Office of the Superintendent of Financial Institutions Canada

Bureau du surintendant des institutions financières Canada

Planification de la continuité des activités

Février 2019
Rapport d'audit interne

BSIF OSFI

Table des matières

Glossaire et abréviations

PCA	Planification de la continuité des activités
GCA	Gestion de la continuité des activités
CPCA	Coordonnateur de la planification de la continuité des activités
ARA	Analyse des répercussions sur les activités
ASB	Agent de sécurité du BSIF
BSIF	Bureau du surintendant des institutions financières
NSO-PPCA	Norme de sécurité opérationnelle – Programme de planification de la continuité des activités
DSSI	Division des services de sécurité et des installations
SCT	Secrétariat du Conseil du Trésor

1. Contexte

Objectif

Fournir l'assurance quant à la capacité du cadre de gouvernance et des principaux mécanismes en place d'appuyer les objectifs de gouvernance de la planification de la continuité des activités, ce qui comprend un examen de la politique de sécurité et des outils stratégiques connexes pour assurer leur harmonisation avec les lignes directrices du gouvernement du Canada, de la pertinence des processus de base pour appuyer les éléments clés de la politique et des outils, dont les procédures et les directives opérationnelles à l'appui, les attributions, la formation et la sensibilisation, de même que les mécanismes de surveillance et d'amélioration.

Portée

L'audit ciblait les éléments de gouvernance de la planification de la continuité des activités (PCA), en particulier les politiques, la formation, la surveillance et les mécanismes d'évaluation en place à l'appui des Services de sécurité. Cet audit ne consistait pas à évaluer l'adéquation et l'efficacité de l'analyse des répercussions sur les activités (ARA) et des plans de continuité des activités.

Déclaration de conformité

L'audit a été effectué conformément aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes (IAI), à la *Politique sur la vérification interne* du Conseil du Trésor (CT) et aux *Normes relatives à la vérification interne au sein du gouvernement du Canada*, qui sont appuyées par les résultats du programme d'amélioration et d'assurance de la qualité.

Contexte

La planification de la continuité des activités (PCA) est une activité clé qui permet à l'organisation d'assurer la disponibilité continue des services prioritaires en cas de perturbation.

La PCA est une exigence de la *Loi sur la gestion des urgences* de Sécurité publique et Protection civile Canada et de la *Politique sur la sécurité du gouvernement* du Conseil du Trésor (CT). L'agent de sécurité du BSIF (ASB) est responsable au premier chef de la PCA dans le cadre du programme de sécurité ministériel global; toutefois, la mise en œuvre de la PCA au Bureau du surintendant des institutions financières (BSIF) est déléguée à la Division des services de la sécurité et des installations (DSSI), qui relève de la Direction des ressources humaines et de l'administration du Secteur des services intégrés.

La *Politique sur la sécurité du gouvernement* du CT renvoie à la *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités* (NSO-PPCA) du CT, qui décrit plus précisément les exigences du programme de PCA, y compris les quatre éléments suivants :

1. l'établissement de la gouvernance des programmes de PCA;
2. la conduite de l'analyse des répercussions sur les activités;
3. l'élaboration de plans et d'ententes de continuité des activités;
4. le maintien de l'état de préparation du programme de PCA.

Conformément à l'obligation d'établir la gouvernance du programme de PCA, le BSIF a adopté sa *Directive sur la gestion de la continuité des activités* (GCA) en février 2014.

Au moment de l'audit, la DSSI effectuait une analyse des répercussions sur les activités (ARA) à l'échelle du BSIF, comme l'exige la *Directive sur la GCA* du BSIF tous les 5 ans. Les ARA aident à déterminer et à prioriser les opérations essentielles et constituent un facteur clé de l'élaboration des plans de continuité des activités de la Division et des décisions d'investissement connexes. Les résultats de l'ARA n'avaient pas encore été communiqués à la haute direction, et les mises à jour correspondantes des plans de continuité des activités des divisions n'avaient pas encore été révisées. Selon la direction, le récent exercice d'ARA a permis de cerner une occasion clé pour passer à des plans plus fonctionnels plutôt que de maintenir des plans de continuité des activités par division.

Compte tenu des efforts organisationnels en cours relativement aux ARA et des révisions respectives des plans de continuité des activités des divisions, l'audit visait à fournir l'assurance que la DSSI a mis en place un cadre de gouvernance et des mécanismes adéquats pour administrer, suivre et améliorer la PCA au nom du BSIF, comme l'exige le gouvernement du Canada.

Un audit de la PCA a été recommandé par le Comité d'audit du BSIF et approuvé par le surintendant aux fins d'inclusion dans le Plan d'audit interne 2018-2019 du BSIF.

2. Résultats de la mission

La Division des services de sécurité et des installations (DSSI) a élaboré un programme robuste de planification de la continuité des activités qui comprend divers outils et procédures de gouvernance pour satisfaire aux exigences du programme. Même si les éléments fondamentaux d'un solide programme de gouvernance sont en place, le programme n'est pas mis en œuvre et la haute direction n'a pris aucun engagement et n'exerce pas de supervision pour en assurer le fonctionnement efficace. La DSSI est en train de mettre à jour la *Politique sur la sécurité* du BSIF, d'évaluer le programme global de sécurité et de faciliter l'établissement de plans fonctionnels de continuité des activités au moyen d'une analyse des répercussions sur les activités (ARA).

La DSSI élabore présentement une feuille de route pour établir des priorités stratégiques en vue d'améliorer les activités du programme de sécurité. À l'appui de cette feuille de route et compte tenu d'une occasion récente mise au jour par l'ARA, la DSSI devrait envisager de centraliser la gestion des plans de continuité des activités à priorité élevée pour s'assurer qu'ils soient considérés comme il se doit et offrent un niveau de confiance dans la prestation continue des services prioritaires.

Le présent rapport renferme d'autres observations et considérations relatives à la mise à jour des politiques et des instruments de politique et au relèvement du niveau de responsabilisation et de gouvernance à l'égard du programme de PCA.

3. Réponse de la direction

La direction est d'accord avec les constatations et les recommandations et reconnaît qu'elles nécessitent une attention particulière. La DSSI forme une petite équipe de trois personnes dont aucune n'est affectée à la PCA. Par conséquent, l'atténuation de ces risques et la mise en œuvre des mesures à court terme présenteraient un défi opérationnel.

Dans le cadre de l'exercice de planification de cette année, la DSSI a noté qu'il fallait investir dans l'équipe de sécurité ministérielle afin d'atténuer les risques. À la suite de cet audit, le Comité de direction a approuvé des ressources supplémentaires pour l'équipe de la sécurité, y compris pour le programme de PCA. L'échéancier du plan d'action a été établi en fonction de ce niveau de ressources accru, mais il demeure tributaire de la capacité de recruter du personnel de talent en temps opportun.

La DSSI tient à remercier l'équipe d'audit d'avoir examiné les pratiques et les documents relatifs à la gestion de la continuité des activités au BSIF.

La DSSI propose que le Comité des opérations (CO) exerce une fonction de supervision en appui aux activités globales de gestion des risques liés à la sécurité au BSIF. Cette gouvernance renforcée sera un élément important de la mise en œuvre réussie du plan d'action.

4. Observations et recommandations

Fournir un niveau d'assurance plus élevé sur la prestation continue des services prioritaires en examinant la faisabilité d'une gestion centralisée des plans de continuité des activités essentielles.

Observation nº 1 à priorité moyenne

La *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités* exige l'examen et la révision continus de tous les plans de continuité des activités afin de tenir compte des changements, de même que la mise à l'essai et la validation périodiques des plans. Conformément à cette exigence, la *Directive sur la GCA* du BSIF impose l'examen trimestriel, la validation et la mise à jour annuelles et la mise à l'essai annuelle des plans de continuité des activités.

La DSSI a mis au point un tableau de bord pour le suivi de la gestion de la PCA à titre de mécanisme de supervision pour surveiller les activités de PCA à l'échelle du BSIF, y compris la fréquence de la mise à jour et de la mise à l'essai des plans de continuité des activités. Elle a toutefois constaté qu'il est difficile de tenir le tableau de bord à jour en raison du peu de mises à jour fournies par les responsables sectoriels. Cette situation est attribuable à la faible mobilisation à l'égard de la PCA en raison des priorités sectorielles concurrentes, du roulement du personnel responsable de la PCA et du manque de formation et de sensibilisation.

Sans assurance que les plans de continuité des activités font l'objet d'un examen et d'un suivi constants, il se pourrait que les plans de continuité des activités soient désuets et que les unités opérationnelles se rendent compte qu'elles ne connaissent pas et ne comprennent pas leurs processus de PCA au moment où elles doivent activer leur plan.

Recommandation

Il faudrait envisager de centraliser à la DSSI la gestion des plans de continuité des activités afin de relever le niveau d'assurance de la continuité des opérations prioritaires en cas de perturbation. La DSSI pourrait alors assurer l'exactitude des plans de continuité des activités et veiller à ce que les mises à l'essai et le suivi soient effectués plus rapidement afin de cerner de meilleures pratiques et leçons apprises qui pourraient contribuer à renforcer les plans et les pratiques.

Plan d'action de la direction

À l'heure actuelle, la DSSI supervise les plans de continuité des activités. Elle propose toutefois de regrouper les plans existants en un seul plan général et organisationnel de continuité des activités, en collaboration avec les responsables sectoriels de la PCA. Nous convenons que la DSSI gérera centralement le plan organisationnel de continuité des activités et le soumettra au Comité des opérations.

Mandat du directeur de la DSSI :

1) **faire approuver l'ARA – 1er trimestre de 2019-2020;**
2) **procéder à l'examen provisoire des plans de continuité des activités existants – 2e trimestre de 2019-2020;**
3) **faire approuver un plan consolidé de continuité des activités – 3e trimestre de 2019-2020.**

4. Observations et recommandations

Assurer le suivi de l'efficacité du programme de PCA et en rendre compte à la haute direction afin de renforcer la gouvernance et la supervision de la gestion efficace des risques.

Observation n^{o} 2 à priorité moyenne

Comme l'exige la *Directive sur la GCA*, l'efficacité du programme global de PCA doit être mise à l'essai et les résultats doivent être transmis au Comité de direction. Ni l'une ni l'autre de ces activités n'est exécutée à l'heure actuelle. Depuis 2014, le BSIF a mené de nombreuses activités pour évaluer les aspects du programme de sécurité, y compris un exercice de simulation à l'échelle divisionnaire (2018), un bilan à la suite d'un incident de sécurité (2014) et une évaluation des répercussions sur les activités (2015). On a toutefois remarqué que les constatations et les mesures de suivi, le cas échéant, ne sont pas signalées à un comité de la haute direction dans le but de cerner les lacunes du programme et toute exposition importante aux risques.

En l'absence de suivi et de rapports sur l'efficacité du programme et de communications officielles concernant les recommandations ou les mesures de suivi découlant des évaluations effectuées, la haute direction pourrait ne pas être en mesure de s'acquitter de ses responsabilités de gouvernance pour gérer efficacement le risque qui pèse sur l'organisation.

Recommandation

La DSSI devrait établir un processus de suivi des recommandations et des mesures de suivi à la suite des évaluations et des exercices de PCA, y compris une méthode de suivi des progrès par rapport aux plans d'action. Des rapports réguliers sur l'efficacité du programme de PCA doivent également être communiqués à un comité décisionnaire de la haute direction afin de combler les lacunes relevées dans le programme; ces rapports doivent inclure des stratégies recommandées dont on aura établi les coûts.

De plus, la présentation de rapports périodiques à un comité de la haute direction renforcera la gouvernance et la surveillance du programme et contribuera à faire connaître les initiatives globales de PCA dans toute l'organisation.

Plan d'action de la direction

La DSSI reconnaît que l'amélioration de la résilience dans un environnement de risque en évolution nécessite une approche plus intégrée.

En réponse à ces recommandations, la DSSI fera régulièrement rapport sur l'efficacité du programme de PCA au Comité des opérations.

Mandat du directeur de la DSSI :

1) **rendre compte au Comité de direction des principales conclusions liées à la tornade qui a frappé la région de la capitale nationale – 4^{e} trimestre de 2018-2019;**
2) **proposer des IRC au Comité des opérations aux fins de rapport trimestriel – 2^{e} trimestre de 2019-2020;**
3) **instaurer la présentation de rapports trimestriels au Comité des opérations – 3^{e} trimestre de 2019-2020**
4) **élaborer un registre des mesures et des risques pour suivre les progrès au regard des plans d'action – 3^{e} trimestre de 2019-2020.**

4. Observations et recommandations

Renforcer les obligations redditionnelles en clarifiant et en harmonisant les instruments de politique pour corriger les incohérences des attributions et refléter avec exactitude les pratiques actuelles.

Observation nº 3 à faible priorité

Le BSIF maintient une *Politique sur la sécurité* à laquelle s'ajoutent des instruments de politique relatifs à la PCA, y compris la *Directive sur la GCA*, le Cadre de GCA et le Cadre de communication de la PCA. Les instruments de politique du BSIF en matière de PCA sont généralement conformes à la *Politique sur la sécurité du gouvernement* et à la *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités* (NSO-PPCA).

Les documents sur la gouvernance du BSIF communiquent les attributions aux chefs des équipes de PCA et décrivent les exigences du programme à l'intention de l'ensemble du personnel du BSIF. Chacun de ces documents doit être examiné tous les cinq ans. Au moment de l'audit, la *Politique sur la sécurité ministérielle* était à l'étude dans le cadre du renouvellement de l'ensemble des politiques du BSIF.

On a remarqué que certains éléments des documents stratégiques sont désuets et ne reflètent pas les exigences et les mesures prises par l'organisation dans l'exécution de son programme de PCA. Plus précisément, les incohérences suivantes ont été relevées :

Attributions

- La *Politique sur la sécurité* confie au directeur de la DSSI la responsabilité de s'acquitter des attributions et des obligations de l'ASB alors que, dans les faits, cette fonction a été déléguée au directeur, Cybersécurité.
- La *Directive sur la GCA* impose un examen trimestriel des plans de continuité des activités des divisions; toutefois, cette exigence n'est pas définie dans les attributions sectorielles énoncées dans les divers documents de gouvernance, et elle n'est pas conforme au Cadre de GCA, qui décrit l'exigence de mise à jour et de mise à l'essai annuelles.
- La *Directive sur la GCA* et le Cadre de GCA attribuent aux responsables des secteurs la responsabilité de créer des plans de continuité des activités de leur secteur; ces plans ne sont toutefois pas requis pour le moment.

Exigences redditionnelles

- Le Cadre de GCA et le cadre de communication de la PCA contiennent des diagrammes de gouvernance et de communication illustrant un rapport hiérarchique direct entre le coordonnateur de la PCA et le Comité de direction, tandis que la Directive sur la GCA établit plutôt ce lien entre l'ASB et le Comité de direction. Dans la pratique, le directeur de la DSSI et le coordonnateur de la PCA commenceront à rendre compte au Comité des opérations de la plus récente ARA à compter de 2018-2019.

Les incohérences entre les exigences formulées dans les documents de gouvernance et les pratiques réelles entraînent un décalage dans les attributions et les obligations redditionnelles à l'égard de la PCA, ce qui risque de compromettre l'efficacité du programme global de PCA.

Recommandation

Dans le cadre de la mise à jour de la *Politique sur la sécurité*, la DSSI devrait examiner et mettre à jour les instruments de politique correspondants pour corriger les incohérences relevées dans les attributions afin de clarifier les obligations redditionnelles relatives au fonctionnement efficace du programme de PCA. En outre, les divers documents doivent être examinés pour s'assurer qu'ils sont conformes aux pratiques actuelles. Il faut aussi éviter les redondances et assurer une communication efficace avec les membres de l'équipe de PCA et le personnel du BSIF.

4. Observations et recommandations

Observation nº 3 à faible priorité (suite)

Plan d'action de la direction

La DSSI poursuivra l'actualisation des politiques de sécurité interne et l'harmonisation avec la *Politique sur la sécurité du gouvernement* du CT. Elle assurera en outre la clarification et l'uniformité des attributions pour l'ensemble du programme de PCA, qui seront soumises à l'approbation du CO.

Mandat du directeur de la DSSI :

1) **Faire approuver le projet de politique sur la sécurité – 4e trimestre de 2018-2019;**
2) **préparer un projet de document sur la gouvernance de la PCA – 3e trimestre de 2019-2020;**
3) **mettre à jour les instruments de politique en matière de sécurité subséquents (4) – 3e trimestre de 2019-2020.**

4. Observations et recommandations

Accroître l'efficacité du programme de PCA en rétablissant le groupe de travail sur la PCA et en élargissant son mandat pour faire participer activement ses membres à la supervision et à l'intégration des activités de PCA au sein de l'organisation.

Observation nº 4 à faible priorité

La *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités* de Sécurité publique et Protection civile Canada exige que le coordonnateur de la PCA établisse des groupes de travail et définisse leurs attributions. Conformément à cette exigence, la *Directive sur la GCA* prévoit, dans le cadre des attributions du coordonnateur de la PCA, l'obligation de présider un groupe de travail sur la PCA (GTPCA) dans le but d'examiner, de suivre et de mettre à jour le programme de PCA. Le GTPCA sera composé de représentants de tous les secteurs et des services organisationnels, fonctionnels et opérationnels du BSIF.

En 2016, le BSIF a mis sur pied un GTPCA composé de représentants des divers secteurs, lequel est chargé de relever des points stratégiques pour améliorer le programme de PCA et d'aider le coordonnateur de la PCA à mettre en œuvre et à suivre les activités à l'appui du programme. Les responsables des secteurs étaient chargés de nommer les membres du groupe de travail et leurs remplaçants, le cas échéant. Le GTPCA ne se réunit pas tous les trimestres comme le prévoit son cadre de référence. Ce manque d'engagement est attribuable aux ressources limitées de la DSSI et au roulement des représentants des secteurs qui ne sont pas remplacés. Comme le GTPCA est inactif, la DSSI n'a pas l'occasion d'aider le coordonnateur de la PCA à exécuter le programme de PCA.

Recommandation

La DSSI devrait se pencher à nouveau sur le groupe de travail et sa composition pour y inclure des chefs d'équipe de la PCA des unités opérationnelles, et envisager de réviser le mandat pour y ajouter des tâches opérationnelles afin de faciliter la mise à l'essai, le suivi et la formation périodiques, et de cerner les possibilités d'amélioration du programme.

Plan d'action de la direction

La DSSI proposera des mises à jour du cadre de référence du GTPCA afin d'assurer une reddition de comptes et une orientation opérationnelle appropriées. Le cadre de référence du GTPCA sera soumis à l'examen et à l'approbation du CO, et l'on sollicitera son appui pour renouveler la composition du groupe de travail, en assurer la représentativité et mobiliser ses membres.

Mandat du directeur de la DSSI :

1) **faire approuver la version révisée du cadre de référence du GTPCA au CO – 2e trimestre de 2019-2020;**
2) **rétablir le GTPCA – 3e trimestre de 2019-2020;**
3) **définir et propos un programme de formation et de sensibilisation – 3e trimestre de 2019-2020.**

Annexe 1

Notation des observations

Les observations sont notées afin d'aider la direction à affecter les ressources nécessaires pour combler les lacunes relevées et / ou améliorer les contrôles internes et / ou l'efficacité opérationnelle. Ces notes sont à titre d'orientation seulement. La direction doit évaluer les notes selon sa propre expérience et propension à prendre des risques.

Les observations sont notées conformément à ce qui suit.

Observation à priorité élevée – observation liée à une situation requérant une attention immédiate compte tenu d'une lacune importante sur le plan d'un contrôle (c.-à-d. qu'il n'y a pas de contrôle ou le contrôle est mal conçu ou ne fonctionne pas efficacement) ou d'une possibilité d'améliorer sensiblement les opérations.

Observation à priorité moyenne – observation visant à combler une lacune sur le plan d'un contrôle ou à améliorer les opérations à court terme.

Observation à faible priorité – observation non essentielle à laquelle on peut donner suite soit en renforçant un contrôle interne soit en améliorant les opérations, normalement à peu de frais et d'efforts.

Les notes individuelles ne doivent pas être analysées en vase clos; il faut tenir compte de leur effet sur d'autres objectifs.