Veterans Affairs Canada
Anciens Combattants Canada

July 2014

AUDIT OF BUSINESS CONTINUITY PLANNING

Audit and Evaluation Division

Canada

Acknowledgements

The audit team would like to gratefully acknowledge Veterans Affairs staff whose contributions were essential to the completion of this audit.

TABLE OF CONTENTS

EXECUTIVE SUMMARY i

1.0 BACKGROUND 1

2.0 ABOUT THE AUDIT 1

2.1 Scope and Objectives 1
2.2 Methodology 1

3.0 AUDIT RESULTS 2

3.1 Governance 2
3.2 Business Impact Analysis 3
3.3 Business Continuity Plans 3
3.4 Maintenance 4
3.5 Audit Opinion 5

APPENDIX A - AUDIT CRITERIA

APPENDIX B - RISK RANKING OF RECOMMENDATIONS AND AUDIT OPINION

EXECUTIVE SUMMARY

Business Continuity Planning (BCP) involves the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets. Business continuity plans outline the strategies, resources, and procedures required to restore critical services to the public, as quickly and effectively as possible.

The objective of this audit was to assess Veterans Affairs Canada's compliance with Treasury Board requirements for BCP. The scope covered the status of BCP within the Department as at December 31, 2013.

The audit team observed that a BCP process had been fully established at Veterans Affairs Canada. Audit results confirmed that the Department was complying with key requirements, although there is a need to update the departmental BCP policy and ensure that a business continuity plan is developed specifically for information technology. Overall, the audit team determined the results to be "*Generally Acceptable"*.

Chief Audit Executive's Signature

_____ _____

Kim Andrews Date
A/Chief Audit Executive

1.0 BACKGROUND

Business Continuity Planning (BCP) involves the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets. Business continuity plans outline the strategies, resources, and procedures required to restore critical services to the public as quickly and effectively as possible.

Disruptions caused by power failures, flooding or hurricanes require effective BCP. Veterans Affairs Canada (VAC) events that have required the implementation of a BCP included a temporary relocation of the Kingston District Office, forest fires in Kirkland Lake and flooding in Calgary. In these cases, business continuity plans were utilized to support staff in maintaining service delivery to Veterans.

The Treasury Board (TB) *Policy on Government Security* and the *Operational Security Standard – Business Continuity Planning Program* establish the requirements for business continuity planning for the Government of Canada. Section 3 of this Standard states that BCP is composed of the following four elements:

- The establishment of BCP Program governance;
- The conduct of a business impact analysis;
- The development of business continuity plans and arrangements; and
- The maintenance of BCP Program readiness.

2.0 ABOUT THE AUDIT

2.1 Scope and Objectives

The scope of the audit covered the status of BCP as at December 31, 2013. Ste. Anne's Hospital was excluded from the scope of this audit due to its pending transfer to the province of Quebec.

The objective of the audit was to assess overall compliance with TB requirements, including governance, risk assessment, planning and maintenance. The audit criteria are provided in Appendix A.

2.2 Methodology

This audit was conducted in conformance with the Internal Audit standards as outlined by the Institute for Internal Auditors, and is in line with the Internal Audit Policy for the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program.

Interviews were conducted with employees in head and area offices to determine employees' understanding of their roles and responsibilities, VAC's BCP policy and

procedures, as well as to assess VAC's BCP governance framework.

A documentation review was conducted of TB policy and TBS guidance as well as VAC's policy relating to BCP. The purpose of this review was to identify the requirements and assess the alignment of VAC policy with TBS guidance. Additionally, VAC's business continuity plans and related reports were reviewed to assess the governance structure, and compliance with the requirements.

3.0 AUDIT RESULTS

BCP is composed of the following four elements:

- The establishment of BCP Program governance;
- The conduct of a business impact analysis (BIA);
- The development of business continuity plans and arrangements; and
- The maintenance of BCP Program readiness.

3.1 Governance

Overall, the audit team observed that roles, responsibilities, and performance standards had been clearly defined and communicated. The Director of Administrative Services, who reports to the Director General (DG) of Information Technology, Information Management and Administration, is responsible for BCP and has a BCP coordinator who is responsible for obtaining senior management support and funding, developing a departmental BCP Program policy, supporting staff in the preparation of business impact analyses (BIA) and action plans, as well as for reviewing and testing these plans.

The Department's BCP Policy (dated 2008) was aligned with TB Policy. The TB Policy requires that departmental policy be formally reviewed every two years by departmental senior managers. A revised departmental policy with new requirements was drafted in November 2011; however, this draft was never approved by senior management nor was it implemented. This draft policy included the intent to establish an Emergency Operations Centre which, in the event of a major disruption, would be responsible for leading the coordination of VAC's response and ensuring that staff with BCP training are immediately engaged. In March 2014, a Strategic Emergency Management Plan was approved by the Deputy Minister. This plan included the establishment of an Emergency Operations Centre.

Annually, the BCP coordinator reviews individual work units business continuity plans. These reviews help to ensure their accuracy and completeness. Based on this review, a report card is produced to identify areas requiring further action. This report card was submitted annually to the Information Technology, Information Management and Administration Division; however, this information was not formally shared with other senior managers nor was there evidence that action items were completed.

R1 It is recommended that the Director General, Information Technology, Information Management and Administration Division, updates the departmental Business Continuity Planning policy and obtains senior management approval. (Essential)

Management Response

Management agrees with the recommendation. Work has been completed to update the Business Continuity Planning policy.

R2 It is recommended that the Director General, Information Technology, Information Management and Administration Division, annually presents the Business Continuity Planning report card to senior management and follows up on any action required. (Essential)

Management Response

Management agrees with this recommendation. The annual Business Continuity Planning report card has been updated and was presented to the Senior Management Committee.

3.2 Business Impact Analysis

The BIA process identifies the resources necessary to continue the delivery of essential programs and services. It is designed to identify risks associated with functions which are essential to the operations of the Department. An effective BIA also identifies the resources necessary to manage these risks.

Departments are required to annually conduct a BIA to assess the impacts of disruptions and to identify and prioritize critical services and associated assets. Annually, VAC utilized a questionnaire which was sent to each work unit that required a BCP Plan. The most recent questionnaire was sent to each work unit in 2012. The BCP coordinator then reviewed these BIAs to ensure their accuracy and completeness as well as to ensure alignment with the business continuity plans.

3.3 Business Continuity Plans

Business continuity plans describe in detail how each work unit would manage a disruption in an orderly manner. TB policy requires periodic updating of business continuity plans. VAC business continuity plans were updated annually to reflect any changes in operations with the exception of 2013 because VAC was in the process of streamlining its BIA and business continuity plan formats. This streamlining exercise was still in progress at the completion of the audit fieldwork.

The audit team reviewed the most current version of the business continuity plan for each work unit and confirmed that all, except one work unit which was missing a BIA, contained the critical components.

The audit team noted that 36% (26/73) of the business continuity plans required updating. In most cases, the “call trees” were not up-to-date or did not contain sufficient contact information to be effective. Although a business continuity plan can be utilized without an up-to-date “call tree”, the “call tree” supports effective communication with staff. This observation was discussed during briefings with management and will be addressed as part of the 2015 business continuity plan review process.

Information Technology (IT) is critical to maintaining services and the *Operational Security Standard – Business Continuity Planning Program* requires that Information Technology continuity plans be fully integrated into the BCP Program. The audit team noted that IT restoration was part of each individual plan, but an overall plan covering major disruptions to VAC’s systems or servers was missing. Shared Services Canada is now responsible for VAC’s IT infrastructure. It was noted that Shared Services Canada had a plan for managing disruptions. However, at the time of the audit, there was no formal business continuity plan in place between the two organizations.

R3 It is recommended that the Director General, Information Technology, Information Management and Administration Division, works with Shared Services Canada to establish Information Technology business continuity plans. (Essential)

Management Response

Management agrees. Work is underway to establish a formal business continuity plan with Shared Services Canada by December 2014. A major component of the business continuity plan will include a BCP test of the Client Service Delivery Network (CSDN) system to ensure that the plan is effective.

3.4 Maintenance

Maintenance is a key requirement of the BCP process. The TB Standard requires ongoing reviews, continual training, periodic testing and regular reporting. The audit team confirmed that these components had been established. For example, business continuity plans are periodically tested using a variety of case scenarios developed by the BCP coordinator. This periodic testing ensures that the business continuity plans are complete and creates a learning opportunity for local managers. One noted gap was that an incident report, although required, had not been developed for the previous three incidents. Incident reports help provide lessons learned which can be used to better manage future disruptions.

R4 It is recommended that the Director of Administrative Services ensures that an incident report is prepared and submitted to the Emergency Operations Centre whenever a business continuity plan is implemented. (Essential)

Management Response

Management agrees with this recommendation. A new incident report template has been develop and an incident report will be submitted to the Emergency Operations Centre whenever an incident occurs and a BCP plan is implemented.

3.5 Audit Opinion

The audit team observed that a Business Continuity Planning process had been fully established at Veterans Affairs Canada. Audit results confirmed that the Department was complying with key requirements, although there is a need to update the departmental BCP policy and ensure that a business continuity plan is developed specifically for information technology. Overall, the audit team determined the results to be "*Generally Acceptable"*.

Appendix A - Audit Criteria

Objective	Criteria *
Assess overall compliance with Treasury Board requirements, including governance, risk assessment, planning and maintenance.	1. Effective oversight bodies are established. (R1)
	2. Appropriate roles, responsibilities, and performance standards have been clearly defined and communicated.
	3. The oversight body/bodies request and receive sufficient, complete, timely and accurate information. (R2, R3, R4)
	4. Management identifies the risks that may preclude the achievement of its objectives.
	5. Management identifies and assesses the existing controls that are in place to manage its risks.
	6. Management assesses the risks it has identified.
	7. Planning and resource allocations consider risk information.
	8. A clear and effective organizational structure is established and documented.
	9. Change initiatives are well communicated.
	10. The organization provides employees with the necessary training, tools, resources, and information to support the discharge of their responsibilities.

* Audit recommendations have been developed for any audit criteria that were not fully met. The recommendations noted above are designed to address the gap identified by the audit team. All other audit criteria were determined to be fully met.

Appendix B – Risk Ranking of Recommendations and Audit Opinion

The following definitions are used to classify the ranking of recommendations and the audit opinion presented in this report.

Audit Recommendations

Critical	Relates to one or more significant weaknesses for which no adequate compensating controls exist. The weakness results in a high level of risk.
Essential	Relates to one or more significant weaknesses for which no adequate compensating controls exist. The weakness results in a moderate level of risk.

Audit Opinion

Well Controlled	Only insignificant weaknesses relating to the control objectives or sound management of the audited activity are identified.
Generally Acceptable	Identified weaknesses, when taken individually or together, are not significant or compensating mechanisms are in place. The control objectives or sound management of the audited activity are not compromised.
Requires Improvement	Identified weaknesses, when taken individually or together, are significant and may compromise the control objectives or sound management of the audited activity.
Unsatisfactory	The resources allocated to the audited activity are managed without due regard to most of the criteria for efficiency, effectiveness and economy.