Office of the Superintendent of Financial Institutions Canada

Bureau du surintendant des institutions financières Canada

Business Continuity Planning

February 2019
Internal Audit Report

OSFI BSIF

Canada

Table of Contents

Glossary and Abbreviations

BCP	Business Continuity Planning
BCM	Business Continuity Management
BCPC	Business Continuity Planning Coordinator
BIA	Business Impact Analysis
DSO	Departmental Security Officer
OSFI	The Office of the Superintendent of Financial Institutions
OSS-BCP	Operational Security Standard – Business Continuity Planning
SFS	Securities and Facilities Services
TBS	Treasury Board Secretariat

1. Background

Objective

Provide assurance on the governance framework and key mechanisms in place to support business continuity planning governance objectives, including a review of the Security Policy and associated policy tools for alignment with the Government of Canada guidelines, adequacy of the core processes to support key elements of the policy and tools, including any supporting operational procedures and guidance; roles and responsibilities; training and awareness; and monitoring and improvement mechanisms.

Scope

The scope of the audit focused on business continuity planning (BCP) governance elements, specifically policies, training, monitoring and assessment mechanisms in place to support Security Services. The scope of this audit excluded the assessment of the adequacy and effectiveness of the business impact analysis (BIA) and business continuity plans.

Statement of Conformance

The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, consistent with the Treasury Board Secretariat (TBS) Policy on Internal Audit and the Internal Auditing Standards of the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program.

Context

Business Continuity Planning (BCP) is a key activity that enables the organization to provide for the continued availability of priority services in the case of disruption.

BCP is a requirement under Public Safety and Emergency Preparedness Canada's *Emergency Management Act* and Treasury Board Secretariat's (TBS) *Policy on Government Security.* The Departmental Security Officer (DSO) is ultimately accountable for BCP, as part of the broader departmental security program; however, the responsibility for operationalizing BCP at the Office of the Superintendent of Financial Institutions (OSFI) is delegated to the Security and Facilities Services (SFS) division under Human Resources and Administration within Corporate Services.

The TBS Policy on Government Services references TBS's *Operational Security Standard - Business Continuity Planning Program (OSS-BCPP)*, which further outlines the requirement of the BCP program, including the following four elements:

1. The establishment of BCP program governance.
2. The conduct of a business impact analysis.
3. The development of business continuity plans and arrangements.
4. The maintenance of BCP Program readiness.

In support of the requirement for establishing a BCP Program governance, OSFI established its *Directive on Business Continuity Management (BCM)* in February 2014.

At the time of the audit, SFS was in the midst of an OSFI-wide Business Impact Analysis (BIA), as required every 5 years per the OSFI *Directive on BCM*. BIAs help to identify and prioritize essential operations and are a key driver for the development of divisional business continuity plans and associated investment decisions. The results of the BIA were pending communication to senior management, and corresponding updates to divisional business continuity plans were yet to be revised. Per management, the recent BIA exercise identified a key opportunity for the move towards functional based plans rather than maintaining divisional business continuity plans.

With organizational efforts underway in the area of BIA and respective revisions to the divisional BCPs, the scope of this audit focused on providing assurance that SFS has an adequate governance framework and mechanisms in place to administer, monitor and improve on business continuity planning on behalf of OSFI, as required by the Government of Canada.

An audit of BCP was recommended by OSFI's Audit Committee and approved by the Superintendent for inclusion in the OSFI 2018-19 Internal Audit Plan.

2. Results of the Engagement

Security and Facilities Services (SFS) has developed a robust business continuity planning program, which includes various governance tools and procedures in place to execute the program requirements. Although the foundational elements of a strong governance program exist, the program is not operationalized and lacks senior management commitment and oversight for effective functioning. SFS is in the process of updating the *Corporate Security Policy*, assessing the overall security program, and facilitating the establishment of functional business continuity plans through an ongoing Business Impact Analysis (BIA).

SFS is developing a roadmap for establishing strategic priorities for the improvement of the security program activities. In support of this roadmap and consistent with a recent opportunity highlighted in the BIA exercise, SFS should explore centrally managing high priority business continuity plans to ensure they receive the appropriate consideration to provide a level of confidence for the continued delivery of priority services.

Additional observations and considerations pertaining to updating policy and policy instruments and the establishment of a higher degree of accountability and governance over the BCP program are contained in this report.

3. Management Response

The management team agrees with the findings and recommendations, and recognizes that the recommendations require attention. SFS has a small team of three resources, none of which is dedicated to BCP. Therefore, mitigating these risks and implementing the actions in the near term would present an operational challenge.

As part of this year's planning exercise, SFS identified the need to invest in the corporate security team in order to mitigate risks. Subsequent to the completion of this audit, the Executive Committee approved additional resources for the Corporate Security team, which includes resources for the BCP program. The timelines in the action plan have been established based on this increased resource level, although still dependent on successfully being able to recruit talent on a timely basis.

SFS would like to thank the audit team for conducting a review of practices and documents as it relates to business continuity management within OSFI.

SFS is proposing that the Operating Committee (OC) provide an oversight function in order to support overall security risk management activities within the Office. This strengthened governance will be an important element in the successful implementation of the action plan.

4. Observations and Recommendations

Provide a higher level of assurance on continued delivery of priority services by exploring the feasibility of centrally managing critical business continuity plans.

Medium Priority Observation #1

The *Operational Security Standard – Business Continuity Planning* requires ongoing review and revision of all business continuity plans to account for changes, as well as regular testing and validation of plans. In line with this requirement, OSFI's Directive on BCM outlines the requirement for quarterly review, annual validation and update and annual testing of business continuity plans.

SFS has developed a Dashboard for BCP management tracking process as an oversight mechanism for monitoring the activities of the BCPs across OSFI, including BCP updates and testing frequency; however, SFS has noted difficulty in maintaining the Dashboard due to lack of updates provided by the sector leads. This is attributable to low BCP engagement due to competing priorities within sectors, BCP Lead staff turnovers, and a lack of training and awareness.

Without assurance that business continuity plans are being reviewed and monitored on a consistent basis, the risk exists of business continuity plans being outdated and business units not having the awareness and understanding of their BCP processes should an event require plan activation.

Recommendation

Consideration should be given to SFS centrally managing the business continuity plans in order to provide a higher level of assurance for the continuity of priority operations in the event of a disruption. This provides the opportunity for SFS to ensure the accuracy of the business continuity plans as well as the completion of more timely testing and monitoring in order to identify better practices and lessons learned that could help strengthen plans and practices.

Management Action Plan

Currently, SFS provides an oversight function for business continuity plans. However, SFS is proposing to consolidate existing plans into a single overarching organizational business continuity plan, in collaboration with Sector BCP Leads. We agree that SFS would centrally manage the enterprise level business continuity plan and present it to the Operating Committee for review and approval.

Director, SFS, Completion:

1) **Present BIA for approval – Q1, FY 2019/20.**
2) **Interim review of existing BCPs – Q2, FY 2019/20**
3) **Present consolidated BCP for approval, Q3, FY 2019/20**

4. Observations and Recommendations, continued

Establish monitoring and reporting on the effectiveness of the BCP program to senior management in order to strengthen governance and oversight for the effective management of risk.

Medium Priority Observation #2

As required in the Directive on BCM, the effectiveness of the overall BCP program should be tested with the results reported to the Executive Committee. This measurement and reporting is not currently taking place. Since 2014 OSFI has conducted multiple activities assessing areas of the security program including a division-wide tabletop exercise (2018), a post-mortem following a security incident (2014) and a business impact assessment (2015); however, it was noted that findings/action items, if any, are not reported to a senior management committee for identifying program gaps and any significant risk exposures.

Without monitoring and reporting on the effectiveness of the program and with no formal communication regarding recommendations and/or action items stemming from assessments conducted, senior management risks not being able to execute their governance responsibilities for effectively managing the risk to the organization.

Recommendation

SFS should establish a process for tracking recommendations and action items as a result of BCP assessments/exercises, including a method to track progress against the action plans. Regular reporting on the effectiveness of the BCP program should also be communicated to a decision-making senior management committee to address noted deficiencies and gaps in the program, including recommended costed strategies.

Additionally, regular reporting to a senior management committee will strengthen governance and oversight over the program and aid in raising the awareness of overall BCP initiatives through the organization.

Management Action Plan

SFS recognizes that enhancing resilience within an evolving risk environment requires a more integrated approach.

In response to these recommendations, SFS will report regularly on the effectiveness of the BCPP to the Operating Committee.

Director, SFS, Completion:

1) **Present summary of key findings related to the tornado in the National Capital Region to EC - Q4, FY 2018/19**
2) **Propose KPIs to OC for quarterly reporting - Q2, FY 2019/20**
3) **Implement quarterly reporting to OC - Q3 FY 2019/20**
4) **Develop an Action and Risk register to track progress against action plans – Q3, FY 2019/20**

4. Observations and Recommendations, continued

Strengthen accountabilities by clarifying, and aligning policy instruments to address inconsistencies in roles and responsibilities and accurately reflecting current practices.

Low Priority Observation #3

OSFI maintains a *Policy on Corporate Security*, which is supplemented by policy instruments pertaining to BCP, including the Directive on BCM, BCM Framework and the BCP Communication Framework. OSFI's BCP policy instruments were generally found to be in line with the over-arching Government of Canada *Policy on Government Security* and *Operational Security Standard – Business Continuity Planning Program* (OSS-BCPP).

OSFI's governance documents communicate roles and responsibilities to BCP Team Leaders as well as outline the requirements of the program to OSFI as a whole. All OSFI governance documents have a requirement to be reviewed every five years. At the time of the audit, the *Policy on Corporate Security* was under review as part of OSFI's corporate policy suite renewal.

It was noted that some elements of the policy documents are outdated and not reflective of the requirements and actions taken by the organization in executing its Business Continuity Planning Program (BCPP). Specifically, the following inconsistencies were noted:

Roles and responsibilities

- The *Policy on Corporate Security* tasks the Director, Securities and Facilities Services (SFS) with the responsibility of discharging the authorities and requirements of the DSO while in practice the Director, Cyber Security has been delegated this function.
- The Directive on BCM indicates a requirement for quarterly review of the divisional business continuity plans; however, this is not defined within the sector roles and responsibilities in the various governance documents and is not in alignment with the BCM Framework, which outlines the requirement for annual update and testing.
- The Directive on BCM and the BCM Framework assigns the Sector Leads with the responsibility for creating Sector Business continuity plans; however, these plans are not currently required to be in place.

Reporting Requirements

- The BCM framework and the BCP Communication Framework contain governance/communication diagrams illustrating a direct reporting relationship between the BCPC and the Executive Committee, while the Directive on BCM assigns the DSO as accountable for this reporting. In practice the Director, SFS with the BCPC will begin reporting to the Operating Committee on the most recent BIA as of 2018-19.

The inconsistencies between the requirements in the governance documents and actual practices leads to the misalignment in BCP roles, responsibilities and accountabilities risking the effectiveness of the overall BCP program.

Recommendation

In updating the *Policy on Corporate Security*, Security and Facilities Services (SFS) should review and update the corresponding policy instruments to address the noted inconsistencies with roles and responsibilities in order to clarify accountabilities for the effective functioning of the BCP program. Additionally, the various documents should be reviewed for alignment with current practices while reducing redundancies and ensure effective communication to BCP Team Members and OSFI staff.

Continued on next page

4. Observations and Recommendations, continued

Low Priority Observation #3, continued

Management Action Plan

SFS will continue its work refreshing internal security policies and ensuring alignment with Treasury Board's security policy evolution. This work will also include clarification and consistency regarding roles and responsibilities for the overall BCPP, which will be presented to OC for approval.

Director, SFS, Completion:

1) **Draft Policy on Corporate Security submitted for approval - Q4, FY 2018/19**
2) **Prepare BCP Governance document for approval - Q3, FY 2019/20**
3) **Update subsequent security policy instruments (4) – Q3, FY 2019/20**

4. Observations and Recommendations, continued

Enhance BCP program effectiveness by reinstating the BCP working group with an expanded mandate to actively engage members in overseeing and integrating BCP activities in the organization.

Low Priority Observation #4

Public Safety and Emergency Preparedness' *Operational Security Standard – Business Continuity Planning* requires that the BCP Coordinator (BCPC) establish working groups and define their roles and responsibilities. In compliance with this requirement, OSFI's Directive on BCM includes, as part of the roles and responsibilities of the BCPC, the requirement to chair a working group on BCP with the aim of reviewing, monitoring and updating the BCP program. The working group is to include representation from all sectors and corporate, functional and operational areas of OSFI.

OSFI established a BCP working group in 2016, including cross-sector representation, with the responsibility for providing strategic considerations for the enhancement of the BCPP and to aid the BCPC in implementing and monitoring activities to support the program. Sector Leads were responsible for the appointment of participants as well as replacements should those participants vacate their positions. The BCP working group is currently not meeting quarterly per the working group terms of reference. This lack of engagement has been attributed to resource constraints in SFS and sector member turnover without an appointed replacement. With the BCP working group inactive, SFS is missing the opportunity for employee involvement to aid the BCPC in executing the BCP program.

Recommendation

Securities and Facilities Services should revisit the working group and its membership to include the representation of BCP Team Leaders for business units, and consider revising the mandate to include operational tasks, to help facilitate regular testing, monitoring and training, as well as identifying opportunities for improvement to the program.

Management Action Plan

SFS will propose updates to the terms of reference of the Business Continuity Planning Working Group (BCPWG) in order to ensure appropriate accountabilities and operational focus. The terms of reference will be presented to the OC for review and approval along with seeking their support for a renewed, engaged and representative membership on the BCPWG.

Director, SFS, Completion:

1) **Present updated terms of reference for the BCP working group to OC for approval - Q2, FY 2019/20**
2) **Reinstate BCP working group – Q3, FY 2019/20**
3) **Define and propose training and awareness program – Q3, FY 2019/20**

Appendix 1

Observation Ratings

Observations are ranked in order to assist management in allocating resources to address identified weaknesses and/or improve internal controls and/or operating efficiencies. These ratings are for guidance purposes only. Management must evaluate ratings in light of their own experience and risk appetite.

Observations are ranked according to the following:

High priority - should be given immediate attention due to the existence of either a significant control weakness (i.e. control does not exist or is not adequately designed or not operating effectively or a significant operational improvement opportunity.

Medium priority – a control weakness or operational improvement that should be addressed in the near term.

Low priority - non-critical observation that could be addressed to either strengthen internal control or enhance efficiency, normally with minimal cost and effort.

Individual ratings should not be considered in isolation and their effect on other objectives should be considered.