



National
Defence

Défense
nationale

Chief Review Services Chef - Service d'examen

CRS  CS Ex

Reviewed by CRS in accordance with the *Access to Information Act (AIA)*.
Information UNCLASSIFIED

Audit of Business Continuity Planning

October 2013

7050-61 (CRS)



Canada 

Table of Contents

Acronyms and Abbreviations	i
Results in Brief.....	ii
Introduction	1
Background	1
Objective	1
Scope	2
Methodology.....	2
Statement of Conformance	2
Findings and Recommendations.....	3
Business Continuity Planning Governance	3
Business Continuity Plans.....	6
General Conclusion	9
Annex A—Management Action Plan	A-1
Annex B—Audit Criteria	B-1



Acronyms and Abbreviations

ADM(Fin CS)	Assistant Deputy Minister (Finance and Corporate Services)
ADM(HR-Civ)	Assistant Deputy Minister (Human Resources – Civilian)
BCP	Business Continuity Planning
CAF	Canadian Armed Forces
CMP	Chief of Military Personnel
CRS	Chief Review Services
DAOD	Defence Administrative Orders and Directives
DND	Department of National Defence
L0	Level 0
L1	Level 1
OPI	Office of Primary Interest
TBS	Treasury Board Secretariat
VCDS	Vice Chief of the Defence Staff



It is recommended that the Vice Chief of the Defence Staff (VCDS) develop, obtain approval for and implement a revised BCP governance structure with clearly defined roles, responsibilities and accountabilities so as to ensure the development, administration and monitoring of the BCP program.

Business Continuity Plans

In 2007, the Defence Management Oversight Committee endorsed a list of 13 critical DND/CAF operations and services. The threat risk assessment and business impact analysis used to develop business continuity plans

||||| While DND/CAF operational plans pertaining to critical operations and services may exist, |||||

It is recommend that the VCDS/Director Defence Security |||||

Note: For a more detailed list of CRS recommendations and management response, please refer to [Annex A](#)—Management Action Plan.

Introduction

Background

In accordance with the CRS Risk-Based Internal Audit Plan 2013/14 to 2015/16, CRS conducted an audit of the DND/CAF BCP program. The Policy on Government Security and the related Operational Security Standard – BCP Program require that plans be put in place to ensure that DND and CAF critical services remain available to help assure the health, safety, security and economic well-being of Canadians and the effective functioning of government.

The most recent DND/CAF Corporate Risk Profile has identified the ability of the Department to have an established defence readiness capability that can meet Government of Canada-assigned missions and tasks during a major unexpected event as one of the eight key risk areas. The absence of a robust BCP program could be considered a contributing factor when determining risk.

Established in 2007, the purpose of the DND/CAF BCP program is to provide confidence to DND employees, CAF members, stakeholders and Canadians that the DND and CAF are capable of continuing critical operations and delivering DND/CAF critical services during any disruption of domestic, continental or international activities. Departmental policy requires DND and CAF to maintain a BCP program that will integrate the fundamentals of BCP into the decision-making process related to capability development and program design, and to communicate responsibilities to ensure that the BCP roles of DND employees and CAF members are clearly defined and understood.

In 2007, the VCDS was responsible for providing leadership at the BCP program corporate level. At the same time, the Assistant Deputy Minister (Finance and Corporate Services) (ADM(Fin CS)) and the Director of Staff – Strategic Joint Staff were responsible for developing and maintaining the program, providing strategic direction, identifying critical operations, and developing a comprehensive program that regularly validates and updates the BCP process. This responsibility was subsequently transferred to Director Strategic Initiatives and Shared Support Services in 2011, and again in February 2013 to the Director Defence Security.

Objective

The objective of the audit was to assess whether the measures to ensure the continuity of critical systems and services in the event of a business disruption are in place, updated as necessary and adequately exercised.



Scope

The audit reviewed BCP documentation and processes in place since the program inception in 2007. The audit did not focus on the technical feasibility of business continuity plan implementation, nor did it examine the business continuity plans of organizations external to DND. The Information Management/Information Technology element of BCP was excluded from the scope of this audit.

Methodology

The following methodology was used by the audit team to gather information necessary to examine the audit criteria:

- reviewed TBS Policy on Government Security (2009), TBS Operational Security Standard – BCP Program (2009), TBS Directive on Departmental Security Management (2009) and DND/CAF policies and directives related to BCP;
- reviewed both Level 0 (L0) and Level 1 (L1) DND BCP documentation, Threat Risk Assessment, Business Impact Analysis, Recovery Strategies;
- reviewed DND L1 business planning and strategic planning documents such as the Reports on Plans and Priorities and the *Canada First Defence Strategy*;
- interviewed key personnel within the BCP Secretariat, along with various L1 BCP Coordinators;
- interviewed key personnel within the BCP program at Public Safety Canada; and
- observed the exercise of an L1 BCP.

Statement of Conformance

The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit thus conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program. The opinions expressed in this report are based on conditions as they existed at the time of the audit and apply only to the entity examined.



The current governance structure has not provided the BCP program with the level of oversight required to ensure ongoing development, administration and monitoring of the program. Tools such as the threat risk assessment and the business impact analysis process have not been updated since 2010. |||||

Recommendation

1. The VCDS should develop, obtain approval for and implement a revised BCP governance structure with clearly defined roles, responsibilities and accountabilities so as to ensure the development, administration and monitoring of the BCP program.

OPI: VCDS



to occur should also be documented at this stage. The results of the business impact analysis are also to be used to develop the countermeasures and mitigating strategies found in business continuity plans.

The departmental L0 business impact analysis identified 13 high-level DND/CAF critical operations under the four categories of Defence of Canada, Defence of North America, Contribute to International Peace and Security, and Continuity of Government. These 13 operations were defined as the Department’s external obligations and were assigned maximum allowable downtimes of either “no fail” (i.e., there can be no interruption) or of less than one day.

|||||

|||||

Business Continuity Plans/Recovery Strategies.

The 2009 Treasury Board Operational Security Standard – BCP Program requires that recovery/continuity strategies be developed for the critical services identified in the business impact analysis. The purpose of the departmental business continuity plan is to outline the processes and procedures to be used to respond, recover and restore DND/CAF critical services and operations to minimum levels following a traumatic event, emergency or disruption.

|||||

<p>Good Practices</p> <ul style="list-style-type: none"> • Headquarters relocation plans exist and have been reviewed and tested. • CAF Operational plans exist and can be leveraged for BCP purposes.

Rather than providing business continuity plans for identified critical operations, the current L0 BCP is a framework document used to assist L1 organizations with the development of their plans.

|||||

|||||



General Conclusion

The 2008/09 Report on Plans and Priorities stated that the establishment of a DND/CAF-wide BCP program and the development of a comprehensive departmental Business Continuity Plan were high priorities of the Deputy Minister and the Chief of the Defence Staff. At this time, roles and responsibilities were assigned to representatives within the Department and policy documents were created to elaborate on TBS guidance.

In the past six years, however, responsibility for program oversight has changed several times.

|||||

|||||

|||||



Annex A—Management Action Plan

CRS uses recommendation significance criteria as follows:

High—Controls are not in place or are inadequate. Important issues are identified that could negatively impact the achievement of program/operational objectives.

Moderate—Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations.

Low—Controls are in place but the level of compliance varies.

Business Continuity Planning Governance

CRS Recommendation (High Significance)

1. The VCDS should develop, obtain approval for and implement a revised BCP governance structure with clearly defined roles, responsibilities and accountabilities so as to ensure the development, administration and monitoring of the BCP program.

Management Action

The Security Reform Team has conducted a stem to stern review of the Department's security program, which includes the BCP program. Clear responsibilities and accountabilities approved by the Deputy Minister and the Chief of Defence Staff will be the result of this initiative.

In the interim, the Departmental Security Officer has engaged a contractor to work with the Director Defence Security BCP analyst to revise the existing program and develop a framework for the way ahead. A decision brief with the Departmental Security Officer's recommendation regarding the administration and monitoring of the BCP program will be staffed to the VCDS for approval in early January 2014.

OPI: VCDS/ Departmental Security Officer

Target Date: February 2014



Annex B—Audit Criteria

Criteria Assessment

The audit criteria were assessed using the following levels:

Assessment Level and Description

Level 1: Satisfactory

Level 2: Needs Minor Improvement

Level 3: Needs Moderate Improvement

Level 4: Needs Significant Improvement

Level 5: Unsatisfactory

Business Continuity Plans Governance

1. Governance Structure is in place to ensure the development, administration and monitoring of the BCP program.
2. Business Process are in place to monitor and amend business continuity plans based on continuous assessment of key BCP operations, activities and assets.

||||| – The established BCP governance structure has not been maintained to a level that can ensure continued development, administration and monitoring of the BCP program. The BCP program has been transferred to three different L1 organizations in the last six years, and oversight bodies |||

Business Continuity Plans

3. Key Operations, Activities and Assets have been identified based on the business impact analysis results and approved by Senior Management.
4. Business continuity plans have been developed based on results of the business impact analysis and have been appropriately approved.

|||||



Sources of Criteria

Audit criteria were based on the four core components of the BCP program as detailed in the TBS Operational Security Standard – BCP Program.

