventory of assets, standardising the types of assets to be considered is essential. An assessment team should be used to identify assets and classify them according to varying levels of granularity[4]. Assets should be listed and classified at consistent levels of granularity.

At the highest level in the NCIAP, PSEPC has identified 10 main sectors: Energy and Utilities, Communications and Information Technology, Finance, Health Care, Food, Water, Transportation, Safety, Government and Manufacturing. These broad sectors are divided into sub-sectors which are further sub-divided into more detailed descriptions of the infrastructure. For example, the Energy and Utilities sector is divided into Electrical Power, Natural Gas and Oil Production and Transmission Systems. Electrical Power is sub-divided into power generation plants, transmission stations, power line corridors (or transmission lines), distribution stations, control centres and nuclear. For the purposes of this paper, it is expected that partners and CI sectors will focus at a comparative level of detail as shown in the Electrical Power sub-sector example[5].

Without standardization of the assets to be considered, prior to any attempted assessment, potentially critical assets might not all be at an equal level of granularity. The level of detail would likely vary from CI sector to CI sector depending on whether the asset and/or service impacts the owner/operator and population at a local, regional, provincial or national level. Before attempting to measure criticality, the asset listing should be validated by the appropriate owners and operators of the infrastructure[6].

3.2 ESTABLISHING CRITICALITY

Experience has shown that it is a fairly straightforward process to identify critical assets[7]. However, it is most often very difficult (1) to establish the criticality of an asset compared to other assets and (2) to quantify the potential impact of the loss or compromise of an asset or service in precise terms such as dollar value. This occurs

---

[4] For example, in considering a hydroelectric power generation infrastructure, certain components such as specially manufactured turbines or bearings could represent a potential single-point-of-failure and be considered critical infrastructure assets. Additionally, one might further consider a critical asset to be at a higher level, such as a power generation substation or dam.

[5] The Health Care sector is divided into Health Care Services; Laboratories; Blood Supply Facilities and Pharmaceuticals. The Health Care Services sub-sector is sub-divided into hospitals, community health centres, community care access centres, regional public health units, primary care physicians and ambulances. For additional sector breakouts see National Contingency Planning Group, *Canadian Infrastructures and their Dependencies*, March 2000 and op.cit. Deloitte & Touche report, Appendix B.

[6] A useful review process is provided in Science Applications International Corporation Contractor's Final Report prepared for The American Association of State Highway and Transportation Officials' Security Task Force, *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, May 2002 available on-line at: www.transportation.org/aashto

[7] Op. cit. Deloitte & Touche report, page 8.

because assessing value is more complex than it first appears. One might consider replacement cost, or book value of an asset, but this may understate the impact of the loss of the asset as the asset takes on acquired value because it supports a service function[8] [9]. While the notion of acquired value is logical, attempting to quantify it is often quite difficult except on simple scales such as "Low, Medium, High, etc." These scales generally provide enough accuracy to identify and prioritize the most critical assets in the infrastructure of the enterprise[10].

Given experience with the various models and methodologies, it is recommended that measurement of criticality employ the qualitative measures "Low, Medium and High". Having an assessment team do this type of evaluation and rationalize different opinions can be very reliable. If necessary, the methodology can be refined using more precise quantitative techniques (one might introduce a quantitative technique for conducting a cost-benefit analysis of options for protecting a particular CI asset).[11]

Successful models must strike a balance between simplicity and validity and should be designed to assess the criticality of various assets. Experience has shown that the process is not an easy one. Initial results should not be viewed as "cast in stone" but should be adjusted as the exercise progresses or is reviewed.

It is envisioned that the development of a rule set comprising critical infrastructure impact factors and consequence criteria (these terms are explained below) where the judgment is based on specific conditions being met will lead to a simpler approach for establishing criticality. In the next sections criticality is broken out into impact factors and consequence criteria.

3.3 IMPACT FACTORS (CRITERIA)

Impact factors, sometimes called critical asset factors, are the criteria used to prioritize critical assets. In this paper, an assessment of the impact of the loss of an asset or service in relation to six impact factors is proposed. A collective review of the impact factors and their associated consequences is used to determine critical infrastructure and its relative ranking. The impact factors below are analyzed considering the scope, the magnitude, time of the year and the effects of time. The impact factors are also scaleable, in that they can also be applied and built up from the basis of the

---

[8] For example, the value of navigational equipment to support air and marine services exceeds its replacement cost. See also RCMP Technical Operations Directorate, Information Technology Security Branch, *Guide to Threat and Risk Assessment for Information Technology,* November 1994, page 2.

[9] Op. cit. Deloitte & Touche report, page 9.

[10] Ibid. page 9.

[11] For example, the economy-wide service impact associated with the loss of a critical telecommunications service asset could affect any number of businesses depending upon electronic commerce, which could in turn affect other enterprises in various CI sectors. The resulting multiplier effect could be estimated quantitatively using techniques, such as input-output modeling. However, attempting to establish precise multipliers and costs is probably not necessary since the goal is to simply identify the most critical assets.

enterprise/company/organization (E) through to individual sector (IS), cross-sectoral (CS) and governance (G), as indicated at the end of the descriptions.

- **Concentration of People and Assets** – This category looks at a measure of the impact of service delivery degradation, attributable to the loss of a critical asset on the physical well-being of co-located people and assets. It is an assessment of possible fatalities, serious injuries, or number of people evacuated due to the loss of the service or facility, but does not include people inconvenienced by the loss of the asset and/or service. This also provides a determination of the potential impact on the surrounding environment (event locations, collateral damage area). The higher the concentration of people and assets, the greater the potential for catastrophic effects. (E)

- **Economic** - This criterion measures potential economic impact (to the enterprise) arising from degraded service attributable to the loss of a critical infrastructure asset. In addition to the direct physical loss or disruption of an asset, it includes a general assessment of the damage on the asset and associated information and people within the organization in general quantitative terms. (E)

- **Critical Infrastructure Sector** – This factor measures the sectoral assessment of how the loss or degradation of the service or asset relates to a critical infrastructure sector, for example, as defined in the NCIAP. (IS)

- **Interdependency** - Interdependency impact is the cross-sectoral assessment of the impact of the loss or degradation of the service to other critical services or sectors. This criterion also provides an assessment of possible dependencies that other critical services or functions may have on the asset being reviewed. The purpose is to determine if there is likelihood of a high cascading effect resulting from the loss of the service or asset on other critical services or functions within the sector and across sectors. (CS)

  Types of interdependencies include:
  - physical (e.g. material output of one infrastructure used by another);
  - geographic (e.g. common corridor); and
  - logical (e.g. dependency through financial markets).

- **Service Delivery** - This impact category is the measurement in qualitative terms of the impact that the destruction or temporary loss of an asset/element of a sector would have in terms of lost or degraded service delivery in the general economy. Initially, a measurement could be made of the allowable downtime before immediate significant impacts occur. Ultimately, the service impact is a combination of the availability of substitutes, the time and costs incurred before the asset or service is restored. (CS)

- **Public Confidence** - This criterion measures how the loss of an asset or service would impact public confidence including employee confidence, customer confidence, perceived value of an asset or service in comparison with other assets or services, the potential impact on a government's ability to continue to function and on public confidence in government that could arise from the loss of the service or asset. Ultimately, it is an assessment of possible impacts on the public's confidence in the ability of the government to preserve public health and safety, economic security, or to assure the provision of essential services. (G)

3.4 CONSEQUENCE CRITERIA

The following questions are posed to the sector experts and the assessment team to develop and provide additional information on the consequences associated with each of the impact factors. A good starting point would be a review of security plans and assessments including Threat and Risk Assessments (TRAs), Vulnerability Assessments (VAs), Business Impact Assessments (BIAs), Business Continuity Plans (BCPs), Business Resumption Plans, Disaster Recovery Plans, Emergency Management Plans, Contingency Plans and Y2K Plans. Users should review the following questions and apply or refine them to their own specific circumstances. Questions to ask:

Concentration of People and Assets

- Could the loss of this asset result in death, serious injury, or evacuation of people?
- How many people will be affected (death, injury, evacuation) by lost or degraded services associated with the lost asset?
- What is the concentration of other assets co-located with the critical asset?

Economic:

- What potential economic impact would occur to the enterprise through lost or degraded services that are likely to arise from the loss of the asset?
- What is the cost of the direct damage to the asset or the cost to restore the asset?
- To what extent are critical information and systems compromised?
- Does the economic impact to the enterprise vary depending on the season?

Critical Infrastructure Sector:

- Is the asset in one of the critical infrastructure sectors as defined by the NCIAP?
- Is the impact of the loss or degradation of the service or asset local, provincial, regional, national or international?

Interdependency:

- Are assets within the sector dependent upon this asset?
- Are assets outside the sector dependent upon this asset?
- List the known assets or services within and external to the asset's sector that are dependent on this asset.
- How do the other infrastructure sectors depend on this asset or service?

- How does this infrastructure asset or service depend on the services or assets of other infrastructure sectors?
- Owners of infrastructure assets that have a historical experience with natural disasters typically have a better understanding of infrastructure interdependencies, and are more likely to have contingency plans to deal with outages. What information and plans exist with respect to this asset?

Service Delivery:
- Is the impact on the general economy instantaneous, rapid or delayed?
- How great will the impact of the loss of this asset be, taking into consideration the subsequent loss or degradation of services associated with losing the asset?
- How long will it take to restore the service or replace the asset?
- What substitutes or alternatives are available?
- Does the service impact to customers vary depending on the season?
- Considering the other questions, such as the availability of substitutes, is the potential impact local, provincial, regional, national or international in scope?

Public Confidence:
- Could the loss of this asset result in death, serious injury or displacement of people?
- Could the loss of this asset result in low morale, loss of national prestige, panic, rioting or civil disorder?
- Will the loss of the asset have an ecological impact of altering the environment?
- What public confidence impact (e.g. ability to defend national sovereignty/ territorial integrity) could the loss of this asset have, either directly or through related service degradation?
- Does the asset or service have symbolic importance?
- Will the loss of this asset significantly reduce the ability of governments and essential utilities to deliver basic services oriented toward promoting public welfare?

3.5 RANKING AND THE USE OF A RULE-SET

In general, the preliminary scales for categorizing impact would be qualitative in nature, and make use of terms such as Low, Medium and High. The qualitative assessment can be refined using quantitative scoring (such as 0 to 15). Estimates can be further refined by having experts examine specific impact factors such as potential impact on people, the environment, confidence in government, etc. either through models or through Business Impact Assessment studies.

The assignment of numeric weights to individual impact factors/consequence criteria should be avoided as this could lend an appearance of mathematical validity that is not present. The better approach is to develop a rule-set where judgment is based upon specific conditions being met.[12]

[12] Op. cit. Deloitte & Touche report, page 24.

A CI priority assessment screening model is proposed on page 11 with a rule-set based on consequence criteria. The consequence criteria employed in the screening model provide a range of consequences from low to medium to high. A severe consequence criterion has been proposed to allow for executive discretion when rating the higher value assets. Finally, if an asset is not critical, as it has negligible impact assessment, a score of "0" should be used (this is not shown on the grid).

4. CONCLUSIONS

The National Critical Infrastructure Assurance Program's chief objective is that NCI is sufficiently resilient, thereby assuring the continued availability of essential services to Canadians. The assurance actions of the partners and the priorities of those actions are based on risk management principles using common national criteria where appropriate. The identification and ranking of CI assets fits squarely within the risk management process of the NCIAP. The use of a common risk management process will encourage partners to address CI consistently.

This paper identifies the following steps to identifying and ranking critical assets:

1. characterize or standardize assets
2. establish criticality
3. assess impact of the loss of an asset
4. assess consequence of the loss of an asset
5. use of a rule-set to rank assets

In the paper, the following six impact factors are proposed:

- concentration of people and assets
- economic impact or direct cost to the enterprise
- critical infrastructure sector
- interdependency or cross-sectoral impact
- service delivery impact to the general economy
- public confidence

A Critical Infrastructure Assessment Screening Model is proposed. As the NCIAP continues to move forward, CI owners and stakeholders will contribute to the development of an overall model for identifying and ranking national CI assets.

CI PRIORITY ASSESSMENT SCREENING MODEL - CONSEQUENCE CRITERIA

IMPACT FACTOR Score	**Severe** 15	**High** 5	**Medium** 3	**Low** 1
CONCENTRATION OF PEOPLE AND ASSETS IMPACT (potential for catastrophic effects)	Greater than 10,000 people	Between 1,000 and 10,000 people	Between 100 1000 people	Less than 100 people
ECONOMIC IMPACT / Direct cost of restoration including critical information and information technology (service relies on or asset contains critical information and I.T.)	Direct damage and restoration > $1 billion	Direct damage and restoration $100 million - $1 B	Direct damage and restoration $10 - 100 million	Direct damage and restoration under $10 million
CRITICAL INFRASTRUCTURE SECTOR IMPACT (service or asset relates to a critical infrastructure sector)	Sector may shut down or international	national	provincial or regional	local
INTERDEPENDENCY IMPACT (high cascading effect resulting from loss of service or asset)	Debilitating impact on other sectors	Significant impact or disruption of other sectors	Moderate impact on important missions of other sectors	Minor impact on important missions of other sectors
SERVICE IMPACT - Potential for immediate significant impacts to the general economy considering allowable downtime (service impact depends on availability of substitutes and the time and cost to restore the asset or service)	High cross-sectoral cost Recovery time longer than one year (years)	High cost Long recovery time (months - year)	Medium cost Significant recovery time (days - weeks)	Low cost Brief recovery time (hours - days)
PUBLIC CONFIDENCE IMPACT loss of asset or service would impact public confidence (employee confidence, customer confidence, value of asset or service in comparison with other assets or services)	High national risk & ability to control in doubt	Public perceives high national risk & low ability to control risk	Public perceives moderate risk & moderate ability to control risk	Public perceives low risk & high ability to control risk
TOTAL SCORE				

Notes:
An inventory of assets and/or services is required for completeness and full documentation.
If an asset is not critical, as it has a negligible consequence, a score of "0" should be used.
This assessment can be refined using quantitative scoring (such as 0 to 15). Estimates can be further refined by having experts examine other variables such as potential impact on people, the environment, confidence in government, etc. either through models or through Business Impact Assessment studies.

SAMPLE WORKSHEET FOR RANKING ASSETS

ASSET LIST	IMPACT FACTOR: Concentration of People & Assets	Economic	CI Sector	Inter-dependency	Service	Public Confidence	TOTAL SCORE