

National Défense Defence nationale

Chief Review Services Chef - Service d'examen

CRS SCS 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)





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	
Business Continuity Plans	
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
LO	Level 0
L1	Level 1
OPI	Office of Primary Interest
TBS	Treasury Board Secretariat
VCDS	Vice Chief of the Defence Staff



Results in Brief

In 2007, the Department of National Defence (DND) established a business continuity planning (BCP) secretariat to help ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians. Ensuring that the continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies is one of the main objectives stated in the 2009 Treasury Board Secretariat (TBS) Policy on Government Security. The Department provides numerous critical services in fulfilling its mission of defending Canada and

Overall Assessment

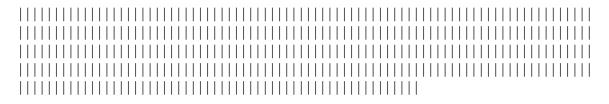
Canadian interests and values while contributing to international peace and security. A business continuity plan that identifies the links between assets, human and financial resources and critical services and/or deliverables reduces the risk of not being able to provide these critical services when a disruption occurs.

As detailed in the Chief Review Services (CRS) Risk-Based Internal Audit Plan 2013/14 to 2015/16, CRS conducted an audit of the DND/Canadian Armed Forces (CAF) BCP program. 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.

Findings and Recommendations

BCP Governance

The Deputy Minister/Chief of the Defence Staff BCP Initiating Directive (2007) and the follow-up Defence Administrative Orders and Directives (DAOD) 1003-0/1003-1 (2009) established a DND/CAF BCP program consistent with the TBS's Operational Security Standard. BCP departmental coordinator responsibilities were assigned to representatives within the Department. Program oversight bodies such as the National Defence Headquarters Coordination Committee, the BCP Action Team, and the BCP Action Team Working Group were also formed, and a BCP review process was developed.





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

Note: For a more detailed list of CRS recommendations and management response, please refer to <u>Annex A</u>—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.



Findings and Recommendations

Business Continuity Planning Governance

As reflected in the June 2007 draft departmental business impact analysis, "to be effective, the BCP development process first requires the establishment of governance that identifies the program policy, executive leadership commitment, integration of the program into the departmental strategic planning framework, expert review and the appointment of a team to chair the development throughout the organization."

Good Practice

Initial 2007 BCP program governance structure had established roles, responsibilities and oversight mechanisms.

Program Oversight. In developing BCP program governance, departmental policy requires the National Defence Headquarters Coordination Committee to act as a steering committee for a BCP Action Team and assist the program with respect to defining roles and responsibilities and ensuring the development and monitoring of business continuity plans.

A BCP Action Team	was established;	;	

Policy. The requirement to implement BCP is outlined in the 2009 Treasury Board Secretariat Policy on Government Security, and is supplemented by the Treasury Board Secretariat Operational Security Standard dealing with BCP. Within DND, BCP guidance was further developed with the issuance of DAOD 1003-0 and DAOD 1003-1 in 2009.

Many of these policy references are now out of date. The DAODs do not reflect the changes in the roles and responsibilities brought about by the recent organizational move of the BCP program to the Director Defence Security. Additional guidance documents pertaining to BCP change management, readiness, testing and exercising were also developed, but are in draft and have not been implemented.



Program Development/Maintenance. The 2009 Treasury Board Secretariat Operational Security Standard on BCP program development requires departments to establish a maintenance cycle consisting of activities such as ongoing review and revision, regular testing and plan validation. Business continuity plans must be maintained so that they remain useful in the event of a disruption so as to ensure the effective recovery of critical operations.

Training. The departmental BCP DAOD 1003-1 assigns BCP training responsibilities to four organizations. Chief of Military Personnel (CMP) and Assistant Deputy Minister (Human Resources – Civilian) (ADM(HR-Civ)) are responsible for conducting BCP specialty training, while Director of Staff – Strategic Joint Staff and Director General Corporate and Shared Services/Director Strategic Initiatives and Shared Support Services are responsible for providing regular training. BCP Secretariat staff indicated that it was difficult to ascertain exactly what training each organization should provide, and that they were not aware of any BCP training provided by CMP or ADM(HR-Civ); no evidence was found to the contrary.

Yet, the BCP Secretariat has provided training to stakeholders such as the BCP action team and the L1 BCP coordinators. In 2009, training was provided to L1 coordinators and representatives at seven locations, and Director Defence Security staff has indicated that they plan to offer similar training in the near future. BCP awareness and training has also been incorporated into the annual Security Awareness Week activities.



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



Business Continuity Plans



The objective of a BCP program as stated in the Policy on Government Security is to develop plans, procedures and arrangements that will ensure minimal or no interruptions to the availability of critical services and assets. The BCP Secretariat developed an eight-step methodology to guide the DND/CAF BCP process. Key activities include the establishment of a departmental BCP governance framework, identification of threats and risks, identification of critical operations and assets, preparation of business continuity plans, and the testing and refinement of the plans.

In order to develop a high-quality business continuity plan, it is important to properly execute each step of the methodology. Performing a detailed threat risk assessment and business impact analysis (two of the initial steps in the methodology) are crucial in the development of a sound business continuity plan.

Threat and Risk Assessment. The purpose of a threat risk assessment is to identify and assess threat agents and risks that could adversely affect the Department and its people, assets and facilities. Conducting a threat risk assessment can provide information to assist in the identification of critical assets and for the design of plans to detect and deter threats and reduce vulnerability to potential incidents.

The 2009 Treasury Board Secretariat Policy on Government Security states that departments are responsible for ensuring that periodic reviews are conducted to assess whether the Departmental Security Program (which encompasses BCP) is effective. BCP program readiness guidance detailed in the 2009 Treasury Board Operational Security Standard – BCP Program also requires that a maintenance lifecycle be established to ensure that any changes in such areas as the threat environment, legislation and stakeholders be maintained. https://www.uc.environment.com and stakeholders be maintained.

Business Impact Analysis. The business impact analysis involves assessing the impact of the threats and risks identified in the threat risk assessment by identifying and prioritizing the critical services and resources that support effected activities and then determining the associated maximum allowable downtimes and the minimal service levels for each activity. Any interdependencies that exist in order for the critical service

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.

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,

Good Practices

- Headquarters relocation plans exist and have been reviewed and tested.
- CAF Operational plans exist and can be leveraged for BCP purposes.



Although this is in line with the DAOD 1003-1 requirement to complete a review of DND and CAF governance structures to ensure clear lines of authority, succession of command and corporate leadership, and alternate headquarters and office are in place, |||

Image: Second Second

development of required business continuity plans and thus save the organization significant effort in the development of departmental business continuity plans.

Recommendation

- 2. The VCDS should:



General Conclusion

The 2008/09 Report on Plans and Priorities stated that the establishment of a DND/CAFwide 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.



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 A

Business Continuity Plans

CRS Recommendation (High Significance)

2. The VCDS should:

a.	
b.	

Management Action

The requirement for a proper threat risk assessment along with the responsibility of conducting threat risk assessments also form part of the Security Reform Team's observations and recommendations.

In its renewal of the BCP program, the Director Defence Security will develop a threat risk assessment template and engage key internal partners to conduct a proper business impact analysis. Furthermore, the BCP template/requirements and the reports and returns to the Departmental Security Officer will also be developed. All of these components will be clearly articulated in the National Defence Security Orders currently being drafted.

OPI: VCDS/ Departmental Security Officer **Target Date:** April 2014 (to coincide with the new DND Security Orders)



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.

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.



Annex B

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.

