Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada

Audit and Ethics Branch
Direction générale de la vérification et de l'éthique

Canada

2003-726

Final Audit Survey Report

Audit of IT Infrastructure Component of the Corporate Business Continuity Plans

2005-04-07

Table of Contents

1 Executive Summary

The objective of the audit is to assess the adequacy of the process that ensures the availability of the Information Technology (IT) Infrastructure component of Corporate Business Continuity Plans, and that this process provides continuous review and updating.

Overall responsibility for managing Public Works and Government Services Canada (PWGSC) Business Continuity Program rests with the Corporate Services, Human Resources and Communications (CSHRC) Branch. Individual business units develop their own Business Continuity Plans following a Business Impact Analysis / Recovery Strategy process using tools made available by the branch. Each branch should make their own arrangements for needed services.

An effective Business Continuity Planning (BCP) Program, as defined in the Government Security Policy (GSP) has five elements:
1. a governance structure establishing authorities and responsibilities for the program,
2. an impact analysis to identify and prioritize the department's critical services and assets,
3. plans, measures and arrangements to ensure continued availability of critical services,
4. activities to monitor the department's level of overall readiness; and,
5. provision for the continuous review, testing and audit of business continuity plans.

PWGSC has Business Continuity Plans (BCP) for business units, as well as a list of critical services, and a Business Continuity Response Management Plan for Place du Portage III. However, the survey has also identified the following weaknesses.

- The current list of Critical Services has not been approved by senior management;
- PWGSC has no process in place to ensure that the Critical Services list is appropriate, since there are no risk management activities tied to BCPs; and
- There is no evidence that BCPs (and their linkages) are co-ordinated to ensure integrated / effective IT Infrastructure solutions for PWGSC in support of the delivery of services to clients (since each BCP is managed independently).

We recommend that the ADM CSHRC with participation from ITSB prepare action plans to address the following*:*

1. A complete process for identifying and approving the list of critical services and their associated BCPs needs to be defined, planned and co-ordinated.

2. Linkages between the list of Critical Services, business units, and the IT Infrastructure components of BCPs required to ensure availability, needs to be established, and a risk management process be included for prioritization of these services.

2 Introduction

2.1 Authority for the Project

This audit was undertaken as part of the 2003-2004 Audit and Review Plan approved by the former Audit and Review Committee (ARC).

2.2 Objectives

The objectives of this audit are:

- to assess the adequacy of the process that is intended to ensure the availability of the Information Technology (IT) Infrastructure in support of the Corporate Business Continuity Plan; and,

- to assess this process to ensure that it provides for the continuous review and updating of the IT Infrastructure component of the Corporate Business Continuity Plan.

2.3 Scope

PWGSC uses IT in support of all of its Business Lines. Ensuring that the IT Infrastructure is available and that the resumption of services is done in a timely manner is important to minimize the business impact in the event of a major disruption.

The Corporate Business Continuity Plans (CBCP) provide for emergency response procedures, alternative communication systems and site facilities, information systems backup, disaster recovery, business impact assessments and resumption plans, procedures for restoring utility services, and maintenance and monitoring procedures for ensuring the readiness of the organization in the event of an emergency or disaster. This is part of a Business Continuity Planning (BCP) Program.

The process that ensures that the required IT Infrastructure is available, should integrate with the overall CBCP and its related Business Line requirements. The IT Infrastructure should include all the required Hardware, Software and Communications etc. to allow the operation of Business Line Applications.

The scope of this audit included the Corporate Services, Human Resources and Communications (CSHRC) Branch, and the Information Technology Services Branch (ITSB). The audit objectives will be addressed using Management Control Framework criteria, focusing on the following two elements:

Governance: All mechanisms established by senior management to lead the department in achieving organizational objectives.

Risk Management: The systems, processes, and practices used to enable the organization to identify, assess and mitigate its significant risks to support the achievement of the organization's objectives.

Some of the detailed control objectives found in the Information Systems Audit and Control Association's (ISACA), Control Objectives for Information and related Technology (COBIT) were also to be used as criteria during the detailed examination phase of this audit.

2.4 Background

The Government of Canada depends on its personnel and assets to deliver services. The Government Security Policy (GSP) and related Standards, which complements other government measures on the management of emergency situations, prescribe the application of safeguards according to baseline security requirements. It states: "Continued delivery of services must be assured through baseline security requirements, including business continuity planning, and continuous security risk management."

Business Continuity Planning (BCP) is identified in the GSP as a means of ensuring that critical services (and assets) remain available in order to assure the health, safety, security and economic well-being of Canadians, and the effective functioning of government.

Public Works and Government Services Canada, has Business Continuity Plans for business units, a list of critical services, as well as a Business Continuity Response Management Plan for Place du Portage III. The Departmental program is documented in the DP 001, the Departmental Emergency Book and the Business Continuity Planning Guide.

Increasingly, information technology (IT) is being relied upon in the provision of government services. The Information Techonolgy Services Branch (ITSB) manages IT Infrastructure that supports both PWGSC program functions as well as those of other government departments.

2.5 Work Performed

Work performed during the Survey phase included:

- reviewing relevant Treasury Board Secretariat and Departmental policies, directives and initiatives as they pertain to the Government Security Policy (GSP);

- reviewing reports and general background information from a variety of sources, including Public Safety and Emergency Preparedness (was OCIPEP), and the private sector;
- conducting interviews with representatives from the offices of primary interest in order to gain an understanding of the processes, practices, activities and directions regarding Business Continuity Planning at PWGSC;
- reviewing other documentation such as those provided by the interviewees, and
- identifying key BCP program elements implemented within PWGSC, as described in the GSP.

There were 12 people interviewed as part of this audit. They provided the audit team with information on the implementation of different aspects of Business Continuity Plans and of the specific areas of the Government Security Policy that discusses BCP requirements (section 10.14) The GSP was approved in February 2002 and lists elements of BCP Program that Departments should follow (see section 3.1 for details). The Standard which provides direction and guidance was released in the summer of 2004

3 Results of the Survey Phase

The purpose of the audit survey was to conduct an initial assessment of the process in place that supports the Corporate Business Continuity Plan. Both MCF and GSP elements were used as criteria.

3.1 The Government Security Policy (GSP)

The GSP identifies five elements for an effective Business Continuity Planning Program:

1. within the context of the departmental security program and organization (section 10.1), a governance structure establishing authorities and responsibilities for the program, and for the development and approval of business continuity plans;
2. within the context of the identification of assets (section 10.6), an impact analysis to identify and prioritize the department's critical services and assets;
3. plans, measures and arrangements to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat and risk assessment;
4. activities to monitor the department's level of overall readiness; and,
5. provision for the continuous review, testing and audit of business continuity plans.

Interviews were conducted to assess the adequacy of the process in place that would ensure the availability of the IT Infrastructure in support of BCP.

3.1.1 Governance

Overall responsibility for managing PWGSC's BCP program rests with the Corporate Services, Human Resources and Communications (CSHRC) Branch, specifically the Corporate Emergency Preparedness Directorate. General and specific responsibilities are listed in the Business Continuity Response Management Plan for Portage III.

Each business unit (of which there are 600) must develop its own BCP. Software tools are being piloted / tested to help in standardizing and updating the large volume of business impact analysis / recovery strategies and business continuity plans.

3.1.2 Impact Analysis for Critical Services

Within the BCP process, potential impacts of disruptions are examined in the Business Impact Analysis (BIA). Through this analysis, critical services are identified along with associated applications, special equipment needs, alternative space requirements, and priorities are assigned. The BCP is the vehicle wherein the business, technology and risk should come together.

There is no evidence that BIAs have been reviewed recently. The list of critical services was revisited for Y2000 and in 2002-2003, yet the list has not been formally approved. While business units have responsibility for developing and maintaining their own BCP, we did not find oversight that would ensure critical services are being supported by the IT infrastructure.

The OAG, in its 2001 chapter 12 follow up, drew attention to the need for the maintenance of this kind of information. The TBS response was to revise the GSP which requires planning for business continuity.

3.1.3 Plans and Arrangements

The Business Continuity Plans require that the necessary arrangements be made to ensure readiness in the event of a disaster. This could include, for example, ensuring the necessary arrangements with the IT sector are in place to provide alternate IT infrastructure when needed .

PWGSC business units identify their needs for specific items (i.e. personal computers) in their BCP, and should make arrangements to have these available and connected to a functioning network. Most assume that the IT infrastructure will be available, and that their plans need only identify requirements for specific items (i.e. PCs), and not arrange for them.

3.1.4 Monitoring Readiness

Although there is a list of thirty three critical services, they have not been formally approved by senior management. There are Disaster Recovery plans but they need to be coordinated with the prioritized list of critical services. It is true that the department's readiness has been tested through actual emergencies (ice storm, power outage). There are lessons learned from these events. A structured cycle of activity is suggested in which essential / critical services are first identified and prioritized, and then a process described and engaged to test, maintain, and update.

3.1.5 Continuous Review

The realignment of PWGSC necessitates a review of PWGSC's Business Continuity Response Management Plan for Portage III, and that the summary of high level critical services be updated (as per their relative priority). A Web based BCP tool, Living Disaster Recovery Planning System (LDRPS)) is being piloted, and once implemented will help in keeping plans up-to-date.

4 Conclusion

The interviews conducted as part of this audit provide sufficient evidence to conclude that the corporate responsibilities of business continuity plans need a much high level of effort to ensure the availability of the IT infrastructure that supports the list of critical services. We found that:

- Roles and responsibilities are well defined
- Best Practices were identified following previous service disruptions
- Initiatives are underway to help manage BCPs; a software product (LDRPS) has been purchased to help manage the large number of business impact analyses / recovery strategies and business continuity plans.

However, the survey has also identified the following weaknesses.

- The current list of Critical Services has not been approved by senior management;
- PWGSC has no process in place to ensure that the Critical Services list is appropriate, since there are no risk management activities tied to BCPs;
- There is no evidence that BCPs (and their linkages) are co-ordinated to ensure integrated / effective IT Infrastructure solutions for PWGSC in support of the delivery of services to clients (since each BCP is managed independently).

5 Recommendations

We recommend that the ADM of CSHRC with support from ITSB prepare action plans to address the following:

1. A complete process for identifying and approving the list of critical services and their associated BCPs, needs to be defined, planned and co-ordinated.

2. Linkages between the list of Critical Services, business units, and the IT Infrastructure components of BCPs required to ensure availability, needs to be established, and a risk management process be included for prioritization of these services.