Environment and Climate Change Canada
Environnement et Changement climatique Canada

Audit of business continuity planning

Final report

December 2017

Canada

List of acronyms and abbreviations

BCP	Business continuity planning
BIA	Business impact analysis
CS	Critical service
CSS	Critical support service
DM	Deputy Minister
EAAC	External Audit Advisory Committee
ECCC	Environment and Climate Change Canada
EPB	Environmental Protection Branch
DSO	Departmental security officer
EMA	Emergency Management Act
IT	Information technology
MSC	Meteorological Service of Canada
NEEC	National Environmental Emergencies Centre
OCG	Office of the Comptroller General
SLA	Service-level agreement
SSC	Shared Services Canada
STB	Science and Technology Branch
TB	Treasury Board
TB-OSS-BCP Program	Treasury Board's Operational Security Standard-Business Continuity Planning Program

Table of contents

Executive summary i
1. Introduction and background 1
2. Objectives, scope and methodology 3
3. Findings, recommendations and management responses 5
3.1 Departmental governance framework for BCP 5
3.2 Departmental business continuity planning processes 8
3.3 Training and awareness 11
4. Conclusion 12
Appendix A: Audit criteria 14
Appendix B: References 15

Executive summary

The Audit of business continuity planning (BCP) was conducted concurrently with the Office of the Comptroller General's (OCG) Horizontal Audit of BCP, which involved selected large and small departments and agencies, including Environment and Climate Change Canada (ECCC).

The objective of the internal audit was to determine whether ECCC had in place a departmental governance framework and processes for BCP.

Why is business continuity planning important

Every department is at risk from potential disasters, including natural disasters, sabotage, power and utility disruptions and cyber-attacks. Critical services or products are those that must be delivered to ensure survival, to avoid causing injury and to meet legal or other obligations of an organization.

Strongly integrated BCP governance and processes are key to enhancing the resilience of government operations. Specifically, in the event of disruptions to normal government business operations, these elements will help enable service delivery to Canadians, with minimal downtime.

What we found

Key elements of departmental BCP governance framework, such as governance committees, formal policy and key BCP roles and responsibilities, were in place. However, monitoring and reporting have been limited to Executive Management Committee (EMC) presentations of an annual BCP status report, a high-level overview of what works well and areas requiring improvement. Furthermore, testing of the plans was limited to table-top exercises instead of full-scale tests. A formal monitoring and reporting frameworks (including testing) to periodically assess the effectiveness and compliance of the BCP program would enable ECCC to proactively identify and address any existing gaps and enhance the Department's resilience to events that disrupt normal business operations.

While the departmental policy and plan provide for training and awareness activities, the audit found that ECCC activities in this area are currently limited to providing some useful tools on BCP and recovery activities.

ECCC has conducted business impact assessments (BIA) and has business continuity plans in place for the critical services sampled. Two of the three critical services reviewed had a service level agreement in place to describe service levels for the restoration of critical services. For the most part, the BIAs and the plans were developed in conformity with government's BCP requirements.

Improvements in the following areas are required for ECCC to be in a better position to ensure the continuity of its operations in the event of a disruption:

- more effectively communicate BCP roles and responsibilities to decision makers by providing an updated BCP program policy that is aligned to the government's security policy framework

- contribute to enhancing the overall effectiveness of the BCP program by ensuring that BCP roles, responsibilities and reporting relationships are clearly defined and formally communicated to all staff involved in the departmental BCP process
- proactively identify and address any gaps that have an impact on departmental effectiveness and compliance with the government's overall BCP requirements by establishing a formal BCP monitoring and reporting framework (including testing the BCP program)
- ensure that business continuity plans are in place and have been developed in accordance with baseline requirements, including a clear external stakeholder relationship for information technology (IT) service delivery and in particular, the establishment of service level agreements describing service levels for the restoration of critical services
- develop and implement a departmental BCP program awareness, training and testing plan

Management agrees with the recommendations and has provided an action plan that will strengthen the management control framework supporting the BCP.

1. Introduction and background

The Audit of business continuity planning (BCP) was conducted concurrently with the Office of the Comptroller General's (OCG) Horizontal Audit of BCP, which involved selected large and small departments and agencies, including Environment and Climate Change Canada (ECCC). As recommended by the External Audit Advisory Committee (EAAC) and approved by the Deputy Minister (DM), the internal audit was included in the Audit and Evaluation Branch's (AEB) 2015 Integrated Risk-Based Audit and Evaluation Plan.

BCP is a proactive security measure to help increase an organization's resilience to disruptive events. Specifically, BCP refers to the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of services and assets when a disruption to normal business operations occurs, regardless of the disruption's origin. On a broader scale, BCP complements emergency management because it supports preparedness, response and recovery activities.

The Emergency Management Act (EMA) requires that all federal departments and agencies prepare plans to deal with emergencies. According to the EMA, the emergency management responsibilities of each deputy head consist of identifying the risks that lie within the purview of their department and:

- preparing emergency management plans (for example, strategic emergency management plan and building emergency evacuation plans) to address these risks
- maintaining, testing and implementing those plans
- conducting exercises and training in relation to those plans

The Treasury Board (TB) Policy on Government Security and its associated standard, the Operational Security Standard – Business Continuity Planning Program, further establish that departmental critical services and associated assets must remain available, to ensure the continued health, safety, security and economic well-being of Canadians and the effective functioning of government.

Under the EMA, departmental emergency management plans must be supported by "programs, arrangements or other measures to provide for the continuity of the operations."[1] Such support is achieved by establishing departmental BCP programs that comprise the following:

- BCP program governance (for example, BCP policy, appointment of a Departmental Security Officer and a BCP coordinator)
- business impact analyses (for example, to assess the impacts of disruptions on the Department and to identify and prioritize critical services and associated assets)
- business continuity plans and arrangements

[1] Emergency Management Act, Article 6 (2)(c). June 22, 2007.

- maintenance of BCP program readiness (for example, review and revision of all plans and regular testing)

The Departmental Security Officer (DSO) is responsible for the departmental BCP program, including the monitoring and coordination of the development, implementation and review of the program.

2. Objective, scope and methodology

Objective

The objective of the audit was to determine whether ECCC had in place a departmental governance framework and processes for business continuity planning (BCP).

Scope

The audit focused on the BCP governance framework and processes that were in place on December 31, 2015. For the assessment of departmental BCP processes, the scope also included a risk-based sample of departmental business continuity plans as of that date.

The audit team expected to find a governance framework and BCP processes that aligned with the government's BCP requirements (for example, TB's Operational Security Standard – Business Continuity Planning Program [TB-OSS-BCP Program]).

Given the unique nature, complexities and risks, ECCC's emergency operations centres and their related standard operating procedures and information technology (IT) continuity planning were excluded from the audit scope.

Methodology

The audit criteria (see Appendix A) were mainly developed using TB's Policy on Government Security and TB-OSS-BCP Program.

The audit approach included the following:

- a review of relevant documentation and systems, including policies, standards, frameworks and processes supporting the BCP program
- interviews with senior management and business continuity plan coordinators and owners
- a review of the compliance of the business impact analysis and business continuity plans for ECCC's critical services and critical support services with the requirements outlined in the TB-OSS-BCP Program (see Table 1 for sample)

Table 1: Sample of ECCC critical services (CS) and critical support service (CSS) reviewed

CS or CSS	Service description	ECCC lead
CS	Weather and environmental forecasts	Meteorological Service of Canada (Canadian Meteorological Centre, Montreal [Quebec])
CS	National hydrometric monitoring	Meteorological Service of Canada (Canadian Centre for Inland Waters, Burlington [Ontario])
CS	Maintain national incident reporting and alerting systems	Environmental Protection Branch (National Environmental Emergencies Centre (NEEC), Montréal [Quebec])
CSS	Emergencies, operational analytical laboratories and research support, including scientific expertise and on-site field support for environmental emergencies and technical support services	Science and Technology Branch and Environmental Protection Branch (for River Road location, Ottawa [Ontario])

As mentioned previously, the Audit of BCP was conducted concurrently with the OCG's Horizontal Audit of BCP**.** The objectives of the OCG's audit consisted in determining whether Government-wide and departmental governance frameworks for BCP and departmental BCP processes were in place.

Statement of conformance

The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

3. Findings, recommendations and management responses

3.1 Departmental governance framework for BCP

The Treasury Board (TB) Policy on Government Security states that deputy heads are accountable for the effective implementation and governance of security within their department. They also share responsibility for the security of government as a whole.

The audit examined whether ECCC carried out its governance-related responsibilities according to the Policy on Government Security, the Directive on Departmental Security Management and the Operational Security Standard – Business Continuity Planning (BCP) Program (TB-OSS-BCP Program).

The audit focused on the following aspects of departmental governance for BCP: governance committees, roles and responsibilities, identification and ranking in order of priority of departmental critical services, testing, monitoring and reporting.

Governance committees

As per the Policy on Government Security, "security is achieved when it is supported by senior management—an integral component of strategic and operational planning—and embedded into departmental frameworks, culture, day-to-day operations and employee behaviours."[2] The Directive on Departmental Security Management requires departments to establish security governance mechanisms, such as committees and working groups, to ensure the coordination and integration of security activities and facilitate decision making. Governance is also identified as a key element of departmental BCP programs under the TB-OSS-BCP Program. Departments are therefore expected to have governance committees in place that are actively involved in overseeing and integrating BCP activities.

The audit found that ECCC has formal senior management committees in place to oversee and support the coordination of BCP activities. It focused particularly on two key governance bodies within the BCP structure.

The Director General (DG) Emergency Management Committee is co-chaired by the Departmental Security Officer (DSO) and the DG, Business Policy, Meteorological Services of Canada. It provides senior leadership, coordination and guidance regarding Emergency Management, including the BCP program. The BCP program working group is chaired by the DSO. It coordinates the development and implementation and monitoring of the BCP program and acts as the main coordination, information exchange and consultative committee for the BCP program.

Based on a review of documentation (such as agendas, records of decisions from committee meetings and terms of reference for committees), the audit found that the two committees supported BCP activities.

[2] Policy on Government Security, Section 3.3. July 1, 2009.

Roles and responsibilities

The TB-OSS-BCP Programstates that the development of a departmental BCP program policy approved by senior management is an essential element of governance. It allows expectations to be formally defined and communicated within the current departmental governance structure.

The Directive on Departmental Security Management requires departments to ensure that more specific internal accountability, delegations, reporting relationships and roles and responsibilities of departmental staff with security responsibilities be defined, documented and communicated to the relevant BCP stakeholders. As a result, the Department was expected to have complied with the requirements on BCP-related roles and responsibilities for staff involved in the departmental BCP process (for example, Departmental Security Officer (DSO), BCP Coordinator and functional managers).

An approved BCP policy was in place but it had not been updated in several years. At the time of the audit, the June 2010 policy was being reviewed.

The BCP policy and the departmental and site business continuity plans detail most of the BCP roles and responsibilities. For key internal stakeholders, the information is available online or through appropriate program managers. The standard operating procedures and the branch or site business continuity plans also provide additional information on roles and responsibilities for key emergency management critical service staff. However, the role of the BCP Coordinator has not been clearly defined and documented in the BCP Policy. Furthermore, the reporting relationship between the DSO and the DM (or EMC) has not been formally documented and communicated to both parties in the BCP Policy.

The DSO and the BCP Coordinator were formally appointed in accordance with the government's requirements. The audit noted that these stakeholders were held accountable for their performance in fulfilling their BCP roles (for example, through their annual performance management agreement).

Roles and responsibilities of external stakeholders were reviewed as part of the review of the business continuity plans in section 3.2 of this report.

Recommendation 1
The Assistant Deputy Minister, Corporate Services and Finance Branch, should ensure that an up-to-date business continuity planning program policy is in place and aligns with the government's security policy framework.
Management response
Management agrees with the recommendation. The Departmental Security Division will review and update the 2010 Environment Canada's Business Continuity Planning Program Policy (and other related policy documents, as required, such as the BIA documentation and the terms of reference for the BCP Working Group). The Departmental Security Division will ensure that the revised version of these documents aligns with

the government's security policy framework. The revised policy will clearly outline roles, responsibilities and reporting relationships through a clear governance structure. The revised policy will be approved by ECCC's Executive Management Committee, will be communicated to employees and posted on ECCC's intranet, and will be reviewed every three years.
Recommendation 2
The Assistant Deputy Minister, Corporate Services and Finance Branch, should ensure that roles, responsibilities and reporting relationships for business continuity planning are clarified and formally communicated to all staff involved in the departmental BCP process.
Management response
Management agrees with the recommendation. The Departmental Security Division will ensure that BCP roles, responsibilities and reporting relationships are communicated to all levels of management, key business continuity stakeholders within ECCC, and all employees. This includes outlining the DSO's functional reporting to the DM. The Departmental Security Division will use presentations to management, communiqués to employees as well as training and table-top exercises.

Identification and ranking of departmental critical services

It is a government requirement to systematically identify, update and rank (in order of priority) the department's critical services, to ease recovery and the continuous delivery of departmental services. If BCP critical services and priorities are not assessed and the results communicated to staff in a timely manner, it could lead to poorly coordinated recovery responses and impede the achievement of BCP objectives.

The audit found that ECCC has put in place a systematic approach for identifying and ranking its critical services in order of priority. This is done through ECCC's Strategic Emergency Management Risk Assessment exercise, which follows the guidelines provided by Public Safety Canada.

Testing, monitoring and reporting

Under the government's security policy framework, departments must put in place monitoring and reporting frameworks to periodically assess the effectiveness and compliance of their BCP programs. The TB-OSS-BCP Program also requires departments to conduct regular testing and validation of all their business continuity plans. Public Safety's A Guide to Business Continuity Planning recommends that all departments conduct internal reviews annually or biannually to ensure the accuracy, relevance and effectiveness of their business continuity plans.

The Department has not fully complied with the requirements and recommended practices. ECCC has not demonstrated that is has put in place BCP monitoring and reporting frameworks to ensure compliance with the government's security policy framework and the overall effectiveness of its BCP program. Monitoring and reporting have been limited to EMC presentations of an annual BCP status report, a high-level overview of what works well and areas requiring improvement.

Regarding the testing of the business continuity plans, the audit found that the Department did not conduct full-scale[3] tests. Moreover, the testing conducted was limited to table-top exercises[4].

The most recent table-top exercise was conducted in February 2016. The Department did not engage a broader range of employees, which would have maximized readiness for emergency scenarios (in addition to employees engaged in operational responses). As a result, ECCC did not demonstrate that it has adopted formal testing programs encompassing regular testing and validation of all business continuity plans, in accordance with the government's policy requirements and recommended practices.

Regular formal monitoring and reporting on the overall compliance and effectiveness of departmental BCP program would enable ECCC to proactively identify and address any existing gaps and enhance the Department's resilience to events that disrupt normal business operations. As a key component of such a monitoring and reporting framework, the periodic testing of business continuity plans would provide ECCC with practical assurance of the likelihood that these plans will work when faced with such disruptions.

Recommendation 3
The Assistant Deputy Minister, Corporate Services and Finance Branch, should establish formal monitoring and reporting frameworks for business continuity planning (BCP), including testing the BCP program, to ensure compliance with the government's security policy framework and the overall effectiveness of BCP program.
Management response
Management agrees with the recommendation. The Departmental Security Division will establish a monitoring and reporting framework which will be an integrated part of ECCC's business continuity planning program. The monitoring and reporting framework will include a testing/exercising component as well as a reporting component to capture the number of plans completed, approved, exercised/tested, as well as compliance to ECCC, TBS and Public Safety's policy instruments and technical guidance. ECCC's goal is to test Branch BCPs, which includes critical services and critical support function recovery strategies, on a yearly basis. The reporting component will be used to keep senior management apprised of the business continuity planning programs' effectiveness and progress. The Branch-level Business Continuity Plan will be reviewed and revised if necessary every year, as outlined in the current iteration of the Branch Business Continuity Plan.

3.2 Departmental business continuity planning processes

As part of baseline security requirements, all departments must have business continuity plans in place to provide for the continuity of government operations. Conducting a business impact

[3] Full-scale tests (such as drills) are exercises that simulate a full deployment to the alternate site and evaluate the entire business continuity plan or plans with all the necessary resources (ADMs, DGs, directors and internal and external stakeholders), personnel or equipment. All critical services are included in the exercises.
[4] Table-top exercises are discussion sessions where certain departmental representatives meet in an informal setting to discuss their roles and responsibilities during an emergency and their responses to a particular emergency scenario.

analysis (BIA) is a fundamental starting point in the process for developing a plan. The government's requirements related to these processes are covered in the TB-OSS-BCP Program.

The audit assessed a risk-based sample (see Table 1) of BIAs and departmental business continuity plans to determine the extent to which the Department complied with these requirements.

Business impact analyses

BIAs provide the basic information that departments need to strategically focus their efforts and limited resources in the areas that matter most for the continuity of their operations. The audit found that the BIAs reviewed were completed and the Department complied with the requirements prescribed for BIAs in the TB-OSS-BCP Program. The BIAs examined included:

- an assessment of services to determine which are likely to cause a high degree of injury to Canadians or the government
- prioritization of services based on their maximum allowable downtimes[5] and minimum service levels[6]
- senior management approval of BIAs
- the identification of internal and external dependencies (for example, with other functions or resources) relied upon for service delivery

Business continuity plans

Business continuity plans are the main outputs of the BCP process. They provide a blueprint for the actions that will need to be undertaken in the event of a disruption to normal business operations. Specifically, they contain pre-established and agreed-upon procedures, including all the relevant information for enabling the continuity and subsequent recovery of departmental business operations impacted by disruptions.

The audit examined plans and concluded that ECCC had business continuity plans that:

- covered all of the services sampled
- included most of the basic information required under the TB-OSS-BCP Program
- generally conformed to the BCP processes outlined in the TB-OSS-BCP Program

The business continuity plans included:

- a description of the critical services
- required resources (personnel, information and assets)

[5] Maximum allowable downtime refers to "the longest period of time for which a service can be unavailable or degraded before a high degree of injury results." (Source: TB-OSS-BCP Program)
[6] Minimum service level refers to "the level of service delivery which is essential to avoid a high degree of injury is maintained until full recovery is achieved." (Source: TB-OSS-BCP Program)

- internal and external dependencies
- approved recovery strategies
- measures to deal with the impact and effect of disruptions on the Department
- identification of the roles and responsibilities of response and recovery teams
- identification of the roles and responsibilities of internal and external stakeholders
- coordination mechanisms and procedures to collaborate with departmental support functions
- communication strategies

The most significant area for improvement is the identification of external dependencies (for example, IT provider) upon which the Department relies. In particular, two of the three critical services reviewed had a service level agreement in place. The purpose of the agreement is to describe, in general terms the ongoing business relationship between the external stakeholder and the partner organization. It is designed to ensure that:

- accountabilities related to the ongoing delivery of services are clear
- the expectations and commitments of both the external service provider and the partner organization are well understood and clear

Without a service level agreement or other formal agreement in place that defines and clarifies expected service levels, business owners have no assurance that their critical service can be restored in keeping with the stated maximum allowable downtime in the event of a disruption or disaster. This then leaves some uncertainty for business owners about whether they can deliver critical services.

Recommendation 4
The Assistant Deputy Minister, Corporate Services and Finance Branch, in collaboration with the business owners, should ensure that business continuity plans are in place and that they have been developed in accordance with baseline requirements. The business continuity plans should include a service level agreement or other formal business arrangement with external service providers, describing service levels for the restoration of critical services.
Management response
Management agrees with the recommendation. Responsible branch heads, RDGs or senior building officers will review and update their business continuity plans to ensure that they align with baseline requirements and revised BCP templates. The Departmental Security Division will also support the review and update of ECCC business continuity plans and review and update their associated business impact analysis. The monitoring and reporting component outlined under Recommendation 3 will be used to ensure that plans are in place and up to date, and to monitor progress. The monitoring and reporting component will also include a questionnaire (TBS Standard -

Section 3.4) to ensure that all essential elements, including service level agreements with external service providers, have been addressed during the Branch BCP development process.

3.3 Training and awareness

Departments are responsible for developing BCP training and awareness plans, a key component of the departmental readiness framework.

ECCC's BCP program policy and its departmental business continuity plan highlight that BCP training and awareness component is delivered at both individual and collective levels. This component includes a range of activities such as technical courses, seminars, workshops, table-top exercises and more elaborate exercises, preferably delivered in partnership with other government departments. Training and awareness involve all managers and employees. The priority is on critical services, associated assets and critical support functions, as informed by threat and risk assessments and the BIAs.

While the departmental policy and plan provide for training and awareness activities, the audit found that ECCC activities in this area are currently limited to providing some useful tools on BCP and recovery activities, such as operational manuals for emergency centres operators, standard operating procedures and senior building officers manual. As well, tools exist for senior management (for example, a BCP related aide-memoire). However, there should be a broader engagement of departmental staff to maximize readiness during an event.

The 2015 annual BCP status report, referred to earlier in the report, highlighted the need to develop a departmental BCP awareness and training plan and set out some areas of improvements. For example, it suggested the development of a targeted awareness, training and testing plan, focused on coordination and communication responsibilities for those with incident response or business continuity responsibilities, including departmental managers, regional director generals, senior management and the Minister's Office.

A lack of proper training and tools could lead to inefficiency and ineffectiveness in the implementation of business continuity plans.

Recommendation 5
The Assistant Deputy Minister, Corporate Services and Finance Branch, should develop and implement a BCP program awareness and training plan.
Management response
Management agrees with the recommendation. The Departmental Security Division will establish a BCP awareness and training plan aimed at providing targeted training to branch BCP Coordinators, as well as providing BCP program awareness and roles and responsibilities to all employees.

4. Conclusion

Every department is at risk from potential disasters, including natural disasters, sabotage, power and utility disruptions and cyber-attacks. Critical services or products are those that must be delivered to ensure survival, avoid causing injury and meet legal or other obligations of an organization.

Strongly integrated BCP governance and processes are key to enhancing the resilience of government operations. More specifically, in the event of disruptions to normal government business operations, these elements will help enable service delivery to Canadians with minimal downtime.

Key elements of departmental BCP governance framework, such as governance committees, formal policy and key BCP roles and responsibilities, are in place. However, monitoring and reporting have been limited to Executive Management Committee presentations of an annual BCP status report, a high-level overview of what works well and areas requiring improvement. Furthermore, testing of the plans was limited to table-top exercises instead of full-scale tests. A formal monitoring and reporting frameworks (including testing) to periodically assess the effectiveness and compliance of the BCP program would enable ECCC to proactively identify and address any existing gaps and enhance the Department's resilience to events that disrupt normal business operations.

While the departmental policy and plan provide for training and awareness activities, the audit found that ECCC activities in this area are currently limited to providing some useful tools on BCP and recovery activities.

ECCC has conducted business impact assessments (BIA) and has business continuity plans in place for critical services sampled. Two of the three critical services reviewed had a service level agreement in place to describe service levels for the restoration of critical services. For the most part, the BIAs and the plans were developed in conformity with government's BCP requirements.

Improvements in the following areas are required for ECCC to be in a better position to ensure the continuity of its operations in the event of a disruption:

- more effectively communicate BCP roles and responsibilities to decision makers by providing an updated BCP program policy that is aligned to the government's security policy framework
- contribute to enhancing the overall effectiveness of the BCP program by ensuring that BCP roles, responsibilities and reporting relationships are clearly defined and formally communicated to all staff involved in the departmental BCP process
- proactively identify and address any gaps that have an impact on departmental effectiveness and compliance with the government's overall BCP requirements by establishing a formal BCP monitoring and reporting framework (including testing the BCP program)

- ensure that business continuity plans are in place and have been developed in accordance with baseline requirements, including a clear external stakeholder relationship for IT service delivery and in particular, the establishment of service level agreements describing service levels for the restoration of critical services
- develop and implement a departmental BCP program awareness, training and testing plan

The areas of improvement that have been noted will collectively strengthen the management control framework supporting BCP.

Appendix A: Audit criteria

Line of enquiry 1: Departmental governance framework – A departmental governance framework is 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 and 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 business continuity plans	
2.1	The Department has conducted the business impact analysis (BIA).
2.2	The Department developed recovery strategies for the critical services identified in its BIAs, which take into account interdependencies with other departments.
2.3	The Department developed business continuity plans to ensure the continuity of its critical services and critical support services.
2.4	The Department coordinates with critical support service providers and other key internal stakeholders when developing, testing and updating its business continuity plan to ensure integration between all parties.
2.5	The Department ensures that sufficient and relevant training and tools are provided to enable BCP and recovery activities.
2.6	The Department ensures that its 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	The Department monitors and reports on the effectiveness of its business continuity plan.
3.2	The Department monitors its compliance with BCP related requirements in the Treasury Board Policy on Government Security and informs the Secretariat of any gaps.

Appendix B: References

Canada. Public Safety Canada. Federal Policy for Emergency Management. Ottawa: January 1, 2016.

Canada. Treasury Board. Directive on Departmental Security Management. Ottawa:July 1, 2009.

Canada. Treasury Board. Operational Security Standard – Business Continuity Planning (BCP) Program. Ottawa:March 23, 2004.

Canada. Treasury Board. Policy on Government Security. Ottawa:April 1, 2012.

Disaster Recovery Institute Canada. Professional Practices for Business Continuity Practitioners. Toronto: 2017.