INDIAN AFFAIRS AND NORTHERN DEVELOPMENT CANADA

Audit of Business Continuity Planning

Prepared by:
Audit and Assurance Services Branch

Project #10-12
June 2011

CIDM# 3632670

Table of Contents

INITIALISMS AND ABBREVIATIONS

ADM	Assistant Deputy Minister
BCP	Business Continuity Plan
BCP Coordinators	Regional/Sector BCP Coordinators
BCP Program	Business Continuity Planning Program
BCM Policy	Business Continuity Management Policy Statement
BIA	Business Impact Analysis
DG	Director General
DDSM	Directive on Departmental Security Standard
DM	Deputy Minister
DRIE	Disaster Recovery Information Exchange
OC	Operations Committee
DRSO	Deputy Regional Security Officer
DSO	Departmental Security Officer
EIMD	Emergency and Issues Management Directorate
HRWSB	Human Resources and Workplace Services Branch
IMB	Information Management Branch
INAC	Indian Affairs and Northern Development Canada
ITSD	IT Security Division
MAF	Management Accountability Framework
NCR	National Capital Region
OSS-BCPP	Operational Security Standard – Business Continuity Planning (BCP) Program
PGS	Policy on Government Security
RDG	Regional Director General
TB	Treasury Board
TBS	Treasury Board Secretariat

KEY DEFINITIONS

Business Continuity Plan: Recognizing that some services or products must be continuously delivered without interruption, Public Safety Canada has encouraged a shift from Business Resumption Planning to Business Continuity Planning. A business continuity plan enables critical services or products to be continually delivered to clients. Instead of focusing on resuming a business after critical operations have ceased, or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available.

Emergency Management Plan: Emergency management (EM) refers to the management of emergencies concerning all hazards, including all activities and risk management measures related to prevention and mitigation, preparedness, response and recovery. Public Safety Canada defines an emergency as "an immediate event, including an IT incident that requires prompt coordination of actions concerning persons or property to protect the health, safety or welfare of people, or to limit damage to property or the environment."

Business Resumption Plan: A BRP describes how to resume business after a disruption (source Public Safety Canada, A guide to business continuity planning).

Disaster Recovery Plan: A DRP deals with recovering Information Technology (IT) assets after a disastrous interruption (source Public Safety Canada, A guide to business continuity planning).

EXECUTIVE SUMMARY

Background

Business continuity planning is "a proactive planning process that ensures critical services or products are delivered during a disruption."[1] It is not meant to cover all of an organization's services or activities, but only those deemed "critical" to the continuing operation of an organization.[2] Business continuity planning is not emergency management, but is a related activity. Whereas business continuity planning focuses on continued delivery of services, emergency management focuses more broadly on minimizing damage from an incident and bringing it under control as quickly as possible.

Several events in recent years have illustrated the importance of business continuity planning, including the events of September 11, 2001 and the 2011 earthquake in Japan. Companies with effective business continuity plans (BCPs) were better equipped to resume critical services despite significant human and infrastructure losses.

The Treasury Board (TB) Policy on Government Security (PGS) and Operational Security Standard – Business Continuity Planning Program (OSS-BCPP) establish the requirements for continuity planning in the Government of Canada. This policy makes the Departmental Security Officer (DSO) accountable for directing the overall security program, including the BCP Program.

At Indian Affairs and Northern Development Canada (INAC), the DSO is accountable for all aspects of the departmental security program, including the BCP Program, but responsibility for implementing the program is assigned to the Director, Information Technology Security Division (Director ITSD). A Departmental BCP Coordinator, reporting to the Director ITSD, has been appointed to manage the BCP Program. Reporting to senior management is performed through Operations Committee on a semi-annual basis, or more frequently, as required.

In 2008, the INAC Deputy Minister (DM) approved the INAC Business Continuity Management Policy (BCM Policy), and in May 2009, directed all regions and sectors to develop and test their BCPs. All INAC BCPs were developed and tested by December 2009. In March 2010, the Department identified its critical services and critical support services; a step normally completed before developing BCPs to enable the Department to focus its limited resources on its most critical functions.

[1] Public Safety Canada, A guide to business continuity planning

[2] Critical services are those whose compromise would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada. Critical support services are services essential to ensure the continuity of critical services or that support Senior Management decision-making and interaction with Other Government Departments.

Objectives and Scope

The objective of this audit is to provide assurance on the adequacy and appropriateness of the management control framework and internal controls established for maintaining and operationalizing the Department's BCP Program.

The scope of the audit included the Department's business continuity planning governance framework, BCP Program management controls, including management controls designed to ensure that BCPs are developed, tested and updated as required. The scope of the audit did not include an in-depth assessment of the adequacy of BCPs to ensure continuity of critical services in a disruption; such a determination can only be made through comprehensive testing of the plans.

Findings and Conclusions

INAC senior executives demonstrate strong support for the BCP Program by regularly stressing its importance to region and sector managers. As a result, awareness of the importance of the program is strong and regions and sectors are committed to its implementation. Notwithstanding this commitment, several key elements of the BCP Program are not functioning as intended or are not in place. We have concluded that these control gaps unduly expose the Department to the risk that critical services and critical support services will not resume within targeted recovery times during a disruption.

Roles and responsibilities as defined by the INAC BCM Policy are not consistent with the way the program is actually managed. The OSS-BCPP and INAC BCM Policy both make the DSO functionally responsible to the deputy head for managing the BCP Program. In practice, the Director ITSD manages the program and the DSO does not play a meaningful role.

While the OSS-BCPP only requires departments to develop BCPs for critical services, INAC opted to have all programs and internal services develop and test BCPs in response to the 2009 H1N1 pandemic. At this time, HQ BCP Program staff and Region/Sector BCP Coordinators (BCP Coordinators) were instrumental in supporting the rapid development and testing of BCPs. The Departmental BCP Coordinator and Senior Advisor IT Security invested significant effort in visiting regions and sectors to raise awareness of the importance of business continuity planning and to assist with testing of plans. Notwithstanding this support, the sheer volume of work and compressed timelines necessitated that a template-driven process be employed. As a result, most INAC BCPs were developed by region and sector managers who were not trained in business continuity planning, and without an effective challenge function from the Departmental BCP Coordinator.

In March 2010, INAC identified its critical services and critical support services through an effective department-wide exercise directed by senior executives. While BCPs dating back to 2009 are in place for all critical services and critical support services, plans and arrangements focus predominantly on responding to a pandemic event. At present, there is limited assurance that BCPs for critical services and critical support services are adequate to ensure preparedness for other forms of disruption. The HQ BCP Program staff and managers of most

critical services recognize that a broader assessment of threats and vulnerabilities is required before BCPs can be appropriately updated.

While the HQ BCP Program staff have engaged senior executives in the development of the BCP Program, we found that inadequate reporting was being provided on the state of the program. To better support the deputy head and senior executives in their oversight role, the DSO or Director IT Security needs to be more actively involved in monitoring the BCP Program, and the Departmental BCP Coordinator needs to provide more robust reporting on program implementation.

Recommendations

Our recommendations to the Director ITSD and DSO to address the audit findings are:

1. Develop a multi-year plan that addresses gaps in the BCP Program and present it to an executive committee for review and approval. The planning process should include a reassessment of the program objectives, establishment of measurable goals and targets, development of fully costed strategies to implement the program, and a reassessment of BCP Program governance.

2. Revise the INAC BCM Policy to ensure that roles and responsibilities for directing and reporting on the BCP Program are clear.

3. Ensure that the Departmental BCP Coordinator plays a more active role in advising and challenging managers of critical services and critical support services throughout the process of developing, testing and updating BIAs and BCPs.

4. Develop a formal training and awareness program for BCP Coordinators and managers of critical services (and critical support services). The level of formal training should consider the extent to which the Departmental BCP Coordinator also provides advice and hands-on support throughout the process of developing and testing BIAs and BCPs.

5. Improve monitoring and reporting of the effectiveness of the BCP Program in regions and sectors to support continuous improvement and oversight (e.g., semi-annual reporting to an executive committee on the state of the BCP Program, including significant program gaps, resolution rates for issues identified through BCP testing and disruptions, completion rates for various levels of BCP testing, completion rates for BCP training, etc.).

1. INTRODUCTION

1.1 Context

Public Safety Canada defines business continuity planning as "a proactive planning process that ensures critical services or products are delivered during a disruption."[3] Business continuity planning is not meant to cover all of an organization's services or activities, but only those deemed "critical" to the continuing operation of an organization. Critical services are identified as services whose compromise would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada.

Business continuity planning is a separate, but related activity to emergency management. Emergency management is the discipline of preventing and mitigating emergencies, with emphasis on the preparation, response and recovery from an emergency. Business continuity planning focuses on 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. In effect, business continuity planning ensures critical services can continue to be delivered throughout a disruption, while emergency management seeks to minimize damage and bring the incident under control as quickly as possible.

Several events in recent years have illustrated the importance of business continuity planning. As Public Safety Canada highlights in its guidance on business continuity planning, "September 11, 2001 demonstrated that although high impact, low probability events could occur, recovery is possible. Even though buildings were destroyed and blocks of Manhattan were affected, businesses and institutions with good continuity plans survived."[4] More recently, the H1N1 pandemic was a major catalyst for reviewing and updating business continuity plans throughout the Government of Canada.

The current Policy on Government Security (PGS) does not make explicit reference to the need for departments to implement a Business Continuity Planning Program (BCP Program). However, an expected result of the PGS is that "continuity of government operations and services is maintained in the presence of security incidents, disruptions or emergencies." Further, the Operational Security Standard – Business Continuity Planning Program (OSS-BCPP) is included as a relevant standard for the policy. The OSS-BCPP requires that departments establish a BCP Program and provides direction and guidance on doing so.

1.2 INAC BCP Organization

The Indian Affairs and Northern Development Canada (INAC) Business Continuity Management Policy (BCM Policy) outlines the roles and responsibilities for the BCP Program. These roles and responsibilities are consistent with the requirements of the OSS-BCPP, but are not

[3] Public Safety Canada, A guide to business continuity planning

[4] Ibid.

consistent with the way the BCP Program has been implemented (Figure 1 and Figure 2 on page 6 provide a side-by-side comparison of the BCP organization as it is described in the INAC BCM Policy and how it has been implemented in practice).

Consistent with the OSS-BCPP, the INAC BCM Policy makes the Departmental Security Officer (DSO) accountable for the overall security program, including the establishment of a BCP Program. In practice, responsibility and accountability for managing and directing the INAC BCP Program rests with the Director ITSD, not the DSO. The INAC BCM Policy does not define any roles or responsibilities for the Director ITSD.

A Departmental BCP Coordinator has been appointed at the AS-05 level to manage the BCP Program. The INAC BCM Policy sets out that the Departmental BCP Coordinator functionally reports to the DSO, and provides reporting on the BCP Program to senior management through the Human Resources Workplace Service Committee. In practice, the Departmental BCP Coordinator functionally reports to the Senior Advisor IT Security, who handles all reporting on the BCP Program to senior management through Operations Committee.

Two BCP Analyst positions have been created to support the Departmental BCP Coordinator, but are not yet funded or staffed on a full-time basis. Currently, these positions are filled by contractors on a temporary basis, and funded from the ITSD Operating and Maintenance budget.

Neither the Departmental BCP Coordinator, Senior Advisor IT Security, nor the BCP Analysts are fully dedicated to BCP. Each devotes an estimated one-third of his/her time to BCP activities, with the remainder spent on IT Security-related duties.

Regional/Sector BCP Coordinators (BCP Coordinators) are appointed in each of the Department's 10 regions and 17 sectors to support the implementation, maintenance, and testing of the BCP Program. They perform this function on a part-time basis and have other full-time duties, generally within their regional corporate services functions. Additionally, most BCP Coordinators also act as Regional Security Coordinators on a part-time basis.

Figure 1

INAC BCP Organization as Defined in INAC BCM Policy

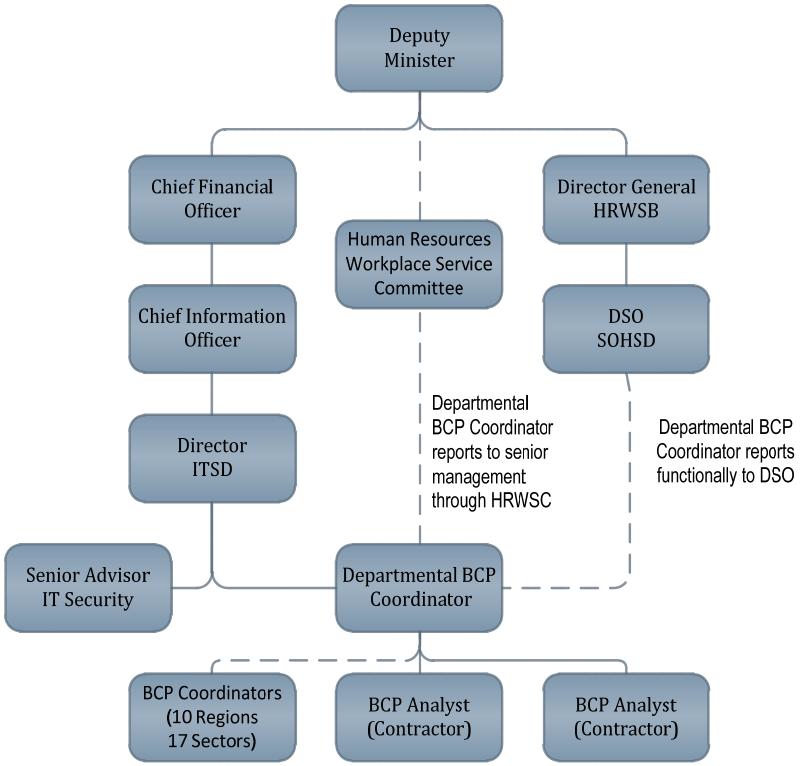
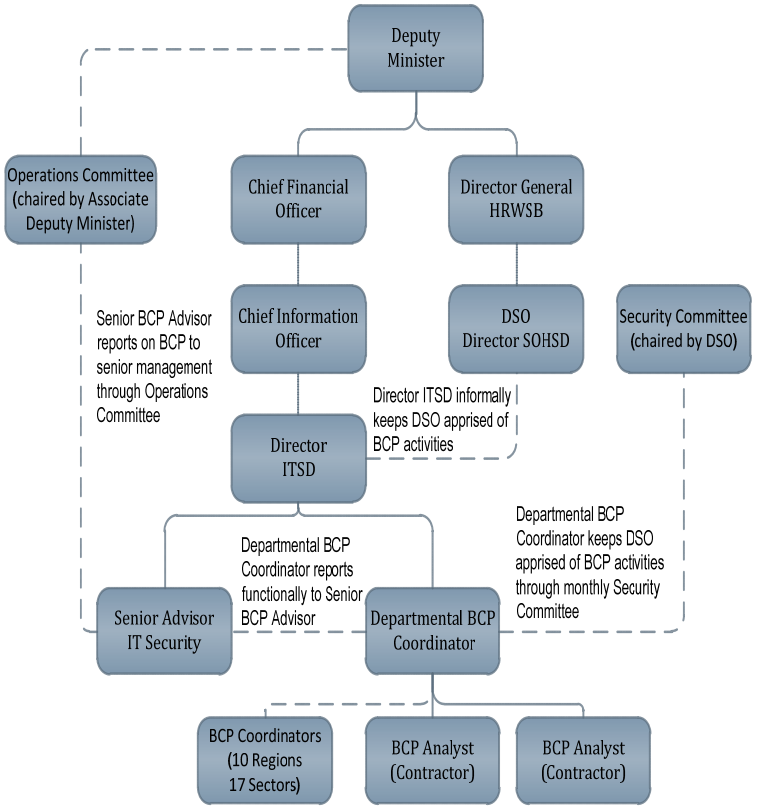


Figure 2

INAC BCP Organization in Practice



1.3 History of BCP Program at INAC

Prior to 2006, the INAC BCP Program resided within the Security Program under the Administrative Services Branch. In May 2006, the Administrative Services Sector was reorganized. As part of the reorganization, the IT Security Division (ITSD) and the BCP Program, along with the Departmental BCP Coordinator and another resource supporting the BCP Program, were split from the Security Program and were assigned to the Information Management Branch (IMB). The remainder of the Security Program (Physical and Personnel security) was assigned to the Human Resources and Workplace Services Branch (HRWSB).

In the fall of 2007, the BCP Program received a Management Accountability Framework (MAF) rating of "Attention Required". Deficiencies identified were:

- No measures in place to provide for the continuity of critical business operations and services;
- BCP Program governance not fully established;
- Critical services not identified and prioritized;
- Development of BCPs and arrangements were in progress but not complete; and
- Significant deficiencies in establishing a maintenance cycle to review, test and audit BCPs.

In August 2008, the INAC Deputy Minister (DM) approved the BCM Policy and a Senior Advisor IT Security was assigned to assist the Departmental BCP Coordinator in the development and implementation of the BCP Program. In February 2009, INAC achieved a score of "Acceptable" in MAF Round VI.

In March 2009, a BCP expert contracted by ITSD completed an assessment of the BCP Program and identified the following gaps:

- Need for strengthened governance around BCP, in line with requirements of the INAC BCM Policy Statement;
- Lack of a BCP training and awareness program;
- Lack of threat, risk and vulnerability assessments to identify vulnerabilities and support the development of BCPs;
- Lack of process to ensure BCPs are regularly updated and tested;
- Lack of effective recovery instructions in BCPs;
- Poor integration of crisis communications, emergency response, and coordinating with external agencies in BCPs; and

- Insufficient testing of the support capabilities of external parties to ensure they can meet INAC's needs.

The results of this assessment formed the basis of the management action plan presented to INAC senior management in response to MAF Round VI.

In May 2009, the DM directed all functions to develop and test BCPs and requested that senior executives be directly involved in the process. Assistant Deputy Ministers (ADMs), Regional Directors General (RDGs) and Directors General (DGs) became active participants in developing Business Impact Analyses (BIA)[5] and BCPs for their functions. A majority of regions and sectors had completed this work by October 2009, and conducted testing in November and December 2009. The Senior Advisor IT Security and Departmental BCP Coordinator visited most regions and sectors at this time to emphasize the importance of the BCP Program and to assist with the testing of plans.

In November 2009, the program again received external validation from Treasury Board Secretariat (TBS) with an "Acceptable" rating in MAF Round VII, and Public Safety Canada awarded its highest score against all criteria in assessing INAC's H1N1 pandemic readiness.

In March 2010, the department identified its critical services, selecting three critical services and nine critical support services; a step normally completed before developing BCPs to enable the organization to focus its limited resources on its most critical functions. The OSS-BCPP supports such an approach, only requiring that BCPs be developed for critical services and critical support services.

2. AUDIT OBJECTIVES AND SCOPE

The objective of this audit is to provide assurance on the adequacy and appropriateness of the management control framework and internal controls established for maintaining and operationalizing the Department's Business Continuity Planning Program.

The audit examined the adequacy and effectiveness of the Department's BCP Program and associated management controls intended to provide assurance that the Department is in compliance with applicable Government of Canada policies, procedures, directives and standards, including the PGS and the OSS-BCPP.

The scope of the audit included the Department's business continuity planning governance framework, BCP Program management controls, including management controls designed to ensure that BCPs are developed, tested and updated as required. The scope of the audit did not include an in-depth assessment of the adequacy of BCPs to ensure continuity of critical services in a disruption; such a determination can only be made through comprehensive testing of the plans.

[5] BIA - A business impact analysis assesses the impacts of disruptions on the department and identifies and prioritizes critical services. It includes a threat and risk assessment to identify potential sources of disruption. BCPs are developed based on the results of the business impact analysis.

3. APPROACH AND METHODOLOGY

This audit was led by Orbis Risk Consulting and was planned and conducted to be in accordance with the *Internal Auditing Standards for the Government of Canada* as set out in the Treasury Board Policy on Internal Audit.

Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the audit conclusion provided and contained in this report.

During the planning phase, preliminary interviews were conducted with BCP Program staff at INAC headquarters, BCP Coordinators from two regions, one RDG, two of three Directors of departmental critical services, and four Directors of critical support services. Program documentation, such as policy documents, meeting minutes, and BIAs and BCPs for critical services were reviewed and analyzed. A risk assessment was conducted to identify and assess the most significant risks to the BCP Program. For each of these risks, the audit team identified mitigating controls they would expect to be in place.

Audit criteria were developed to cover areas of highest risk as well as the requirements of the PGS and OSS-BCPP, and the Generally Accepted Practices of the Disaster Recovery Information Exchange[6] (DRIE). The criteria served as the basis for developing the detailed audit program for the conduct phase of the audit.

The conduct phase included the completion of audit procedures at HQ, as well as three regions and three sectors. The regions and sectors were selected in order to ensure adequate coverage of all three departmental critical services.

Audit fieldwork was conducted between January 2011 and March 2011. The principal audit procedures completed by the audit team included:

- Document Review and Analysis – Documentation examined included, but was not limited to: departmental BCP policies, procedures, and standards; BIAs, BCPs and other related documents for critical services and critical support services; BCP training and awareness materials; and BCP exercise/testing documentation.

- Interviews – For each region and sector, interviews were conducted with managers and staff involved in the BCP Program to gauge their understanding of BCP requirements and the state of the BCP Program.

- Walkabout Survey – Walkabout surveys were conducted in all regions and sectors to assess the BCP awareness levels among staff. When possible, staff working in critical services and critical support services were selected to participate in the survey.

[6] DRIE is a non-profit association of professionals dedicated to the exchange of information on all aspects of business continuity management, from emergency response to the resumption of business as normal.

4. CONCLUSIONS

INAC senior executives demonstrate strong support for the BCP Program by regularly stressing its importance to region and sector managers. As a result, awareness of the importance of the program is strong and regions and sectors are committed to its implementation. Notwithstanding this commitment, several key elements of the BCP Program are not functioning as intended or are not in place. We have concluded that these control gaps unduly expose the Department to the risk that critical services and critical support services will not resume within targeted recovery times during a disruption.

Roles and responsibilities as defined by the INAC BCM Policy are not consistent with the way the program is actually managed. The OSS-BCPP and INAC BCM Policy both make the DSO functionally responsible to the deputy head for managing the BCP Program. In practice, the Director ITSD manages the program and the DSO does not play a meaningful role.

While the OSS-BCPP only requires departments to develop BCPs for critical services, INAC opted to have all programs and internal services develop and test BCPs in response to the 2009 H1N1 pandemic. At this time, HQ BCP Program staff and Region/Sector BCP Coordinators (BCP Coordinators) were instrumental in supporting the rapid development and testing of BCPs. The Departmental BCP Coordinator and Senior Advisor IT Security invested significant effort in visiting regions and sectors to raise awareness of the importance of business continuity planning and to assist with testing of plans. Notwithstanding this support, the sheer volume of work and compressed timelines necessitated that a template-driven process be employed. As a result, most INAC BCPs were developed by region and sector managers who were not trained in business continuity planning, and without an effective challenge function from the Departmental BCP Coordinator.

In March 2010, INAC identified its critical services and critical support services through an effective department-wide exercise directed by senior executives. While BCPs dating back to 2009 are in place for all critical services and critical support services, plans and arrangements focus predominantly on responding to a pandemic event. At present, there is limited assurance that BCPs for critical services and critical support services are adequate to ensure preparedness for other forms of disruption. The HQ BCP Program staff and managers of most critical services recognize that a broader assessment of threats and vulnerabilities is required before BCPs can be appropriately updated.

While the HQ BCP Program staff have engaged senior executives in the development of the BCP Program, we found that inadequate reporting was being provided on the state of the program. To better support the deputy head and senior executives in their oversight role, the DSO or Director IT Security needs to be more actively involved in monitoring the BCP Program, and the Departmental BCP Coordinator needs to provide more robust reporting on program implementation.

5. OBSERVATIONS AND RECOMMENDATIONS

5.1 Program Governance and Management

5.1.1 Senior Management Involvement

Senior management has been actively involved in supporting the BCP Program, but is not receiving sufficient information to support its program oversight responsibilities.

The DM provides strong leadership and actively supports the BCP Program. In August 2008, he approved the INAC BCM Policy and in May 2009, he directed all departmental services and support services, including non-critical services, to develop and test BCPs.

Other senior executives have also been very involved, both through the Operations Committee (OC), chaired by the Associate DM and in their own sectors and regions. Since 2009, the BCP Program has reported to OC on a semi-annual basis and more regularly during periods of increased activity, including eight times before and during the H1N1 pandemic, and three times to assist in the identification and approval of the Department's critical services. Our interviews with staff in all regions and sectors highlighted that most staff are aware of the importance placed on BCP by senior management.

Although significant engagement from senior management has been evident, our audit found that they have not received adequate information on the state of the overall BCP Program. Reporting to senior management has identified some of the most significant gaps in the BCP Program, but has not adequately conveyed the significance of these gaps and resource requirements. As an example, discussions at OC during 2009 revolved primarily around H1N1 preparedness, while significant deficiencies and resource constraints identified in the March 2009 Criticality and Gap Assessment were not highlighted, nor were additional resources requested to address known gaps. The BCP Program indicated that this information was not reported due to the heavy focus on H1N1 pandemic planning at the time, followed by a focus on identifying departmental critical services. While the BCP Program took some action to address a majority of the deficiencies, as we note in the following sections of this report, we found that not all of the actions were adequate to sufficiently address the known deficiencies.

Without an effective and regular results reporting framework in place, senior executives have had little reason to suspect that major program deficiencies exist. The INAC BCP Program received passing grades on MAF in November of 2008 and 2009 (Rounds VI and VII), and from Public Safety in November 2009 for the Department's pandemic readiness work. No significant program deficiencies were identified in these reports.

5.1.2 INAC BCM Policy

Although the INAC BCM Policy aligns to the requirements of the PGS and OSS-BCPP, it needs to be revisited as it is inconsistent with actual roles and responsibilities and the manner in which the program is being implemented.

The INAC BCM Policy is appropriately aligned to the requirements of the PGS and OSS-BCPP, and clearly defines the program's objectives. However, some weaknesses were noted in the area of roles, responsibilities and accountabilities.

The INAC BCM Policy makes the DSO accountable for directing the BCP Program and makes the Departmental BCP Coordinator responsible for reporting to senior management on the current state of the program, but does not define a role or responsibility for the Director ITSD. In practice, the Director ITSD is responsible for directing the BCP Program, and functionally reports to senior management through the Operations Committee. The nature and challenges of this complex reporting structure are not adequately considered in the INAC BCM Policy, and as such, the current policy does not adequately support the effective functioning of the BCP Program.

5.1.3 BCP Program

5.1.3.1 Training and Awareness

Awareness of business continuity planning is strong among executives, but a formal training program is required to ensure BCP Coordinators and managers of critical services have sufficient knowledge to develop adequate BCPs.

The INAC BCM Policy requires that a training and awareness program be implemented by the Departmental BCP Coordinator. High turnover of personnel within the Department and frequent changes to programs, systems and processes make regular training on BCP a necessity at INAC. Our audit found that a formal BCP training and awareness program did not exist, although some awareness activities had been conducted.

Our audit found strong awareness of BCP among senior executives at both HQ and in two of the three regions visited. BCP Coordinators and managers of critical services also demonstrated a strong understanding of the importance of the BCP Program, but generally had not been provided with sufficient training to enable them to develop adequate plans. Of note, two of three regions visited had staff assisting the BCP Coordinator who were Associate Business Continuity Professionals.

The lack of a formal training and awareness program contributed to the deficiencies identified in the business continuity planning controls of the Department and is further detailed in section 6.2 of this report.

5.1.3.2 Support to Regions and Sectors

The Departmental BCP Coordinator has not adequately supported BCP Coordinators and managers of critical services in developing plans for critical services. This gap was being proactively addressed at the time of our audit.

A key responsibility of the Departmental BCP Coordinator is to provide a challenge function to ensure that BIAs and BCPs are adequate. This role is of even greater significance when formal training is not provided to BCP Coordinators and managers of critical services. Our audit found that the Departmental BCP Coordinator did not provide a sufficient challenge function during development of BIAs and BCPs to ensure that plans addressed significant risks and that interrelated plans were well coordinated.

The Departmental BCP Coordinator reviewed the plans of critical services and critical support services, but did not consistently provide feedback to managers and ensure consistency between critical service BCPs and related critical support service BCPs. For example, one critical service BCP identified is a need for access to regional IT applications; however, the related regional IT BCP listed the first priority as shutting down the server. Our audit found a general lack of coordination across plans, and found that plans in all but one region visited were generally inadequate to ensure continuity of service in the event of a significant disruption (discussed in detail in section 6.2.2). Notably, BIAs and BCPs were developed prior to the identification of departmental critical services, and consequently, all BCPs were given equal focus in their development.

A BCP Working Group was created to provide a forum to support the development, testing and maintenance of plans. While this working group met regularly in 2009, it has not met since then.

5.1.3.3 Monitoring and Reporting

Reporting by the Departmental BCP Coordinator to the DSO and senior executive committees has not adequately covered the state of implementation of the BCP Program.

Monitoring of the development of BCPs by the HQ BCP Program staff leading up to the H1N1 pandemic was very strong and helped to ensure that all programs and services had plans in place. Since this time, monitoring has been very limited, particularly as it relates to the plans of critical services and critical support services.

Monitoring and reporting are essential elements of any effective management system, ensuring that a program is functioning as expected and achieving its objectives.

In 2009, the Departmental BCP Coordinator and Senior Advisor IT Security met with BCP Coordinators and managers from most regions and sectors to increase awareness of the BCP Program and to assist with the testing of plans. This approach helped to ensure that all programs and services had BCPs in place and was recognized by Public Safety Canada during their assessment of the INAC's pandemic preparedness.

In 2010, no onsite visits were performed and monitoring activities were limited to tracking the completion of plans. More specifically, monitoring did not include reviews or assessments of the quality of plans, sufficiency of testing and exercises, or other measures of plan effectiveness. Onsite visits were resumed in 2011 on an ad hoc basis, but no plan or schedule is in place to ensure that all critical services and critical support services will be covered.

The BCP Program briefs senior management through Operations Committee on its current activities and solicits input on important aspects of the program (e.g., identification of departmental critical services). However, limited reporting has been provided to senior executives on the overall state of the BCP Program. Some examples of the type of reporting not provided to senior management include gaps in the BCP Program (and plans to address them), assessments of the adequacy of BCPs for critical services and critical support services, and significant risk exposures that are not being mitigated by existing BCPs and arrangements.

5.2 BCP Plans and Arrangements

5.2.1 Identification of Critical Services

The Department has recently identified its critical services with adequate input from the Deputy Minister and senior executives.

The process used in identifying critical services was generally adequate.

In October 2009, the Departmental BCP Coordinator compiled the results of all BIAs, identifying over 100 potential critical services. This listing was aggregated and refined by the Departmental BCP Coordinator, and in December 2009, a revised list of 14 critical services was presented to OC. OC challenged the services identified and directed the Departmental BCP Coordinator to further refine the list and vet the critical services with other government departments.

In March 2010, the final listing of three critical services and nine critical support services was approved by OC. These services were identified based on the PGS definition of a critical service and guidance from the OSS-BCPP. The PGS definition outlines the requirements for a service to be deemed critical and OSS-BCPP allows departments to set a Maximum Allowable Downtime to serve as the basis for determining which services are critical. INAC has set its threshold at 24 hours (i.e., services that cannot be down for longer than 24 hours are deemed critical). Our audit found the process that the Departmental BCP Coordinator and senior executives employed for identifying critical services was appropriate.

While the process for identifying critical services at the departmental level was generally adequate, we found that regions and sectors had not revised their BIAs and BCPs to align with the final list of departmental critical services. More specifically, regions and sectors had many services identified as critical that were not on the departmental list, and all three regions visited had not developed plans for at least one of the departmental critical services or critical support services.

5.2.2 Development of Business Continuity Plans

5.2.2.1 Process for Developing Business Continuity Plans

The INAC BCP Program was successful in developing and testing a large volume of plans in a short period of time leading up to and during the H1N1 pandemic. The process for developing plans was rushed and insufficient time and process were devoted to identifying other potential business interruptions and developing alternate recovery strategies.

There are several key steps that must be performed to develop an effective BCP. First, an organization must identify its critical services, define recovery timelines and requirements, and conduct a threat, risk and vulnerability assessment. Second, alternative strategies to recover from disruptions must be developed and assessed, with the most appropriate strategies being included in the BCP. Next, comprehensive plans are developed and documented, providing sufficient detail to allow someone unfamiliar with the business operations to resume services during or after a disruption. Lastly, necessary arrangements are made to ensure that plans can be readily implemented in the event of a disruption.

All INAC regions and sectors developed BCPs in a short period of time leading up to and during the 2009 H1N1 pandemic, prior to INAC having identified its departmental critical services. As over 100 plans were completed in this six-month period, it was necessary for the process to be template-driven, with limited involvement of the HQ BCP Program staff and Departmental BCP Coordinator. As a result several key steps were missed or performed inadequately.

Although the Departmental BCP Coordinator developed a strong Threat and Risk Assessment Framework in June 2009, the framework was not distributed to BCP Coordinators or managers of critical services and remains in draft form. Our interviews indicated that while managers of critical services and critical support services did attempt to consider likely threats and vulnerabilities when developing their BCPs, this process was generally ad-hoc and not documented. One of the three critical services did conduct a formal risk assessment for emergency management purposes, but did not fully address all significant threats of business disruption. As a result, there is limited assurance that BCPs for critical services and critical support services adequately address the most likely and significant threats.

We also found that the processes for identifying and selecting alternate recovery strategies were informal and not documented. Plans for critical services and critical support services did not include multiple strategies for recovery, and none of the regions or sectors could provide documentation of the process used in evaluating and selecting strategies. By not adequately documenting these discussions and not having a structured process in place, there is limited assurance that the best and most cost-effective solutions have been chosen and implemented. This lack of documentation also makes it very difficult for new managers to understand why recovery strategies were chosen by their predecessors, and can lead to significant additional work in the future.

5.2.2.2 State of Completion of Business Continuity Plans for Critical Services

Bearing in mind that INAC has only recently identified its critical services, BCPs supporting two of the three departmental critical services are not adequate to address disruptions other than a pandemic outbreak. Our interviews with managers of critical services and critical support services indicated that many aspects of their continuity plans were unwritten and not included in their BCPs (e.g., operating procedures not referred to in BCP).

While BCPs for critical services and support services were generally appropriate to satisfy their original purpose of ensuring continuity during a pandemic event, other potential disruptions were not adequately considered or addressed. By extension, it is uncertain whether the current recovery strategies are appropriate and whether all necessary arrangements are in place. There were three exceptions to these findings: firstly, the department's communications plans are well developed, having recently been updated to address lessons learned from disruptions; secondly, one of the regions visited had well developed and integrated critical service and critical support services plans; and thirdly, the BCP of one departmental critical service was well developed.

Our audit found that the standard BCP process and template suggested by the HQ BCP Program are appropriate for general pandemic planning, but overly simplified for complex critical services. BCPs that followed the INAC template generally provided only vague guidance and did not reference any other operating procedures. For two of the three departmental critical services, regional and HQ BCPs contained insufficient procedures to permit timely recovery and resumption of services. Our interviews with managers of critical services indicated that their ideas and unwritten plans for responding to business interruptions were better developed than their written plans indicated.

We found that the dependencies of departmental critical services were not generally considered or addressed in the plans of critical support services. For example, the identified IT needs of two of the three departmental critical services were not addressed or considered in the region or HQ IT BCPs.

Over the course of our audit, the HQ BCP Program began working more closely with a critical service to support the update of its BCPs and to ensure that critical support services understand and address the needs of EIMD in their own BCPs. This close interaction between the Departmental BCP Coordinator and managers of critical services and critical support services is important for ensuring that managers understand and appreciate the importance and characteristics of good business continuity planning.

5.2.3 Testing of Business Continuity Plans

Tabletop testing of an H1N1 Pandemic scenario was completed department-wide in 2009.Testing of other scenarios and more in-depth exercises that would be reasonably expected for critical services have not yet been performed.

Testing of BCPs allows managers to identify deficiencies and gaps, and to ensure readiness for potential disruptions. To be effective, the rigour of testing must be incremental, simulating increasingly complex scenarios and gradually moving from tabletop exercises[7] to an integrated, full interruption test[8]. Debriefings should be held after all exercises and lessons learned documented in After Action Reports to allow current and future managers to improve upon their plans.

Our audit found that the H1N1 pandemic scenario testing completed by all regions and sectors in October and November 2009 was appropriate for the circumstances and adequate as an initial test. This testing consisted of a basic tabletop exercise simulating an H1N1 pandemic scenario and included testing of remote connectivity capabilities for two of the three critical services. No testing was conducted in 2010. Additional testing was planned at the senior executive level in 2010 but has been delayed to later in 2011.

More complex testing of alternate scenarios is required to fully evaluate BCPs for critical services and ensure readiness to respond to potential disruptions. The Departmental BCP Coordinator distributed a good testing template to all regions and sectors in September 2009 to guide testing and to ensure that test results were formally documented. However, managers and staff interviewed demonstrated little understanding of the requirements for testing and were generally ill-equipped to test their plans. While we observed instances of the testing template being used in all three regions visited, insufficient information was documented to preserve testing results and to allow for meaningful evaluation and follow-up.

We found that the Departmental BCP Coordinator and BCP Coordinators do not hold managers of BCPs accountable by tracking and reporting on testing and the resolution of identified gaps. In two of three regions visited, we observed BCPs that had not been revised to address all approved actions.

6. RECOMMENDATIONS

Our recommendations to the Director ITSD and DSO to address the audit findings are:

1. Develop a multi-year plan that addresses gaps in the BCP Program and present it to an executive committee for review and approval. The planning process should include a reassessment of the program objectives, establishment of measurable goals and targets, development of fully costed strategies to implement the program, and a reassessment of BCP Program governance.

[7] A tabletop exercise is a structured walk-through exercise that simulates an incident in an informal environment. This is usually accomplished in a three to four hour session with the participants gathered in a boardroom or training room.

[8] A full interruption test includes a simulated recovery under a “worst case” scenario. The test also includes critical support service, external service providers, first responders and other partners on which the critical service relies.

2. Revise the INAC BCM Policy to ensure that roles and responsibilities for directing and reporting on the BCP Program are clear.

3. Ensure that the Departmental BCP Coordinator plays a more active role in advising and challenging managers of critical services and critical support services throughout the process of developing, testing and updating BIAs and BCPs.

4. Develop a formal training and awareness program for BCP Coordinators and managers of critical services (and critical support services). The level of formal training should consider the extent to which the Departmental BCP Coordinator also provides advice and hands-on support throughout the process of developing and testing BIAs and BCPs.

5. Improve monitoring and reporting of the effectiveness of the BCP Program in regions and sectors to support continuous improvement and oversight (e.g., semi-annual reporting to an executive committee on the state of the BCP Program, including significant program gaps, resolution rates for issues identified through BCP testing and disruptions, completion rates for various levels of BCP testing, completion rates for BCP training, etc.).

7. MANAGEMENT ACTION PLAN

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
1. Develop a multi-year plan that addresses gaps in the BCP Program and present it to an executive committee for review and approval. The planning process should include a reassessment of the program objectives, establishment of measurable goals and targets, development of fully costed strategies to implement the program, and a reassessment of BCP Program governance.	The Director, ITSD – in collaboration with the DSO – will: • Conduct an organizational assessment to determine the best-fit placement of the function, and options for management consideration regarding changes to program governance for improving the effectiveness of the program. Assessment will include capacity options given current state (eg. BCP Coordinator position is currently vacant), and the training requirements associated to BCM-related responsibilities. • Develop a 3 year tactical plan which prioritizes and addresses the identified gaps within the Business Continuity Management (BCM) file commensurate with the risk each gap presents, and present the plan to the Departmental Operations Committee (DOC) for approval. This plan will include: i. Establishment of	Director ITSD and DSO	

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	measureable goals/targets ii. Development of fully costed strategies and options for DOC consideration (human resources, systems, etc) **<u>Actions</u>** • Draft of organizational assessment for circulation and comments • Draft of tactical plan for circulation and comments • Presentation of organizational assessment and tactical plan including viable options to DOC		End Q2, 2011-12 Mid Q3, 2011-12 End Q3, 2011-12
2. Revise the INAC BCM Policy to ensure that roles and responsibilities for directing and reporting on the BCP Program are clear.	The Director, ITSD – in collaboration with the DSO – will: • Consult with key stakeholders, including but not limited to: the three (3) Critical Service program areas, a sample of Critical Support Service program areas and Regions, Communications, and Public Safety Canada to refresh roles and responsibilities pertaining to BCM.	Director ITSD and DSO	

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	• Update the BCM Policy to reflect: updated roles and responsibilities, mandatory seniority level of BCM representation in Regions and Sectors, and input from organizational assessment (Item #1 above), including the more explicit definition of the BCP Coordinator's challenge function identified within Item #3. **<u>Actions</u>** • Begin consultations with key stakeholders • Updated BCM policy presented to DOC for approval		 Mid Q2, 2011-12 Mid Q4, 2011-12
3. Ensure that the Departmental BCP Coordinator plays a more active role in advising and challenging managers of critical services and critical support services throughout the process of developing, testing and updating BIAs and BCPs.	Director, ITSD – in collaboration with the DSO – will: • Working with Communications, develop a communication plan to ensure that the authority of the new BCP Coordinator is readily shared with all stakeholders in the department. Emphasis will be placed on the advisory services provided by	Director ITSD and DSO	

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	the BCP Coordinator. • Implement operationalized processes based on new BCM policy similar to IT Security Certification and Accreditation process (CIO, DSO, and DG of responsible program area will need to formally sign off on yearly BIA/BCP updates) for existing Critical Services and Critical Support Services. This process will include a provision by which the CIO and DSO will not endorse the signoff of BIA/BCP without appropriate endorsement by BCP Coordinator. • Other actions as necessary will be developed and implemented, based on direction set by DOC as related to organizational assessment and tactical plan options outlined in Item #1. **<u>Actions</u>** • Communication Plan developed • Updated BIA/BCP sign off process designed and developed, presented in		End Q3, 2011-12 Mid Q4, 2011-12

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	conjunction with BCM refreshed policy to DOC.		
4. Develop a formal training and awareness program for BCP Coordinators and managers of critical services (and critical support services). The level of formal training should consider the extent to which the Departmental BCP Coordinator also provides advice and hands-on support throughout the process of developing and testing BIAs and BCPs.	Director, ITSD – in collaboration with the DSO – will: • Consult with Public Safety to determine if new training and awareness products are available for use by client departments. • Review existing BCM-related material available to the department (such as the Institute for Continuity Management or the Canada School of Public Service) and establish baseline mandatory and/or recommended training for BCM-related roles, in consideration of DOC guidance provided regarding Item #1. • Other actions as necessary will be developed and implemented, based on direction set by DOC as related to organizational assessment and tactical plan options outlined in Item #1. *Note: INAC's BCP Awareness/Training approach was approved by Public Safety during H1N1 – ie. providing templates and*	Director ITSD and DSO	

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	being available for consultation on an "as needed basis". However, we do agree with the audit results that a more comprehensive approach, particularly for Critical Services and Critical Support Services would continue to mature the BCM function and increase the effectiveness of BCP-efforts. **<u>Actions</u>** • Consultation with Public Safety • Formalize training material for managers of Critical Services and Critical Support Services • Integrate training coverage as part of reporting process implemented for Item #5.		End Q1, 2011-12 Beginning Q4, 2011-12 Beginning Q4, 2011-12
5. Improve monitoring and reporting of the effectiveness of the BCP Program in regions and sectors to support continuous improvement and oversight (e.g., semi-annual reporting to an executive committee on the state of the BCP Program, including significant program gaps, resolution rates for issues identified through BCP testing and	Director, ITSD – in collaboration with the DSO – will: • Build upon the policy update (Item #2) and operationalized process development (Item #3) to ensure that biannual updates are provided across Regions	Director ITSD and DSO	

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
disruptions, completion rates for various levels of BCP testing, completion rates for BCP training, etc.).	and Sectors which are signed off at a sufficiently senior level (DG or above), including training coverage. • Develop a "scorecard" for Critical Services and Critical Support Services (NCR and Regionally) and provide to responsible DGs on a biannual basis, which considers: o Existing BCM gaps – BIA/BCP completion rates and completeness of plans o Status of testing (exercises) o Post mortems (both testing and post-events) **Actions** • Pilot Critical Service is identified, with review in Q1 2012 • Rollout to remaining Critical Services and Critical Support Services throughout 2012		Mid Q4 , 2011-12 FY 2012

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
	• Aggregation of scorecards presented to DOC biannually, beginning in early 2012.		FY 2012

Appendix A: Audit Criteria

Audit Criteria and Controls	Reference (See last page for acronyms)
BCP Program Governance	
1. A departmental BCP Program is in place with appropriate and clearly defined objectives, roles, responsibilities and accountabilities.	OSS-BCPP 3.1
1.1. Adequate BCP policy, operational security standards and technical documentation are developed within the department or adapted from GoC policy. BCP policy has been approved by senior management, and describes key roles and responsibilities for managing the organization's BCP activities, and the organization`s approach to conducting BIAs, developing plans and arrangements, and maintaining readiness.	OSS-BCPP 3.1 BCPP CR 1.3
1.2. The DSO directs and coordinates the BCP Program.	OSS-BCPP 3.1
1.3. A Departmental BCP Coordinator has been formally appointed to fulfill roles and responsibilities established in the Operational Security Standard – Business Continuity Planning Program.	OSS-BCPP 3.1 BCPP CR 1.1
1.4. A BCP working group has been appointed by senior management, has had appropriate roles and responsibilities defined, meets regularly and presents to the Executive Committee on a regular basis.	OSS-BCPP 3.1 BCPP CR 1.4
1.5. The Departmental BCP Coordinator maintains regular communication on, and coordination of, BCP activities with the IT Security Coordinator and Departmental Security Officer (DSO).	OSS-BCPP 3.1
2. Senior management actively and appropriately supports the development and implementation of the BCP Program.	OSS-BCPP 3.1 BCPP CR 1.2
2.1. Senior management is responsible for supporting, overseeing, directing, approving and funding the development, implementation and testing of the Business Continuity program, policy, plans, activities and arrangements.	OSS-BCPP 3.1 BCPP CR 1.2
2.2. Sufficient financial and other resources are committed to BCP.	OSS-BCPP 3.1 BCPP CR 1.2 BCPP CR 3.2

Audit Criteria and Controls	Reference (See last page for acronyms)
Business Impact Analysis	
3. The department's business and critical services have been identified and a Business Impact Analysis conducted.	OSS-BCPP 3.2
3.1. Processes exist to determine the nature of the department's business (e.g. role, mandate) and the services it must deliver according to its constituent or other legislation, government policy, obligations to other departments, and service sharing arrangements, treaties, contracts, memoranda of understanding or other agreements.	OSS-BCPP 3.2 BCPP CR 2.1
3.2. Critical services have been identified and prioritized based on: ▪ Minimum Service Levels (MSL); ▪ Maximum Allowable Downtimes (MAD); ▪ Recovery Point Objectives (RPO); and ▪ Recovery Time Objectives (RTO).	OSS-BCPP 3.2 BCPP CR 2.2 DDSM App. C GAP 3 ST3.4
3.3. A recent threat and risk/vulnerability assessment has been performed for critical services to identify and assess: ▪ All potential sources of disruption; ▪ The direct and indirect impacts of disruptions on the department; and ▪ Degrees of injury to Canadians and the government in the event of their disruption.	OSS-BCPP 3.2
3.4. Dependencies that support critical services directly or indirectly, both internally and externally to the department have been identified.	OSS-BCPP 3.2 BCPP CR 2.3
3.5. Senior management reviews and approves the departmental Business Impact Analysis.	OSS-BCPP 3.2 BCPP CR 2.4
Business Continuity Plans and Arrangements	
4. Business continuity and recovery strategies have been identified, assessed, selected and approved for each critical service.	DDSM App. C OSS-BCPP 3.3
4.1. Business continuity and recovery options have been identified for all critical services.	OSS-BCPP 3.3 BCPP CR 3.2
4.2. An assessment of each option has been performed, considering impacts on the department, benefits, risks, feasibility, capacity requirements, and cost.	OSS-BCPP 3.3 GAP 6 ST62.1

Audit Criteria and Controls	Reference (See last page for acronyms)
5. Business continuity plans are developed to support the implementation of approved strategies and are consistent with policy requirements.	PGS 5 OSS-BCPP 3.3
5.1. Business continuity plans are developed identifying: ▪ Critical services, information assets, and dependencies identified in the Business Impact Analysis; ▪ Approved continuity and recovery strategies; ▪ Measures to deal with the impacts and effects of disruptions on the department; ▪ Response and recovery teams, including membership and contact information; ▪ Roles, responsibilities and tasks of the teams, including internal and external stakeholders, and clearly identify organizational authorities and replacements; ▪ Resources and procedures for continuity of service; ▪ Coordination and reporting mechanisms and procedures, including processes to liaise with other departments, agencies and first responders as necessary to coordinate BCP; ▪ Authority for activation of BCP (GAP 6 ST1.2); ▪ Emergency Operation Centres at all levels (local, regional and national) (GAP 5 ST2.7); and ▪ Procedures for evacuation and sheltering in place (GAP 5 ST2.8).	OSS-BCPP 3.3 GAP 5 ST2.7 GAP 5 ST2.8 GAP 6 ST1.2
5.2. All single points of failure have been identified and addressed in business continuity plans.	GAP2 ST3
5.3. Adequate communications plans and materials are developed to support crisis communications with employees, business partners, vendors, government, external media and other key stakeholders.	OSS-BCPP 3.3 GAP 9 ST1 GAP 9 ST2
5.4. Senior management reviews, approves and funds selected continuity plans, including review and approval of third party plans.	OSS-BCPP 3.3
5.5. BCPs are available in readily accessible location(s) and format(s) in the event of a disruption.	GAP 3 ST3.6

Audit Criteria and Controls	Reference (See last page for acronyms)
6. Arrangements are completed to ensure that plans can be put into effect, and where necessary, formal contracts or MOUs are in place.	OSS-BCPP 3.3 BCPP CR 3.6
6.1. All necessary arrangements have been completed and formalized to ensure that plans can be put into effect, and where necessary, contracts or MOUs are in place to formalize arrangements and establish priorities for access amongst competing interests.	OSS-BCPP 3.3 BCPP CR 3.6
6.2. Where departments and/or third parties share in the delivery of a critical service, arrangements exist to ensure that the plans of the sharing departments are concerted.	OSS-BCPP 3.3 BCPP CR 3.6
Maintenance of BCP Program Readiness	
7. An effective training and awareness program for BCP is in place.	OSS-BCPP 3.4 BCPP CR 3.5
7.1. The Departmental BCP Coordinator has been appropriately trained to undertake the functions and responsibilities assigned.	OSS-BCPP 3.4 BCPP CR 3.5 GAP 7
7.2. An appropriate BCP training (including cross-training) and awareness program is in place, is documented, includes a training and awareness plan, and has been delivered to all levels of the organization.	OSS-BCPP 3.4 BCPP CR 3.5 GAP 7
7.3. BCP training (including cross-training) and awareness is continually reinforced, periodically verified and validated.	OSS-BCPP 3.4 BCPP CR 3.5 GAP 7
8. Business Continuity Plans are reviewed and updated on a regular basis.	OSS-BCPP 3.4 BCPP CR 4.1
8.1. Processes exist to ensure BCPs are updated and validated for any changes such as contact lists, new programs, strategic planning frameworks, legislative changes, and physical relocations and reviewed annually by management and the BCP Coordinator.	OSS-BCPP 3.4 BCPP CR 4.1
8.2. An up-to-date inventory of critical services and associated information, assets and dependencies is maintained and provided to Public Safety Canada as requested.	DDSM App. C
9. Business Continuity Plans are regularly tested and validated through exercises to ensure efficient and effective response and recovery.	OSS-BCPP 3.4 DDSM App. C
9.1. Testing and validation of all plans occurs on a regular basis and includes stress testing and exercise documentation.	OSS-BCPP 3.4 BCPP CR 4.3
9.2. An After Action Report and action plan are prepared following all exercises and any disruptions, and action plans have been approved by senior management and implemented.	OSS-BCPP 3.4 BCPP CR 4.4

Audit Criteria and Controls	Reference (See last page for acronyms)
9.3. Business Continuity Plans are revised to reflect lessons observed.	OSS-BCPP 3.4 BCPP CR 4.4
10. Where identified as necessary, Emergency Operations Centres (EOCs) and alternate sites are supplied and maintained in a ready state.	GAP 5 ST2.10 GAP 5 ST2.11
10.1. Procedures exist to ensure emergency supplies and resources are acquired and maintained for EOCs and alternate sites.	GAP 5 ST2.10 GAP 5 ST2.11
11. The Departmental BCP Coordinator monitors all activities of the BCP Program, including BIAs, BCPs, exercises, After Action Reports, and training and awareness programs.	GAP 3 GAP 6 GAP 7
11.1. The Departmental BCP Coordinator reviews all BIAs to ensure completeness of justifications and specifications (MSLs, MADs, RTOs, and RPOs).	
11.2. The Departmental BCP Coordinator reviews all BCPs to ensure completeness and currency of content.	
11.3. The Departmental BCP Coordinator reviews all exercise materials and After Action Reports for appropriateness and completeness.	
11.4. The Departmental BCP Coordinator monitors training and awareness activities to verify they have been delivered as scheduled.	

Acronyms related to TBS references:

BCPP CR: Business Continuity Planning Program (BCPP) Compliance Report – Government of Canada PGS
DDSM: Directive on Departmental Security Management, issued July 2009
OSS-BCPP: Operational Security Standard, Business Continuity Planning (BCP) Program, issued 2004
PGS: Policy on Government Security (PGS), issued July 2009
PSEPC: Public Safety and Emergency Preparedness Canada Guide to Business Continuity Planning

Acronyms related to DRIE GAP:

GAP 2: Generally Accepted Practices – Risk Evaluation and Control
GAP 3: Generally Accepted Practices – Business Impact Analysis
GAP 5: Generally Accepted Practices – Emergency Response and Operations
GAP 6: Generally Accepted Practices – Developing and Implementing BC Plans
GAP 7: Generally Accepted Practices – Awareness and Training
GAP 9: Generally Accepted Practices – Public Relations and Crisis Coordination
GAP 10: Generally Accepted Practices – Coordination with External Agencies