Industry Canada Industrie Canada

Audit Report

Audit of Business Continuity Planning Program

Audit and Evaluation Branch

May 2015

Recommended for Approval to the Deputy Minister by the
Departmental Audit Committee on May 5, 2015

Approved by the Deputy Minister on May 13, 2015

Canada

This publication is also available online at: http://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/h_03783.html

To obtain a copy of this publication or an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact the:

Web Services Centre
Industry Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (Ottawa): 613-954-5031
TTY (for hearing-impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: info@ic.gc.ca

Permission to Reproduce

Cat. No. Iu4-165/2015E-PDF
ISBN 978-0-660-02764-7

Aussi offert en français sous le titre *Audit du Programme de planification de la continuité des activités.*

Table of Contents

List of Initialisms and Acronyms Used in Report

ADM	Assistant Deputy Minister
AEB	Audit and Evaluation Branch
BCP	Business Continuity Plan
BCPWG	Business Continuity Planning Working Group
BIA	Business Impact Analysis
CFO	Chief Financial Officer
CFSB	Corporate Facilities and Security Branch
CIO	Chief Information Office Sector
CMS	Corporate Management Sector
DG	Director General
DMC	Departmental Management Committee
GC	Government of Canada
IC	Industry Canada
IMT	Incident Management Team
IS	Industry Sector
IT	Information Technology
MAD	Maximum Allowable Downtime
OSB	Office of the Superintendent of Bankruptcy
OSS-BCP	Operational Security Standard – Business Continuity Planning Program
PSC	Public Safety Canada
SITT	Spectrum, Information Technologies and Telecommunications
SPS	Strategic Policy Sector
TBS	Treasury Board Secretariat

1.0 Executive Summary

1.1 Background

The Industry Canada (IC) Business Continuity Planning Program is intended to manage and facilitate the continued delivery of essential departmental operations[1], in the event of a business disruption or incident and to restore activities to normal operations after the event. The Business Continuity Plan (BCP) also identifies and considers, as a highest priority, the six critical services that IC fulfills in regard to the Government of Canada emergency management responsibilities (*refer to Appendix A for more information*).

The Program responds to federal requirements identified in the following legislative and policy instruments:

- *Emergency Management Act* (2007);
- Federal *Policy for Emergency Management* (issued by Public Safety Canada, 2009);
- *Policy on Government Security* (revised by Treasury Board (TB), 2012); and
- Operational Security Standard-Business Continuity Planning (OSS-BCP) (issued by TB, 2004).

The Program requires the development and timely execution of departmental and sectoral level Business Continuity plans, measures, procedures and arrangements during a business disruption or incident. Key dependencies (e.g. Information Management; Information Technology; and Facilities Services) that support the execution of the BCPs also need to be identified in the plans.

The Corporate Facilities and Security Branch (CFSB), within the Corporate Management Sector (CMS), is responsible for coordinating the execution of the Program at IC. While business continuity activities had been undertaken by the Department for many years, a departmental BCP Renewal Project was launched in 2011-12 to ensure the effectiveness of the plans.

The resulting updated departmental BCP plan was approved in March 2013 and is formally updated as part of the annual departmental Integrated Planning and Reporting cycle. Sectoral level BCPs are approved by sector heads and are also part of the annual review cycle.

A key input of BCP plans are Business Impact Analyses (BIAs) which serve to identify and prioritize IC essential operations (e.g. bankruptcy filing; support to the Minister and Deputy Minister offices; intellectual property date stamping, IT Support, Accommodation Services and Management), including the identification and consideration of the six critical services on behalf of the Government of Canada as the highest priority.

Business continuity plans include arrangements and information to address events that can impact negatively on key business resources such as IM/IT and facilities. For example, the BCP has arrangements to address disruptions localized to a specific building by identifying alternate sites with

[1] In this report, “essential operations” terminology is used instead of “critical operations” to distinguish between the Department critical operations and the critical services IC manages on behalf of the Government of Canada. Sometimes, reference to “critical operations” is common in TBS and IC BCP documentation.

network connectivity for laptops to facilitate the continuity of business operations. The plans also define governance and reporting structures to allow key decision makers to gather quickly to assess and respond to a business disruption.

Furthermore, the Chief Information Office (CIO) Sector maintains various controls to mitigate the risk or minimize the duration of an IT outage including the establishment of incident management procedures to guide a prioritized recovery and/or re-establishment of IT applications based on their support for critical Government services.

The BCP Program, however, is not responsible for establishing plans and arrangements for the emergency management of the telecommunications and manufacturing sector. The responsibilities for developing and managing these fall under the Spectrum, Information Technologies and Telecommunications (SITT) sector and the Industry Sector (IS) and are addressed by distinct additional measures as explained below.

Industry Canada Responsibilities for Emergency Management

In the context of the Government of Canada emergency management, Industry Canada is responsible for the provision of six critical services (refer to Appendix A). Five of these critical services relate to telecommunications and are the responsibility of SITT. The other critical service is related to the coordination of the manufacturing infrastructure in the event of an emergency and is the responsibility of IS. While there are linkages and recognition of these critical services in the sector and Department BCP, a separate set of plans and arrangements have been developed to ensure the delivery of these services in emergency situations. For instance, SITT has put in place a unique BCP along with emergency plans specific to the critical services which include special communications arrangements (e.g. satellite phones), the ability to transfer headquarters functions to the regions, and the ability to work temporarily in the event of an IT outage. IS's responsibility has been primarily focused on developing a database containing the capabilities and contact information of key companies in the manufacturing sector that is available to federal departments and agencies on the Public Safety website.

1.2 Audit Objective, Scope and Conclusion

Audit Objective

The objective of the audit was to provide reasonable assurance that Industry Canada's BCP Program is operating effectively in the following areas:

1. BCP Program governance;
2. Business impact analysis;
3. Business continuity plans and arrangements; and
4. BCP Program maintenance and readiness.

Audit Scope

The scope of the audit included an assessment of key BCP activities, processes and controls in the specific areas identified in the audit objective at the departmental and sectoral levels within Industry Canada. The focus of the audit was solely on the BCP Program, and does not cover plans and arrangements specific to the Department's Government of Canada emergency management responsibilities.

The scope of the audit did not include an in-depth assessment of the adequacy of BCPs to ensure continuity of operations in a business disruption, because such a determination could only be made through a real-time invocation of the BCP.

Five organizations were selected for testing: 1) Industry Sector (IS); 2) Spectrum, Information Technologies and Telecommunications (SITT); 3) Chief Information Office (CIO); 4) Corporate Management Sector (CMS); and 5) Office of the Superintendent of Bankruptcy (OSB).

Documents reviewed were the in-use versions for fiscal years 2012-13 and 2013-14.

Audit Conclusion

The results of the audit revealed that the BCP Program is operating effectively in the area of program governance. Opportunities for improvement and associated recommendations were identified to address low to moderate risks to the Department in the areas of business impact analysis, business continuity plans and program maintenance and readiness.

Overall, the Department has a well-established BCP governance structure and process. The findings and recommendations are geared toward strengthening the program and plans and enhancing its usefulness to senior management.

1.3 Main Findings and Recommendations

Governance

There is a well-defined governance structure for the BCP program in place. Sector Heads oversee the development, implementation, and maintenance of the BCPs under their respective area of responsibility and support the departmental BCP program. CMS provides a central coordination function, provides guidance, support as well as an ad hoc challenge function to sectors and supports the departmental working group. CMS and BCPWG are responsible for providing documents for review to oversight committees -- the Director General Management Advisory Committee and the Departmental Management Committee as required. Yearly departmental BCPs are signed-off by the Chief Financial Officer (CFO) who is the delegated authority for Security which includes BCP.

Business Impact Analysis

While there is guidance provided on how to assess the criticality of business functions/services, the audit found that not all sector/branch BIAs were completed in accordance with this guidance. As well, it is difficult to determine whether business functions/services have been assessed for criticality correctly because the BIAs lack sufficient rationale. Without knowing that the criticality assessments have been done in a consistent fashion across the Department, the BIAs cannot be totally relied upon to provide senior management a clear view of how to prioritize business functions/services.

Recommendation 1: In order to enhance the ability to have a prioritized departmental view of business functions/services, CMS should:

a) Review and amend the BIA template and guide to better assist branches/sectors in providing additional information and rationale to support the criticality assessments and improve consistency across the Department; and
b) Provide a more rigorous challenge function to ensure consistency and alignment of the branches/sectors' BIAs with current guidance.

BIAs are subject to review and approval at multiple levels, including ultimate approval by branch/sector heads.

Detailed IT requirements documented in branch/sector BIAs are not validated by the CIO during the annual BIA process.

Recommendation 2**:** Sectors/branches should ensure that stakeholders responsible for the provision of services defined in BIAs, including CIO, have been consulted for validation.

Business Continuity Plans and Recovery Strategies

BCPs reviewed addressed many elements required by the OSS-BCP; however, there were opportunities for improvement. Furthermore, while there are documented recovery strategies in the BCPs, these strategies could benefit from being more detailed and adaptable to a range of disruptions with varying severity.

Recommendation 3**:** Sectors/branches, in collaboration with CMS, should ensure that BCPs address all of the OSS-BCP requirements. As well, it should ensure that recovery plans, resource requirements, measures and procedures respond to a range of disruptions of varied severity.

Program Maintenance and Readiness

BCPs are kept current through processes initiated by a combination of formal and ad-hoc triggers to account for changes to the Department and its operating environment.

Communication and awareness activities are ongoing to support employees to execute their BCP roles and responsibilities.

Some sector management indicated that additional training would be beneficial to support employees with BCP related activities.

***Recommendation 4*:** Sector/branch management, with the assistance of CMS, should assess whether additional training is needed for employees with BCP responsibilities. If the assessment reveals that there is a common training need across sectors/branches, CMS should coordinate the provision of the training.

Table top exercises have occurred at the departmental level as well as in some sectors. However, this testing could be enhanced with a formal testing approach for the Department to ensure that it is occurring frequently enough and at varying levels of complexity.

***Recommendation 5*:** CMS should develop and document a testing approach which outlines an appropriate frequency and complexity of testing, along with testing of key dependencies.

The best practice of capturing lessons learned following an actual business disruption or a testing exercise is being done. However, it is done informally and inconsistently. As well, action items raised from lessons learned are not tracked to completion. There is an opportunity to share lessons learned with personnel with BCP responsibilities across the Department as well as ensure these lessons learned are applied to improve BCP processes and practices.

***Recommendation 6*:** Sectors/branches should:

a) Share lessons learned with all BCPWG members via the departmental BCP coordinator ; and
b) Ensure action items following from lessons learned are addressed in order for BCP processes and practices to be improved.

1.4 Audit Opinion

In my opinion, the Business Continuity Planning Program at Industry Canada is operating effectively, with exceptions noted. Opportunities for improvement and associated recommendations were identified to address low to moderate risks to the Department in the areas of business impact analysis, business continuity plans and program maintenance and readiness.

1.5 Conformance with Professional Standards

This audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada, as supported by the results of the Audit and Evaluation Branch's quality assurance and improvement program.

Brian Gear
Chief Audit Executive, Industry Canada

2.0 About the Audit

2.1 Background

In accordance with the approved Industry Canada (IC) 2014-2017 Multi-Year Risk-Based Internal Audit Plan, the Audit and Evaluation Branch (AEB) undertook an audit of the Business Continuity Planning (BCP) Program.

BCP Program

The Industry Canada (IC) Business Continuity Planning Program is intended to manage and facilitate the continued delivery of essential departmental operations, in the event of a business disruption or incident and to restore activities to normal operations after the event. The Business Continuity Plan (BCP) also identifies and considers as a highest priority the six critical services that IC fulfills in regard to the Government of Canada emergency management responsibilities (*refer to Appendix A for more information*).

The BCP Program is to be done in accordance with federal requirements identified in the following legislative and policy instruments:

- *Emergency Management Act* (2007);
- Federal *Policy for Emergency Management* (issued by Public Safety Canada, 2009);
- *Policy on Government Security* (revised by Treasury Board (TB), 2012); and
- Operational Security Standard-Business Continuity Planning (OSS-BCP) (issued by TB, 2004).

Industry Canada Responsibilities for Emergency Management: In the context of the Government of Canada emergency management, Industry Canada is responsible for the provision of six critical services. Five of these critical services relate to telecommunications and are the responsibility of the Spectrum, Information Technologies and Telecommunications (SITT). The other critical service is related to the coordination of the manufacturing infrastructure in the event of an emergency and is the responsibility of the Industry Sector (IS). While there are linkages and recognition of these critical services in the sector and Department BCP, a separate set of plans and arrangements have been developed to ensure the delivery of these services in emergency situations. For instance, SITT has put in place a unique BCP along with emergency plans specific to the critical services which include special communications arrangements (e.g. satellite phones), the ability to transfer headquarters functions to the regions, and the ability to work temporarily in the event of an IT outage. IS's responsibility has been primarily focused on developing a database containing the capabilities and contact information of key companies in the manufacturing sector that is available to federal departments and agencies on the Public Safety website. Furthermore, the CIO maintains various controls to mitigate the risk or minimize the duration of an IT outage including the establishment of incident management procedures to guide a prioritized recovery and/or re-establishment of IT applications based on their support for critical Government services.

The Corporate Facilities and Security Branch (CFSB), within the Corporate Management Sector (CMS), is responsible for coordinating the Program at IC. While business continuity activities have been ongoing in the Department for many years, a departmental BCP Renewal Project was launched in 2011-12 to ensure the effectiveness of the plans.

The renewal project activities included:

- Reviewing existing departmental governance structures to ensure roles and responsibilities remain relevant and align with government-wide BCP program requirements;
- Undertaking sectoral and departmental Business Impact Analysis (BIA) exercises to evaluate the impacts of business disruption and identifying and prioritizing essential operations and associated assets;
- Creating or revising sector/branch and departmental level BCPs based on BIA exercises; and
- Establishing a permanent BCP maintenance cycle which is integrated within the Department's annual planning cycle.

IC's Departmental Management Committee members were briefed on the development of the departmental BCP in March 2013. Emphasis was placed on the need for managers and employees to be familiar with what to do in the event of business disruptions or incidents that require the departmental or sector/branch level BCPs to be invoked. The departmental BCP was formally approved by the Assistant Deputy Minister (ADM) of CMS/CFO and came into effect on May 3, 2013.

A departmental Incident Management Team (IMT) led by the ADM of CMS has been assigned to coordinate departmental efforts during a disruption. Where appropriate, sectors have established their own teams to execute sector level BCPs.

There have been no business disruptions requiring the invocation of the departmental BCP since the completion of the renewal project.

A key input of BCP plans are Business Impact Analyses (BIAs) which serve to identify and prioritize IC essential operations (e.g. bankruptcy filing; support to the Minister and Deputy Minister offices; intellectual property date stamping, IT Support, Accommodation Services and Management), including the identification and consideration of the six critical services on behalf of the Government of Canada as the highest priority.

Business continuity plans include arrangements and information to address events that can negatively impact key business resources such as IM/IT and facilities. For example, the BCP has arrangements to address disruptions localized to a specific building by identifying alternate sites with network connectivity for laptops to facilitate the continuity of business operations. The plans also define governance and reporting structures to allow key decision makers to gather quickly to assess and respond to a business disruption.

The BCP Program, however, is not responsible for establishing plans and arrangements for the emergency management of the telecommunications and manufacturing sector. The responsibilities for developing and managing these fall under the Spectrum, Information Technologies and Telecommunications (SITT) sector and the Industry Sector (IS) and are addressed by distinct additional measures as explained in the text box above.

2.2 Objective and Scope

The objective of the audit was to provide reasonable assurance that Industry Canada's BCP Program is operating effectively in the following areas:

1. BCP Program governance;
2. Business impact analysis;
3. Business continuity plans and arrangements; and
4. BCP Program maintenance and readiness.

The scope of the audit included an assessment of key BCP activities, processes and controls in the areas identified in the audit objective at the departmental and sectoral levels within Industry Canada. The audit did not asses the emergency support plans and related measures undertaken by SITT and IS to ensure delivery of the six critical services.

The period reviewed included fiscal-year 2012-13 and 2013-14.

Five organizations were selected for testing: 1) Industry Sector (IS), 2) Spectrum, Information Technologies and Telecommunications (SITT), 3) Office of the Superintendent of Bankruptcy (OSB) 4) Chief Information Office (CIO), and 5) Corporate Management Sector (CMS).

The scope of the audit did not include an in-depth assessment of the adequacy of BCPs to ensure continuity of operations in a business disruption, because such an assessment could only be made through comprehensive testing of the plans that would necessitate a real-time invocation of the BCP.

2.3 Audit Approach

The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion and opinion provided and contained in this report. This opinion is based on a review of the policies, procedures and plans in place over the time period identified in the scope section of this report, based on pre-established audit criteria agreed upon with management. This opinion applies only to the area under audit and described in the report.

The audit was performed in three phases: planning, conduct and reporting. A risk assessment was executed during the planning phase of this audit to confirm the audit objective and identify areas requiring more in-depth review during the conduct phase.

Based on the identified risks, the audit team developed audit criteria that linked back to the overall audit objective (*refer to Appendix B*).

The methodology used to address the audit's objective included:

- Documentation review; and
- Interviews with 18 personnel that have BCP accountabilities and responsibilities.

A debrief meeting was held with CMS management on July 8, 2014 to validate the accuracy of the findings contained in this report.

3.0 Findings and Recommendations

3.1 Introduction

The findings of this audit are based on evidence and analysis from the initial risk assessment and the execution of the audit procedures. In addition to the findings below, AEB has communicated to management, verbally, findings for consideration that were either non-systemic or of a very low risk and did not warrant inclusion in the audit report.

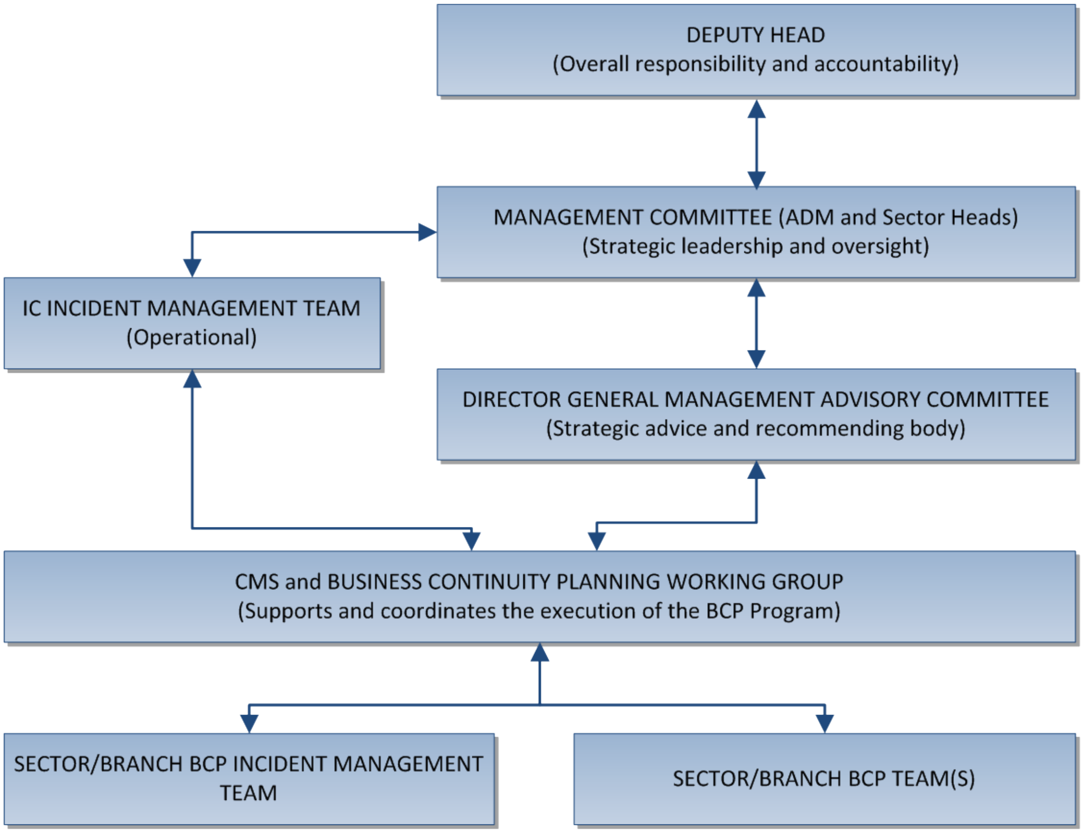
3.2 Governance

> There is a well-defined governance structure for the BCP program in place. Sector Heads oversee the development, implementation, and maintenance of the BCPs under their respective area of responsibility and support the departmental BCP program. CMS provides a central coordination function, provides guidance, support as well as an ad hoc challenge function to sectors and supports the departmental working group. CMS and BCPWG are responsible for providing documents for review to oversight committees -- the Director General Management Advisory Committee and the Departmental Management Committee as required. Yearly departmental BCPs are signed-off by the Chief Financial Officer who is the delegated authority for Security which includes BCP.

Well-defined governance structures provide guidance, oversight and manage how programs deliver value and mitigate risk. Additionally, governance structures contribute to effective decision making, stakeholder engagement and communication across the organization.

The IC BCP Program has adopted a multi-tiered governance structure framework for executing the BCP program and managing business disruptions or incidents. The governance structure in place for the BCP program is depicted below:

Figure 1 – IC BCP Program Governance Structure:


DEPUTY HEAD
(Overall responsibility and accountability)
MANAGEMENT COMMITTEE (ADM and Sector Heads)
(Strategic leadership and oversight)
IC INCIDENT MANAGEMENT TEAM
(Operational)
DIRECTOR GENERAL MANAGEMENT ADVISORY COMMITTEE
(Strategic advice and recommending body)
CMS and BUSINESS CONTINUITY PLANNING WORKING GROUP
(Supports and coordinates the execution of the BCP Program)
SECTOR/BRANCH BCP INCIDENT MANAGEMENT TEAM
SECTOR/BRANCH BCP TEAM(S)

Sector/branches are responsible for conducting their own BIAs that feed relevant information into each sector’s BCP. Sector Heads oversee the development, implementation, and maintenance of the BCPs under their respective area of responsibility and support the departmental BCP program. The audit found that branch/sector BIAs and BCPs were approved by Sector Heads.

CMS is responsible for the ongoing central coordination of the BCP Program. They provide guidance, support as well as an ad hoc challenge function to sectors for the development and maintenance of BIAs and BCPs. CMS is also responsible for supporting and leading the department’s BCP Working Group which includes representatives from all sectors/branches. CMS and the BCPWG are responsible for providing updates and documents for review to the oversight bodies -- DGMAC and DMC -- as required. Yearly departmental BCPs are signed-off by the CFO who is the delegated authority for Security which includes BCP.

In the event of an incident causing a business disruption, CMS and the BCPWG support the department’s Incident Management Team, headed by the CMS ADM. Sectors also have Incident Management Teams established.

The audit found that these roles and responsibilities were well communicated and understood. BCP Program roles and responsibilities have been defined and communicated on either the departmental intranet or BCP Wiki through the following instruments:

- Departmental Security Policy;

- BCPWG Terms of Reference;
- BCPs (i.e. sector/branch and departmental plans); and
- BCP tools (e.g. BCP FAQ for Employees and Managers, Incident Action Plans, Personal BCP Checklists).

3.3 Business Impact Analysis

The business impact analysis (BIA) is used to identify and prioritize essential operations, including the proper identification of critical services delivered by SITT and IS, and to assess the impact of disruptions. According to the requirement of the Treasury Board *Operational Security Standard – Business Continuity Planning Program (*OSS-BCP), the departmental Business Impact Analysis should include the following:

- the nature of the Department's business (e.g. role, mandate) and the services it must deliver. Internal and external functions on which the services depend;
- the direct and indirect impacts of disruptions on the Department, including the quantitative and qualitative effects;
- an assessment of services to determine which are likely to cause high degree of injury to Canadians and the Government;
- a prioritization of critical operations and list of the resources that support them directly or indirectly within or outside the Department; and
- Approval from senior management before proceeding with the development of continuity plans.

Business Impact Analysis Process

While there is guidance provided on how to assess the criticality of business functions/services, the audit found that not all sector/branch BIAs were completed in accordance with this guidance. As well, it is difficult to determine whether business functions/services have been assessed for criticality correctly because the BIAs lack sufficient rationale. Without knowing that the criticality assessments have been done in a consistent fashion across the Department, the BIAs cannot be totally relied upon to provide senior management a clear view of how to prioritize business functions/services.

The process of completing BIAs is supported by the use of structured BIA templates and an accompanying user guide that were developed by CMS. The tools provide guidance for the key factors that should be analyzed when considering the impacts of disruption on the Department, as well as a structured approach to prioritizing services. As a result, these tools should assist the completion of the BIAs in a consistent manner across the Department.

The Department relies on the sectors/branches to effectively analyse and prioritize the criticality of their own functions/services. It is, however, also important that a central function performs a review for consistency across sectors and challenge ratings and prioritization of business functions/services. With the level of detail within the current BIAs, there is insufficient information provided to allow CMS to adequately perform this challenge function.

The audit found issues related to the template that limited the capture of detailed information to support decisions regarding impact assessments (e.g. The Injury Assessment data field is a static dropdown and does not include a rationale supporting why each service disruption was deemed to be of High, Medium or Low injury to Canadians).

As per the OSS-BCP, BIAs should identify and prioritize essential operations. Priority should be assigned based on the maximum allowable downtime (MAD) and the minimum service level required before high degree of injury result. However, the audit found anomalies in the prioritizations of business functions/services in the departmental BIA as follows:

- Some business functions/services classified as moderately critical were assessed with a high degree of injury whereas some business functions/services categorized as critical were assessed with a low degree or medium degree of injury. These assessments are inconsistent with the direction provided in the BIA guide (i.e. critical category assigned a high degree of injury and moderately critical a medium degree of injury). Over 50% of business functions/services listed in the Departmental BIA did not align with the guidance provided on how to assess their importance during a disruption. Out of the 80 business functions/services listed, 71 indicated a maximum allowable downtime (MAD) of less than 24 hours which seems a very high percentage given the nature of IC essential operations.

These deficiencies in the sector ⁄ branch BIAs affect the ability to have a prioritized departmental view of business functions ⁄ services. By not prioritizing business functions/services in a consistent way across the Department, there is a risk of misallocating key resources during business disruptions thereby impacting the ability to manage and facilitate the continuity of essential operations within IC.

Note that the BIA process has properly identified the critical services that support the Department’s GoC emergency management responsibilities. As a result, the BCP program has acknowledged consideration of the highest priority to these services.

Recommendation 1: In order to enhance the ability to have a prioritized departmental view of business functions/services, CMS should:

a) Review and amend the BIA template and guide to better assist branches/sectors in providing additional information and rationale to support the criticality assessments and improve consistency across the Department; and
b) Provide a more robust challenge function to ensure consistency and alignment of the branches/sectors’ BIAs with current guidance.

Approval of Business Impact Analysis

BIAs are subject to review and approval at multiple levels, including ultimate approval by branch/sector heads.

The Department undertakes a “bottom up” approach to the BIA development process, beginning at the branch level and progressing to a sector level BIA, which self-identify essential operations that they provide. BIAs are subject to a multi-layered review and approval process. Completed BIAs are ultimately approved by their respective branch/sector heads. The collection of approved branch/sector BIAs constitutes the departmental BIA.

Validation by Stakeholders

Detailed IT requirements documented in branch/sector BIAs are not validated by CIO during the annual BIA process.

Internal stakeholders to the BIA process include Facilities Management and the Chief Information Office Sector who are responsible for the provision of resources and services defined within other sector/branch BIAs and should validate that those related requirements are accurate and feasible. Once completed, BIAs are submitted to the departmental BCP Coordinator and a representative from Facilities Management has the opportunity to validate the facility requirements defined by each sector/branch (e.g. number of people, office space). The departmental BCP demonstrates that primary and secondary backup facilities have been assigned to each branch/sector.

Nevertheless, IT requirements are not fully validated once the BIAs are submitted to the departmental BCP Coordinator. The validation by the coordinator and Facilities Management primarily focusses on having a sufficient number of network connections available at backup facilities for critical branch/sector employees; the CIO does not review the specific IT applications or IM resources that a branch/sector cites as required during a business disruption. As well, branches/sectors do not always directly discuss IT requirements with the CIO Sector during the development of their BIAs. There is a risk that the IT requirements as defined in branch/sector BIAs to support the continued delivery of essential operations cannot be met.

Note that for critical services, the CIO has acknowledged the IT requirements; the CIO BCP document has identified the mapping between the Department's critical services and their respective IT applications so priority is given to these when necessary.

Recommendation 2: Sectors/branches should ensure that stakeholders responsible for the provision of services defined in the BIAs, including CIO, have been consulted for validation

3.4 Business Continuity Plans

The results of the BIA are fed into the development of the respective sector's BCP. The BCP must include sufficient details to execute the required actions during a business disruption. A BCP should be able to respond to a wide range of potential threats (including high-impact, low-likelihood scenarios), and should include IM and IT continuity plans. The OSS-BCP requires the following for a BCP:

- Critical operations along with their reliance on internal/external services, assets and resources (i.e. dependencies) as identified in the business impact analysis;
- Approved recovery strategies;
- Measures to deal with the impacts and effects of disruptions on the Department;
- Response and recovery teams, including their membership and members' contact information;

- Roles, responsibilities and tasks of the teams, including those of internal and external stakeholders. Stakeholders include employees and organizations responsible for provisioning dependencies as well as other stakeholders such as vendors, clients, other GoC departments, etc;
- Resources and procedures for recovery;
- Coordination mechanisms and procedures; and
- Communication strategies.

Furthermore, the PSC guide to BCP states that plans should include detailed response/recovery measures and arrangements to facilitate continuity.

Business Continuity Plans and Recovery Strategies

Sectoral and departmental BCPs reviewed addressed many elements required by the OSS-BCP; however, there were opportunities for improvement. Furthermore, while there are documented recovery strategies in the BCPs, these strategies could benefit from being more detailed and adaptable to a range of disruptions with varying severity.

BCPs reviewed were effective in addressing elements required by the OSS-BCP in the following areas:

- Response and recovery teams including membership and contact information;
- Roles and responsibilities for key internal stakeholders;
- Authority to activate BCPs;
- Communication strategies and contingencies in the event of a disruption;
- Coordination mechanisms (e.g. Incident Command System); and
- Arrangements for monitoring and managing costs of business disruptions or incidents are defined by the BCP program and are supported by financial frameworks and processes.

The following exceptions were observed:

- Although external dependencies were defined and documented as part of the BIAs, they were not all reported in the BCPs. Roles and responsibilities for external stakeholders are also not documented (e.g. Shared Services Canada, emergency services).
- Although information assets required to continue delivery of services were defined and documented as part of the BIAs, they were not reported in the BCPs.
- IM and IT continuity plans and arrangements, that support the continuous delivery of critical IT services in the event of business disruptions, have not been established and integrated into the BCP Program. These documents are currently being drafted, and to mitigate this risk, sectors responsible for critical services (i.e. SITT and IS) have stated that they have arrangements in place to access key information in the event of an IT outage. Furthermore, the CIO maintains various controls to mitigate the risk or minimize the duration of an IT outage.

Specific to recovery strategies, Industry Canada has adopted an all-hazards approach to prepare for potential business disruptions. As stated by PSC, this is an emergency management approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the incident, thereby permitting an optimization of planning, response and support resources. However, the departmental BCP recovery strategies could benefit from more detailed information to address a range of interruption scenarios.. The Department is highly dependent on the knowledge of the current individuals that have been assigned BCP roles (i.e. BCP Coordinators, and members of the various IMTs) to tailor the response to the specific disruption.

The following aspects of the Department's BCPs could benefit from a more detailed planning approach:

- The BCPs reviewed as part of this audit, do not address a range of disruptions of varied severity to IT systems (e.g. outage of one or more corporate applications, the entire network, intranet, internet, shared drives and phones).
- Plans do not address a range of disruptions to facilities. BCPs have plans to address building-specific disruptions, such as overcoming the unavailability of a primary facility (e.g. 235 Queen Street) by defining a secondary work location; however the distance between the primary and secondary locations is such that it is plausible that a disruption could affect both locations simultaneously. Facility arrangements assume that alternate buildings in the NCR will be accessible and available as a suitable work environment, but there are plausible situations where this would not be the case. Note that the BCP states that the IMT would approve the allocation of available resources among the Sectors/Branches based on the Department's operational priorities, with critical services on behalf of the Government of Canada being paramount. BCPs also identify various continuity options for infrastructure outages (e.g. teleworking, working from an alternative site or suspending services that are not as critical as others for a short period of time), but there is a lack of details to describe how each option would be chosen and implemented.

While planning for each potential incident that could result in the invocation of the BCP is not realistic or an effective use of resources, planning for the Department's response in greater detail will strengthen IC's position to effectively minimize the impacts of a potential incident.

In the absence of more detailed recovery plans, the onus is on management to perform analysis and make decisions on potential recovery options during an incident and potentially at a time of crisis. There is a risk decisions made in these situations may not be optimal.

Recommendation 3**:** Sectors/branches, in collaboration with CMS, should ensure that BCPs address all of the OSS-BCP requirements. As well, it should ensure that recovery plans, resource requirements, measures and procedures respond to a range of disruptions of varied severity.

3.5 Program Maintenance and Readiness

BCPs are kept current through processes initiated by a combination of formal and ad-hoc triggers to account for changes to the Department and its operating environment.

Once BCPs are developed, approved and put into effect, it is important that a permanent maintenance cycle be established that includes ongoing review of all plans to account for changes to the Department and its operating environment (e.g. operations, dependencies, legislation, management, mandate, organization, stakeholders and threat environment).

Interviews and documentation review demonstrated that processes initiated by a set of formal and ad-hoc (i.e. event driven) triggers exist to update BCPs and supporting documents outside of the annual review cycle, including:

- **Formal triggers:**
    - Annual review cycle; and
    - BCPWG monthly call outs for updated contact lists.

- **Ad-hoc triggers:**
    - Lessons learned and improvements that are discussed at BCPWG meetings;
    - Organizational structure changes; and
    - Staff changes.

The results demonstrated that BCPs are kept current through ongoing updates to account for changes to the Department and its operating environment.

Awareness and Training

Communication and awareness activities are ongoing to support employees in executing their BCP roles and responsibilities.

Effective awareness and training activities help employees in the execution of their responsibilities pertaining to BCP program maintenance (i.e. BIA and BCP development) and incident response.

The BCP communication and awareness strategy, which was defined and documented in 2012-13, describes how the Department would inform senior management and employees of the BCP program Renewal Project, and their associated roles and responsibilities. The communication and awareness strategy included the following activities:

- Debriefs to senior management on the status of the BCP program;
- Distribution of awareness messages in This Week @ IC, a weekly departmental newsletter for all staff;
- Periodic BCPWG meetings;
- Periodic table top exercises; and
- Posting of the departmental and sector/branch BCPs on the IC Wiki.

Although the communication and awareness strategy was not updated for fiscal year 2013-14 and 2014-15, interviews and documentation review demonstrated that the BCP Program has performed the following activities to prepare individuals to execute their BCP roles and responsibilities; which is in line with the 2012-13 BCP communication and awareness strategy:

- Debriefs to senior management on the status of the BCP program;
- Periodic BCPWG meetings which provided BCP coordinators with the opportunity to share best practices and lessons learned;

- Table top exercises (i.e. facilitated simulation) were conducted at the Departmental Management Committee (DMC) and the BCPWG levels. As well, some branches/sectors have held their own internal table top exercises to train and refresh designated employees on BCP response; and
- Templates, guides and awareness products (e.g. checklists and incident action plans) were produced that support the development of BIAs and BCPs.

Some sector management indicated that additional training would be beneficial to support employees with BCP related responsibilities.

Key BCP roles and responsibilities for staff are twofold; program maintenance (i.e. BIA and BCP development) and incident response.

The knowledge and awareness to carry out program maintenance relies primarily on templates and guides. As well, designated employees participate in BCPWG meetings and receive support from the BCP coordinator to oversee the development of BIAs and BCPs. There is no formal training for program maintenance.

The second set of responsibilities relates to incident response. Table top exercises have been the main vehicle to train and refresh designated employees on incident response and overall roles and responsibilities. However, some sector management interviewed indicated that additional training would be beneficial to support individuals with BCP related activities.

Without sufficient training, there is a risk that key staff may not fully understand their role and responsibilities when the BCP plan is invoked, and BCP coordinators or their delegates may not have adequate knowledge or skills to effectively develop or refresh BIAs and BCPs on an annual basis.

Recommendation 4: Sector/branch management, with the assistance of CMS, should assess whether additional training is needed for employees with BCP responsibilities. If the assessment reveals that there is a common training need across sectors/branches, CMS should coordinate the provision of the training.

Testing and Validation

Table top exercises have occurred at the departmental level as well as in some sectors. However, this testing could be enhanced with a formal testing approach for the Department to ensure that it is occurring frequently enough and at varying levels of complexity.

Regular testing and validation of BCPs should be performed to determine if the Department is well-positioned to effectively respond to a wide range of incident types and potential threats (including high-impact, low-likelihood scenarios), and to identify areas for improvement.

Sectors/branches are encouraged at BCPWG meetings to perform at least one table top exercise per year during the annual refresh cycle. With the participation of branch/sector representatives, table top exercises have been held at the DMC and BCPWG levels. In addition, some branches/sectors have held their own internal table top exercises.

While BCPWG table top exercises occur on an annual basis, sectors/branches engage in testing activities on an ad hoc basis. Although numerous testing exercises have been held, a regular testing approach does not exist that coordinates the testing at the various levels of the organization. To better formalize the frequency of testing exercises, the BCP program expects that annual table top exercises will be mandatory for branches/sectors starting as of the next BCP refresh cycle (November 2014); this is in line with the departmental Security Policy which states that BCPs for critical business processes shall be continuously reviewed and tested for currency.

It is also important that testing exercises are performed at varied levels of complexity to adequately validate plans. Additionally, testing should include validation of key dependencies, including IT resources and facilities.

Interviews and documentation review indicated that testing in some sectors was limited. In many cases, test exercises were described to have been used as a training tool (i.e. refreshing employees on roles and responsibilities and BCP concepts) rather than to validate BCPs and test effectiveness. The testing of key dependencies has not been incorporated into table top exercises, and independent testing of key dependencies such as IT resources (including connectivity and access) and facilities has been inconsistent.

There is a risk that all sector/branch BCPs have not been adequately tested and validated to identify gaps, including key dependencies such as IT resources and facilities.

Recommendation 5: CMS should develop and document a testing approach which outlines an appropriate frequency and complexity of testing, along with testing of key dependencies.

Lessons Learned

The best practice of capturing lessons learned following an actual business disruption or a testing exercise is being done. However, it is done informally and inconsistently, and action items raised from lessons learned are not tracked to completion.

The program can continuously improve capturing lessons learned from business disruptions and testing exercises and tracking these lessons to completion/implementation.

Auditors reviewed post mortem and situational reports from two actual incidents and three testing exercises, and found that in all cases, there was no formal mechanism in place to track action items to completion/implementation. There is a risk that plans and tools may not be updated appropriately to reflect lessons learned from actual business disruptions or testing.

***Recommendation 6*:** Sectors/branches should:

a) Share lessons learned with all BCPWG members via the departmental BCP coordinator ; and
b) Ensure action items following from lessons learned are addressed in order for BCP processes and practices to be improved.

3.6 Management Response and Action Plan

The findings and recommendations of the audit were presented to the Corporate Facilities and Security Branch within CMS as well as to the CIO. Management has agreed with the findings included in this report and will take action to address the recommendations. Most of the action items will be implemented by CMS by May 2015. The CIO agreed to finalize an “IT Service Continuity Management Program Framework” and an “Implementation Plan” that align with the OSS-BCP by May 2015. Subsequently, the CIO will implement the program by March 2017. This entails designing, developing, documenting, testing and maintaining procedures to support IT continuity response plans. Also, there will be some portions of these plans that are subject to shared accountability between IC and Shared Services Canada.

The BIA process, including tools, will be reviewed and amended to better assist in the criticality assessment and requirements definition of business functions and services. As well, the BCP documents will be updated to ensure a complete coverage of the TBS Operational Security Standard– BCP. To support BCP program readiness, the need for additional training will be assessed. In addition, the testing approach will be formally documented and action items arising from lessons learned will be formally tracked.

4.0 Overall Conclusion

The focus of the audit was solely on the BCP Program which provides direction to IC with regards to its responsibilities during business disruptions. The audit did not assess the emergency support plans and related measures undertaken by SITT and IS to ensure delivery of the six critical services.

The audit results revealed that the BCP Program is operating effectively in the area of program governance. Opportunities for improvement and associated recommendations were identified to address low to moderate risks[2] to the Department, in the areas of business impact analysis, business continuity plans and program maintenance and readiness.

[2] "Low to moderate" because it is Low in most audited areas and Moderate in two areas: 1) CIO (in collaboration with SSC): The length of time required to implement the IT service continuity program (2016-17 per the MAP); and 2) CMS: Criticality assessment/prioritization – i.e. the BIA process should categorize business functions and services consistently across the organization based on provided guidelines.

Appendix A: Industry Canada’s Emergency Support Function responsibilities to the Government of Canada and related critical services

I. Industry Canada’s Emergency Support Function responsibilities to the Government of Canada

The *Emergency Management Act* defines emergency management as the prevention and mitigation of, preparedness for, response to, and recovery from emergencies. Under the *Emergency Management Act*, the Minister of Public Safety is responsible for coordinating the Government of Canada’s response to an emergency. The Federal Emergency Response Plan (FERP) is the Government of Canada’s “all-hazards” response plan.

Public Safety Canada developed the FERP in consultation with other federal government institutions. The FERP outlines the processes and mechanisms to facilitate an integrated Government of Canada response to an emergency and to eliminate the need for federal government institutions to coordinate a wider Government of Canada response.

Industry Canada (IC) has been identified as a primary Department in support of the telecommunications and manufacturing sectors. A primary Department is a federal government institution with a mandate directly related to a key element of an emergency. Their responsibilities are further detailed in each Emergency Support Function.

Emergency Support Functions (ESF) provide the mechanisms for grouping functions most frequently used in providing federal support to provinces and territories or federal-to-federal assistance in response to a request for assistance during an emergency. ESFs are allocated to federal government institutions in a manner consistent with their respective mandated areas of responsibility, including policies and legislation, planning assumptions and a concept of operations. In turn, these ESFs are used to augment and support the primary federal government programs, arrangements or other measures to assist provincial/territorial governments and through these governments, to local authorities or to support the Government Operations Centre (GOC) in coordinating the Government of Canada’s response to an emergency.

The relationship between Emergency Response and Business Continuity

During an emergency response, IC is responsible for managing the information flow to and from stakeholders (i.e. telecom and manufacturing) and other government departments, particularly Public Safety Canada (PSC). IC may become more deeply involved as situations deteriorate and requests for assistance are made from the telecom community, such as additional frequencies for first responders.

It is worth noting that IC’s emergency response may or may not occur during the context of a business disruption to the Department.

IC’s ESF responsibilities involve six critical services which are the following:

1. International Radio Frequency Coordination

2. Emergency Telecom and Cyber Security Response
3. Remediation to Terrestrial Interference
4. Licensing of Terrestrial Services
5. Certification, Coordination and Technical Analysis for Broadcast, Radio and TV
6. Critical Infrastructure Protection (Manufacturing) Secure Industrial Supply

Five of the six critical services are related to telecommunications and reside with the SITT sector. To ensure delivery of these critical services, if required, the SITT sector has developed:

- A unique BCP document for the telecommunications critical services to complement the SITT and departmental BCP. The document provides contact information for management and key representative of critical services (in case there is a telecommunications emergency during a BCP incident). As well, the document describes the transfer of the chain of command to the regions in the event that the business disruption has a large impact on the NCR.
- Strategic and operational telecommunications emergency plans to support the delivery of critical services. One of the regional emergency plans describes operational processes based on a series of the most common emergency situations including receiving a request for assistance from another region (thereby leveraging the Sector's distributed workforce in support of these critical services).
- Communication arrangements that include the use of wireless priority services and satellite phones in the event of congestion on terrestrial and wireless networks.

To fulfil its emergency responsibility for manufacturing, the Department's IS has focussed their efforts on developing a database of information to quickly reach and monitor the largest possible number of companies in the manufacturing sector (thereby establishing a sourcing network).

For the ability to deliver critical services in a business disruption, both SITT and IS work closely with PSC, other government departments as well as key stakeholders on emergency preparedness. Consequently, both sectors have indicated that they have participated in testing exercises at the federal and provincial level. SITT and IS have stated that they have arrangements in place to access key information in the event of an IT outage at IC. In addition, the CIO has acknowledged the IT requirements for critical services; the CIO BCP document has identified the mapping between the Department's critical services and their respective IT applications so priority is given to these when necessary.

Therefore, the Department has arrangements in place to fulfill their ESF responsibilities that can apply within the context of a business disruption.

Appendix B: Audit Criteria

Criteria	Criteria Met/ Met with Exception(s) / Not Met
BCP Program Governance	
1. Governance structures provide guidance and oversight to the BCP Program.	Met
Business Impact Analysis	
2. BIAs assess the impacts of disruptions on the Department and prioritize critical operations and associated assets.	Met with exceptions
Business Continuity Plan and Arrangements	
3. Business continuity and recovery strategies have been identified, assessed, selected and approved, and BCPs are consistent with policy requirements.	Met with exceptions
BCP Program Maintenance and Readiness	
4. BCPs are kept current through ongoing review to account for changes to the Department and its operating environment (e.g. legislation, critical operations, organization, mandate, management, threat environment, stakeholders and dependencies).	Met
5. BCP training and awareness program activities prepare employees to execute their roles and responsibilities pertaining to the BCP Program.	Met with exceptions
6. BCPs are subject to testing and validation, which includes the preparation of lessons learned reports and the updating of BCPs after testing activities or actual events.	Met with exceptions