Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Canada

Audit of Business Continuity Planning

Published: 2013-00-20

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT66-57/2013E-PDF
ISBN: 978-0-660-25634-4

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Vérification de la planification de la continuité des activités

Government of Canada Gouvernement du Canada

Audit of Business Continuity Planning

Internal Audit and Evaluation Bureau

Table of Contents

Assurance Statement

The Internal Audit and Evaluation Bureau has completed an audit of the Business Continuity Planning Program (BCPP) for the Treasury Board of Canada Secretariat

(Secretariat). The objective of the audit was to assess the adequacy and effectiveness of the Secretariat's management control framework for the BCPP, including compliance with Treasury Board policies, directives, standards, and internal policies and procedures. The audit approach and methodology conforms to the *Internal Auditing Standards for the Government of Canada* and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

We conclude with a reasonable level of assurance that the management control framework of the Secretariat's BCPP complies with most aspects of the Treasury Board's *Policy on Government Security*, *Directive on Departmental Security Management* and *Operational Security Standard – Business Continuity Planning Program (BCP)*. Improvement is required to address key elements of the management control framework for the BCPP, specifically with respect to roles and responsibilities, governance, training, and mechanisms for monitoring and reporting. It is also critical that the Secretariat:

- Complete the development of the remaining sector Business Impact Analysis (BIA) and Business Continuity Plan (BCP) documents;
- Assess all sector BIA and BCP documents; and
- Develop and implement a testing cycle for BCPs as well as a regular maintenance cycle for the BCPP overall.

The examination was conducted during the period of June 2011 to January 2012 and covered the framework in place for the BCPP up to August 2011. The audit consisted of interviews, documentation review, and an examination of sector BIA and BCP documents using a judgmental sampling methodology. The audit evidence gathered is sufficient to provide senior management with reasonable assurance of the results derived from this audit.

In the professional judgment of the Chief Audit Executive, sufficient and appropriate audit procedures have been conducted, and evidence has been gathered to support the accuracy of the opinion provided in this report. The opinion is based on a comparison of the conditions, as they existed at the time of the audit, against pre-established audit criteria. The opinion is only applicable for the entities examined and for the time period specified.

Executive Summary

Preamble

Business continuity planning in a federal government setting is a component of baseline security requirements and forms a process that aims to ensure that critical government services can be continually delivered in the event of a potential disaster, a security incident, a disruption or an emergency. These security requirements are contained in the *Emergency Management Act* (2007) and the Treasury Board *Policy on Government Security*. Business continuity planning is important in order to provide "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" [1] should such an eventuality occur. The Treasury Board's *Operational Security Standard – Business Continuity Planning (BCP) Program* requires departments to implement a Business Continuity Planning Program (BCPP) and to plan for emergencies or disruptions that could affect the delivery of critical government services.

Background

Public Safety Canada uses the Treasury Board *Policy on Government Security* definition of critical service, "A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or the effective functioning of the Government of Canada." [2] For a service to be identified as critical, it must be evident that interruption of the service will begin to cause injury within a specific period of time, up to 30 days.

Based on this definition, the Treasury Board of Canada Secretariat (Secretariat) determined that it does not have critical services; however, a number of critical support functions [3] and one critical dependency [4] were identified. In order to ensure that there is no confusion between the Treasury Board *Policy on Government Security* definition of a critical service and the terminology used in the Secretariat's BCPP documentation, the Secretariat uses the term "critical operation" to identify its critical support functions and dependencies.

The departmental BCPP is intended to manage temporary business disruptions lasting up to 30 days. Business continuity planning is based on two scenarios:

1. Workforce outage, where sufficient staff may be unable to report for duty, such as in a pandemic.
2. Infrastructure outage, where premises occupied by Secretariat personnel may be uninhabitable due to damage or lack of utilities.

Objective and Scope

The objective of the audit was to assess the adequacy and effectiveness of the Secretariat's management control framework for the BCPP, including compliance with Treasury Board policies, directives, standards, and internal policies and procedures.

The audit focused on the departmental BCPP activities within the Secretariat. The review of the management control framework included the following components: objectives; accountabilities, roles and responsibilities; organizational structure; planning and risk management; policies and procedures; training; and monitoring and reporting.

Key Findings

Since the fall of 2009, the Secretariat has undertaken many initiatives to develop and implement the elements of a sound management control framework for the BCPP. These initiatives included:

- Appointing a Departmental Security Officer and a coordinator to lead the BCPP;
- Creating key working groups required in a BCPP as per standards and policy;
- Integrating business continuity planning in the departmental business planning and risk management cycles;
- Drafting and issuing a series of departmental documents that comply with Treasury Board policies and standards, and define objectives, roles, responsibilities and departmental procedures for Business Impact Analyses (BIAs), Business Continuity Plans (BCPs) and other activities in the BCPP;
- Communicating many of the elements and processes of BCPP activities on the departmental InfoSite; and
- Ad hoc reporting to senior management on the activities of the BCPP, which included obtaining decisions regarding critical operational priorities and the approval of key documents.

Notwithstanding the above, the audit identified a number of management control framework elements for improvement:

- While roles and responsibilities are defined in a comprehensive suite of documents developed since 2009, the role of employees has not been defined, and certain documents remain in draft mode. Further, roles and responsibilities for certain stakeholders are defined partially across a number of documents, without a comprehensive definition at a single source.
- The existing BCPP governance structure requires enhancement to ensure ongoing strategic-level direction and oversight.
- Responsibilities for training and communication of the BCPP are distributed between the corporate BCP group and the sector heads. However, communication

and training strategies have not yet been developed to ensure that individuals who are involved in the BCPP have the knowledge to execute their responsibilities when their sector BCP is activated.
- The audit found that there was a need to further articulate measurable and quantifiable expected results, beyond the existing objectives, to support monitoring and reporting. Formal processes for regular monitoring and reporting have not been developed.

The audit also found that the business continuity planning cycle is still evolving within the Secretariat. Specifically, not all sector BIA and BCP documents had been submitted to the corporate BCP group. The assessment of sector BIAs and BCPs had been initiated during the time of the audit, but had not progressed sufficiently for the audit team to assess the process. Further, the development of testing and maintenance processes in support of the BCPP were not developed at the time of the audit.

Conclusion

We conclude with a reasonable level of assurance that the management control framework of the Secretariat's BCPP complies with most aspects of the Treasury Board's *Policy on Government Security*, *Directive on Departmental Security Management* and *Operational Security Standard – Business Continuity Planning Program*. Improvement is required to address key elements of the management control framework for the BCPP.

Specifically, there is a need to:

- Review roles and responsibilities to ensure that they are streamlined, address all stakeholders and are formally approved;
- Define and formalize the integration of the BCPP within senior management committees to ensure ongoing strategic-level direction and oversight;
- Develop training and communication strategies that, in addition to other needs identified, serve to increase BCPP awareness for employees and for those involved in critical operations; and
- Develop and implement formal processes for regular monitoring and reporting.

To ensure that the Secretariat is at an appropriate stage of readiness to effectively respond to a BCP incident, it is also critical that remaining work relating to BCPP development be completed.

Specifically, there is a need to:

- Complete the development of remaining sector BIA and BCP documents;
- Assess all sector BIAs and BCPs; and

- Develop and implement a testing cycle for BCPs as well as a regular maintenance cycle for the BCPP overall.

A management action plan has been developed by the Secretariat and is presented in Appendix 2.

1. Introduction

1.1 Business Continuity Planning in the Federal Government

Business continuity planning in a federal government setting is a component of baseline security requirements and forms a process that aims to ensure that critical government services can be continually delivered in the event of a potential disaster, a security incident, a disruption or an emergency. These requirements are contained in the *Emergency Management Act* (2007) and the Treasury Board *Policy on Government Security*. Business continuity planning is important in order to provide 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" [5] should such an eventuality occur. The Treasury Board's *Operational Security Standard – Business Continuity Planning (BCP) Program* requires departments to implement a Business Continuity Planning Program (BCPP) and to plan for emergencies or disruptions that could affect the delivery of critical government services.

Events such as the 1998 ice storm, the 2003 power blackout, the 2009 H1N1 pandemic and the 2010 Ottawa earthquake have highlighted the importance of business continuity plans across the organization.

The BCPP is composed of four elements:

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

1.2 Business Continuity Planning in the Treasury Board of Canada Secretariat

The Treasury Board of Canada (Secretariat's) departmental Business Continuity Plan (BCP) supports the Secretariat in fulfilling its mandate, including its responsibilities relating to the Federal Emergency Response Plan, the Public Service Readiness Plan and internal operations.

In the fall of 2009, the Secretariat developed its Departmental Policy on Business Continuity Planning. One year later, the Secretariat developed its departmental BCP, which is a high-level overview of the Secretariat's response to an incident. Sector BCPs, once they are validated and tested, become components of the departmental BCP and provide the detail on how a sector will respond to an incident, should the support of a sector's critical operation be required.

Public Safety Canada uses the *Policy on Government Security* definition of a critical service, "A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or the effective functioning of the Government of Canada." [6] For a service to be identified as critical, it must be evident that interruption of the service will begin to cause injury within a specific period of time, up to 30 days.

During a tabletop exercise of the Secretariat's senior executives in December 2010, it was determined that the Secretariat has no critical services, as defined above. However, they identified a number of critical support functions [7] and one critical dependency. [8] In order to ensure that there is no confusion between the Treasury Board *Policy on Government Security* definition of a critical service and the terminology used in the Secretariat's BCPP documentation, the Secretariat uses the term "critical operation" to identify its critical support functions and dependencies.

As noted previously, the BCPP comprises four key elements, including the conduct of a BIA and the development of a BCP.

The purpose of a BIA is to identify the organization's mandate and critical services or products; rank the order of priority of services or products for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions. [9]

The departmental BCP is intended to manage temporary business disruptions lasting up to 30 days. Business continuity planning is based on two scenarios:

1. Workforce outage, where sufficient staff may be unable to report for duty, such as in a pandemic.
2. Infrastructure outage, where premises occupied by the Secretariat may be uninhabitable due to damage or lack of utilities.

The BCP provides for the continued availability of services that are critical to the security of employees and the effective functioning of the department in times of an emergency incident or disruption.

The BCP explains what an organization has developed in terms of governance, processes (including approval processes) and tools to make sure it can respond in an emergency incident or disruption—whether the emergency incident or disruption lasts a few hours, days or much longer. The BCP clearly defines the roles and responsibilities of key people and groups, with a view to ensuring that operations that are critical to the effective functioning of the Secretariat will be maintained. The BCP will be activated when a critical operation is at risk of not being delivered and will provide for additional support from employees in non-critical operations.

Operating Environment

At the Secretariat, responsibility for the BCPP is distributed between the corporate BCP unit in the Administration and Security Directorate, Corporate Services Sector, and the 17 Secretariat sectors and branches. [10]

The Director of Security, Administration and Security Directorate, has been designated as the Departmental Security Officer (DSO), who has the responsibility for developing and maintaining the BCPP.

A BCP coordinator, who reports to the DSO, is responsible for coordinating and supporting the development, management, delivery, and ongoing monitoring and maintenance of the Secretariat's BCPs. In turn, the BCP coordinator is supported by the BCP working group.

Sector heads and their management teams are accountable for assessing an incident, determining the most appropriate response within their respective areas, and developing a sector BIA and BCP to identify and document their responses. Each sector appoints a sector BCP coordinator and an alternate to represent them on the BCP working group and to support the sector head during an incident.

The Secretariat BCP working group, made up of sector BCP coordinators and their alternates, coordinates the development and implementation of the BCPP. This working group is chaired by the DSO.

The Secretariat Incident Management Team (IMT), made up of key stakeholders in communications, information technology, human resources and security services, supports the DSO and the BCP coordinator in the activation and coordination of the Secretariat's departmental BCP and sector BCPs during an incident, in accordance with the following:

- *Emergency Management Act*;
- *Policy on Government Security*;

- *Operational Security Standard – Business Continuity Planning (BCP) Program*; and
- Secretariat's Departmental Policy on Business Continuity Planning.

The Assistant Secretary, Corporate Services Sector, is the chair of the IMT.

Activation of the Secretariat's BCP will occur upon instruction from the Secretary, or the Secretary's alternate, in response to an incident that jeopardizes the Secretariat's ability to deliver its critical operations. In the event that both the Secretary and the alternate are not available, the decision will be taken by the IMT chair. Sector BCPs, as well as components of the Secretariat's departmental BCP, will be activated during an incident, as required.

2. Audit Details

2.1 Objective and Scope

The objective of the audit was to assess the adequacy and effectiveness of the Secretariat's management control framework for business continuity planning, including compliance with Treasury Board policies, directives, standards, and internal policies and procedures.

The audit focused on the following elements of the management control framework:

- Objectives;
- Accountabilities, roles and responsibilities;
- Organizational structure
- Planning and risk management;
- Policies and procedures;
- Training; and
- Monitoring and reporting.

The audit examined the departmental BCPP activities within the Secretariat.

Details on the audit criteria can be found in Appendix 1.

Scope Exclusions

The audit excluded the Secretariat's central agency responsibilities for supporting the Public Service Readiness Plan [11] and other security measures across the federal government. These activities are distinct from the Secretariat's operations and are governed by different processes and procedures. They also involve different departmental stakeholders.

2.2 Lines of Enquiry

The audit had two lines of enquiry:

- **Management control framework**—A management control framework is in place to ensure that the Secretariat is properly administering its responsibilities regarding the Treasury Board's *Policy on Government Security*, *Operational Security Standard – Business Continuity Planning (BCP) Program*, and *Directive on Departmental Security Management*.
- **Business continuity planning readiness**—Business continuity planning is part of a permanent maintenance cycle that includes the regular testing and validation of plans.

The audit assessed whether the management control activities and mechanisms were clearly defined, whether they addressed known risks, were sufficient and effectively communicated, were adequately monitored, and whether they reported risks and major issues related to the BCPP. The audit also assessed the level of compliance with applicable authorities through a detailed examination of a sample of BIAs and BCPs submitted to the BCP unit in 2011.

2.3 Approach and Methodology

The audit approach and methodology is risk-based and conforms to the *Internal Auditing Standards for the Government of Canada* and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. These standards require that the audit be planned and performed in such a way as to obtain reasonable assurance that audit objectives are achieved.

The audit included various tests and procedures considered necessary to provide such assurance, including the following:

- Interviews with key personnel; research; review of key documents; assessment of risk to identify potential risk exposure; and analysis of departmental and sector BIAs and BCPs for compliance, trends and readiness.
- Validation and assessment of the management control framework elements described in the scope. In addition, the key documents for the BCPP were reviewed to assess the level of compliance with applicable authorities. The examination phase of this audit was conducted from June 2011 to January 2012, based on the information and documents obtained by August 2011.

3. Audit Results

3.1 Line of Enquiry 1: Management Control Framework

It was expected that a sound management control framework would be in place to facilitate management in achieving the Secretariat's objectives for business continuity, to support effective decision making, and to flag significant control issues on a timely basis. It was also expected that the information required to implement and maintain the BCPP would be documented, maintained and effectively communicated to all stakeholders involved in the BCPP activities.

Since the fall of 2009, the Secretariat has undertaken many initiatives to develop the BCPP. These initiatives have included:

- Appointing a DSO and a coordinator to lead the BCPP;
- Creating key working groups required in a BCPP as per standards and policy;
- Integrating business continuity planning in the departmental business planning and risk management cycles;
- Drafting and issuing a series of departmental documents that comply with Treasury Board policies and standards, and define objectives, roles, responsibilities and departmental procedures for BIAs, BCPs and other activities in the BCPP;
- Communicating many of the elements and processes of BCPP activities on the departmental InfoSite; and
- Ad hoc reporting to senior management on the activities of the BCPP, including obtaining decisions on key documents and critical operational priorities.

While the Secretariat has put into place many of the essential elements required for the BCPP, the program is maturing in its development and implementation.

Objective

The objective of the BCPP has been broadly defined in the Departmental Policy on Business Continuity Planning as well as in the Secretariat's BCP. The stated objective aligns with the expected results of the Treasury Board *Policy on Government Security* pertaining to the BCP. However, there is a need to further articulate measurable and quantifiable expected results to support monitoring and reporting on the BCPP.

Organizational Structure

In line with the accountabilities and responsibilities of individual sectors, the organizational structure of the BCPP is decentralized. A formal and documented organizational structure is in place to support the BCPP activities for the corporate BCP group in the Corporate Services Sector. However, these individuals also have responsibilities for other security activities such as the Departmental Security Plan, Emergency Management, and Occupational Health and Safety. As these additional activities fell outside the scope of the audit, it was not possible to assess the sufficiency of resources dedicated to the BCPP.

The organizational structure for other employees performing BCP activities, such as the sector BCP working group coordinators, is informal and employees are assigned based on the requirements of the sector.

Accountabilities, Roles and Responsibilities

Overall, the majority of the accountabilities, roles and responsibilities have been clearly defined in key documents. The audit also found that key stakeholders, including the members of the BCP working group, the IMT and the corporate BCP unit of the Administrative and Security Directorate, Corporate Services Sector, were generally aware of their responsibilities regarding the BCPP.

However, certain documents that define roles and responsibilities were not approved as of the time of the audit. Also, while employees have responsibilities under the Treasury Board *Directive on Departmental Security Management*, these were not defined in departmental documentation, including the Departmental Policy on Business Continuity Planning and the BCP. Finally, roles and responsibilities for certain stakeholders were defined partially across a number of documents, without comprehensively defining them in a single document.

Planning and Risk Management

Strategic direction and key decisions related to the BCPP were made by senior management through various mechanisms such as presentations to the Secretariat's Executive Committee and Management and Infrastructure Committees on an ad hoc basis. Similarly, there was evidence that BCPP activities were included and considered in the Secretariat's planning and risk management cycles.

While senior management committees discuss BCPP-related topics periodically, there is no formal role for providing ongoing strategic-level direction and support, as recommended by the Treasury Board *Operational Security Standard – Business Continuity Planning (BCP) Program*. A BCP working group exists and meets at the call of the chair; however, its membership is largely below the executive level.

Departmental Policies, Procedures and Guidelines

Substantial efforts have gone into the development of a suite of documents that contain the key policy, plans, procedures, templates and guidelines expected for a BCPP. The key policy and plan documents are generally compliant with the Treasury Board's *Policy on Government Security* and *Operational Security Standard – Business Continuity Planning*. However, at the time of the audit, some documents were awaiting formal approval before they could be implemented and communicated to individuals in the BCPP. In addition, some of the documents require revisions in order to address elements related to training and performance monitoring.

Training

Responsibilities for training are distributed between the corporate BCP group and the sector heads. Training has occurred for some of the BCP working group members, and a number of guidance documents have been posted on the Secretariat's intranet site. However, communication or training strategies have not yet been developed to ensure that individuals who are involved in the BCPP have the knowledge to execute their responsibilities when their sector BCP is activated. Based on interviews, some of the BCP working group and IMT members relied on previous experiences and ad hoc practices in place throughout the Secretariat. Given that the Secretariat experienced a turnover of approximately 1,000 employees each year in the last two years, training and communication strategies are critical to ensure that employees are aware of the program details and have the appropriate information to respond to a BCP incident. The completion of the previously mentioned suite of documents would help create the foundation for a training program.

Monitoring and Reporting

The *Policy on Government Security*, the *Directive on Departmental Security Management*, and the *Operational Security Standard – Business Continuity Planning (BCP) Program* include requirements for monitoring and reporting activities. The audit team therefore expected to find documentation that identified the approach for ongoing monitoring and reporting, including the key results that would be monitored and reported on over time. In addition to meeting policy requirements, such an approach helps ensure, among other things, that management is aware of key results attained by the program, as well as significant risks or issues as they arise.

While monitoring and reporting processes were not formally defined, the audit found that monitoring of certain BCPP activities occurred periodically through ad hoc reporting to senior management. These activities pertained to the development of BCP documents such as the Departmental Policy on Business Continuity Planning, the departmental BCP, the departmental Threat and Risk Assessment, the Disaster Recovery Plan, the PIN-to-PIN testing results, and the BCP priorities presented to senior management in February

2011. The roll-up of initial BIA sector submissions was also presented to senior management and became one of the triggers for the tabletop exercise held with the Secretariat's Executive Committee in December 2010. Tracking of the sector submissions of BIA and BCP documents was also found to occur.

The level of monitoring and reporting previously noted represents significant progress for the Secretariat's BCPP over the last two fiscal years. The formal definition of such processes, including details on what should be monitored and reported on, would enhance senior management's awareness of critical aspects of the program and would further support timely direction and oversight.

Key results that could be monitored and reported on regularly include:

- Training and awareness activities (e.g., for new employees and key BCPP stakeholders);
- Results of testing and maintenance activities;
- Issues and risks identified via the BCPP, and their disposition; and
- Status and results of critical BCPP activities.

Recommendations:

It is recommended that the Assistant Secretary, Corporate Services Sector, undertake the following:

1. Review the suite of documents defining BCPP roles and responsibilities, with a view to ensuring that they address all stakeholders, are streamlined, and are formally approved.
   Priority ranking: High
2. Formally integrate the BCPP into the senior management committee structure to ensure ongoing strategic-level direction and oversight.
   Priority ranking: High
3. In collaboration with sector heads, develop and implement communication and training strategies to meet identified needs.
   Priority ranking: High
4. Formally define monitoring and reporting processes, including key expected results, in order to effectively support BCPP activities.
   Priority ranking: Medium

3.2 Line of Enquiry 2: Business Continuity Planning Readiness

It was expected that the Secretariat would have completed the preparation and validation of sector BIAs and BCPs. It was also expected that these BIAs and BCPs would be compliant with the Departmental Policy on Business Continuity Planning and that a testing and maintenance cycle for the BCPP would exist.

To ensure that the Secretariat is prepared to respond to an incident and to activate the necessary sector BCPs, it is necessary that every sector have an approved BIA and BCP that represents their planned response for both critical and non-critical operations.

It was found that the business continuity planning cycle is still evolving within the Secretariat. In 2008–09 the first set of sector BIAs was prepared. These were summarized into a departmental document that identified the critical operations and the number of employees required during a BCP incident. This report became one of the triggers for a review and prioritization of critical operations, which was done by the Secretariat's Executive Committee in December 2010.

At that time, the top seven critical operations that needed to be addressed within the first 24 hours of an incident were identified. An additional nine critical operations were prioritized. In 2011, the sectors BIAs were updated, and the development of the first cycle of sector BCPs was initiated.

During this time, the corporate BCP group in the Corporate Services Sector provided guidance and developed tools to assist the sectors in the development of their BIA and BCP documents.

Sector BIAs and BCPs were prepared and submitted by most sectors; however, four sectors, which contain critical operations, did not submit. Most sectors made use of the departmentally designed templates; however, information in many of the documents contained gaps and ambiguities.

At the time of our audit, the corporate BCP unit had initiated the review and validation process for sector BIAs and BCPs; however, this had not progressed sufficiently for the audit team to assess the process. The testing and maintenance cycles had not commenced.

Further work is required to:

- Complete the development of the remaining sector BIA and BCP documents;
- Assess all sector BIAs and BCPs; and

- Develop and implement a testing cycle for BCPs as well as a regular maintenance cycle for the BCPP overall.

During the engagement, the audit team identified a potential opportunity to further streamline the program through the use of generic BIA and BCP documents that would handle non-critical, as well as certain critical, operations. The audit found that most sectors have non-critical operations and that the BCP responses are often the same or similar. As such, use of generic responses, while still allowing for sector specific requirements, has the potential to reduce overall effort. This possible approach is identified for management's consideration only, and is therefore not included in the recommendations that follow.

Recommendation:

It is recommended that the Assistant Secretary, Corporate Services Sector, undertake the following:

5. In collaboration with sector heads, complete the remaining work relating to BCPP development.

Specifically, there is a need to:

- Complete remaining sector BIA and BCP documents, and ensure that all are assessed; and
- Develop and implement a testing and maintenance cycle for BIA and BCP documents and activities.

Priority ranking: High

3.3 Overall Conclusion

Significant progress has been made by the Secretariat in developing and implementing a management control framework for the BCPP since September 2009.

We conclude with a reasonable level of assurance that the management control framework of the Secretariat's BCPP complies with most aspects of the Treasury Board's *Policy on Government Security*, *Directive on Departmental Security Management* and *Operational Security Standard – Business Continuity Planning (BCP) Program*. Improvement is required to address key elements of the management control framework for the BCPP.

Specifically, there is a need to:

- Review certain roles and responsibilities to ensure that they are formally approved and that all stakeholders are addressed;
- Define and formalize the integration of the BCPP within senior management committees, to ensure ongoing strategic-level direction and oversight;
- Develop training and communication strategies that, in addition to other needs identified, serve to increase BCPP awareness for employees and for those involved in critical operations; and
- Develop and implement formal processes for regular monitoring and reporting.

To ensure that the Secretariat is at an appropriate stage of readiness to effectively respond to a BCP incident, it is also critical that the remaining work relating to BCPP development be completed.

Specifically, there is a need to:

- Complete the development of remaining sector BIA and BCP documents;
- Assess all sector BIAs and BCPs; and
- Develop and implement a testing cycle for BCPs as well as a regular maintenance cycle for the BCPP overall.

Appendix 1—Audit Criteria

Line of Enquiry 1—Management Control Framework

A management control framework is in place to ensure that the Secretariat is properly administering its responsibilities with regard to the following:

- Treasury Board *Policy on Government Security*;
- Treasury Board *Operational Security Standard – Business Continuity Planning (BCP) Program*; and
- Treasury Board *Directive on Departmental Security Management*.

1. Objectives and goals are clearly defined, formally approved, current and communicated.
2. Accountability, roles and responsibilities are clearly defined, formally approved and communicated.
3. The organizational structure is formal and is supported by the appropriate resources.

4. Planning and risk management are undertaken on a regular basis.
5. Departmental policies, procedures and guidelines are compliant with applicable authorities and are complete, current and communicated.
6. Training of management and staff with business continuity planning responsibilities for awareness and compliance with applicable policies, directives and practices, effectively supports the Business Continuity Planning Program (BCPP).
7. An effective monitoring and reporting mechanism is in place.

Line of Enquiry 2—Business Continuity Planning Readiness

Business continuity planning is part of a permanent maintenance cycle that includes regular testing and validation of plans.

1. Sector Business Impact Analyses (BIAs) are compliant, validated, tested and maintained.
2. Departmental and sector Business Continuity Plans (BCPs) are compliant, validated, tested and maintained.

Appendix 2—Management Action Plan

Recommendation 1:

It is recommended that the Assistant Secretary, Corporate Services Sector review the suite of documents defining BCPP roles and responsibilities, with a view to ensuring that they address all stakeholders, are streamlined, and are formally approved.

Priority ranking: **High**

Management Action	Completion Date	Office of Primary Interest (OPI)

We agree with the recommendation		
CSS will review and revise the Departmental BCP policy to clarify roles and responsibilities of all individuals involved in the BCP process.	Q3 2012-13	CSS
All supporting documentation will be updated and streamlined, where appropriate	Q3 2012-13	CSS
Documents with implications external to CSS, including policies, will be approved by the Secretary subsequent to review by the Management and Infrastructure Committee (MIC).	Q4 2012-13	CSS

Recommendation 2:

It is recommended that the Assistant Secretary, Corporate Services Sector formally integrate the BCPP into the senior management committee structure to ensure ongoing strategic-level direction and oversight.

Priority ranking: **High**

Management Action	Completion Date	Office of Primary Interest (OPI)
We agree with the recommendation.		
CSS will review and revise current governance for the BCP Program to ensure formal integration of strategic level direction and oversight into the senior management committee structure.	October 2012	CSS
Revised governance structure to be presented to EXCO for review prior to approval.	November 2012	CSS
NOTE: The Strategic Emergency Management Plan (SEMP) will be approved by the Secretary by December 2012. The SEMP will integrate all levels of emergency response and will incorporate building emergencies, BCP considerations	December 2012	CSS / IASJ [12]

and the central agency role that TBS leads with respect to the Federal Emergency Response Plan (FERP)		

Recommendation 3:

It is recommended that the Assistant Secretary, Corporate Services Sector, **in collaboration with sector heads**, develop and implement communication and training strategies to meet identified needs.

Priority ranking: **High**

Management Action	Completion Date	Office of Primary Interest (OPI)
We agree with the recommendation.		
CSS and the Strategic Communication and Ministerial Affairs sector (SCMA) will develop a communication strategy as part of the 2012-13 BCPWG work plan.	January 31, 2013	CSS / SCMA
CSS will obtain approval from the Assistant Secretary CSS, for the communication strategy.	March 31, 2013	CSS
The communications strategy will be implemented.	May 2013	CSS / SCMA
CSS will develop, obtain approval from the Assistant Secretary CSS, and commence a three year training strategy to target both sector and corporate engagement.	March 31, 2013	CSS
CSS will develop generic tools and training to be provided to the BCPWG to assist with BCP exercises for sectors in 2012-13.	September 2012	CSS
Using the generic tools developed by CSS, and with assistance from CSS (if required), sectors will:		
Hold information training sessions for all employees, critical or non-critical, within the sector, in accordance with the needs outlined in the sector plan.	December 2012	Sector Heads CSS / SCMA

Provide additional training to staff with duties relating to the Sector's critical operations to ensure adequate knowledge of BCP requirements, in accordance with the needs outlined in the sector plan.	March 2013	Sector Heads CSS / SCMA

Recommendation 4:

It is recommended that the Assistant Secretary, Corporate Services Sector formally define monitoring and reporting processes, including key expected results, in order to effectively support BCPP activities.

Priority ranking: Medium

Management Action	Completion Date	Office of Primary Interest (OPI)
We agree with the recommendation.		
CSS will develop a monitoring process. This process will provide a framework to oversee the development of strategic objectives, formal reporting mechanisms, and provide clear measures consistent with the monitoring process.	Q4 2012-13	CSS
This monitoring process will be approved by the Assistant Secretary CSS, and implemented	March 31, 2013	CSS
Formal reporting on BCP activities will be implemented	Q3 2013-14	CSS

Recommendation 5:

It is recommended that the Assistant Secretary, Corporate Services Sector, **in collaboration with sector heads**, complete the remaining work relating to BCPP development.

Specifically, there is a need to:

- Complete remaining sector BIA and BCP documents, and ensure that all are assessed; and

- Develop and implement a testing and maintenance cycle for BIA and BCP documents and activities.

Priority ranking: High

Management Action	Completion Date	Office of Primary Interest (OPI)
We agree with the recommendation.		
All completed 2011/12 sector BCP and BIA plans were assessed in January 2012. Sectors were provided with written feedback on their plans and were encouraged to meet with CSS for further discussion.	Completed	CSS
Sectors will be required to submit approved BCP plans and Business Impact Analysis for 2012/13 on or before the deadline provided by CSS.	June 29, 2012	Sector Heads
Assessments of the 2012/13 plans will be completed by CSS.	October 2012	CSS
A testing cycle will be developed and approved by the Assistant Secretary, CSS.	March 31, 2013	CSS
The testing cycle will be implemented	Q1 2013-14	CSS
A maintenance cycle will be developed and approved by the Assistant Secretary, CSS.	March 31, 2013	CSS
The maintenance cycle will be implemented and monitored by CSS. Sector representatives will contribute to the implementation of maintenance activities.	Q1 2013-14	CSS / Sector representatives

[1] *Policy on Government Security*, Appendix A – Definitions, effective July 1, 2009.

[2] Ibid.

[3] A critical support function is an interdepartmental or intradepartmental policy or service that supports a critical service.

[4] A critical dependency is a business process arrangement where one department is responsible for a critical service but depends on another department for completion, production or delivery of the output.

[5] *Policy on Government Security*, Appendix A – Definitions, effective July 1, 2009.

[6] *Policy on Government Security*, Appendix A – Definitions, effective July 1, 2009.

[7] A critical support function is an interdepartmental or intradepartmental policy or service that supports a critical service.

[8] A critical dependency is a business process arrangement where one department is responsible for a critical service but depends on another department for completion, production or delivery of the output.

[9] Public Safety Canada, A Guide to Business Continuity Planning.

[10] For purposes of this report, all Secretariat sectors and branches will be referred to as "sectors."

[11] The purpose of the Public Service Readiness Plan (PSRP) is to provide the planning architecture, processes and guidance required for deputy heads to horizontally manage the crosscutting, public service–wide consequences of an emergency. The PSRP may be activated when emergencies result in workforce and service delivery issues impacting a number of departments and agencies that cannot be effectively managed within the scope of individual departmental Business Continuity Plan. The PSRP engages a small group of deputy heads, who will consider interdepartmental solutions to facilitate the delivery of critical services.

[12] International Affairs, Security and Justice Sector (IASJ)

▶ Report a problem or mistake on this page

Share this page

Date modified: 2013-08-20

Contact us

Departments and agencies

Public service and military

News

Treaties, laws and regulations

Government-wide reporting

Prime Minister

How government works

Open government

- Social media
- Mobile applications
- About Canada.ca
- Terms and conditions
- Privacy

Top of page ^

Canada