Government of Canada
Gouvernement du Canada

Office of Critical Infrastructure Protection and Emergency Preparedness

Bureau de la protection des infrastructures essentielles et de la protection civile

A Guide to Business Continuity Planning

Canada

THIS PUBLICATION WAS PRODUCED BY THE OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY PREPAREDNESS.

An electronic version is available on the Internet.

Cette publication est aussi disponibile en français.
Elle s'intitule : *Guide de planification de la continuité des activités.*

ISBN 0-662-33764-6
Catalogue No. D82-37/2003E
Minister of Public Works and Government Services

1.0 INTRODUCTION

1.1 OVERVIEW

This publication provides a summary and general guidelines for Business Continuity Planning (BCP).

While governments, not-for-profit institutions, and non-governmental organizations also deliver critical services, private organizations must continuously deliver products and services to satisfy shareholders and to survive. Although they differ in goals and functions, BCP can be applied by all organizations.

1.2 CHANGES IN THE WORLD OF BUSINESS CONTINUITY PLANNING

1.2.1 BUSINESS CONTINUITY PLANNING VERSUS BUSINESS RESUMPTION PLANNING AND DISASTER RECOVERY PLANNING

A Business Resumption Plan describes how to resume business after a disruption. A Disaster Recovery Plan deals with recovering Information Technology (IT) assets after a disastrous interruption. Both imply a stoppage in critical operations and are reactive.

Recognizing that some services or products must be continuously delivered without interruption, there has been a shift to business continuity from business resumption to business continuity planning.

A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available.

1.2.2 THE EFFECTS OF SEPTEMBER 11TH

September 11, 2001 demonstrated that although high impact, low probability events could occur, recovery is possible. Even though buildings were destroyed and blocks of Manhattan were affected, businesses and institutions with good continuity plans survived.

The lessons learned include:

- plans must be updated and tested frequently;
- all types of threats must be considered;
- dependencies and interdependencies should be carefully analyzed;
- key personnel may be unavailable;
- telecommunications are essential;
- alternate sites for IT backup should not be situated close to the primary site;
- employee support (counselling) is important;
- copies of plans should be stored at a secure off-site location;
- sizable security perimeters may surround the scene of incidents involving national security or law enforcement, and can impede personnel from returning to buildings;
- despite shortcomings, Business Continuity Plans in place pre September 11 were indispensable to the continuity effort; and
- increased uncertainty (following a high impact disruption such as terrorism) may lengthen time until operations are normalized.

1.2.3 EMERGING ISSUES

Continuous Service Delivery Assurance (CSDA) is a commitment to continuous delivery of critical services that avoids immediate severe disruption to an organization. A BCP includes both risk evaluation, management and control and effective plans, measures and arrangements for business continuity.

Continuous risk management lowers the risk of disruption and assesses the potential impacts of disruptions when they occur. An example would be the business impact analysis component of a BCP program.

WHAT IS BUSINESS CONTINUITY PLANNING?

Critical services or products are those that must be delivered to ensure survival, avoid causing injury, and meet legal or other obligations of an organization. Business Continuity Planning is a proactive planning process that ensures critical services or products are delivered during a disruption.

A Business Continuity Plan includes:

- Plans, measures and arrangements to ensure the continuous delivery of critical services and products, which permits the organization to recover its facility, data and assets.
- Identification of necessary resources to support business continuity, including personnel, information, equipment, financial allocations, legal counsel, infrastructure protection and accommodations.

Having a BCP enhances an organization's image with employees, shareholders and customers by demonstrating a proactive attitude. Additional benefits include improvement in overall organizational efficiency and identifying the relationship of assets and human and financial resources to critical services and deliverables.

1.2.4 WHY IS BUSINESS CONTINUITY PLANNING IMPORTANT?

Every organization is at risk from potential disasters that include:

- natural disasters such as tornadoes, floods, blizzards, earthquakes and fire;
- accidents;
- sabotage;
- power and energy disruptions;
- communications, transportation, safety and service sector failure;
- environmental disasters such as pollution and hazardous materials spills; or
- cyber attacks and hacker activity.

Creating and maintaining a BCP helps ensure that an institution has the resources and information needed to deal with these emergencies.

2.0 CREATING A BUSINESS CONTINUITY PLAN

A BCP typically includes five sections:

1. BCP Governance
2. Business Impact Analysis (BIA)
3. Plans, measures, and arrangements for business continuity
4. Readiness procedures
5. Quality assurance techniques (exercises, maintenance and auditing)

2.1 ESTABLISH CONTROL

A BCP contains a governance structure often in the form of a committee that will ensure senior management commitments and define senior management roles and responsibilities.

The BCP senior management committee is responsible for the oversight, initiation, planning, approval, testing and audit of the BCP. It also implements the BCP, coordinates activities, approves the BIA survey, oversees the creation of continuity plans and reviews the results of quality assurance activities.

Senior managers or a BCP Committee would normally:

- approve the governance structure;
- clarify their roles, and those of participants in the program;
- oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan;
- provide strategic direction and communicate essential messages;
- approve the results of the BIA;
- review the critical services and products that have been identified;
- approve the continuity plans and arrangement;
- monitor quality assurance activities; and
- resolve conflicting interests and priorities.

This BCP committee is normally comprised of the following members:

- Executive sponsor has overall responsibility for the BCP committee; elicits senior management's support and direction; and ensures that adequate funding is available for the BCP program.
- BCP Coordinator secures senior management's support; estimates funding requirements; develops BCP policy; coordinates and oversees the BIA process; ensures effective participant input; coordinates and oversees the development of plans and arrangements for business continuity; establishes working groups and teams and defines their responsibilities; coordinates appropriate training; and provides for regular review, testing and audit of the BCP.
- Security Officer works with the coordinator to ensure that all aspects of the BCP meet the security requirements of the organization.
- Chief Information Officer (CIO) cooperates closely with the BCP coordinator and IT specialists to plan for effective and harmonized continuity.
- Business unit representatives provide input, and assist in performing and analyzing the results of the business impact analysis.

The BCP committee is commonly co-chaired by the executive sponsor and the coordinator.

2.2 BUSINESS IMPACT ANALYSIS

The purpose of the BIA is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

2.2.1 IDENTIFY THE MANDATE AND CRITICAL ASPECTS OF AN ORGANIZATION

This step determines what goods or services it must be delivered. Information can be obtained from the mission statement of the organization, and legal requirements for delivering specific services and products.

2.2.2 PRIORITIZE CRITICAL SERVICES OR PRODUCTS

Once the critical services or products are identified, they must be prioritized based on minimum acceptable delivery levels and the maximum period of time the service can be down before severe damage to the organization results. To determine the ranking of critical services, information is required to determine impact of a disruption to service delivery, loss of revenue, additional expenses and intangible losses.

IDENTIFY IMPACTS OF DISRUPTIONS

The impact of a disruption to a critical service or business product determines how long the organization could function without the service or product, and how long clients would accept its unavailability. It will be necessary to determine the time period that a service or product could be unavailable before severe impact is felt.

IDENTIFY AREAS OF POTENTIAL REVENUE LOSS

To determine the loss of revenue, it is necessary to determine which processes and functions that support service or product delivery are involved with the creation of revenue. If these processes and functions are not performed, is revenue lost? How much? If services or goods cannot be provided, would the organization lose revenue? If so, how much revenue, and for what length of time? If clients cannot access certain services or products would they then to go to another provider, resulting in further loss of revenue?

IDENTIFY ADDITIONAL EXPENSES

If a business function or process is inoperable, how long would it take before additional expenses would start to add up? How long could the function be unavailable before extra personnel would have to be hired? Would fines or penalties from breaches of legal responsibilities, agreements, or governmental regulations be an issue, and if so, what are the penalties?

IDENTIFY INTANGIBLE LOSSES

Estimates are required to determine the approximate cost of the loss of consumer and investor confidence, damage to reputation, loss of competitiveness, reduced market share, and violation of laws and regulations. Loss of image or reputation is especially important for public institutions as they are often perceived as having higher standards.

2.2.3 INSURANCE REQUIREMENTS

Since few organizations can afford to pay the full costs of a recovery; having insurance ensures that recovery is fully or partially financed.

When considering insurance options, decide what threats to cover. It is important to use the BIA to help decide both what needs insurance coverage, and the corresponding level of coverage. Some aspects of an operation may be overinsured, or underinsured. Minimize the possibility of overlooking a scenario, and to ensure coverage for all eventualities.

Document the level of coverage of your institutional policy, and examine the policy for uninsured areas and non specified levels of coverage. Property insurance may not cover all perils (steam explosion, water damage, and damage from excessive ice and snow not removed by the owner). Coverage for such eventualities is available as an extension in the policy.

When submitting a claim, or talking to an adjustor, clear communication and understanding is important. Ensure that the adjustor understands the expected full recovery time when documenting losses. The burden of proof when making claims lies with the policyholder and requires valid and accurate documentation.

Include an expert or an insurance team when developing the response plan.

2.2.4 RANKING

Once all relevant information has been collected and assembled, rankings for the critical business services or products can be produced. Ranking is based on the potential loss of revenue, time of recovery and severity of impact a disruption would cause. Minimum service levels and maximum allowable downtimes are then determined.

2.2.5 IDENTIFY DEPENDENCIES

It is important to identify the internal and external dependencies of critical services or products, since service delivery relies on those dependencies.

Internal dependencies include employee availability, corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and support services such as finance, human resources, security and information technology support.

External dependencies include suppliers, any external corporate assets such as equipment, facilities, computer applications, data, tools, vehicles, and any external support services such as facility management, utilities, communications, transportation, finance institutions, insurance providers, government services, legal services, and health and safety service.

2.3 PLANS FOR BUSINESS CONTINUITY

This step consists of the preparation of detailed response/recovery plans and arrangements to ensure continuity. These plans and arrangements detail the ways and means to ensure critical services and products are delivered at a minimum service levels within tolerable down times. Continuity plans should be made for each critical service or product.

2.3.1 MITIGATING THREATS AND RISKS

Threats and risks are identified in the BIA or in a full-threat-and-risk assessment. Moderating risk is an ongoing process, and should be performed even when the BCP is not activated. For example, if an organization requires electricity for production, the risk of a short term power outage can be mitigated by installing stand-by generators.

Another example would be an organization that relies on internal and external telecommunications to function effectively. Communications failures can be minimized by using alternate communications networks, or installing redundant systems.

2.3.2 ANALYZE CURRENT RECOVERY CAPABILITIES

Consider recovery arrangements the organization already has in place, and their continued applicability. Include them in the BCP if they are relevant.

2.3.3 CREATE CONTINUITY PLANS

Plans for the continuity of services and products are based on the results of the BIA. Ensure that plans are made for increasing levels of severity of impact from a disruption. For example, if limited flooding occurs beside an organization's building, sand bagging may be used in response. If water rises to the first floor, work could be moved to another company building or higher in the same building. If the flooding is severe, the relocation of critical parts of the business to another area until flooding subsides may be the best option.

Another example would be a company that uses paper forms to keep track of inventory until computers or servers are repaired, or electrical service is restored. For other institutions, such as large financial firms, any computer disruptions may be unacceptable, and an alternate site and data replication technology must be used.

The risks and benefits of each possible option for the plan should be considered, keeping cost, flexibility and probable disruption scenarios in mind. For each critical service or product, choose the most realistic and effective options when creating the overall plan.

2.3.4 RESPONSE PREPARATION

Proper response to a crisis for the organization requires teams to lead and support recovery and response operations. Team members should be selected from trained and experienced personnel who are knowledgeable about their responsibilities.

The number and scope of teams will vary depending on organization's size, function and structure, and can include:

- Command and Control Teams that include a Crisis Management Team, and a Response, Continuation or Recovery Management Team.
- Task Oriented Teams that include an Alternate Site Coordination Team, Contracting and Procurement Team, Damage Assessment and Salvage Team, Finance and Accounting Team, Hazardous Materials Team, Insurance Team, Legal Issues Team, Telecommunications/Alternate Communications Team, Mechanical Equipment Team, Mainframe/Midrange Team, Notification Team, Personal Computer/Local area Network Team, Public and Media Relations Team, Transport Coordination Team and Vital Records Management Team

The duties and responsibilities for each team must be defined, and include identifying the team members and authority structure, identifying the specific team tasks, member's roles and responsibilities, creation of contact lists and identifying possible alternate members.

For the teams to function in spite of personnel loss or availability, it may be necessary to multitask teams and provide cross-team training.

2.3.5 ALTERNATE FACILITIES

If an organization's main facility or Information Technology assets, networks and applications are lost, an alternate facility should be available. There are three types of alternate facility:

1. Cold site is an alternate facility that is not furnished and equipped for operation. Proper equipment and furnishings must be installed before operations can begin, and a substantial time and effort is required to make a cold site fully operational. Cold sites are the least expensive option.
2. Warm site is an alternate facility that is electronically prepared and almost completely equipped and furnished for operation. It can be fully operational within several hours. Warm sites are more expensive than cold sites.
3. Hot site is fully equipped, furnished, and often even fully staffed. Hot sites can be activated within minutes or seconds. Hot sites are the most expensive option.

When considering the type of alternate facility, consider all factors, including threats and risks, maximum allowable downtime and cost.

For security reasons, some organizations employ hardened alternate sites. Hardened sites contain security features that minimize disruptions. Hardened sites may have alternate power supplies; back-up generation capability; high levels of physical security; and protection from electronic surveillance or intrusion.

2.4 READINESS PROCEDURES

2.4.1 TRAINING

Business continuity plans can be smoothly and effectively implemented by:

- Having all employees and staff briefed on the contents of the BCP and aware of their individual responsibilities; and
- Having employees with direct responsibilities trained for tasks they will be required to perform, and be aware of other teams' functions.

2.4.2 EXERCISES

After training, exercises should be developed and scheduled in order to achieve and maintain high levels of competence and readiness. While exercises are time and resource consuming, they are the best method for validating a plan. The following items should be incorporated when planning an exercise:

- Goal – The part of the BCP to be tested.
- Objectives – The anticipated results. Objectives should be challenging, specific, measurable, achievable, realistic and timely.
- Scope – Identifies the departments or organizations involved, the geographical area, and the test conditions and presentation.
- Artificial aspects and assumptions – Defines which exercise aspects are artificial or assumed, such as background information, procedures to be followed, and equipment availability.
- Participant Instructions – Explains that the exercise provides an opportunity to test procedures before an actual disaster.
- Exercise Narrative – Gives participants the necessary background information, sets the environment and prepares participants for action. It is important to include factors such as time, location, method of discovery and sequence of events, whether events are finished or still in progress, initial damage reports and any external conditions.
- Communications for Participants – Enhanced realism can be achieved by giving participants access to emergency contact personnel who share in the exercise. Messages can also be passed to participants during an exercise to alter or create new conditions.
- Testing and Post-Exercise Evaluation – The exercise should be monitored impartially to determine whether objectives were achieved. Participants' performance, including attitude, decisiveness, command, coordination, communication, and control should be assessed. Debriefing should be short, yet comprehensive, explaining what did and did not work, emphasizing successes and opportunities for improvement. Participant feedback should also be incorporated in the exercise evaluation.

Exercise complexity level can also be enhanced by focusing the exercise on one part of the BCP instead of involving the entire organization.

2.5 QUALITY ASSURANCE TECHNIQUES

Review of the BCP should assess the plan's accuracy, relevance and effectiveness. It should also uncover which aspects of a BCP need improvement. Continuous appraisal of the BCP is essential to maintaining its effectiveness. The appraisal can be performed by an internal review, or by an external audit.

2.5.1 INTERNAL REVIEW

It is recommended that organizations review their BCP:

- on a scheduled basis (annually or bi-annually);
- when changes to the threat environment occur;
- when substantive changes to the organization take place; and
- after an exercise to incorporate findings.

2.5.2 EXTERNAL AUDIT

When auditing the BCP, consultants nominally verify:

- the procedures used to determine critical services and processes; and
- the methodology, accuracy, and comprehensiveness of continuity plans.

3.0 WHAT TO DO WHEN A DISRUPTION OCCURS

Disruptions are handled in three steps:

1. response;
2. continuation of critical services; and
3. recovery and restoration.

3.1 RESPONSE

Incident response involves the deployment of teams, plans, measures and arrangements. The following tasks are accomplished during the response phase:

- incident management;
- communications management; and
- operations management.

3.1.1 INCIDENT MANAGEMENT

Incident management includes the following measures:

- notifying management, employees, and other stakeholders;
- assuming control of the situation;
- identifying the range and scope of damage;
- implementing plans;
- identifying infrastructure outages; and
- coordinating support from internal and external sources.

3.1.2 COMMUNICATIONS MANAGEMENT

Communications management is essential to control rumors, maintain contact with the media, emergency services and vendors, and assure employees, the public and other affected stakeholders. Communications management requirements may necessitate building redundancies into communications systems and creating a communications plan to adequately address all requirements.

3.1.3 OPERATIONS MANAGEMENT

An Emergency Operations Center (EOC) can be used to manage operations in the event of a disruption. Having a centralized EOC where information and resources can be coordinated, managed and documented helps ensure effective and efficient response.

3.2 CONTINUATION

Ensure that all time-sensitive critical services or products are continuously delivered or not disrupted for longer than is permissible.

3.3 RECOVERY AND RESTORATION

The goal of recovery and restoration operations is to, recover the facility or operation and maintain critical service or product delivery. Recovery and restoration includes:

- re-deploying personnel;
- deciding whether to repair the facility, relocate to an alternate site or build a new facility;
- acquiring the additional resources necessary for restoring business operations;
- re-establishing normal operations; and
- resuming operations at pre-disruption levels.

4.0 CONCLUSION

When critical services and products cannot be delivered, consequences can be severe. All organizations are at risk and face potential disaster if unprepared. A Business Continuity Plan is a tool that allows institutions to not only to moderate risk, but also continuously deliver products and services despite disruption.

ADDITIONAL REFERENCES

Additional information on Business Continuity Planning can be obtained by visiting the following organizational web sites:

The Disaster Recovery Information Exchange (DRIE) has chapters throughout Canada. For more information visit the DRIE website at http://www.drie.org.

The Disaster Recovery Institute Canada (DRI) provides valuable services, certification and international standards for contingency planning and business continuity planning professionals. For more information visit the DRI website at http://www.dri.ca.

ADDITIONAL INFORMATION

For additional information on emergency preparedness, contact the Office of Critical Infrastructure Protection and Emergency Preparedness or your provincial or territorial emergency measures organization.

OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY PREPAREDNESS

Public Affairs Division
122 Bank St., 2nd Floor, Ottawa, ON K1A 0W6
Telephone: (613) 944-4875
1-800-830-3118
Fax: (613) 998-9589
E-mail: communications@ocipep-bpiepc.gc.ca
Internet: http://www.ocipep-bpiepc.gc.ca

PROVINCIAL/TERRITORIAL EMERGENCY MEASURES ORGANIZATIONS

NEWFOUNDLAND AND LABRADOR

Emergency Measures Organization
Telephone: (709) 729-3703
Fax: (709) 729-3857

PRINCE EDWARD ISLAND

Emergency Measures Organization
Telephone: (902) 888-8050
Fax: (902) 888-8054

NOVA SCOTIA

Emergency Measures Organization
Telephone: (902) 424-5620
Fax: (902) 424-5376

NEW BRUNSWICK

Emergency Measures Organization
Telephone: (506) 453-2133
Toll free: (800) 561-4034
Fax: (506) 453-5513

QUÉBEC

Direction générale de la sécurité civile et de la sécurité incendie
Telephone: (418) 646-7950
Fax: (418) 646-5427
Toll Free Emergency Number: 1 866 776-8345
Emergency Number: (418) 643-3256

Or one of the Direction générale de la sécurité civile regional offices:
Bas-Saint-Laurent-Gaspésie-Îles-de-la-Madeleine: (418) 727-3589
Saguenay-Lac-St-Jean-Côte-Nord: (418) 695-7872
Capitale Nationale-Chaudière- Appalaches-Nunavik: (418) 643-3244
Mauricie-Centre-du-Québec: (819) 371-6703
Montréal-Laval-Laurentides-Lanaudière: (514) 873-1300
Montérégie-Estrie: (514) 873-1324
Outaouais-Abitibi-Témiscamingue-Nord-du-Québec: (819) 772-3737

ONTARIO

Emergency Management Ontario
Telephone: (416) 212-3468
Fax: (416) 212-3498

MANITOBA

Emergency Measures Organization
Telephone: (204) 945-4772
Toll free: 1-888-826-8298
Fax: (204) 945-4620

SASKATCHEWAN

Saskatchewan Emergency Planning
Telephone: (306) 787-9563
Fax: (306) 787-1694

ALBERTA

Emergency Management Alberta
Telephone: (780) 422-9000
Toll free in Alberta, dial 310-0000-780-422-9000
Fax: (780) 422-1549

BRITISH COLUMBIA

Provincial Emergency Program (PEP)
Telephone: (250) 952-4913
Fax: (250) 952-4888

NORTHWEST TERRITORIES

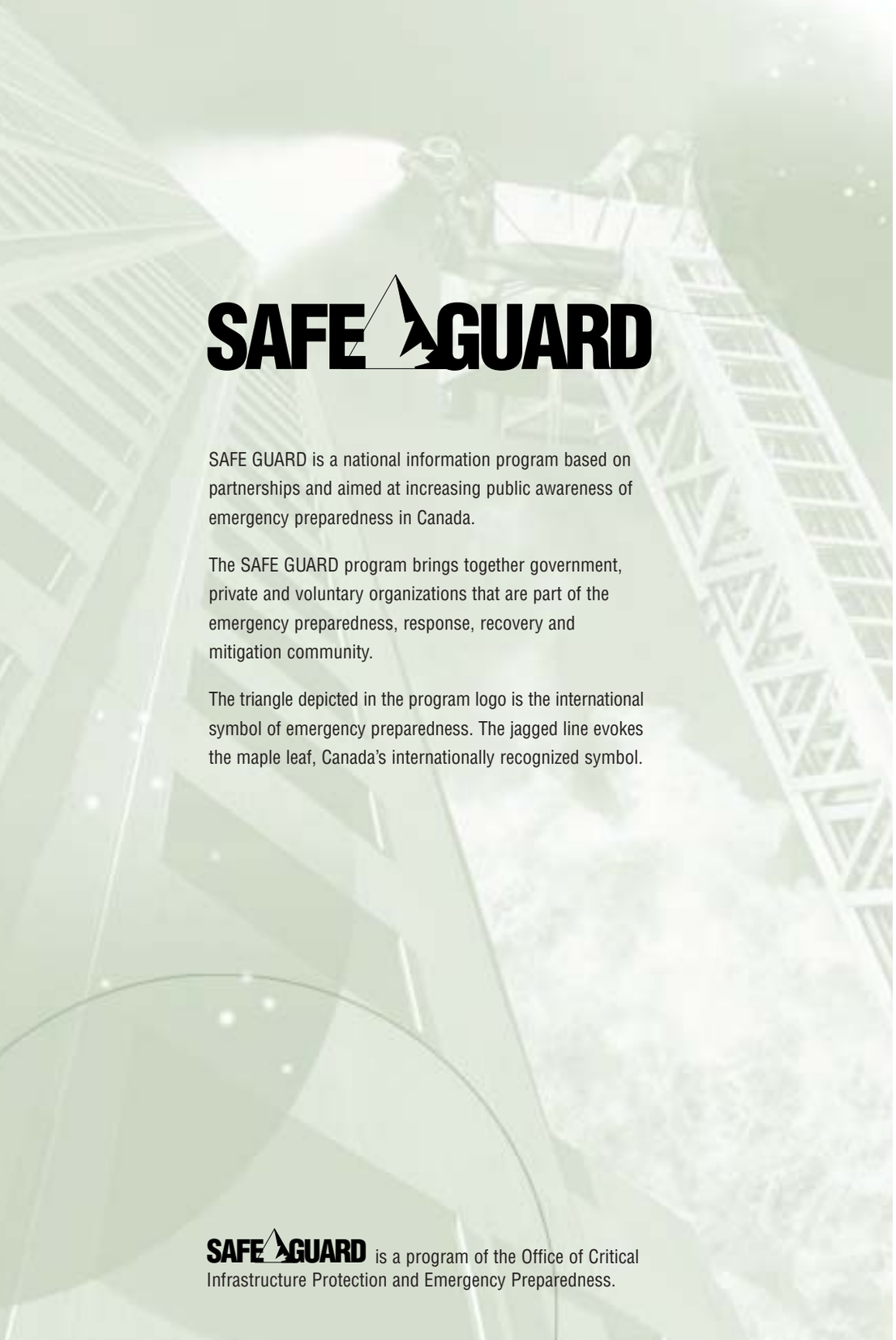
Emergency Measures Organization
Telephone: (867) 873-7785
Fax: (867) 873-8193

YUKON

Emergency Measures Organization
Telephone: (867) 667-5220
Fax: (867) 393-6266

NUNAVUT

Nunavut Emergency Management
Telephone: (867) 975-5300
Fax: (867) 979-4221)



SAFE GUARD

SAFE GUARD is a national information program based on partnerships and aimed at increasing public awareness of emergency preparedness in Canada.

The SAFE GUARD program brings together government, private and voluntary organizations that are part of the emergency preparedness, response, recovery and mitigation community.

The triangle depicted in the program logo is the international symbol of emergency preparedness. The jagged line evokes the maple leaf, Canada's internationally recognized symbol.

SAFE GUARD is a program of the Office of Critical Infrastructure Protection and Emergency Preparedness.