Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Operational Security Standard - Business Continuity Planning (BCP) Program

Published: Mar 23, 2004

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-17/2004E-PDF
ISBN: 978-0-660-09863-0

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Norme de sécurité opérationnelle - Programme de planification de la continuité des activités (PCA)

Operational Security Standard - Business Continuity Planning (BCP) Program

1. Preamble

In accordance with sections 10.1, 10.14 and10.12.4 of the Government Security Policy (GSP), the continued delivery of government services must be assured through baseline security requirements, business continuity planning, including Information Management (IM) and Information Technology (IT) continuity planning, and continuous risk management. The GSP and its associated standards describe these baseline security requirements. They are based on a government-wide threat and risk assessment and are designed to protect the resources on which the government relies to deliver services: employees, information and other assets.

As part of baseline security requirements, departments must establish a Business Continuity Planning (BCP) Program to provide for the continued availability of:

a. Services and associated assets that are critical to the health, safety, security or economic well-being of Canadians, or the effective functioning of government. Unavailability would result in a high degree of injury to Canadians and government.
b. Other services and assets when warranted by a threat and risk assessment.

This standard provides direction and guidance to departments in establishing such a program. It is supplemented by technical documentation that includes suggestions, examples, best practices and other guidance.

The BCP Program complements emergency preparedness that is mandated by legislation or government policy (e.g. fire and building evacuation plans; civil emergency plans). It also supports planning that is necessary to restore other-than-critical services and their associated assets and resources; departments should use this program to incorporate their planning for other-than-critical services.

2. Definitions

See Glossary in Appendix 1

3. Business Continuity Planning Program

The BCP Program is composed of four elements:

a. The establishment of BCP Program governance.
b. The conduct of a business impact analysis.
c. The development of business continuity plans and arrangements.
d. The maintenance of BCP Program readiness.

3.1 Governance

An essential element of governance is the development of departmental BCP Program policy to apply GSP requirements to new and existing departmental programs and operations, pursuant to any constituent or other legislative requirements.

It is therefore essential that Senior departmental managers commit to the BCP Program, integrate it into a strategic planning framework, ensure compliance with government policy, ensure appropriate departmental expert review (e.g., legal, policy, finance, communications, information management and human resource specialists), and appoint participants. This can be done through a senior management committee. Its support is essential to:

a. Provide strategic direction and communication.
b. Approve departmental BCP Program policy and governance.
c. Commit financial and other resources.
d. Review and approve identified critical services and associated assets.
e. Resolve conflicting interests and priorities.
f. Approve business continuity plans and activities.
g. Ensure regular training, review, testing and audit.
h. Ensure BCP Program activities are supported by IM, IT, and other continuity plans and arrangements, as required.

Governance includes the appointment of a Departmental BCP Coordinator to:

a. Obtain senior management support and funding.
b. Develop a departmental BCP Program policy and governance.
c. Ensure the development of a strategy to communicate BCP activities to employees and stakeholders.
d. Establish working groups and define their roles and responsibilities.
e. Ensure the completion of the business impact analysis and the development and maintenance of business continuity plans.
f. Ensure that IM, IT, and other continuity plans and arrangements are fully integrated into the BCP Program.
g. Provide for regular training, review, testing and audit.
h. Liaise with other departments and agencies as necessary to coordinate BCP.

i. Collaborate with the IT Security Coordinator throughout the process.
j. Inform the Departmental Security Officer (DSO) throughout the process if the Coordinator does not functionally report to the DSO.

Please note that in accordance with 10.1 of the GSP, the Departmental Security Officer is to direct and coordinate the security program, which includes the BCP.

3.2 Business Impact Analysis

The coordinator and the working groups must conduct a business impact analysis to assess the impacts of disruptions on the department and to identify and prioritize critical services and associated assets. This analysis involves the following steps:

a. Determine the nature of the department's business (e.g. role, mandate) and the services it must deliver according to its constituent or other legislation, government policy, obligations to other departments, and service sharing arrangements, treaties, contracts, memoranda of understanding or other agreements. Internal and external functions on which services depend must also be identified.
b. Determine the direct and indirect impacts of disruptions on the department, including the quantitative and qualitative effects.
c. Assess services to determine which are likely to cause high degree of injury to Canadians and the government, if disrupted. It is vital to achieve immediate recovery or maintain minimum levels of service until full service is restored.
d. Identify and prioritize critical services and list the resources (personnel, contractors, suppliers, information, systems and other assets) that support them directly or indirectly, within or outside the department. Priority is assigned based on the maximum allowable downtime and the minimum service level required before high degree of injury will result. Services that must always be available, for which a disruption is not acceptable and immediate recovery is essential, are ranked at the top.
e. Obtain senior management approval of the results of the business impact analysis before proceeding with the development of continuity plans.

3.3 Business continuity plan and arrangements

Based on the results of the business impact analysis, business continuity planning activity must include:

a. Development of recovery options, from which to determine a recovery strategy for each critical service.
b. Assessment of each option in terms of possible disruption, impacts on the department, benefits, risks, feasibility, and cost in order to select the most appropriate strategy.
c. Obtaining senior management approval to support and fund selected strategies.
d. Development of business continuity plans, including IM and IT continuity plans, **identifying**:
    i. Critical services, information assets, and dependencies identified in the business impact analysis.
    ii. Approved recovery strategies.
    iii. Measures to deal with the impacts and effects of disruptions on the department.
    iv. Response and recovery teams, including the membership and contact information.
    v. Roles, responsibilities and tasks of the teams including internal and external stakeholders.
    vi. Resources and procedures for recovery.
    vii. Coordination mechanisms and procedures.
    viii. Communications strategies.
e. Obtaining senior management approval of developed plans.
f. Completion of arrangements to ensure that plans can be put into effect, and where departments share in the delivery of a critical service, arrangements to ensure that the plans of the sharing departments are concerted.
g. Briefing and training of staff.

3.4 BCP Program readiness

With continuity plans developed, approved and ready to be put into effect, a permanent maintenance cycle must be established to include:

a. Ongoing review and revision of all plans to account for any changes (legislation, critical services, organization, mandate, management, threat environment, stakeholders, dependencies, etc.).
b. Additional training as required.
c. Regular testing and validation of all plans, including the preparation of a lessons learned report after testing activities or actual events (validation can range from a questionnaire through table top exercises to departmental or interdepartmental live exercises -frequency as determined by departments).
d. Development of an audit cycle for the BCP Program, as the basis of regular reporting to the Treasury Board Secretariat.

3.5 Special Provision for the RCMP and Canadian Forces

It is recognized that the Royal Canadian Mounted Police (RCMP) and the Canadian Forces (CF), for the purpose of their business continuity planning, may include additional measures as necessary to provide for the protection of personnel and assets resulting from their legal responsibilities with respect to the protection of critical infrastructure during any emergency.

4. Enquiries

For enquiries regarding this policy instrument, please contact the Security and Identity Management Division.

For assistance on the development and maintenance of a BCP program, contact:

BCP Helpdesk
Public Safety Canada
340 Laurier Avenue West
Ottawa, Ontario K1A 0P8
Telephone: 613-949-6522
Email: BCP.Helpdesk@ps-sp.gc.ca

Public Safety Canada Website:
http://www.publicsafety.gc.ca/index-eng.aspx

Appendix 1: Glossary

Continued
can be interrupted but must be restored within an acceptable timeframe.

Continuous
must have no interruption.

Department
as defined in section 5 of the February 1, 2002 Government Security Policy.

Dependency
the reliance of a service on internal/external services, assets and resources (including individuals).

Disruption
any interruption in the continued delivery of critical services.

High degree of injury
severe harm related to the provision of sustenance (e.g., food, water, shelter, energy), public order, emergency care and response, a life-sustaining environment, vital communications and transportation, fundamental economic services, continuity of government, territorial integrity and sovereignty.

Information Management (IM) Continuity Planning
as an element of the Business Continuity Planning Program, and in accordance with the Management of Government Information Policy, is the development of plans, measures, procedures and arrangements (using BCP methodology) to ensure minimal or no interruption in the availability of information assets.

Information Technology (IT) Continuity Planning
as an element of the Business Continuity Planning Program, IT Continuity Planning is the development of plans, measures, procedures and arrangements (using the BCP methodology) to ensure minimal or no interruption to the availability of critical IT services and assets.

Maximum allowable downtime
the longest period of time for which a service can be unavailable or degraded before a high degree of injury results.

Minimum service level
the level of service delivery which is essential to avoid a high degree of injury; is maintained until full recovery is achieved.

Recovery
the restoration of full levels of service delivery.

Response
activating mechanisms to deal with a disruption.