Public Safety Canada Sécurité publique Canada

Public Safety Canada

Audit of the Business Continuity Planning Program

October 2016

Canada

Cat: PS4-208/2016E-PDF
ISBN: 978-0-660-06766-7

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

A business continuity planning program is an integrated management process addressing the development and implementation of activities that ensure the continuity and recovery of critical services and operations during security incidents, disruptions and emergencies. The implementation of such a program supports the Minister in respect to obligations for overall security in accordance with relevant legislation and the 2009 Treasury Board's *Policy on Government Security*[1].

According to the 2004 Treasury Board (TB) *Operational Security Standards*[2], a business continuity planning program is comprised of the following components:

1. The establishment of a business continuity planning program governance;
2. The conduct of a Business Impact Analysis (BIA);
3. The development of business continuity plans (BCP) and arrangements; and
4. The maintenance of business continuity planning program readiness.

The audit team took into consideration various changes related to business continuity that occurred during the conduct of this assurance engagement. These included the TB policy reset and the Public Safety (PS) business continuity planning program renewal. More specifically, consultations on a new TB *Policy on Government Security* were underway with a draft copy of the proposed policy available to departments. While this draft policy is not yet finalized, PS has begun to update its internal security policies and procedures to align them with the proposed changes.

The PS 2011 BIA identified one critical service for the Department, namely the management of the integrated federal response to emergencies provided by the Government Operations Centre (GOC). To address this critical service, PS developed the 2013 BCP for the GOC that currently serves as the departmental business continuity plan. Under the business continuity planning program renewal initiative, PS is in the process of developing a new BCP based on a BIA updated in 2015. The new 2016 BCP is scheduled to be presented to management for approval in the fall of 2016.

The audit of the business continuity planning program was included in the Risk-based Audit Plan of the Department approved by the Deputy Minister for the period 2014-15 to 2016-17.

[1] Treasury Board, *Policy on Government Security*, 2012.

[2] Treasury Board, *Operational Security Standard – Business Continuity Planning (BCP) Program*, 2004.

Audit Objective and Scope

The objective of this audit was to assess that the Department has established an internal business continuity planning program that ensures the continued availability of its critical services and related assets.

The scope of the audit included an examination of the Department's business continuity planning program governance and risk management arrangements as well as the adequacy of the continuity plans. This included the BCPs for the GOC and the Canadian Cyber Incident Response Centre and related supporting documents as of March 2016.

The audit scope excluded the Department's emergency management plans, response frameworks and protocols in place to lead, inform, facilitate and coordinate an integrated federal response to a threat or emergency.

Summary of Findings

The *Emergency Management Act* confirms the emergency management responsibilities of each Minister in preparing, maintaining and testing emergency management plans in accordance with policies, programs and other measures set at the departmental level. We found that the Department is in a transitional period to implement the 2015 *Departmental Continuity Management Policy* by developing an appropriate BCP. While progress has been achieved as evidenced by the development of the 2016 Critical Services Framework and the streamlining of the Critical Services Inventory, the Department currently remains at risk of being unable to restore successfully and on a timely basis the 30 critical services until the 2016 BCP has been finalized and operationally tested.

Business Continuity Planning Program

PS is operating under a BCP that was approved in 2013 which lists the GOC as the department's only critical service. The BCP has not been updated to reflect changes to critical services since 2013. Therefore, it may not be able to support a timely recovery and /or continuity of the 30 current critical services identified in the Critical Services Inventory. Communication exercises were conducted in 2011 and 2015. The 2013 BCP, however, has not been operationally tested to ensure readiness.

The Department is undertaking a review of the business continuity planning process under the guidance of the Departmental Security Officer (DSO). In October 2015, the DSO developed a road map, which was approved by the Departmental Management Committee.

Based on the information available at the time of the audit, the Chief Information Officer has indicated that the current level of IT resources and the absence of formal agreements with suppliers of critical IT services may hinder the implementation of the 2013 BCP were it to be activated.

Business Continuity Planning Program Roles, Responsibilities and Processes

The Department has implemented the 2015 *Departmental Continuity Management Policy*[3]. However, the policy does not include the DSO's responsibilities in the event of a reported incident, as well as reference to other departmental guidance documents such as the Activation and Response Protocol. It also has not identified operating procedures that clearly delineate the process and control mechanisms to rate its success.

Audit Opinion

Improvements are required[4] to the business continuity planning program to ensure that the Department has a comprehensive process and a robust BCP to support the effective recovery of all critical services.

Statement of Conformance and Assurance

Sufficient and appropriate audit procedures were conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined and within the scope described herein. The evidence was gathered in compliance with the Treasury Board Policy and Directive on Internal Audit. The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program. The procedures used meet the professional standards of the Institute of Internal Auditors. The evidence gathered is sufficient to provide Senior Management with proof of the opinion derived from the internal audit.

Recommendations

1. The Assistant Deputy Minister, Corporate Management Branch, should ensure that:
    - the Departmental Continuity Management Plan (CMP)[5] presented for approval in 2016 addresses the 30 critical services of the Department identified in the 2016 Critical Services Inventory and is supported by an appropriate recovery and/or continuity strategy; and
    - the CMP is tested on a regular basis to achieve and maintain high levels of competence and readiness.
2. The Assistant Deputy Minister, Corporate Management Branch should ensure that:
    - formal arrangements are in place to support accessibility to the IT services needed when the CMP is activated; and

[3] *Departmental Continuity Management Policy* – October 2015

[4] Audit opinion assessment scale can be found in Annex C.

[5] The 2016 Business Continuity Plan is now referred to as the Continuity Management Plan, which complies with the 2015 Departmental Continuity Management Policy.

- the Disaster Recovery Plans address the recovery strategy for all the IT services deemed necessary to support continuity and/or recovery process of critical services identified in the CMP.

3. The Assistant Deputy Minister, Corporate Management Branch, should ensure that:
   - the roles and responsibilities, procedures and policies for the business continuity planning program align and provide clear direction for the successful delivery of the program.

Management Response

Management accepts the recommendations of Internal Audit.

The key actions to be taken by management to address the findings and recommendations and the associated timelines can be found in the "Management Response and Action Plan" section of the report.

CAEE Signature

____

Audit Team Members

Denis Gorman, Chief Audit and Evaluation Executive
Gabrielle Duschner, Director Internal Audit and Evaluation
Sonja Mitrovic, Internal Audit Project Leader
Sophie Carrier, Senior Auditor
Spearhead Management Canada Ltd, consultants

Acknowledgements

Internal Audit would like to thank all those who provided advice and assistance during the audit.

1 INTRODUCTION

1.1 Background

The business continuity program integrates management processes that address the continuity and recovery of critical services during incidents, disruptions and emergencies. The program supports the Minister in respect to obligations for overall security in accordance with relevant legislation and Treasury Board's *Policy on Government Security*[6].

According to the 2004 Treasury Board (TB) *Operational Security Standards*[7], a business continuity planning program comprises the following components:

1. Program governance;
2. Business Impact Analysis (BIA);
3. Business Continuity Plans (BCP) and arrangements; and
4. Program readiness.

The audit team took into consideration various changes related to business continuity that occurred during the conduct of this assurance engagement. These include the TB policy reset and the Public Safety (PS) business continuity planning program renewal. More specifically, consultations on a new TB *Policy on Government Security* were underway with a draft copy of the proposed policy available to departments. Although the policy is not yet finalized, PS has begun to update its internal security policies and procedures to align them with the proposed changes.

The PS 2011 BIA identified one critical service for the Department, namely the management of the integrated federal response to emergencies provided by the Government Operations Centre (GOC). The 2013 BCP addresses this critical service. PS is in the process of developing a new BCP based on the 2015 BIA. The new BCP is scheduled to be presented to management for approval in the fall 2016.

The audit of the business continuity planning program was included in the Risk-based Audit Plan of the Department approved by the Deputy Minister for the period 2014-15 to 2016-17.

1.2 Audit Objective

The objective of this audit assessed that the Department has established an internal business continuity planning program that ensures the continued availability of its critical services and related assets.

[6] Treasury Board, *Policy on Government Security*, 2012.
[7] Treasury Board, *Operational Security Standard – Business Continuity Planning (BCP) Program*, 2004.

1.3 Scope of audit

The scope of the audit included an examination of the Department's business continuity planning program governance and risk management arrangements as well as the adequacy of the continuity plans. This included the BCPs for the GOC and the Canadian Cyber Incident Response Centre and related supporting documents as of March 2016.

The audit scope excluded the Department's emergency management plans, response frameworks and protocols in place to lead, inform, facilitate and coordinate an integrated federal response to a threat or emergency.

1.4 Risk Assessment

The assessment conducted during the planning phase, has identified risks in the following areas:

- Governance
- Assessment of the critical services
- Development of the business continuity plan

The detailed inherent risks are available in Annex A. The audit scope and criteria were established based on these risks (see Annex B).

1.5 Audit Opinion

Improvements are required[8] to the business continuity planning program to ensure that the Department has a comprehensive business continuity process and a robust BCP to support the effective recovery of all critical services.

1.6 Statement of Conformance and Assurance

Sufficient and appropriate audit procedures were conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined and within the scope described herein. The evidence was gathered in compliance with the Treasury Board Policy and Directive on Internal Audit. The audit conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program. The procedures used meet the professional standards of the Institute of Internal Auditors. The evidence gathered is sufficient to provide Senior Management with proof of the opinion derived from the internal audit.

[8] Audit opinion assessment scale can be found in Annex C.

2 FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

2.1 Business Continuity Planning Program

We expected to find:

- A Business Impact Analysis (BIA) that includes the identification and the prioritization of critical services and associated assets;
- A Business Continuity Plan (BCP), with IM/IT recovery plans for the critical services; the approved recovery strategies; the response and recovery teams and their roles, responsibilities and tasks; the resources, procedures and coordination mechanisms for recovery; and the communications strategies; and
- A program readiness that defines a permanent maintenance cycle established to include an ongoing review and revision, additional training, and regular testing.

The 2013 Business Continuity Plan was neither operationally tested nor was it updated to reflect the 2015 assessment of the Department's critical services.

Business Impact Analysis and Business Continuity Plan

In 2013, the Department developed and approved a BCP based on the 2011 BIA. This BIA only identified the management of the federal response to emergencies provided by the GOC as a critical service. There is no BCP for the Canadian Cyber Incident Response Centre.

Last year, PS conducted a review of the 2011 BIA, which identified 174 critical services, which was re-visited three times (February, May and December 2015) thereby reducing the number to 37 critical services. Notwithstanding this reduction, the Chief Information Officer (CIO) has indicated that the Department does not have sufficient dedicated IT resources to support the continuity and/or recovery of 37 critical services on a timely basis. Furthermore, the majority of supporting IM/IT services are provided by Shared Services Canada (SSC), Industry Canada and the RCMP. With the exception of the recovery agreement signed with SSC to support the GOC's operations centre interconnectivity portal, PS has not secured any other formal arrangements with these service providers that would ensure availability of IT services needed to support the critical services identified in the 2013 BCP.

In 2015, the Department assessed the following IT applications as critical to the continuity and/or recovery process: CTSN, CCM Mercury, Dragon, RDIMS, News Desk and the PS website for public sharing of information. Although an IT Disaster Recovery Plan (DRP) was not developed for these departmental applications, we found that Disaster Recovery Procedures were established for News Desk and RDIMS. As a result, PS is at risk of being unable to access the IT services necessary to support the BCP should the non-supported applications fail during an emergency. It is important to note that PS must obtain IT services to support critical services exclusively through SSC and are not permitted to meet IT requirement for that service internally[9].

[9] Shared Services Canada Act, S.C. 2012, c. 19, s. 711, Section 6 (c)

To confirm the departmental critical services, the DSO analyzed the 2015 BIA against the 2016 Critical Services Framework to produce a new Critical Services Inventory (CSI) listing 30 departmental critical services. The DSO is currently drafting the 2016 BCP to address this inventory, which has precluded the need to update the 2013 BCP. The new BCP is scheduled to be presented to senior management in the fall of 2016.

Program Readiness

The TB *Operational Security Standard* requires a permanent maintenance cycle that includes:

- Ongoing review and revision of all plans to account for any changes (legislation, critical services, organization, mandate, management, threat environment, stakeholders, dependencies, etc.);
- Additional training as required; and
- 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 tabletop exercises to departmental or interdepartmental live exercises -frequency as determined by departments).

We found that the 2013 BCP has not been operationally tested to ensure continuity of services during an incident. Two exercises were conducted ("Triangle effect" in 2011 and "Keep abreast of situations (KAOS) in 2015), which focused on communication lines upon activation of the BCP. The Department has not fully addressed the recommendations stemming from these exercises. For example, the KAOS report identified issues related to information technology including the unavailability of networks, reduced functionality of MobiKey devices, slow connectivity and the need for portable equipment, all of which will have an impact on the successful implementation of the BCP when activated. Nevertheless, we acknowledge that the DSO is working on enhancing and updating the business continuity planning program that includes the 2015 *Departmental Continuity Management Policy (DCM)*[10] and Activation and Response Protocol, as well as the 2017-20 Departmental Exercise Strategy and the 2016-2017 Interim Departmental Exercise Plan.

Until the 2016 BCP is finalized, there is a risk that the 30 critical services cannot be recovered on a timely basis. This may hinder the Department in achieving its objectives in the event of an emergency.

Recommendations:

1. The Assistant Deputy Minister, Corporate Management Branch, should ensure that:
   - the Departmental Continuity Management Plan (CMP)[11] presented for approval in 2016 addresses the 30 critical services of the Department identified in the 2016 Critical

[10] PS, *Departmental Continuity Management Policy* – October 2015

[11] The 2016 Business Continuity Plan is now referred to as the Continuity Management Plan, which complies with the 2015 Departmental Continuity Management Policy.

Services Inventory and is supported by an appropriate recovery and/or continuity strategy; and
- the CMP is tested on a regular basis to achieve and maintain high levels of competence and readiness.

2. The Assistant Deputy Minister, Corporate Management Branch should ensure that:
- formal arrangements are in place to support accessibility to the IT services needed when the CMP is activated; and
- the Disaster Recovery Plans address the recovery strategy for all the IT services deemed necessary to support continuity and/or recovery process of critical services identified in the CMP.

2.2 Business Continuity Planning Program Roles, Responsibilities and Processes

A program governance structure includes the appointment of a DSO and clearly defined roles and responsibilities pertaining to business continuity.

The business continuity planning program roles, responsibilities, and processes are not clearly aligned.

In January 2011, PS implemented the *Public Safety Canada Security Policy* [12] as a replacement to the 2006 version. Section 2.2 of the Policy states that the ADM of Corporate Management Branch has the authority to develop and/or amend directives that support the policy in the following subject areas: 1. Identity management; 2. IT security; and 3. Business Continuity Planning.

Corporate Management Branch has revised the 2008 *Business Continuity Planning Policy and Program Guide*[13] and replaced it with the DCM Policy that aligns with the upcoming TB *Government Security Policy*. The Departmental Management Committee approved the DCM Policy on October 13, 2015. It identifies the roles and responsibilities of stakeholders involved in supporting the continuity and the recovery of critical services within an acceptable timeframe during and after an emergency.

We found that the roles and responsibilities are defined and documented in the 2015 DCM Policy, the Activation and Response Protocol, and job descriptions. More specifically:
- the DCM Policy lists the business continuity roles and responsibilities for stakeholders supporting the continuity of critical services;
- the appointment of a business continuity planning coordinator and the responsibility for the development of the BCP are identified in the job description of the Departmental Emergency Management Services Manager; and
- the DSO responsibility for incident management is explained in the PS Activation and Response Protocol.

[12] Public Safety Canada Security Policy – January 2011

[13] Business Continuity Planning Policy and Program Guide – July 2008

However, the comprehensive list of business continuity roles and responsibilities is not easily accessible because these key documents are not available in a centralized repository and are not linked.

The DSO is revising and updating the procedures for business continuity. Contributing to the development of the 2016 BCP, the DSO has also developed a three-year continuity management awareness and exercise strategy, and has reviewed the continuity management planning tools and templates.

Until the new BCP and Continuity Management guidelines are completed, the lack of business continuity procedures and the centralized comprehensive list of roles and responsibilities may prevent the Department from successfully responding to an emergency and ensuring timely recovery and/or continuity of services.

Recommendation:

3. The Assistant Deputy Minister, Corporate Management Branch, should ensure that:

- the roles and responsibilities, procedures and policies for the business continuity planning program align and provide clear direction for the successful delivery of the program.

2.3 Overall Conclusion

The Department is in a transitional period while it develops an appropriate BCP. Progress has been achieved by developing the 2016 Critical Services Framework and streamlining the Critical Services Inventory. Nevertheless, the Department is at risk of being unable to restore the 30 critical services within described timelines until the 2016 BCP has been finalized and operationally tested.

2.4 Management Response and Action Plan

Actions Planned	Target Completion Date
Recommendation #1: The Assistant Deputy Minister, Corporate Management Branch, should ensure that: • the Departmental Continuity Management Plan (CMP)[14] presented for approval in 2016 addresses the 30 critical services of the Department identified in the 2016 Critical Services Inventory and is supported by an appropriate recovery and/or continuity strategy; and • the CMP is tested on a regular basis to achieve and maintain high levels of competence and readiness.	
The 2016 PS Continuity Management Plan (CMP) addresses all 30 PS critical services and identifies recovery/continuity strategies for each critical service.	October 31, 2016
The 2016 Continuity Management Plan is tested through senior management tabletop.	June 30, 2017
A 2017-2020 exercise strategy is developed as part of the next iteration of the Departmental Security Plan.	May 31, 2017
Recommendation #2: The Assistant Deputy Minister, Corporate Management Branch should ensure that: • formal arrangements are in place to support accessibility to the IT services needed when the CMP is activated; and • the Disaster Recovery Plans address the recovery strategy for all the IT services deemed necessary to support continuity and/or recovery process of critical services identified in the CMP.	
Confirm IT Disaster Recovery requirement for all PS critical services.	March 31, 2017
Determine existing levels of recovery for critical systems and applications with internal and Government of Canada partners, and identify gaps and mitigation options, including cost of establishing required recovery level or mitigation.	March 31, 2018*
Determine recovery plan and procedures for all critical systems and applications.	March 31, 2019*

*confirmation of recovery capabilities, mitigation options and establishment of arrangements is dependent on partners (SSC, central agencies, and other providers).

[14] The 2016 Business Continuity Plan is now referred to as the Continuity Management Plan, which complies with the 2015 Departmental Continuity Management Policy.

Recommendation #3: The Assistant Deputy Minister, Corporate Management Branch, should ensure that: • the roles and responsibilities, procedures and policies for the business continuity planning program align and provide clear direction for the successful delivery of the program.	
PS Continuity Management Policy is updated to include reference to other relevant PS security policy instruments.	Completed
Supporting policy instruments are developed to support all steps of the planning process laid out in the Policy. PS Security policy suite includes: • Continuity Management Planning Procedures • Critical Services Identification Guidelines • Critical Services Mapping Guidelines • Continuity Management Plan Development Guidelines • Readiness Exercise and Disaster Simulation Guide • Guidelines for internal communications during emergencies	March 31, 2020

ANNEX A: PRELIMINARY AUDIT RISKS

The following is a summary of the key risks identified during the planning phase.

Key Area	Risk Statement
Governance	The BCP Program may not comply with policies, regulations and government standards.
Assessment of critical services	PS critical services may not be defined.
	PS critical services dependencies may not be identified for all services.
	The Business Impact Analysis may be incomplete.
Development of the Business Continuity Plan	BCP developed by PS may be incomplete, untested and not maintained properly.
	PS may not recover on a timely basis from major incidents.

ANNEX B: AUDIT CRITERIA

Audit Criteria	
Criterion 1:	A governance framework is in place that is integrated with the Federal Emergency Response Plan and includes approved descriptions of roles, responsibilities, policies, oversight committees and resources.
Criterion 2:	A BIA exists that clearly identifies critical business services integral to keeping the business functioning during an incident and to determine the recovery requirements and priority of the critical services to be recovered.
Criterion 3:	Business continuity and recovery strategies have been identified, assessed, selected and approved, and BCPs are consistent with policy, government standards and guidelines.
Criterion 4:	BCPs are subject to testing and validation, which includes the preparation of lessons learned reports and the updating of BCPs after testing activities or actual events to reflect lessons learned and to account for changes to the Department and its operating environment.

ANNEX C: INTERNAL AUDIT AND EVALUATION DIRECTORATE OPINION SCALE

The following is the Internal Audit and Evaluation Directorate audit opinion scale by which the significance of the audit collective findings and conclusions are assessed.

Audit Opinion Ranking	Definition
Well Controlled	• Well managed, no material weaknesses noted; and • Effective
Minor Improvement	• Well managed, but minor improvements are needed; and • Effective
Improvements Required	Improvements are required (at least one of the following two criteria are met): • control weaknesses, but exposure is limited because likelihood of the risk occurring is not high; • control weaknesses, but exposure is limited because impact of the risk is not high;
Significant Improvements Required	Significant improvements are required (at least one of the following two criteria are met): • Financial adjustments material to line item or area or to the Department; • Control deficiencies represent serious exposure; • Major deficiencies in overall control structure;