Canada Border Services Agency

[Home](#) □ [About the CBSA](#) □ [Corporate documents](#) □ [Audit and Evaluation Reports](#)

Audit Report

Audit of Business Continuity Planning

December 2016

Note

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

Table of contents

1.0 Introduction [1]

Emergency Management is a key function of the Government of Canada that is legislated by the *Emergency Management Act* (the Act). The function ensures the safety and security of Canadians through the management of all-hazard emergencies [2]. Business Continuity Planning (BCP) is complementary to Emergency Management planning, where BCP focuses on the internal efforts [3] to ensure the continued availability of critical services and recovery from disruption events and Emergency Management planning focuses on the external [4] environment [5].

BCP refers to 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 [6]. Critical services and assets are "those 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 function of the Government of Canada" [7].

The requirements for BCP are primarily established in the *Emergency Management Act*, Treasury Board *Policy on Government Security*, *Operational Security Standard – BCP (OSS-BCP)* and *Operational Security Standard – Management of Information Technology Security*. The *Public Safety Guide to BCP* also provides a summary and general guidelines for BCP. The Act, policy, and operational standards provide guidance to departments in developing business continuity processes that support departmental objectives. In addition, they define roles, responsibilities and accountabilities for departments and Lead Security Agencies. For the purpose of this audit, Lead Security Agencies are departments who have a role in providing government-wide advice and guidance on business continuity planning, and include Privy Council Office, Public Safety, and Treasury Board Secretariat.

The OSS-BCP outlines that a BCP Program (the Program) is composed of four elements [8]:

1. The establishment of BCP Program governance.
2. The conduct of a business impact analysis, which is used to assess the impacts of disruptions on the department and to identify and prioritize critical services and associated assets.
3. The development of business continuity plans and arrangements.
4. The maintenance of BCP Program readiness.

The objective of the Canada Border Services Agency (the CBSA or the Agency) BCP Program is to achieve effective coordination for the continued availability of critical services in the event of a service disruption [9]. At the CBSA, the BCP Program is managed by the Security and Professional Standards Directorate, within the Comptrollership Branch, and carried out by critical service managers across the Agency. Critical service managers are those responsible for identifying critical services and developing, exercising and maintaining plans and arrangements for their critical services. They are also responsible for the activation and deactivation of their plans in the event of a disruption. The Business Continuity Management (BCM) team, within the Security and Professional Standards Directorate, is responsible for:

- establishing program governance;

- developing and maintaining the CBSA BCM policy;
- developing tools and templates for critical service managers to use in preparing their Business Impact Analysis (BIA) and Business Continuity Plan (BCP);
- ensuring BCPs are in place for critical services;
- coordinating the update process for BCPs;
- providing advice and guidance on the development of business impact analyses and BCPs; and
- maintaining program readiness.

To support the BCM team, all Branches have appointed their own dedicated BCP Coordinators. These coordinators work directly with critical service managers within their respective branches and play a coordination role between the critical service managers and the Comptrollership BCM team, who is responsible for the overall management and administration of the Program.

The Agency has a total of 421 BCPs for critical services and critical support services [10]. ISTB BCP coordinator manages (i.e. updates, coordinates, and tests) [*] BCPs for the Branch. Another [*] BCPs are managed by the Operations Branch BCP coordinator, primarily for Ports of Entry (POEs). The remaining [*] BCPs are managed by the Comptrollership BCM team.

The ISTB BCP coordinator works within the IT Security and Continuity Division, whose key activities include providing leadership, guidance and coordination for the planning and development of the ISTB BCPs [11]. Although the Comptrollership BCM team is responsible for managing the BCP Program, ISTB has created its own toolkit for the development of business impact analyses and business continuity plans, due to the unique elements required for IT critical services and support services. The IT Security and Continuity Division is responsible for sharing their BCPs with the Comptrollership BCM team and coordinating with the team on other BCP matters (i.e. testing, updates, etc.). They are also responsible for liaising with critical service managers across the Agency to ensure IT needs are identified and addressed in the BCP process.

The Operations Branch BCP coordinator is responsible for the BCPs for [*] POEs and [*] headquarter BCPs. The coordinator uses the tools and templates provided by the BCM team and works closely with this team to ensure ongoing communication and coordination between the branches. The Operations Branch BCP coordinator works with regional counterparts to review all BCPs twice yearly to ensure that the BCPs are re-validated and up-to-date. All Operations Branch BCPs are provided to the BCM team, for inclusion in the Comptrollership BCP inventory.

As part of Emergency Management, the National Border Operations Centre (NBOC) and a structured 24/7 regional and national level duty executive roster also plays key roles in ensuring business continuity. The NBOC is not directly involved in the regional port of entry planning for business continuity, though it plays a significant role in national level BCP planning and in ensuring business continuity on a daily basis given the Agency's 24/7 operating environment. Among other things, the NBOC is responsible for ensuring border services and security situational awareness, leading to the integration of border services with whole of government business continuity activities, a national level coordination of tactical responses to emergencies, threats, and issues management, and for monitoring the current state of operations, maintaining and enhancing the flow of information between regional enforcement partners and the [12]

Agency's operations, and responding to and managing unforeseen events .

In addition, the NBOC manages the Operational Exercise Program whose mandate is to develop, coordinate and maintain an Exercise Program which will best meet the identified needs and training objectives for the Agency at large. The Program serves as a platform upon which to monitor progress on operational readiness and plan future requirements for operational exercises [13]. This includes some testing of Operations Branch BCPs, either directly (if identified as a priority) or indirectly (through other operational exercises).

2.0 Significance of the Audit

This audit is of interest to management due to the operational nature of the Agency and the requirement for business continuity to deliver on the Agency's mandate.

The CBSA participated in this horizontal internal audit of BCP with the Office of the Comptroller General (OCG). BCP was ranked as an audit priority in the OCG's risk-based audit planning process because BCP continues to be of high inherent risk as it is fundamental in supporting the Government of Canada's ability to maintain a state of readiness and ultimately the continued achievement of its mandates [14].

The OCG intends to issue its own, government-wide report on BCP. The report may not name specific departments or agencies and recommendations will be made based on shared observations and themes.

This CBSA internal audit report communicates the results of the audit and provides recommendations from the Agency's perspective. While this report may include similar themes to those identified in the OCG report, it intends to provide greater detail about the CBSA's BCP framework and processes.

The audit objective was to determine whether:

- An Agency governance framework for BCP is in place; and
- Agency BCP processes are in place.

The audit scope and criteria can be found in Appendix A.

3.0 Statement of conformance

The audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program. The audit approach and methodology followed the *International Standards for the Professional Practice of Internal Auditing* as defined by the Institute of Internal Auditors and the *Internal Auditing Standards for the Government of Canada*, as required by the Treasury Board's *Policy on Internal Audit*.

4.0 Audit opinion

The Agency has implemented the key elements of a comprehensive BCP Program that includes a governance framework and processes to support business continuity planning across the Agency. Some opportunities to strengthen the process for developing and approving business continuity plans and monitoring the BCP Program exist. This will ensure compliance with requirements established by Lead Security Agencies and an effective BCP Program.

5.0 Key findings

The CBSA has a governance framework in place for Business Continuity Planning. Governance committees have been established and meet regularly. Roles and responsibilities of key stakeholders have been defined and communicated and an approved BCP policy, which aligns with the government's BCP policy framework, exists. An approach to identify and prioritize critical services has been established.

The Agency has processes in place for the development and updating of departmental business impact analyses and BCPs. Tools and templates are provided to critical service managers for developing business impact analyses and BCPs. Although no formal training has been identified, on-the-job training is provided to BCP coordinators. Some testing of BCPs occurs across the Agency and all BCPs are updated on a regular basis. Opportunities for improvement exist to identify documentation expectations for the analysis of recovery strategy options and BCP testing activities, identifying required training for BCP coordinators, and formalizing the approval process for business impact analyses and BCPs.

As per the CBSA BCM policy, the Security and Professional Standards Directorate is responsible for monitoring the BCP Program. Although monitoring and reporting on the BCP Program is taking place, there is opportunity to formally define this process, including the identification of the scope and frequency of monitoring activities related to the effectiveness of BCP and compliance with the government's requirements.

6.0 Summary of recommendations

The audit makes three recommendations relating to:

- Formalizing the approval process for business impact analyses and business continuity plans and identifying the documentation requirements supporting the recovery option analysis;
- Defining Agency-wide expectations for BCP testing activities; and
- Identifying BCP program monitoring and reporting requirements.

7.0 Management response

The Comptrollership Branch is in agreement with the overall audit report, as well as the recommendations. Appropriate steps and actions are currently under way to effectively reshape the current processes taking place within the BCP program.

8.0 Audit findings

8.1 Governance framework

Audit Criteria:

- Departmental governance structures that actively support business continuity planning are in place and, their roles as well as responsibilities have been documented, approved and communicated to all stakeholders.
- A departmental policy framework defining roles, responsibilities and expectations for BCP is in place.
- A department-wide systematic approach to identify and prioritize departmental critical services is in place.

Program governance is essential for providing direction and oversight, which guides the achievement of program objectives. The OSS-BCP requires the development of departmental BCP program policy to apply the Government Security Policy requirements [15] to new and existing departmental programs and operations. This can be done through the use of senior management committees and the appointment of a BCP coordinator.

The Agency has established a governance structure that actively supports BCP. It includes two security-related governance committees: the Security Management Committee and the Continuity of Operations and Security Working Group. Our review of the terms of reference and meeting minutes for both committees confirmed that roles and responsibilities had been defined, that the committees actively supported BCP, that membership included appropriate representatives from across the Agency, and that the committee responsibilities outlined in the OSS-BCP were met. The established governance structure is periodically reviewed, through the BCM policy review process, as well as on an as-needed basis.

The CBSA BCM policy is available on the Agency's intranet and was approved by the Security Management Committee. Roles and responsibilities for members of the governance structure, including the Departmental Security Officer and the BCP Coordinators, have been documented, defined and communicated through the BCM policy. The BCM policy also defines expectations for BCP and is updated periodically (usually every 3 years). This update involves a review of the established governance structure in place for BCP as well as an update to the BCP tools and templates provided to critical service managers, including the approach to identifying critical services.

Section 3.2 of the OSS-BCP outlines that a business impact analysis must be conducted to assess the impacts of disruptions on the Agency and to identify and prioritize critical services and associated assets [16] . The CBSA has a systematic approach in place to identify and prioritize critical services. All critical service managers are required to complete a business impact analysis, using standardized Agency tools and templates, in order to identify critical services. Once this analysis has been completed, the OSS-BCP expectation is that the results are approved by senior management before proceeding with the development of the BCPs. The two business impact analyses [17] that the audit examined were completed using the appropriate tools and templates; however, there was a lack of documented approval by senior management.

Once the critical services are identified, the OSS-BCP requires that they be prioritized. Priority is established based on the maximum allowable downtime and the minimum service level required before a high degree of injury will result. Services that must always be available are ranked at the top [18].

All services that the Agency has identified as critical have a maximum allowable downtime of [*] hours. Because they all have the same maximum allowable downtime, the Agency has made the decision that no further formal prioritization will occur. The CBSA is a law enforcement agency and therefore every service that is deemed critical is a priority and must be addressed with equal urgency. As all services have the same maximum allowable downtime and must always be available, the Agency's approach to prioritization is consistent with the OSS-BCP requirements.

The audit findings confirm that a governance framework has been established for BCP. It actively supports the Program and defines roles and responsibilities. The approach to identify and prioritize critical services is in place; however, an opportunity to formalize the approval process is recommended in the following section, under Recommendation 1.

8.2 BCP processes

Audit Criteria:

- Departments have conducted Business Impact Analysis.
- Departments developed recovery strategies for the critical services identified in their BIA(s) which take into account interdependencies with other departments.
- Departments developed business continuity plans to ensure the continuity of their critical services and critical support services.
- Departments coordinate with Critical Support Service Providers and other key internal stakeholders when developing, testing and updating their BCP to ensure integration between all parties.
- Departments ensure that sufficient and relevant training as well as tools are provided to enable BCP and recovery activities.
- Departments ensure that their business continuity plans are periodically tested, updated and reflect interdependencies with other stakeholders.

The OSS-BCP outlines that business impact analyses are to be conducted to assess the impacts of disruptions on the Agency and to identify and prioritize critical services. Based on the results of the business impact analyses, business continuity planning activities are to be conducted that include the following:

- Development and assessment of recovery options, from which a recovery strategy is determined;
- Approval of recovery strategy to support and fund selected strategies;
- Development of BCPs, that include specific elements outlined in the OSS-BCP;

- Senior management approval of the BCPs;
- Arrangement to ensure plans can be put into effect; and
- Briefing and training of staff.

To support critical service managers in carrying out their BCP responsibilities, the BCM team within the Comptrollership Branch has developed a suite of tools and templates to be used in the development of business impact analyses and BCPs. Guidance and support is provided over the phone and via email on an ongoing basis to critical service managers by the BCP coordinators.

A sample of four critical services was selected for the purpose of the audit. An assessment tool, which was based on the OSS-BCP requirements and the recommendations made in the Public Safety Guide to BCP, was developed by the OCG and used to assess the business impact analyses and BCPs for the sample.

The Agency conducts business impact analyses to identify critical services, with the exception of POEs as they all provide the same critical services and are all deemed critical. Two of the sampled critical services did not have documented business impact analyses as they were POEs. The other two sampled services did have documented business impact analyses that were assessed against the OCG assessment tool. While most of the elements required by the OSS-BCP were included within the business impact analyses themselves or their related BCP, some of the elements recommended by the Public Safety Guide to BCP were not addressed. These included elements such as quantitative and qualitative effects of impacts on other federal government departments and other key stakeholders were not included and dependencies on external corporate assets and services were not identified. This is because the Agency has not considered the Public Safety Guide in the development of the business impact analysis tools as the BCM team determined that its guidance was too broad and vague.

For the four critical services sampled, all had documented BCPs that included most of the elements in the assessment tool, including information technology continuity considerations. One element that was not consistently addressed was the documented approval of the BCPs by senior management (i.e. Director-level or above). This is a requirement under the OSS-BCP and two of the four BCPs sampled did not have evidence of senior management approval.

Another area where gaps were identified was in relation to the recovery option analysis. The OSS-BCP Section 3.3 requires the development of recovery options, from which a recovery strategy is determined. It requires an assessment of each recovery option in order to select the most appropriate option. The analysis is expected to include considerations such as impacts on the department, benefits, risks, feasibility and cost [19]. Although each BCP sampled included the selected recovery strategy for the critical service, there was a lack of evidence supporting that an assessment of each recovery option was performed. Therefore, it was difficult for the audit to conclude whether this assessment took place and if other recovery options had been considered.

With respect to briefing and training of staff, BCPs are communicated to internal stakeholders during the development and update process. The BCM team within the Comptrollership Branch maintains an inventory of BCPs that is backed up regularly. Interviews indicated that there have been some coordination challenges between ISTB and Comptrollership, such as obtaining updated BCPs from all Branches, but these challenges are currently being addressed. BCP coordinators liaise directly with critical service managers on a regular basis during the update process, which occurs every six months. Critical service managers share updated BCPs with relevant stakeholders and their BCP coordinators. The IT Continuity team also communicates directly with critical service managers to ensure IT needs are considered.

On-the-job training is provided to BCP coordinators but no formal training opportunities have been provided or identified by Lead Security Agencies for BCP or the Agency's BCM team in the Comptrollership Branch. Interviews with BCP coordinators confirmed that formal training opportunities would be beneficial in carrying out their BCP responsibilities. Sufficient and appropriate training assists with ensuring that the Agency's program is effective and that it meets Lead Security Agency requirements. The NBOC also informed the audit team of the need for greater Agency-level training for implementing and executing BCPs, also known as the Incident Command System.

For the testing of BCPs, the Management Accountability Framework (MAF) identifies three categories of testing: communication exercises, discussion exercises and operational exercises. For the purpose of this audit, testing included discussion exercises and operational exercises only, as communication exercises did not meet the elements of a testing exercise that the OCG expected. The OCG expectation for testing exercises was based on the Public Safety Guide to BCP and was that testing exercises have defined objectives, scope, assumptions, limitations and test criteria that would be communicated to various stakeholders such as recovery teams, facilitators, observers, time keepers, etc.

The Agency conducts a combination of all three types of BCP exercises. Communication exercises are conducted during the update process for all BCPs as phone conversations and email discussions are held with all critical service managers. Some tabletop exercises, which fall under the discussion exercise category, are conducted by the BCM team within Comptrollership as well as by the Operations Branch. Operational exercises are also carried out by the Operations Branch as part of the Operational Exercise Program.

The Exercise Program promotes a consistent branch-wide method for improving awareness and preparedness for emergency, new or infrequently used processes and procedures; improving internal and interdepartmental plans and procedures; monitoring progress on readiness; and to support planning for future exercises. The exercises are conducted at various levels and may occur concurrently, which include National Government of Canada exercises; Agency level exercises; Operations Branch exercises; regional exercises and local exercises. Exercise development is a collaborative process between the NBOC and Emergency Management Section (EMS) staff to ensure clear objectives and timely completion of after action reviews.

The exercise process involves a planning phase which includes the identification of Operations Branch priorities, objectives, resources, partners and participants. The testing phase is the execution of the exercise objectives through scenario-based discussions and/or operational responses. Each exercise is then evaluated, to identify what went well, what can be improved, potential gaps and tracking of recommendations. This is completed through after action reports and improvement action plans. The Operational Exercise Program includes the elements of a testing exercise as defined by the OCG for this audit.

In 2014-2015, BCP was identified as a priority for testing by the Operational Exercise Program. Specific exercises were conducted to test some BCPs. In addition, elements of some BCPs were also tested under other priorities (i.e. other testing activities) as part of the Program. It is not clear the extent to which BCPs were included in other testing activities as they are not tracked specifically if covered under other testing activities.

ISTB also conducted a number of scenario-based planning exercises as part of the BIA data collection process which included in-person meetings with most service managers in the branch.

Although the Agency is conducting a variety BCP testing exercises, a conscious approach to testing and a clear understanding of the coverage obtained through the various testing activities is needed. There is a lack of a documented Agency-wide approach to BCP testing that would include clear expectations for testing exercises (i.e. scope, type of testing activity, frequency, development of lessons learned, coordination, etc.) and a process for tracking and monitoring testing activities.

In conclusion, the Agency has processes in place for the development, implementation, testing and updating of BCPs; however some opportunities for process improvements were identified.

Recommendation 1:

The Vice President Comptrollership should formalize the approval process for Business Impact Analyses and Business Continuity Plans and identify the documentation requirements to support the assessment and determination of recovery strategy options.

Management Response:	Completion Date:
The Vice President Comptrollership Branch accepts the recommendation and will lead the update of the Business Continuity Management suite (i.e. policy, templates, etc.) to include a formalized approval process for Business Impact Analysis, Business Continuity Plans. These documents will also identify the documentation requirements to support the assessment and determination of recovery strategy options.	August 2017

Recommendation 2:

The Vice President Comptrollership should define Agency-level expectations for Business Continuity Plan testing activities, including scope, frequency, and how these activities will be communicated, tracked and monitored.

Management Response:	Completion Date:
The Vice President Comptrollership Branch accepts the recommendation and will implement an updated BCM Suite that includes BCP testing requirements as recommended. Comptrollership will work with the other Branches to ensure coordinated exercising and reporting.	April 2017 / Ongoing

8.3 Monitoring

Audit Criteria:

- Departments monitor and report on the effectiveness of their BCP.
- Departments monitor their compliance with BCP related requirements in the TB Policy on Government Security and inform the Secretary of any gaps identified.

Program monitoring is an essential element of governance and program management. Monitoring and reporting on BCP Program effectiveness and compliance ensure that in the event of a disruption, business continuity plans are in place, and are readily available, to ensure continuity. This is critical for CBSA due to the Agency's operational nature and 24/7 environment.

The OSS-BCP monitoring requirements specify that an audit cycle should be established for the BCP Program. The audit expected that the frequency for monitoring would be defined and communicated and would include how the results will be reported, who is responsible, and who will participate. The scope of monitoring activities should include a review of the governance structures, the Agency's policy, the approach to identifying and prioritizing critical services, training, tools and service level agreements.

The CBSA BCM policy formally assigns the responsibility for monitoring and reviewing the effectiveness of BCP to the BCM team and the Security and Professional Standards Directorate. The BCM policy states that the Security and Processional Standards Directorate will periodically review the policy and is responsible for identifying and undertaking any monitoring and assessment activities to determine whether its objective remains relevant and achievable and whether its requirements are being adhered to. The policy states that reporting requirements will be captured through recommendations made and reported to the President and/or the Executive Vice-President (EVP) on an annual basis.

At the time of the audit, the BCM team was reviewing the policy and updating the tools and templates used in the identification of critical services and for the development of BCPs. This type of update is conducted every three years and BCPs are updated every six months to ensure they reflect the current operating environment, although not specified in the BCM policy. In terms of reporting, a BCP program report is prepared by the BCM team and provided to the Departmental Security Officer who then provides the update to the Vice-President (VP) of the Comptrollership Branch. The BCM policy does not reflect what is occurring in practice as these reports are not provided to the other VPs or the President and/or the EVP. It is at the discretion of the VP Comptrollership to report to Executive Management on BCP.

Although it is evident that monitoring and updates are occurring, Agency documentation does not formally describe the scope or the frequency of monitoring activities to ensure the effectiveness of BCP. The current monitoring and updates do not include a review of all of the expected elements (i.e. review of the approach to prioritizing critical services, training and service level agreements).

The audit expected that departments monitor their compliance with BCP related requirements and inform the Treasury Board Secretariat of any gaps. The CBSA BCPs are updated every six months to ensure they meet the Agency's standard, which is based on the OSS-BCP. The Agency also uses the Management Accountability Framework (MAF) to monitor and report on compliance with requirements. Although the MAF elements are not as comprehensive, they still provide some coverage of compliance with requirements. Agency documentation does not outline the responsibility for monitoring compliance and interviews indicated that there are no other specific reviews or assessments conducted to monitor and report on compliance with Lead Security Agency guidance.

In summary, the Agency has developed and implemented processes to monitor the BCP program as well as ensure its compliance with government requirements; however, the approach has not yet been clearly documented and the BCM policy does not reflect what is occurring in practice.

Recommendation 3:

The Vice President Comptrollership should define the scope and frequency of the Business Continuity Planning program monitoring and reporting activities that ensure program effectiveness and compliance. This should be clearly reflected in the CBSA BCM policy.

Management Response:	Completion Date:
The Vice President Comptrollership Branch accepts the recommendation and will update the CBSA BCM Policy (BCM Suite) to ensure program effectiveness and compliance.	April 2017 / Ongoing

Appendix A – About the Audit

Audit objectives and scope

The objectives of the audit were to determine whether:

- Agency governance frameworks for BCP are in place; and
- Agency BCP processes are in place.

The scope of the audit included the current (as at December 31, 2015) BCP governance frameworks used within the Agency to ensure continuity of critical services and support services at the agency level.

Risk assessment

Based on the risk assessment conducted by the OCG for this audit, the following prominent risks were identified and are applicable to BCP within departments and across government:

- Governance and Strategic Direction
    - Risk that at the government-wide and departmental levels, governance and oversight structures are not in place and roles and responsibilities are not clearly articulated and communicated.
    - Risk that BCP priorities and strategic direction (including human and financial resourcing) are not set and communicated at the government-wide and departmental levels, resulting in BCP initiatives not being implemented due to its lack of perceived value.
- Policy Development and Implementation
    - Risk that BCP policy frameworks are not developed, implemented and updated in a timely manner to effectively support Government of Canada BCP readiness.
- Stakeholders and Partnerships and Communication
    - Risk that on a government-wide level, there is a lack of collaboration and coordination between government departments in the prioritization of critical services and recovery strategies.
    - Risk that on a departmental level, there is a lack of coordination between departmental sectors and/or between departments and Critical Support Service Providers external to the department in the development, establishment, testing and update of departmental business continuity plans required for departmental critical services and/or assets.
- Business Processes
    - Risk at the departmental level, that the BCP program is not sufficiently integrated within departmental business planning cycles, resulting in a lack of prioritization and attention given to BCP.
    - Risk that processes are not in place or inconsistently applied around the development, implementation, testing and update of business continuity plans and that BCP procedures, guidance and tools are not developed, implemented and updated in a timely manner.
- Information Management and Information Technology Strategy
    - Risk that business continuity plans do not integrate service continuity plans of critical Information Management (IM) and IT services in BCP recovery strategies
- Human Resources
    - Risk that there is a lack of capacity to implement BCP due to inadequate provision of BCP training, tools and templates to BCP Coordinators, sector managers and employees or a lack of succession planning and knowledge transfer
- Reputation

- Risk that the Government of Canada is unable to provide continuity of critical services during disruption events, leading to a loss of public confidence and trust.

Audit approach and methodology

The OCG completed the planning and the reporting phases of the audit using OCG internal resources. The internal audit functions of large and small departments (including the CBSA) conducted the examination of their own departments under the guidance and technical expertise of the OCG. The CBSA completed its own reporting phase as well to provide CBSA-specific findings, in the form of this report.

During the examination phase, sources of information included, but were not limited to, interviews with key stakeholders at various levels, documentation review and observations of key processes and the assessment of a sample of business continuity plans. The audit team reviewed governance, controls, and risk management practices surrounding BCP, applying the audit criteria detailed below.

Audit criteria

The following criteria were selected by the OCG, based on the audit work completed in the planning phase that included a risk assessment, and were applicable to the CBSA [20]:

Lines of Enquiry	Audit Criteria
Line of Enquiry 1: Departmental Governance Framework: Departmental governance frameworks are in place for the management of departmental BCP.	1.1 Departmental governance structures that actively support business continuity planning are in place and, their roles as well as responsibilities have been documented, approved and communicated to all stakeholders. 1.2 A departmental policy framework defining roles, responsibilities and expectations for BCP is in place. 1.3 A department-wide systematic approach to identify and prioritize departmental critical services is in place.
Line of Enquiry 2: Departmental BCP Processes: Departmental BCP processes are in place for the development, implementation, testing and update of departmental BCP.	2.1 Departments have conducted Business Impact Analysis (BIA). 2.2 Departments developed recovery strategies for the critical services identified in their BIA(s) which take into account interdependencies with other departments. 2.3 Departments developed business continuity plans to ensure the continuity of their critical services and critical support services. 2.4 Departments coordinate with Critical Support Service

	Providers and other key internal stakeholders when developing, testing and updating their BCP to ensure integration between all parties. 2.5 Departments ensure that sufficient and relevant training as well as tools are provided to enable BCP and recovery activities. 2.6 Departments ensure that their business continuity plans are periodically tested, updated and reflect interdependencies with other stakeholders.
Line of Enquiry 3: Monitoring: Departmental monitoring processes are in place for the oversight of BCP readiness.	3.1 Departments monitor and report on the effectiveness of their BCP. 3.2 Departments monitor their compliance with BCP related requirements in the TB *Policy on Government Security* and inform the Secretary of any gaps identified.

Appendix B – List of acronyms

BCP	Business Continuity Planning
BCM	Business Continuity Management
BIA	Business Impact Analysis
CBSA	Canada Border Services Agency
CSM	Critical Service Managers

DSO

Departmental Security Officer

EM

Emergency Management

IT

Information Technology

ISTB

Information, Science and Technology Branch

LSA

Lead Security Agencies

MAD

Maximum Allowable Downtime

MAF

Management Accountability Framework

MSL

Minimum Service Level

NBOC

National Border Operations Centre

OCG

Office of the Comptroller General

OSS

Operational Security Standard

POE

Port of Entry

SPSD

Security and Professional Standards Directorate

Footnotes

[1] Introduction was taken from the OCG Horizontal Audit of BCP Audit Plan, Audit Plan Context Section.

[2] Public Safety Emergency Management Planning Guide 2010-2011, Section 2

[3] "Internal efforts" refer to the departmental activities completed within the operational environment of the Government of Canada to ensure the continuity of Government of Canada critical services.

[4] "External environment" refers to processes that are outside of the operational environment of the Government of Canada (i.e. critical infrastructure and services not provided or managed by the Government of Canada such as Telecommunications, energy provision, etc.)

[5] Public Safety Emergency Management Planning Guide 2010-2011

[6] TB *Policy on Government Security*, Appendix A: Definitions

[7] TB *Policy on Government Security*, Appendix A: Definitions

[8] OSS-BCP Section 3

[9] CBSA BCM policy, Section 7.1

[10] Critical support services are support services that are required for the continuity of critical services.

[11] http://atlas/istb-dgist/ites-seti/its_sit_eng.asp

[12] http://atlas/ob-dgo/directorates-directions/bocme-cfoge/index_eng.asp

[13] http://atlas/ob-dgo/divisions/opr-pir/em-gu/oep_peo_eng.asp

[14] OCG Horizontal Audit of BCP, Audit Plan

[15] The Policy on Government Security defines roles and responsibilities and includes various requirements related to the development and maintenance of departmental security plans and programs. It explains that business continuity management is part of the management of security requirements for departments. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=html

[16] OSS-BCP Section 3.2

[17] The OCG selected a sample of four critical services for the purpose of the audit. Under LOE 2, the audit tested whether or not the critical services had documented and approved business impact analyses, recovery strategy options and BCPs. Two of the sample services did not have business impact analyses as they were Ports of Entry (POE). The Agency made the decision that all POE provide the same critical services and therefore business impact analyses were not conducted for POE. All POE had recovery strategy options and BCPs.

[18] OSS-BCP Section 3.2 (d)

[19] OSS-BCP Section 3.3 (b)

[20] Note that there was one other Line of Enquiry included in the OCG audit that was not applicable to CBSA as it applied only to LSA. Some criteria were also only applicable to LSA and therefore not included in this appendix.

Date modified: 2017-02-13