[*] An asterisk appears where sensitive information has been removed in accordance with the *Access to Information Act* and *Privacy Act*.

PRIVY COUNCIL OFFICE

Follow-up Audit of Business Continuity Management

Audit and Evaluation Division

Final Report

December 19, 2014

Table of Contents

Acronyms Used in this Report

BCM	Business Continuity Management
BCP	Business Continuity Planning
DSEMP	Departmental Security and Emergency Management Plan
IT	Information Technology
ITSD	Informatics and Technical Services Division
MOU	Memorandum of Understanding
PCO	Privy Council Office
PGS	Policy on Government Security
PMO	Prime Minister's Office
SecOps	Security Operations (Division)
SEM	Security and Emergency Management
SSC	Shared Services Canada
TBS	Treasury Board Secretariat

Statement of Conformance

In my professional opinion as Chief Audit Executive, this audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of PCO's quality assurance and improvement program.

Original signed by

_____

CHIEF AUDIT EXECUTIVE
JIM HAMER
DIRECTOR, AUDIT AND EVALUATION

Director, Audot and Evaluation

1.0 Introduction

Business continuity management (BCM) provides a framework to ensure an organization's resilience to any event and to help ensure the continuity of services it delivers. In a federal government setting, BCM is a component of baseline security requirements and forms a process that aims to ensure 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* (PGS). 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" (PGS) should such an eventuality occur. The Treasury Board's *Operational Security Standard – Business Continuity Planning Program* requires departments to implement a business continuity program and to plan for emergencies or disruptions that could affect the delivery of critical government services.[1]

PCO's *Policy on Business Continuity Management*, issued in 2009 under the authority of the Clerk, is intended to provide for the continued availability of critical services, assets and dependencies, regardless of the magnitude of a disruption in service. This is realized in accordance with the Government of Canada's requirement to achieve an appropriate state of emergency readiness for continuity of government operations and services in the presence of security incidents, disruptions or emergencies. Non-compliance with this policy could result in PCO's lack of ability to maintain continued delivery of its critical services and may result in a breach of emergency management responsibilities under the *Emergency Management Act* and/or the *Policy on Government Security* pertaining to business continuity planning.

The PCO Departmental Security and Emergency Management Plan (DSEMP) depicts a three-tiered approach that has been adopted for business continuity planning. The three tiers, or levels as they are described, are defined as follows:

- Level I - Divisional business continuity plans and arrangements developed to support a minor disruption such as a flood on a floor where only one secretariat or division is impacted.
- Level II - Departmental plans including alternate site arrangements to respond to and recover from a moderate disruption such as a fire where one or more PCO buildings are impacted.
- Level III - Preparations for a catastrophic disruption such as a city-wide event affecting not only PCO and PMO, but the Continuity of Constitutional Government. [*]

As noted in the Scope section below, Level III business continuity planning was not included in this audit.

Results from the Original Audit

[1] Reference: 2012 TBS Audit of Business Continuity Planning

In 2010, the Audit and Evaluation Division conducted an Audit of Business Continuity and Emergency Preparedness – Final Report dated May 2011. [*] Following the 2010 audit, PCO adjusted their planning approach to include a small number of critical functions [*] which are now depicted in the DSEMP.

1.1 Authority

This Follow-up Audit of Business Continuity Management was approved by the Clerk of the Privy Council as part of PCO's Risk-Based Audit Plan for completion in 2014-2015.

1.2 Objective

The overall objective of the audit was to assess the effectiveness of the governance structure and controls in place to support the delivery of the BCM program and continued delivery of PCO critical functions in the event of a disruption.

1.3 Scope

In May 2011, PCO's Audit and Evaluation Division completed an Internal Audit of Business Continuity and Emergency Preparedness. This follow-up audit focused on changes in business continuity management practices and activities occurring subsequent to October 2010, the end of the period covered by the former audit. While the initial audit addressed both business continuity and emergency preparedness, this audit was limited to business continuity management. It did not examine any other elements of the overall PCO Security and Emergency Management (SEM) Program such as building emergency operations, safety/fire prevention activities, or physical security.

The audit scope included the governance structure established to administer and oversee Level I divisional plans for minor disruptions, Level II relocation plans for moderate disruptions, and critical function planning activities, including the development and testing of business continuity plans and oversight of the program. The scope did not extend to examining Level III BCM activities which include planning for a catastrophic event impacting the continuity of constitutional government as these activities are administered through involvement with external partners and were not included in the original audit.

1.4 Audit Criteria

During the audit's planning phase, the audit team established four main audit criteria, which were agreed to by management. These criteria are expressed in terms of reasonable expectations for this program to achieve expected results and formed the basis on which the effectiveness of the BCM program was assessed.

1. An effective governance structure is in place where roles, responsibilities, and accountabilities are clearly communicated and understood and sufficient resources are in place to enable an effective BCM program.
2. Mechanisms are in place to track and report on BCM activities on a regular and timely basis, and take corrective action as necessary.
3. Business continuity plans and activities are comprehensive and reflect areas of priority and criticality to PCO.
4. Information and tools related to BCM are provided to those stakeholders responsible for BCM activities on a timely basis to support the effective delivery of the program.

1.5 Approach and Methodology

The audit began with a planning phase, conducted from February to March 2014, during which the audit team identified relevant risks to the achievement of the objectives and expected results of PCO's BCM program. From these risks, the audit team established audit criteria, identified above, which are primarily based on the Treasury Board Secretariat (TBS) reference document – *Audit Criteria related to the Management Accountability Framework: A Tool for Internal Auditors*. Prior to moving to the examination phase, the Chief Audit Executive communicated planning phase results with management and received their agreement with the audit criteria.

The audit examination phase, conducted from March to June 2014, consisted of a review of the governance structure established to oversee and administer the BCM program, the comprehensiveness of business continuity plans and activities, and the mechanisms in place for monitoring and reporting on BCM activities. The audit approach included interviews with officials from PCO's Security Operations (SecOps) Division involved in business continuity planning activities and stakeholders outside SecOps Division with business continuity planning responsibilities. This included examining defined roles, responsibilities and accountabilities of individuals with formal obligations for BCM as well as information and reporting provided for effective oversight of the program.

At the end of the examination phase, audit findings were discussed with management and a draft report was prepared and sent by the Chief Audit Executive to the Assistant Secretary to the Cabinet, Security and Intelligence for response and development of an action plan to address the audit recommendations. Audit reports and management action plans are provided to PCO's Audit Committee for review and recommendation to the Clerk of the Privy Council for approval.

2.0 Conclusion

While a governance structure for the BCM program has been documented in two departmental policies and in the DSEMP, [*]

Rapid improvements were made following completion of the 2010 Audit of Business Continuity and Emergency Preparedness, which included articulation of a concise number of PCO critical functions and establishment of alternative site arrangements; [*]

The following sections detail the audit findings and recommendations.

3.0 Findings and Recommendations

3.1 Governance Structure

Roles, responsibilities, and accountabilities for PCO's BCM program have been defined in the Policy on Business Continuity Management, the Security and Emergency Management Policy and in the DSEMP. [*]

PCO has two departmental policies that address business continuity requirements – the (2009) *Policy on Business Continuity Management* and the (2012) *Policy on Security and Emergency Management*. The former describes the responsibility framework specific to the BCM program while the latter positions business continuity within the context of the overall SEM Program that also includes physical and personnel security, safety and fire prevention, information technology and information management security, and emergency management and response planning. The SEM Program operates under direction from the Departmental Security Officer who reports to the Assistant Secretary to the Cabinet, Security and Intelligence.

Within this governance framework, the PCO Executive Committee is charged with responsibility for ensuring an effective state of readiness to mitigate, prepare for, respond to and recover from a business continuity disruption, including direct oversight of the BCM program. [*]

Both policies mentioned above present an approach to business continuity planning that position SecOps Division as a functional leader or coordinator to guide and support PCO branches, secretariats and divisions through preparation, validation, update and maintenance of their business continuity plans. [*]

[*]

[*]

We recommend that the Assistant Secretary to the Cabinet, Security and Intelligence, as the primary senior manager responsible for overseeing the SEM Program, under the overall accountability of the National Security Advisor to the Prime Minister, ensure implementation of audit recommendations.

Recommendation 1: [*]

3.2 BCM Reporting

Limited reporting on BCM activities does occur within the context of the Security and Emergency Management Program; [*]

While SecOps Division has developed a Performance Management Strategy that defines outputs, outcomes and performance indicators, during the audit [*]

[*]

Recommendation 2: [*]

3.3 Business Continuity Plans and Validation Activities

While secretariat / divisional business continuity plans exist and some testing activities have been conducted to validate recovery efforts, [*]

3.3.1 Level I Business Continuity Plans

In practice, BCM planning activities are [*] which states that business continuity planning "is a planning process focused on ensuring that critical functions are delivered during a disruption or emergency". Level I business continuity plans for minor disruptions are developed at the secretariat / divisional level for 30 business units aligned with the organizational structure of PCO. For Level I planning, each secretariat or division is asked to identify the secretariat / divisional critical services and required recovery time, resulting in the identification of critical activities at an operational level, intended to be used to define needs for Level II planning. As the planning activities are structured to reflect individual PCO business units, [*]

For the audit, we reviewed [*] Level I business continuity plans; [*] Though the Level I business continuity plans did exist, [*]

See recommendation #1

3.3.2 Level II Business Continuity Plans

While Security Operations has worked with critical function leads through the Standing Working Group on PCO Mission-Critical Functions, [*] The existing Level II Plan is essentially a recovery strategy designed to ensure that PCO/PMO employees who are required to move to an alternate work site can do so safely, efficiently and in a coordinated manner.

Many of the Level II planning documents date from the 2010-2011 period, having been completed concurrently or just after the original Audit of Business Continuity and Emergency Preparedness. In October 2010, PCO entered into a memorandum of understanding (MOU) with another government department that would enable PCO to use office space in an alternate location in the event of a disruption affecting PCO accommodations. While the MOU remains in effect, [*]

As part of Level II planning, a number of documents supporting the MOU were developed to articulate IT and telecommunications requirements for the primary alternate site. [*]

[*]

[*]

3.3.3 Testing of Plans

Interviews with SecOps personnel and individuals responsible for critical functions indicate that testing of business continuity plans has been [*] In 2013, SecOps Division was involved in table top exercises for [*] Level I plans, during which participants met to discuss how they would respond during an event affecting continuity of operations.

As indicated above, Level II planning documents are [*]

[*] At time of reporting this was still a work in progress.

Testing or exercising business continuity plans is an essential component of plan maintenance as recognized in the TBS *Operational Security Standard – Business Continuity Planning Program*. [*]

3.4 Information and Tools

Engagement mechanisms and tools exist to help stakeholders understand their duties with respect to BCM activities.

The BCM program is supported by a number of tools, including the BCM planning document used by secretariats to develop and update their Level I BCM plan, as well as exercises and standard reporting for Level I validation activities. While business continuity planners in secretariats and divisions appeared to be satisfied with tools provided to support Level I validation activities, [*]

[*]

In the past, SecOps officials also met annually with stakeholders from the primary alternate site to reconfirm the arrangements in support of Level II plans. [*]

While the audit has no formal recommendations regarding information and tools provided to stakeholders, we encourage continued engagement with critical function leads and involvement from Business Continuity Planners as planning activities are coordinated under a [*]

4.0 Management Response and Action Plan

Management has accepted all audit recommendations; their action plan is presented on the following pages.

Management Action Plan

Follow-up Audit of Business Continuity Management

The Assistant Secretary to the Cabinet, Security and Intelligence has overall responsibility for the Action Plan.

Recommendation	Planned Actions	Responsibility	Due Date
We recommend that the Assistant Secretary to the Cabinet, Security and Intelligence, as the primary senior manager responsible for overseeing the SEM Program, under the overall accountability of the National Security Advisor to the Prime Minister, ensure implementation of the following recommendations:			
1. [*]	Management agrees. [*] [*]	Director, Planning and Issues Management, SECOPS	December 2015
2. [*]	Management agrees. [*] [*] [*]	Director, Planning and Issues Management, SECOPS	November 2014 and ongoing
3. [*]	Management agrees. [*]	Director, Planning and Issues Management, SECOPS, [*]	December 2015