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

PRIVY COUNCIL OFFICE

Audit of Business Continuity and Emergency Preparedness

Audit and Evaluation Division

Final Report

May 5, 2011

Table of Contents

Acronyms used in this Report

AoM	Area of Management
ATE	Awareness, Training, and Exercises
BCM	Business Continuity Management
BCP	Business Continuity Planning
BCPP	Business Continuity Planning Program (Compliance Report)
BEO	Building Emergency Organization
BIA	Business Impact Analysis
CBEW	Chief Building Emergency Warden
CMC	Crisis Management Cell
CONOPS	Concept of Operations
DSO	Departmental Security Officer
EM	Emergency Management
EPPT	Emergency Planning Project Team
FPEM	Federal Policy on Emergency Management
HR	Human Resources
ICS	Incident Command System
IM	Information Management
IT	Information Technology
ITSD	Informatics and Technical Services Division
MAF	Management Accountability Framework
OHS	Occupational Health and Safety
OI	Opportunity for Improvement
PCO	Privy Council Office
PGS	Policy on Government Security
PMO	Prime Minister’s Office
PSB	Postal Station ‘B’ (building)
PWGSC	Public Works and Government Services Canada
SecOps	Security Operations Division
TB	Treasury Board

Executive Summary

Authority

The Audit of Business Continuity and Emergency Preparedness was approved by the Clerk as part of the Privy Council Office (PCO) Risk-Based Internal Audit Plan 2009-2010 to 2011-2012.

Audit Objectives

There were two objectives for this internal audit:

1. To assess the adequacy and effectiveness of mechanisms and capabilities to respond to emergencies in an effective manner to prevent loss of life, and minimize injury and property damage.

   For the first objective, the audit focused on the mechanisms established and capabilities developed for immediate response to emergencies such as fire, smoke, or gas; civil disruptions; and bomb threats.

2. To assess the adequacy and effectiveness of controls in place to achieve effective business continuity ensuring minimal or no interruption to the availability of critical services and assets.

   For the second objective the audit focused on the four elements of a business continuity planning (BCP) program as described in the Treasury Board (TB) BCP Operational Security Standard including:
   - Establishment of BCP program governance;
   - Conduct of a business impact analysis (BIA);
   - Development of business continuity plans and arrangements; and
   - Maintenance of BCP program readiness.

Audit Scope

Organizationally the audit focused on the Security Operations Division (SecOps), which coordinates the PCO Emergency Management (EM) program. SecOps is located within the Security and Intelligence Secretariat, which reports to the National Security Advisor to the Prime Minister. Other PCO organizational units were included as each Deputy Secretary / Deputy Minister has responsibility for the implementation of their respective business continuity plans during an emergency.

The audit scope included an examination of the process PCO followed to identify critical services; however, it did not challenge management's final determination as to what has, or has not, been identified as a critical service. The audit scope did not include

arrangements with respect to PCO's role in ensuring the Continuity of Constitutional Government.

The audit scope included PCO business continuity and emergency preparedness activities from 2007 to October 2010. At end of the scope period there were a number of initiatives that were planned or underway; outcomes from these initiatives realized after October 2010 were not included in the audit scope.

Audit Findings and Conclusions

Emergency Preparedness

Experienced and skilled personnel have been brought to PCO to establish a framework and implement required changes to position the department to effectively respond and recover from an emergency or catastrophic event, [*]

[*]

Business Continuity Management

At its core, business continuity management is about being able to deliver on those aspects of your business that matter most, no matter what. For PCO this means being able to continue providing professional, non-partisan advice and support to the Prime Minister, ministers within the Prime Minister's portfolio and the Cabinet. [*]

A management framework for business continuity management (BCM) exists and is consistent with the Treasury Board *Operational Security Standard – Business Continuity Planning.* In 2009, PCO established its own *Policy on Business Continuity Management* that clearly describes the roles and responsibilities of senior management and functional leaders, including the BCM Coordinator.

In recent years, PCO has undertaken a full BIA to identify and clarify the department's critical services and functions in support of its strategic objective. The 2008 BIA yielded a list of 161 critical services, which was focused down, in 2009, to 89 mission critical services that must be operating within 24 hours of an emergency event. [*]

Individual business continuity plans have been established, [*]

[*]

Recommendations

All recommendations are directed to the National Security Advisor to the Prime Minister as the senior management lead responsible for business continuity and emergency preparedness.

We recommend that the National Security Advisor to the Prime Minister:

1. [*]

2. Continue progress on performance measurement including development, approval, and implementation of a performance measurement strategy that includes emergency preparedness; and

3. [*]

Management Response

Management's response and action plan are included as Section 3.0 in the body of the report.

Statement of Assurance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support a reasonable level of assurance as to the accuracy of the conclusion provided and contained in this report. The conclusion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed with management. The conclusion is applicable only to the entity examined.

Original signed by the Chief Audit Executive

_____

SIGNATURE OF CHIEF AUDIT EXECUTIVE
JIM HAMER
DIRECTOR, AUDIT AND EVALUATION

1.0 Introduction

1.1 Authority

The Audit of Business Continuity and Emergency Preparedness was approved by the Clerk as part of the Privy Council Office (PCO) Risk-Based Internal Audit Plan 2009-2010 to 2011-2012.

1.2 Audit Objectives

There were two objectives for this internal audit:

1. To assess the adequacy and effectiveness of mechanisms and capabilities to respond to emergencies in an effective manner to prevent loss of life, and minimize injury and property damage.

   For the first objective, the audit focused on the mechanisms established and capabilities developed for immediate response to emergencies such as fire, smoke, or gas; civil disruptions; and bomb threats.

2. To assess the adequacy and effectiveness of controls in place to achieve effective business continuity ensuring minimal or no interruption to the availability of critical services and assets.

   For the second objective the audit focused on the four elements of a business continuity planning (BCP) program as described in the Treasury Board (TB) BCP Operational Security Standard including:
   - Establishment of BCP program governance;
   - Conduct of a business impact analysis (BIA);
   - Development of business continuity plans and arrangements; and
   - Maintenance of BCP program readiness.

1.3 Audit Scope

Organizationally the audit focused on the Security Operations Division (SecOps), which coordinates the PCO Emergency Management (EM) program. SecOps is located within the Security and Intelligence Secretariat, which reports to the National Security Advisor to the Prime Minister[1]. Other PCO organizational units were included as each Deputy Secretary / Deputy Minister has responsibility for the implementation of their respective business continuity plans during an emergency.

[1] Prior to November 29, 2010 Security and Intelligence Secretariat reported to the Foreign and Defence Policy Advisor to the Prime Minister and Deputy Secretary to the Cabinet.

The audit scope included business continuity planning for departmental interests, i.e. services affecting the PCO mandate, as well as national interests, for example, effective functioning of the Government of Canada, as described in the PCO *Policy on Business Continuity Management*.

The audit scope included an examination of the process PCO followed to identify critical services; however, it did not challenge management's final determination as to what has, or has not, been identified as a critical service. The audit scope did not include arrangements with respect to PCO's role in ensuring the Continuity of Constitutional Government.

All buildings, leased and Crown-owned, occupied by PCO personnel were included in the audit scope; however the focus was on buildings in which PCO is the major tenant.

The audit scope included PCO business continuity and emergency preparedness activities from 2007 to October 2010. At end of the scope period there were a number of initiatives that were planned or underway; outcomes from these initiatives realized after October 2010 were not included in the audit scope.

1.4 Background

The PCO mandate is to serve Canada and Canadians by providing the best professional, non-partisan advice and support to the Prime Minister, the ministers within the Prime Minister's portfolio and the Cabinet. In the event of an emergency, the safety of PCO and Prime Minister's Office (PMO) employees, the protection of assets and the continuity of critical services are paramount. PCO has established an EM program to ensure that policies, plans and procedures are in place to enable PCO to mitigate, prepare for, respond to, and recover from a service disruption, emergency, disaster or crisis with the least impact on the safety and security of PCO/PMO resources. The EM program is also responsible to ensure the uninterrupted delivery of the PCO's critical services in support to the PMO, the Cabinet, and the Clerk.

SecOps coordinates the PCO EM program and must ensure that emergency and business continuity plans (including information technology (IT) contingency plans) and procedures are developed, tested, and kept up to date in order to effectively respond to and recover from emergencies. Each Deputy Secretary / Deputy Minister is responsible for implementing their respective business continuity plans during an emergency.

[*]

1.5 Policy / Legislative Context

A number of legislative and policy directives activate and drive the emergency preparedness and business continuity actions in government departments. This

framework, evolved over a period of several years, shows the changing focus and guidance within the government of Canada.

First, the *Emergency Management Act* (2007) sets out clear roles and responsibilities for all federal ministers across the full spectrum of emergency management. The Act reinforces efforts to ensure that Canada is well prepared to mitigate, prepare for, respond to, and recover from natural and human-induced risks to the safety and security of Canadians.

The *Federal Policy on Emergency Management* (FPEM) was promulgated in December 2009 under the authority of the *Emergency Management Act*. The objective of the FPEM is to promote an integrated and resilient whole-of-government approach to emergency management, which includes better prevention/mitigation of, preparedness for, response to, and recovery from emergencies. The policy promotes an all-hazards approach to emergency management and risk-based emergency management planning. It positions Public Safety Canada as the lead department in coordination of federal government emergency management activities.

In July 2009, the TB *Policy on Government Security* (PGS) was introduced as a replacement for the 2002 *Government Security Policy*. The objectives of the PGS are to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management. To those ends, one of the expected results of the Policy is that continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies.

The *Operational Security Standard – Business Continuity Planning (BCP) Program* was established in 2004 in support of the *Government Security Policy* and continues to be in effect under the new PGS. The Standard organizes the expected BCP program elements under governance, BIA, business continuity plans and arrangements, and BCP program readiness. BCP programs are described as being complimentary to emergency preparedness that is mandated by legislation or government policy (e.g. fire and building evacuation plans; civil emergency plans). The Standard is supplemented by technical documentation that includes suggestions, examples, best practices, and other guidance.

The *Canada Occupational Health and Safety Regulations* Part XVII, include the legislated requirements for safe occupancy of the workplace. The Regulations specify several safety measures that employers, covered by Part II of the *Canada Labour Code,* are required to put in place including: emergency evacuation plans, emergency procedures, instruction and training, and emergency wardens.

The TB *Standard for Fire Safety Planning and Fire Emergency Organization* (Chapter 3.1) guides departments and agencies on planning and organizing for fire emergencies. It identifies the senior officer, defined as the highest ranking official of any

department or agency occupying space in a building, as being responsible for the fire safety plan and emergency organization. In buildings occupied by a number of departments, the senior officer of the department having the largest number of employees (the major tenant) is responsible to prepare and administer the fire safety plan and establish and administer the fire emergency organization. Senior officers from other occupying departments (minor tenants) are expected to cooperate in the formation and operation of the fire safety plan and emergency organization, and for providing necessary fire emergency wardens for the areas occupied by their respective departments.

PCO occupies space in many buildings including Langevin, Blackburn, Postal Station 'B' (PSB), and Hope/O'Brien, where the department is the major tenant and a PCO senior officer has primary responsibility for the fire safety plan and emergency organization. In other buildings occupied by PCO, other departments or agencies are the major tenant. In those buildings, senior officers from the major tenant department or agency take the lead role and the PCO senior officers are expected to operate in a supporting capacity.

In April 2010, the TB *Fire Protection Standard* was introduced as a replacement for the (1994) *Policy on Fire Protection, Investigation and Reporting.* The *Fire Protection Standard* is linked to the TB *Policy on Management of Real Property*. It establishes the requirement for deputy heads to designate a senior official as Departmental Fire Protection Coordinator for the purpose of overseeing the implementation of the Standard. The Departmental Fire Protection Coordinator is responsible to ensure that real property administered by the department complies with applicable fire and building codes; fire protection equipment is inspected, tested and maintained; and compliance with the Directive is monitored.

The PCO *Security Policy*, dated June 2005, was issued under the authority of the Clerk of the Privy Council and Secretary to the Cabinet who, as stated in the Policy, is accountable for safeguarding employees and assets under his/her area of responsibility, and for implementing the *Government Security Policy* (now the PGS). The authority of the Departmental Security Officer (DSO) to oversee the PCO security program is also articulated in the *Security Policy*.

PCO's *Policy on Business Continuity Management* (May 2009) is intended to contribute to the continued availability of critical PCO services, assets and dependencies throughout, regardless of the magnitude of the disruption in service. The Policy points out that, although the overall departmental accountability rests with the Clerk, each Deputy Secretary / Deputy Minister has responsibility for the implementation of their respective business continuity plans during a disruption in service. The PCO BCM program's objective is to support the national interest and the PCO departmental interests, including mandate and business objectives, by assuring the continued delivery of its critical services regardless of the disruption. BCM is described as a fundamental cornerstone of PCO's EM program.

1.6 Terminology

Notes on terminology used in this report:

- PCO describes its business continuity program as a Business Continuity Management Program as opposed to the Business Continuity Planning Program label used in the TB Operational Security Standard. Generally, this report uses the PCO preferred term Business Continuity Management or BCM; however, when referencing the Operational Security Standard or quoting policy, the original terminology is retained.
- For Emergency Preparedness; wherever possible this report describes the findings specific to measures taken by PCO to ensure effective response and recovery from emergencies. However, there are sections where emergency preparedness could not be logically separated from the larger construct of emergency management. Emergency management should be interpreted to include activities designed to prevent and mitigate, prepare for, respond to, and recover from emergencies.

Other key definitions are included in Appendix A.

1.7 Approach and Methodology

The audit was started in July 2010 with a planning phase to develop an understanding of the entity under review – in this case, the organizations responsible for PCO emergency preparedness and BCM. During the planning phase the audit team established audit criteria that were agreed to with management. These criteria are presented in Appendix B. The examination phase was conducted from late August to October, followed by a reporting phase that included presentation and validation of audit results with management and development of the audit report.

The audit team consulted with stakeholder groups involved in emergency preparedness including SecOps and management delegates responsible for leadership of the building emergency organizations in three of the buildings within PCO's main complex, namely Langevin, Blackburn and PSB. Other key stakeholders consulted included representatives of the service provider for property management services (PWGSC) and PCO Administrative Services management.

A short non-statistical telephone survey was conducted involving 17 of 90 volunteer members (i.e. floor wardens) of the building emergency organizations for the Langevin, Blackburn, PSB and Thomas D'Arcy McGee buildings, covering over 20 floors of PCO occupied space. The purpose of the survey was to obtain a "ground-level" perspective from these key participants in PCO's emergency preparedness and response program. Additionally, on-site visits were conducted for these buildings, as well as the Hope/O'Brien building, to observe compliance with policies and regulations.

The audit team further consulted with stakeholders involved in BCM. These individuals included management and staff of SecOps, responsible for the EM program, and functional specialists from Administration, Human Resources (HR), and Informatics and Technical Services (ITSD) Divisions.

A selection of business impact analyses and continuity plans was reviewed and interviews were conducted with business continuity planners and coordinators to assess the effectiveness of procedures followed to develop these documents. PCO Secretariats and Divisions of Corporate Services Branch were selected based on linkages to activities identified in the departmental Program Activity Architecture. This line of inquiry included BIAs and business continuity plans from Operations Secretariat (Operations), Plans and Consultations Secretariat (Communications), Legislation and House Planning and Machinery of Government Secretariat (Cabinet Confidences), Foreign and Defence Policy Secretariat (Security and Intelligence), Senior Personnel & Public Service Renewal Secretariat, and Corporate Services Branch (Administration Division and ITSD).

Approximately 70 documents were requested and made available to the audit team. The documents generally represented a mix of high-level government policy direction, relevant departmental policy, procedures and guidelines and a variety of reports and analyses relevant to the audit objectives.

2.0 Findings, Conclusions, and Recommendations

The audit findings are organized around the two audit objectives: 1) Emergency Preparedness, 2) Business Continuity. Additionally, due to the pervasiveness nature of the topic areas and the potential impact on the organization and staff of PCO, the findings are prefaced with a section titled Organizational Evolution to provide the reader with important contextual information. Since emergency preparedness and business continuity encompass many elements, the audit produced several findings, some positive and some requiring management attention.

2.1 Organizational Evolution

The *Emergency Management Act* (2007) requires emergency plans which include arrangements or other measures to provide for the continuity of the operations of the government institution in the event of an emergency. PCO responded to the requirements of the new legislation and identified EM as a departmental priority in the 2007-2008 Report on Plans and Priorities. In May 2007, the PCO Executive Committee directed that priority be given to addressing the most probable risk situations and to modernizing planning and readiness posture. The Emergency Planning Project Team (EPPT) was established in June of that year to guide the modernization of PCO's BCM program. Reporting to the Assistant Deputy Minister; Corporate Services Branch, the EPPT worked with SecOps and Corporate Services Branch and Secretariat representatives to advance this effort.

In 2008-2009 the EPPT, which had been set up as a “special project team,” was integrated within Security and Intelligence Secretariat’s SecOps Division. Hence, business continuity, fire and occupational health and safety (OHS) as well as the emergency operations came together within the one organization.

The PCO EM program has been developed with the stated objective to ensure that policies, plans and procedures are in place to enable PCO/PMO to mitigate, prepare for, respond to, and recover from a service disruption, emergency, disaster or crisis with the least impact on the safety and security of PCO/PMO resources. The EM program must also ensure the uninterrupted delivery of the organization’s critical services in support to the PMO, the Cabinet, and the Clerk.

SecOps coordinates the PCO EM program and must ensure that emergency and business continuity plans (including IT contingency plans) and procedures are developed, tested and kept up to date in order to effectively respond to and recover from emergencies.

Specifically, SecOps' responsibilities within PCO include:

- managing the physical security program by:
    - controlling and monitoring access to departmental facilities;
    - conducting threat and risk assessments of facilities;
    - ensuring the security design of new or reconfigured accommodation;
    - establishing requirements and measures for safeguarding sensitive information, and providing related training and monitoring;
    - implementing measures for the protection of employees from threats of violence; ensuring security in contracting requirements are met; and
    - conducting security incident investigations;
- maintaining emergency management operations as well as developing strategic plans, awareness and training and exercises in support of business continuity and emergency preparedness for PMO/PCO; and
- managing the BCM program to provide for the continued availability of critical services and functions.

SecOps relies on Corporate Services Branch partners to play important roles to enable achievement of security and emergency responsibilities.

- ITSD's role is to ensure the effective and efficient management of the department's IT assets, including their security and protection.
- The Administration Division has a facilities management role that supports the security program by facilitating physical security of all locations, providing logistical support for emergency management and business continuity alternate site planning; and delivering security of information in mail and messengers services.
- Corporate Information Services Division's role is to provide strategies, services, advice, and training for the protection of and access to essential records that support critical PCO business services and functions.

A key initiative that will have an impact on the PCO EM program and the SecOps organization is the recent approval of funding for certain PCO security related projects. Funding was granted for a number of projects including establishment of a Crisis Management Cell (CMC) to support PCO's emergency response, continuity of operations, as well as continuity of constitutional government. Because resources for these projects were approved near the end of the audit period, the effectiveness of approved projects could not be assessed, though at the time of writing this report, implementation of the CMC was well underway.

2.2 Emergency Preparedness

For the first objective, the audit team looked for evidence to show that management has put in place mechanisms and established capabilities to respond to emergencies in an effective manner to prevent loss of life, and minimize injury and property damage. This was done by examining the way the function is organized and resourced, how performance is measured and improved in response to feedback received, and whether the department is in compliance with applicable federal policies, standards and regulations.

2.2.1 Organization (Governance) and Resources

In this section the audit looked for evidence to confirm that:

- *Processes are in place to plan, organize, direct, and communicate the activities of the emergency preparedness function; and*
- *Sufficient resources at the appropriate level are available to provide service.*

Roles and Responsibilities

The accountability of PCO's DSO for emergency preparedness is rooted in the TB *Policy on Government Security*. The Clerk, as PCO deputy head, is responsible for establishing a security program for the coordination and management of departmental security activities.

The PCO *Security Policy* identifies that responsibility to manage the departmental security program, including EM (and thus emergency preparedness), has been assigned to the Director of Security Operations who also holds the title of DSO. The incumbent DSO has been granted authority to pursue a significant organizational renewal that directly impacts emergency preparedness. Activities are being organized into functional units dealing with physical security, EM operations, and EM planning. [*] key managers responsible for these major business objectives within SecOps have declared their roles as clear, albeit evolving in parallel with the ongoing organizational changes.

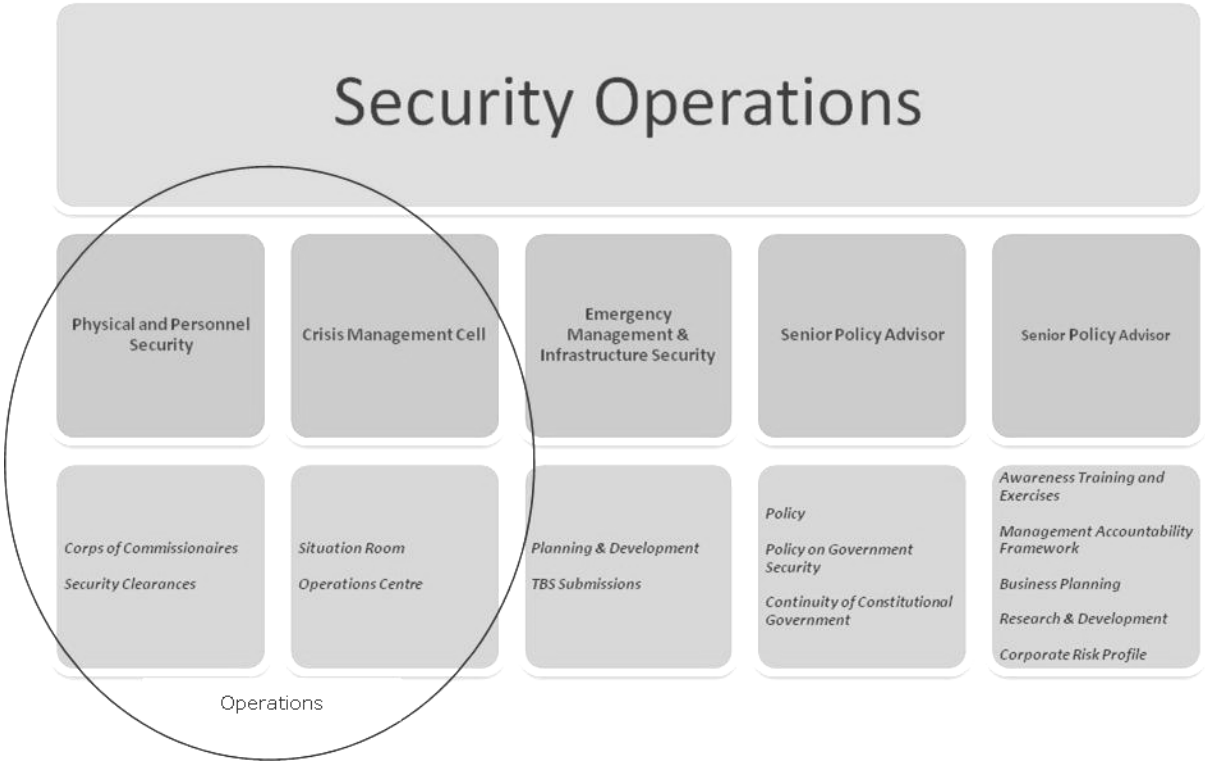
[*]

The *Canada Occupational Health and Safety Regulations* identify the requirements for appointing, instructing, and training chief [building] emergency wardens (CBEWs), deputy emergency wardens, and floor wardens. Collectively these individuals make up the building emergency organizations (BEOs). [*]

The TB *Fire Protection Standard* establishes the requirement for a senior official to be designated by the deputy head as the Departmental Fire Protection Coordinator in order to protect federal buildings and the safety of those who occupy and use such buildings. [*]

Organizational Structure

The entire SecOps Division is being strengthened as and when resources are available. At present, the Director has five direct reports. These include the Physical and Personnel Security Unit, the Crisis Management Cell, the Emergency Management and Infrastructure Security Unit and two Senior Policy Analysts, as in the figure below.



SecOps is moving to an organizational model where the CMC is the operational nucleus, intersecting simultaneously with OHS, BCM, Building Emergency Coordination and Security (i.e. Personnel and Physical Security).

The CMC organization, when fully resourced, will reflect an appropriate structure to allow PCO to address EM response for all-hazards in an integrated and coordinated manner. The CMC's conceptual design updates and extends the previous emergency operations centre model, and is planned to be the hub of the emergency management /response operation as a key linkage between all contributing stakeholders. When complete, the CMC will comprise a situation room for decision makers, an Incident Commander and a PCO Emergency Management Team, complemented by an Operations Room / Centre for data collection and manipulation.

A basic building organizational structure for emergency preparedness (the BEOs) is evolving in PCO occupied buildings. The composition of BEOs is currently tracked by SecOps and BEO member lists for seven buildings are now being posted on the PCO

Intranet; a relatively new improvement. While the coordination and management support for BEOs is not yet fully evident, SecOps is addressing the coordination of PCO's personnel base that is widely dispersed across multiple buildings. One new approach to coordination being considered within the BEO structure is the creation of a Coordination Warden position – a position that would supplement the normal BEO structure. This individual would coordinate staff after evacuation and have a means of communication with the CMC.

Planning and Policy Framework

Strategic direction for emergency preparedness, enmeshed in related issues like security and business continuity, is being actively pursued. For example, a revised go-forward five-year strategy is being presented to PCO Executive Committee for internal requirements. Business requirements have been identified in successive documentation, including a SecOps business case (2009) [*]

SecOps is developing an Emergency Response Concept of Operations (CONOPS) document, which is currently in draft. The CONOPS is intended to provide a generic response template, process, and procedure applicable in all hazardous situations to generate a predictable, timely, and effective response to planned and un-planned events. The CMC will be implemented within that concept and is being designed to incorporate best practices in emergency management as identified by federal policy direction.

Consistent with the government-wide direction, SecOps aims to have a significant proportion of the planning represent all-hazards, with the remainder for very specific threats. Tactical, or contingency plans, have been developed for events such as pandemic and electrical blackout; [*]

The PCO *Security Policy* was created in 2005; the SecOps management team acknowledges that this policy needs review and revision. The *Security Policy* includes a section on Emergency Management and Business Continuity Planning with a reference to a PCO Emergency Management Policy; [*] Other related policies have been recently created, including the PCO *Policy on Business Continuity Management* (May 2009) and the PCO *Policy on Occupational Health and Safety,* which took effect in April 2009.

Directing and Communicating

[*]

[*]

Resourcing

Emergency preparedness is a function ultimately dependent on a sufficiently resourced and properly trained complement of staff. [*] With the recent funding approval, including money for the CMC, it is expected that the department's capacity to effectively respond and recovery from emergencies should be improved.

[*]

A formal needs assessment was conducted and an *Emergency Management and Business Continuity Training Program* was developed, [*]

[*]

2.2.2 Performance Measurement and User-focused Service

In this section the audit looked for evidence to confirm that:

- *Management has practices in place to measure and disseminate the performance of emergency preparedness activities; and*
- *Emergency preparedness services are designed and delivered based on client needs and expectations and evolve in response to client feedback.*

Performance Measurement & User-Focused Service

After-action evaluations and reporting have been diligently conducted following significant exercises or incidents, including lessons learned at the end of the H1N1 pandemic exercises, an incident summary from an incident at the [*] and a report on the June 2010 Ottawa Valley earthquake. That being said, performance measurement and reporting for the EM domain remains quite basic at present.

At PCO, increased sophistication in performance measurement will likely come about as the renewed SecOps organization is more fully implemented. To that end, a logic model has been drafted to accompany the Security Operations strategy document. The draft logic model covers activities, outputs, immediate outcomes, intermediate outcomes and final outcomes to meet the strategic EM outcome.

Some performance data have been collected and reported periodically. For example OHS has produced the gap analysis, referenced in the previous section, which assessed performance against requirements, some of which relate directly to emergency preparedness. Reporting for MAF purposes, such as AoM 19 (Effective Management of Security and Business Continuity), has been done for TBS on a self-assessment basis.

Staff engagement in the building emergency program is seen [*], given the feedback received from 17 floor wardens surveyed.

- [*]
- [*]
- [*]

2.2.3 Policy and Standards Compliance

In this section the audit looked for evidence to confirm that PCO complies with sections of the FPEM relevant to emergency preparedness as well as provisions of Part XVII of the Canadian Occupational Health and Safety Regulations – Safe Occupancy of the Workplace; TB Fire Protection Standard; and TB Standard for Fire Safety Planning and Fire Emergency Organization – Chapter 3.1.

Many areas of emergency preparedness compliance were identified as being under improvement or well in hand. Strides have been taken in improving elements under OHS and fire safety. For example, the audit team observed that, in the Langevin Block, fire protection equipment appeared to be well maintained and tags indicated updated maintenance. Monthly alarm testing was being done by the property manager and a survey was recently conducted to identify persons requiring assistance for evacuation. In the Blackburn Building specifically, bi-monthly workplace health and safety floor inspection reports were being sought and received and a Workplace Emergency Evacuation Plan was successfully finalized in August 2010.

[*]

2.2.4 Conclusion

Many elements of emergency preparedness have been reviewed, studied, and assessed at PCO and recommendations have been made. Some improvements have resulted, [*] Over recent years, experienced and skilled personnel have been brought to PCO to establish a framework and implement required changes to position the department to effectively respond and recover from an emergency or catastrophic event, [*]

One very positive observation made during the audit is that the management team responsible for emergency preparedness is cognisant of the areas that need to be improved and they have already taken steps or have stated that they intend to take actions to improve the situation. Recent funding approval has enabled PCO to move forward in strengthening known areas of weakness, including the creation of the CMC. [*]

2.2.5 Recommendations

All recommendations are directed to the National Security Advisor to the Prime Minister as the senior management lead responsible for business continuity and emergency preparedness.

We recommend that the National Security Advisor to the Prime Minister:

1. [*]

2. Continue progress on performance measurement including development, approval, and implementation of a performance measurement strategy that includes emergency preparedness.

2.3 Business Continuity

For the second objective, the audit team looked for evidence to show that a management framework exists to oversee the planning, organization, control, and direction of the business continuity activity. The audit team assessed if a BIA had been conducted to identify and prioritize the organization's critical services or functions and identify impacts of disruptions. Furthermore, the audit team assessed whether detailed response/recovery plans and arrangements to ensure continuity have been developed, and a permanent maintenance cycle has been established.

2.3.1 Management Framework

In this section the audit looked for evidence that a management framework exists to oversee the planning, organization, control, and direction of the creation, approval, management, and testing of the business continuity activity.

The PCO *Policy on Business Continuity Management* addresses all the required topics and elements to enable successful implementation of the BCM program at PCO. The Policy provides for a high-level set of responsibilities and cites the Operational Security Standard for BCP, while not reiterating all of the TB policy and standard guidance. Specifically, Annex B of the Policy adequately describes BCM responsibilities including the responsibilities of the Clerk, senior management (Deputy Secretaries / Deputy Ministers), the PCO Executive Committee, the DSO, and the BCM Coordinator.

The PCO DSO was appointed to establish and direct the PCO security program, including business continuity planning. The DSO is responsible for coordinating and implementing BCM policy requirements, issues and functions; assigning a BCM Coordinator; and providing strategic advice to both the BCM Coordinator and senior managers on BCM issues.

The PCO Executive Committee is responsible for ensuring an effective state of readiness to mitigate, prepare for, respond to and recover from a business continuity disruption. In that regard, the Committee provides strategic direction and guidance, approves the departmental BCM policy and governance structure, and commits financial and other resources. In addition, the Committee is responsible to review and approve the list of PCO critical services, and to ultimately approve business continuity plans and activities.

Within this governance structure, the Clerk retains overall departmental accountability. In addition, each Deputy Secretary / Deputy Minister has responsibility for the effectiveness and maintenance of their business continuity plans.

The BCM Coordinator position exists, reporting to the Deputy Director Emergency Management and Infrastructure Security. The role of the BCM Coordinator is adequately

described as per the BCP Operational Security Standard. The responsibilities outlined in the PCO Policy include:

- Obtaining senior management support and funding;
- Developing BCM program policy and governance structure;
- Ensuring development of a strategy to communicate BCP activities to employees and stakeholders;
- Establishing working groups and defining their roles and responsibilities as required;
- Ensuring the completion and updating of business impact analysis and maintenance of business continuity plans;
- Ensuring that HR, information management (IM), IT and other continuity plans and arrangements are fully integrated into the BCM program;
- Providing for regular training, review, testing and audit.

It should be noted that the incumbent BCM Coordinator was on [*] leave at the time of the audit and was being replaced by the program officer. The recent return of the BCM Coordinator and the filling of a Manager of Planning position have strengthened SecOps' capacity to support the management framework.

2.3.2 Business Impact Analysis

For BIA, the audit team looked for evidence that a BIA had been conducted to: identify the organization's critical services; rank the order of priority of services or functions for continuous delivery or rapid recovery; and identify internal and external impacts of disruptions.

In 2007-2008 PCO undertook a complete re-work of its BIA. This project was spearheaded by the EPPT under the direction of the Assistant Deputy Minister; Corporate Services Branch. That process resulted in a list of 161 critical PCO services that were reported to the Executive Committee in 2008. Deloitte was engaged to review the process and results, and produced a report for management in June 2008.

The BIA effort featured engagement of a BCP Coordinators and Planners Network consisting of representatives from all PCO units. Secretariat/Branch coordinators and planners were provided templates to help identify their critical services in relation to PCO strategic objectives and strategic outcome. [*] the Network continues to operate and is seen to be functioning well. It places the role of business continuity planning on the organizational units, in line with the PCO Policy on BCM.

The 161 critical services and functions identified in the 2008 BIA process were characterized as High impact [*] /Medium impact [*] /Low impact [*] services or functions. In 2009, the list was revisited and revised to focus on 89 "mission critical" services, including 37 internal services to support the needs of PCO in delivery of other secretariat program services. As stated in the scope section, the audit did not challenge

management's final determination as to what has, or has not, been identified as a critical service. [*]

[*]

While successfully resulting in a BIA report and subsequently business continuity plans, the complexity of the process was reflected in the BIA documentation. The BIA procedure is now being reviewed with the intent of improving its effectiveness by revising templates and questionnaires. SecOps is also looking to acquire BCP software to improve data capture and management reporting.

2.3.3 Business Continuity Plans

In this section the audit team looked for evidence that detailed response/recovery plans and arrangements to ensure continuity have been developed.

Similar to the BIA process, templates were developed and provided to BCP planners and coordinators to generate business continuity plans. The template seems well designed although it has not been used consistently in all cases.

Business continuity plans have been built based on the critical services and functions identified during the BIA process; however due to the large number identified, they represent a huge challenge and recovery effort in a time of crisis. There are a number of reasons for this situation including:

- The all-hazards approach has resulted in business continuity plans which must plan for the worst case scenario. This caused the generation of a larger requirement for each BCP.
- [*]

The business continuity plans examined each have dependencies upon which those plans rely for activation. Those dependencies have not yet been fully explored, analyzed, costed or documented. [*]

Business continuity plans from PCO organizational units are sent to the BCM Coordinator in SecOps once developed and approved within the Secretariat or Branch. [*] Under the *Policy on Business Continuity Management,* the PCO Executive Committee is responsible for approving business continuity plans and activities. Presentations were made to the Executive Committee and SecOps management understood that they had the endorsement of the Executive Committee; [*]

The procedure has been successful in that business continuity plans exist for critical business services and functions in PCO. The BCM procedure was seen by participants as very challenging (long and detailed process) – the all-hazards approach made it quite complex. [*] Such a plan would then facilitate a full analysis of dependencies.

2.3.4 BCP Lifecycle (Maintenance) Process

The audit team looked to determine if management established a permanent maintenance cycle for business continuity plans that have been developed, approved and ready to be put into effect.

The BCP Operational Security Standard calls for the annual review of business continuity plans. Working sessions are conducted with all BCP planners. These sessions consist in sharing information, providing tools and developing awareness. The procedure is not documented; a more formalized and complete approach is presently being formulated.

The BIA and BCP maintenance is performed by each organizational unit at the request of the BCM Coordinator through an annual call letter issued by SecOps. Updated plans are expected in the third quarter of the fiscal year. The update process seemed to be functioning well, as four of the nine plans reviewed for the audit had been recently updated, and another four were dated 2009 - one was undated. Although changes are received by the BCM Coordinator, it is difficult to determine what has changed and who has approved the changed plan. Interviews with the BCP Network representatives revealed that the majority of changes to business continuity plans involve the adjustment of personal, professional, or organizational information.

Exercises have been conducted; [*] The proposed ATE program mentioned in the section on emergency preparedness was intended to include the design, development, and delivery of business continuity exercises. The department wide approach is particularly relevant for PCO given the high number of critical services and functions relative to the size of the department.

[*]

PCO develops and submits reports as requested by Public Safety Canada – a Business Continuity Planning Programs (BCPP) Compliance Report is one such feedback mechanism. No BCPP report was required last year; the 2010 report is being finalized and will be submitted for use in this year’s MAF assessment. Internal reporting and management feedback has not yet been formally arranged, developed and documented. After-event reports are an expected part of the process put forward by Public Safety Canada in their Business Continuity Planning Guide. Analyses are conducted in PCO, though the end reports take a variety of forms.

[*] During most of the audit period, the effort to build and manage the BCM procedure and outputs has been sustained by the Deputy Director EM Planning and the Acting BCP Coordinator; with the return and addition of key individuals this situation has improved. [*]

2.3.5 Conclusion

The BCM framework exists and is based on TB policy. Expectations for senior management support as described in the *Operational Security Standard – Business Continuity Planning* are clearly described in the PCO *Policy on Business Continuity Management*. A BCM Coordinator has been assigned and responsibilities defined. Ongoing organizational changes and the return or addition of key individuals including the BCM Coordinator and the Manager of Planning have augmented the overall BCM capacity.

A procedure exists within PCO to produce both a BIA and related business continuity plans with a set of templates used to analyze business functions and record continuity arrangements. A BCP Coordinators and Planners Network was initiated as part of the overall procedure to ensure the BIAs and BCPs were completed. [*] It is understood within SecOps that, while successful in that the BIA was completed and BCPs delivered for each Deputy Secretary/Branch, the procedure requires refinement.

[*]

2.3.6 Recommendation

3. [*]

3.0 Management Response and Action Plan

Audit of Business Continuity and Emergency Preparedness
The National Security Advisor to the Prime Minister has overall accountability for the Action Plan.

Recommendation	Response and Planned Actions	Responsibility	Due Date
We recommend that the National Security Advisor to the Prime Minister:			
1. [*]	[*] [*] [*] •[*] •[*] •[*] •[*]	Director, Security Operations	4 buildings – major tenant: [*] [*] Other buildings – minor tenant: June 30, 2011 June 30, 2011 June 30, 2011
2. Continue progress on performance measurement including development, approval, and implementation of a performance measurement strategy that includes emergency preparedness.	[*] [*] [*]	Director, Security Operations	Development and Approval June 30, 2011

Recommendation	Response and Planned Actions	Responsibility	Due Date
	• [*] • [*] • [*] [*]		Implementation and validation Dec. 31, 2011
3. [*]	[*] [*] [*] [*] • [*] • [*] • [*]	Director, Security Operations	May 31, 2011 September 1, 2011 March 31, 2012

Appendix A: Key Definitions

Emergency - A present or imminent event, including IT incidents, that requires prompt coordination of actions to protect the health, safety or welfare of people, or to limit damage to assets or the environment. [1]

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 to the effective functioning of the Government of Canada. [2]

Business continuity planning - 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. [2]

Service disruption - A situation [i.e. an emergency] that results in an interruption in the provision of critical services (denied/limited access to people, systems/processes, workspaces). [3]

Preparedness - Measures taken in advance of an emergency to ensure effective response and recovery. [4]

Response - Actions taken during or immediately after an emergency to manage its consequences. [4]

Departmental interest - A service whose compromise in terms of availability or integrity would result in a high degree of injury to the mandate of the Privy Council Office or business objectives as directed by the Clerk. [5]

National interest - 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 to the effective functioning of the Government of Canada. [5]

Sources:
[1] *Emergency Management Act*
[2] Treasury Board, *Policy on Government Security*
[3] PCO Emergency Management Internal Communications Strategy
[4] CSA Standard Z1600-08 Emergency Management and Business Continuity Programs
[5] PCO, *Policy on Business Continuity Management*

Appendix B: Audit Criteria

Audit Objective 1

To assess the adequacy and effectiveness of mechanisms and capabilities to respond to emergencies in an effective manner to prevent loss of life, and minimize injury and property damage.

Category	Audit Criteria
Organization (Governance)	Processes are in place to plan, organize, direct and communicate the activities of the emergency preparedness activity.
Resources	Sufficient resources at the appropriate level are available to provide service.
Performance Management	Management has practices in place to measure and disseminate the performance of the emergency preparedness activities and plans that support decision-making and accountability.
User-focused Service	Emergency preparedness services are designed and delivered based on client needs and expectations, and evolves in response to client feedback.
Policy and Standards Compliance	PCO complies with the relevant provisions of the Federal Policy for Emergency Management. PCO complies with the relevant provisions of: Part XVII of the Canadian Occupational Safety and Health Regulations – (Safe Occupancy of the Work Place), Treasury Board Fire Protection Standard, and 3-1 – Fire Safety Planning and Fire Emergency Organization Standard.

Audit Objective 2

To assess the adequacy and effectiveness of controls in place to achieve effective business continuity ensuring minimal or no interruption to the availability of critical services and assets.

Category	Audit Criteria
Management Framework	A management framework exists to oversee the planning, organization, control, and direction over the creation, approval, management, and testing of the business continuity activity.
Business Impact Analysis (BIA)	A BIA has been conducted to identify the organization's 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.
Business Continuity Plans	Management has ensured that detailed response/recovery plans and arrangements to ensure continuity have been developed.
BCP Lifecycle (Maintenance) Process	A permanent maintenance cycle has been established for business continuity plans that have been developed, approved and ready to be put into effect.