Employment and Social Development Canada
Emploi et Développement social Canada

Now and Tomorrow
Excellence in Everything We Do

Unclassified

Audit of Business Continuity Planning

May 2017

Internal Audit Services Branch

Audit of Business Continuity Planning

This publication is available for download at canada.ca/publicentre-ESDC . It is also available upon request in multiple formats (large print, Braille, audio cassette, audio CD, e-text diskette, e-text CD, or DAISY), by contacting 1 800 O-Canada (1-800-622-6232). By teletypewriter (TTY), call 1-800-926-9105.

PDF

Cat. No. : Em20-69/2017E-PDF
ISBN: 978-0-660-09174-7

ESDC

Cat. No. : SP-1149-07-17

Table of Contents

1. Background

1.1 Context

As part of Treasury Board's policy instruments on government security, departments must establish a Business Continuity Planning (BCP) Program. The intent of the Program is to plan for the continued availability of services and associated assets that are critical to the health, safety, security or economic well-being of Canadians, or to the effective functioning of government.

BCP is a preventive control that builds resiliency before disaster strikes. As per Treasury Board's *Operational Security Standard on BCP Program*, business continuity plans are required for all services that, if interrupted, would result in a high degree of injury to Canadians or the working of government.

As per the above standard, a BCP Program is composed of four elements:

- The establishment of BCP Program **governance** to integrate BCP into the Department's strategic business planning framework and ensure key stakeholder participation in the decision making process.
- The conduct of a business impact analysis to **identify and prioritize critical services** and associated assets based on maximum allowable downtime and the minimum service level required before high degree of injury will result.
- The **development of business continuity plans** and arrangements (with service providers and other departments) that include senior management approval to support and fund selected strategies.
- The maintenance of BCP Program **readiness** through regular testing and validation of all plans as well as training as required.

1.2 Audit Objective

The objective of this audit was to determine whether the Department has adequately planned for the continued availability of its critical services.

1.3 Scope

The scope of this audit included the Department's BCP Program and all services required to complete a business impact assessment. It focused on BCP for critical services (i.e. excluding any plans for non-critical services) and did not include emergency management.

This audit used Treasury Board's *Operational Security Standard on BCP Program* (in accordance with the *Policy on Government Security*) as well as Public Safety's *Guide to Business Continuity Planning* as its reference framework to build its criteria.

1.4 Methodology

The audit team has reviewed the Department's BCP Program including its governance, select business impact analysis and their corresponding business continuity plans and arrangements for critical services. The audit team also reviewed how the BCP Program readiness is maintained.

In addition to these document reviews, the audit team observed a department-wide table-top testing exercise and interviewed key stakeholders in the BCP Program such as the Integrity Services Branch (ISB) management and management from client branches.

2. Audit Findings

2.1 The Department has planned for the continued availability of its critical services

The following section summarizes key observations on the state of continuity planning within the Department.

Continuity Program Governance

- The Department has established a BCP Program with supporting directives and tools. However, integration within the strategic planning framework is challenging given the Department's decentralized siloed approach to continuity planning.
- The Emergency Management and Business Continuity (EMBC) Division, within ISB, is responsible for the national coordination of the departmental BCP Program (along with a number of other emergency management responsibilities). The EMBC Division has been found to provide the required guidance and direction to branches and regions with respect to continuity planning.
- Key stakeholders up to and including the Branch Assistant Deputy Ministers (ADMs) are involved in the development, approval, implementation and testing of plans.

Critical Services Identification and Prioritization

- All departmental services have been assessed as to criticality, however current processes have not been formalized and are inconsistent. As a result, timely and coherent assessments of services are challenging.
- The EMBC Division extracted a list of 22 programs and services that were deemed critical, 12 of which require recovery within a 0–72 hours range. Supporting these services, a number of activities were identified and provide a foundation for a change to a "service-based" approach.
- Critical services that require recovery within a 0–72 hours range have not been prioritized amongst themselves. In the event of a horizontal disaster affecting multiple services, prioritization of services would benefit from being defined and agreed upon prior to the disruption.

Continuity Plans

- All 22 critical services have documented continuity plans and their associated recovery strategies. However, most selected recovery strategies rarely detail their benefits, risks, feasibility and costs.
- The integration of continuity plans between branches and regions into "service-based" horizontal plans is not consistently performed but is improving.

- The Department relies on other government entities, such as Shared Services Canada (SSC) and Public Services and Procurement Canada (PSPC), for achieving the delivery of some of its critical services. Arrangements are rarely documented or formalized to integrate the Department's plans and the plans of these government entities. Even so, dialogue and collaboration is happening. For example, SSC and PSPC were in attendance at the November 2016 table-top exercise.

- Adopting a horizontal approach to continuity planning could facilitate coordination between the Department and other government entities; this is not only desirable in cases where the Department relies on external partners but also in cases where other government departments rely on Employment and Social Development Canada (ESDC) for the delivery of their critical services (e.g. Immigration, Refugees and Citizenship Canada for the Passport Program).

Maintenance of Readiness

- Table-top exercises are conducted by some branches and at the departmental level to validate the content of plans. One of the key lessons learned from the department-wide November 2016 table-top exercise was that "service-based" horizontal plans where multiple branches coordinate their efforts are essential to ensure the continued availability of critical services.

- The department-wide November 2016 table-top exercise was also valuable in identifying challenges and provided a platform for discussing continuity planning in a horizontal manner. Internal Audit observed an increase in continuity planning related activities in the weeks preceding the exercise (e.g. increased branch working group meetings). We consider the regular conduct of continuity exercises a best practice to be continued. Furthermore, external service providers and partners have been involved in the testing of business continuity plans. This is also a best practice that ought to be continued.

- Lessons learned from exercises as well as real-life incidents are considered when reviewing and updating continuity plans. However, the technical testing of recovery strategies is often limited and provides little assurance as to the viability of the Information Technology (IT) components of continuity plans.

Overall Observations

- Better information management tools are required to allow for effective and efficient management of the BCP Program.

- BCP coordinators within branches and regions don't always have the time or training to be effective continuity planning agents. The leadership of the EMBC Division alone is not sufficient to ensure adequate governance.

- The continuity planning community could benefit from additional training to promote consistent understanding of terminology and practices. The evolution towards continuity "subject matter experts" should be explored; the Innovation, Information and Technology Branch is moving in that direction.

2.2 The implementation of a horizontal "service-based" approach to continuity planning is required

Treasury Board's *Operational Security Standard on BCP Program* promotes a "service-based" view of the organisation. Consequently, impact assessments and continuity plans ought to target services, rather than operational units, directorates, branches or even business lines.

The Department's approach to continuity planning is outlined in the *Operational Directive on Business Continuity Management*. This Directive requires "managers at all levels across the portfolio, branches and regions" to complete business impact analyses and directors to complete continuity plans. This approach creates an environment where the following processes supporting continuity planning become challenging to sustain.

Business Impact Analyses for Identification and Prioritization of Critical Services

The current approach to completing business impact analyses leads to the following issues:

- Internal Audit observed duplication of work between managers responsible for similar services. For example, call or processing centre managers are required by the Directive to individually complete an impact analysis for the services their centre provides. This has led some regions to group offices together that offer similar services in order to avoid duplication. However there is still duplication across regions resulting in impact analyses covering the same services.
- The current approach results in individuals across the Department to assess similar services, often in isolation. To alleviate this issue, the EMBC Division has developed a *Business Impact Assessment Companion Guide* to assist managers in completing their analysis in a comparable and coherent manner. Nonetheless, through its review of impact analyses, Internal Audit noted inconsistencies that could have been avoided if a "service-based" approach was adopted.
- Internal Audit observed some cases of over-classification where some non-critical services were assessed as critical. This could result in resources being spent on planning for the continuity of non-critical services and could lead to increased confusion and risks in case of a disrupting event.
- The number of business impact analyses completed (963) throughout the Department makes the review and challenge function by the EMBC Division difficult to sustain. The idea behind the current approach was that data from the analyses could be extracted and reported on. This was intended to allow the EMBC Division to review, challenge and compile a list of prioritized critical services with limited effort. However, the data repository used to collect and analyse the information had system limitations and performance problems that compromised data entry, data integrity and reporting capability. For example, data entry was abandoned by some managers following technical issues; data integrity could not be enforced to ensure meaningful reporting; and half of expected reports could not be generated. As a result, a manual review and challenge had to be performed on thousands of business functions that were identified as "critical".

Continuity Plans

Continuity plans across the Department have been developed by directors and approved by Directors General and ADMs. The resulting collection of division-level plans suffers issues similar to the issues associated with the impact analysis process such as duplication of effort to develop plans for similar services, time-consuming review and maintenance of the hundreds of resulting plans. Furthermore, this approach which is aligned with the organisational structure of the Department reinforces existing silos and does not foster a "service-based" view of the organization:

- Current tactical division-level continuity plans are rarely integrated into branches' operational or strategic plans. When recovery strategies are fully implemented, this is not an issue. However, when the recovery strategies are not fully funded or implemented, integration in a branch strategic or operational plan allows for better oversight of these strategies.
- Plans developed in isolation cannot be effectively coordinated across the Department. To ensure their continued delivery, all critical services require multiple interdependent branches to coordinate their recovery strategies. Realizing that a more horizontal approach was necessary, the EMBC Division worked with key branches to develop service-based "horizontal" plans. These plans for Employment Insurance (EI), the Canada Pension Plan (CPP) and Old Age Security (OAS) were tested in the November 2016 department-wide table-top exercise. Other service-based "horizontal" continuity plans are expected to be completed in the coming years.
- While silos are still a challenge, and current "horizontal" plans are owned by distinct branches with references to other plans (e.g. EI plan referring to the Citizen Service plan), the Department is moving in the right direction with the development of comprehensive horizontal plans. Collaborative efforts between national headquarter branches and regional delivery networks need to be supported to have a fully integrated approach to business continuity planning.

Recommendation

1. The ADM of ISB should adopt a horizontal "service-based" approach to continuity planning that seeks to minimize effort duplication. This approach should be sustainable, coherent and consistent across the Department.

Management Response

ISB agrees with the recommendation. The Department already adopted a horizontal service-based approach to business continuity planning which has been used for its most critical benefit services. The Business Continuity Management Directive will be reviewed and revised to: align BCP activities with a horizontal service-based approach; streamline non-critical business line business continuity plans and minimize the need for manager level business impact assessments; and reduce duplication of effort for individual plans with similar business functions through horizontal service-based planning applying standardized business functions.

ISB, in collaboration with branches and regions, will adopt a prioritization approach working from highest risk to lower risk to ensure that detailed planning, recovery strategies and resources are put in place for all critical services.

ISB, working with the Innovation, Information and Technology Branch will continue the process to acquire a suitable tool to support data management. The intent is that this application will address business continuity, disaster recovery, building emergency planning and emergency response. A strong emphasis is being placed on application efficiency and the ability to interact with existing data sources.

As of January 2017, these planned actions have already commenced with key activities scheduled to be completed over the next three fiscal years with full completion by March 2020.

2.3 Changes affecting the delivery of critical services require a stronger oversight of recovery options development, assessment, selection and implementation

In an increasingly automated environment, complete and well-articulated assessments of recovery strategies are paramount if they are to be adequately funded and effectively supported by external service providers.

For example, following years of automation efforts, EI has become highly dependent on IT for both its intake and processing activities. In 2009, Internal Audit completed an assessment of EI's continuity plan and concluded that, even at this early stage in the automation, "some functions essential to providing the service could not be restored within an acceptable timeframe at a minimum acceptable level should a disruptive event occur". More than ever now, the capacity of the EI program to operate without its IT infrastructure is limited considering the declining capacity to manually process claims. On the other hand, as observed by Internal Audit during the November 2016 table-top exercise, processes related to pension programs have a certain resiliency to IT disruptions because they are still mostly paper-based.

The Department has prioritized the implementation of digital tools and automated processes so Canadians can access departmental services using digital self-service. To achieve this, a number of initiatives supported by investment projects are underway (e.g. CPP and OAS Service Improvement Strategies, EI Automation Agenda, Benefits Delivery Modernization). These initiatives will require the development, assessment, selection and implementation of updated recovery strategies. These new strategies have to take into account the increasing reliance on technology to deliver critical services and address the following issues noted by the audit:

- Although recovery strategies are considered and proposed as part of investment or Treasury Board submission, they often receive limited funding leading to gaps in the recovery capability of the critical services they support.
- When pressed for time, technical testing of the recovery strategies is often limited and provides little assurance as to the viability of the IT components of continuity plans.
- SSC is now responsible for critical components of the IT infrastructure supporting the delivery of departmental services. As a result, ensuring that roles and responsibilities are well defined for SSC and ESDC is foundational to continuity. To this effect, the Department has been working since 2015 on an IT service continuity management framework that defines how SSC and ESDC share the responsibility for service resumption.

Recommendation

2. The ADM of ISB, in collaboration with the senior ADM of the Transformation and Integrated Service Management Branch, should develop processes to oversee the development, assessment, selection, funding and implementation of updated recovery options for critical services impacted by the implementation of digital tools and automated processes.

Management Response

Management agrees with the recommendation. ISB, in collaboration with Transformation and Integrated Service Management Branch, will develop a process to ensure that BCP is incorporated into all transformation initiatives and projects.

These measures will ensure that transformational projects adopt a BCP by design approach and measures for recovery strategies and associated costs are put in place during the project and for the future state.

This activity will build upon the development of a refined list of critical business functions grouped by service.

Actions are expected to be completed by October 2017.

3. Conclusion

The audit concluded that the Department has planned for the continued availability of its critical services. However, to be effective and efficient, a horizontal "service-based" approach to continuity planning needs to be implemented. Furthermore, in an increasingly automated environment, recovery strategies need adequate management support, funding and coordination with internal and external supporting services to ensure the continued availability of the Department's critical services.

4. Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the Audit of Business Continuity Planning. The evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*.

Appendix A: Audit Criteria Assessment

Audit Criteria			Rating
BCP Governance	BCP is integrated into the Department's strategic and operational plans		◉
	BCP involves key stakeholders that can provide adequate decision making and oversight		●
Conducting Business Impact Assessments	All departmental services have been assessed to determine which ones are likely to cause a high degree of injury to Canadians or the working of government, if disrupted		●
	Critical services have been prioritized based on maximum allowable downtime and the minimum service level required before a high degree of injury will result		◉
Development of Business Continuity Plans and Arrangements	For each critical service, continuity or recovery options have been analysed to recommend the most appropriate strategy		◉
	For each critical service, comprehensive continuity plans based on the selected strategy are, as per applicable standards and policies:	Developed	●
		Approved	●
		Funded	◉
	Arrangements with internal and external service providers are in place so plans can be put into effect, and where the Department shares in the delivery of a critical service, the plans are coordinated		◉
Maintenance of BCP Program Readiness	Continuity plans are reviewed and updated as needed to account for changes to the services the Department must deliver		◉
	Continuity plans are regularly tested and updated based on the results of those tests	Table-top exercises	✪
		IT technical aspects	◉

✪ Best practice
● Sufficiently controlled, low risk exposure
◉ Controlled, but should be strengthened, medium risk exposure
○ Missing key controls, high risk exposure

Appendix B: Glossary

ADM	Assistant Deputy Minister
BCP	Business Continuity Planning
CPP	Canada Pension Plan
EI	Employment Insurance
EMBC	Emergency Management and Business Continuity
ESDC	Employment and Social Development Canada
ISB	Integrity Services Branch
IT	Information Technology
OAS	Old Age Security
PSPC	Public Services and Procurement Canada
SSC	Shared Services Canada