Audit de la gestion du risque d’entreprise – Agence de la santé publique du Canada

Rapport définitif

Avril 2023

Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada

Bureau de l’audit et de l’évaluation

PROMOUVOIR ET PROTÉGER LA SANTÉ DES CANADIENS GRÂCE AU LEADERSHIP, AUX PARTENARIATS, À L'INNOVATION ET AUX INTERVENTIONS EN MATIÈRE DE SANTÉ PUBLIQUE.

— Agence de la santé publique du Canada

Also available in English under the title:
Audit of Enterprise Risk Management – Public Health Agency of Canada

Pour obtenir plus d'information, veuillez communiquer avec :

Agence de la santé publique du Canada
Indice de l'adresse 0900C2
Ottawa (Ontario) K1A 0K9
Tél. : 613-957-2991
Sans frais : 1-866-225-0709
Téléc. : 613-941-5366
ATS : 1-800-465-7735
Courriel : publications-publications@hc-sc.gc.ca

Date de publication : avril 2023

Cat. : HP5-166/2023F-PDF
ISBN : 978-0-660-67926-6
Pub. : 230418

Résumé

Introduction

L'intégration efficace de la gestion des risques dans la gouvernance, les structures et les programmes d'une organisation appuie la prise de décisions et les principales fonctions de gestion à tous les niveaux d'une organisation, notamment l'élaboration de politiques, la planification et l'établissement de priorités, l'affectation des ressources et l'évaluation du rendement.

L'Agence de la santé publique du Canada (ASPC) gère deux types de risque : les **risques d'entreprise**, qui sont les risques concernant les objectifs administratifs et de services internes de l'Agence, tels que les ressources humaines, le financement et la TI; et les **risques pour la santé publique**, qui sont les risques concernant la santé des Canadiens. L'ASPC est en cours de renouveler son approche à la gestion des risques. Dans cette nouvelle approche, la gestion des risques pour la santé publique sera menée par le Centre d'évaluation intégrée des risques (CEIR) au sein de la Direction générale des données de gestion et de la surveillance (DGDGS), tandis que la gestion du risque d'entreprise (GRE) sera assurée par l'unité des risques d'entreprise et planification (REP) de la Direction générale du dirigeant principal des finances et services intégrés de gestion (DGDPFSIG).

Les principes directeurs de la GRE sont décrits dans divers cadres, notamment les normes internationales de gestion du risque énoncées dans les principes et les lignes directrices concernant le management du risque de l'Organisation internationale de normalisation (ISO 31000) et le cadre de gestion du risque d'entreprise du Committee of Sponsoring Organizations (COSO). Le Cadre stratégique de gestion du risque (2010) du Secrétariat du Conseil du Trésor du Canada (SCT) fournit également aux administrateurs généraux et à leur ministère des principes généraux et des orientations en matière de gestion des risques. Le Guide de gestion intégrée du risque du SCT (2014) s'appuie sur les principes du Cadre et fournit des orientations sur la conception, la mise en œuvre, l'exécution et l'amélioration continue de la gestion intégrée du risque. Les critères utilisés pour évaluer le cadre et les pratiques de gestion des risques de l'Agence reflètent les principes de gestion des risques et les attentes énoncées dans les cadres ci-haut.

Objectif de la mission

L'objectif de l'audit est de déterminer si le cadre et les pratiques de gestion du risque d'entreprise (GRE) de l'Agence appuient adéquatement l'identification, l'évaluation et l'intégration de l'information sur les risques à des fins de planification, de surveillance et de prise de décisions. Il vise aussi à identifier les possibilités d'amélioration comme partie de l'initiative en cours de renouvellement de la gestion des risques.

Portée de l'exercice

La portée de l'audit était axée sur les activités et les processus fondamentaux de GRE réalisés à l'échelle de l'organisation et des directions générales entre le 1er avril 2019 et le 31 mars 2022. L'audit portait en particulier sur l'examen des politiques et des cadres de gouvernance, des rôles et responsabilités, des processus, des outils et des procédures mis en place pour identifier les risques, les évaluer et y répondre, ainsi que les processus de suivi et de communication des risques et d'intégration de l'information dans les cycles de planification et de production de rapports de l'Agence. La portée ne comprenait pas une évaluation de l'approche de l'Agence en matière de gestion des risques pour la santé publique, ni la pertinence des risques ciblés, ni les niveaux ou les cotes de risques réels et les interventions déterminées par la direction.

Nos observations

Dans les années qui ont précédé le début de la COVID-19, l'ASPC avait en place un processus rigoureux pour identifier et évaluer de manière formelle ses risques stratégiques grâce à son processus de profil de risque de l'organisation (PRO). Notre examen indique que le PRO et les processus de gestion des risques qui y sont associés étaient bien appuyés par des activités telles que des exercices d'analyse comparative, des ateliers sur la gestion des risques, des initiatives de formation et des évaluations des modèles de la capacité en matière de gestion des risques. Cet appui était renforcé par des outils comme les guides des participants et les guides de référence, des fiches de renseignements et des questionnaires sur la gestion des risques, ainsi qu'un logiciel de vote qui facilite l'évaluation et la compilation des risques. Il avait aussi un comité de surveillance de la gestion du risque mis sur pied pour s'occuper des pratiques à cet égard dans l'ensemble de l'Agence.

Depuis le début de la COVID-19, et jusqu'à la réorganisation des responsabilités en matière de GRE en 2021, le leadership centralisé était limité pour soutenir et coordonner la GRE, et il y avait peu de processus, d'outils et de formation officiels pour appuyer les pratiques courantes en la matière. Au cours de cette période, l'ASPC n'a ni mis à jour ni approuvé son PRO, pour les raisons suivantes :

- les changements de priorités et l'incidence de la COVID-19 sur tous les aspects des opérations et des ressources de l'Agence;
- les complexités organisationnelles et opérationnelles engendrées par l'expansion importante et la réorganisation de l'Agence;
- le transfert des responsabilités de la direction de la GRE de la Direction générale de la politique stratégique (DGPS) à la Direction générale du dirigeant principal des finances et services intégrés de gestion (DGDPFSIG).

Comme la responsabilité de la direction de la GRE a été transférée à la DGPFSG à la fin de 2021, l'Agence a recentré ses efforts sur les pratiques de gestion des risques et renforcé sa capacité en mettant sur pied l'unité des risques d'entreprise et de la planification (REP). Cette unité dirige une approche de GRE qui permet d'améliorer le cadre et les pratiques de gestion des risques dans l'ensemble de l'Agence. Comme prévu, l'approche comprend des orientations convenables sur la gestion des risques, des structures de gouvernance bien définies et des processus formels d'identification, d'évaluation, de réponse et de surveillance en matière de risques. Pour progresser avec la nouvelle approche et la mise en œuvre du cadre de gestion des risques aux fins de la GRE, l'Agence devrait :

- normaliser les processus et les outils de gestion des risques, et établir des attentes de base concernant les résultats et les produits livrables de gestion des risques pour les directions générales et les unités fonctionnelles organisationnelles à l'aide des lignes directrices en matière de gestion intégrée du risque;
- s'assurer que la surveillance par la haute direction fait l'objet d'examens réguliers, d'évaluations et de rapports sur l'état des pratiques de GRE grâce à l'examen annuel du profil de risque de l'organisation;
- établir et mettre en œuvre des processus et des pratiques plus robustes de suivi et de communication des risques qui :
  - tiennent compte de la gravité des risques et des seuils de tolérance aux risques établis;
  - permettent d'identifier adéquatement les exigences relatives à l'information sur le suivi des risques;

- appuyer l'identification et l'évaluation continues des risques, et favoriser la discussion sur l'incidence des interventions sur les risques sous-jacents grâce à l'établissement d'un registre des risques organisationnels.

Critère 1 – Gouvernance

Contexte

L'intégration de la gestion des risques dans les processus de gouvernance aide la direction à s'acquitter de son mandat en facilitant et en accélérant la prise de décisions plus éclairées, en favorisant une meilleure affectation des ressources et en assurant la conformité avec les politiques et les lois. Elle aide également l'Agence à reconnaître les nouveaux défis et les nouvelles possibilités, à les comprendre, à s'y adapter et à en tirer parti, ainsi qu'à adopter une approche stratégique et globale pour traiter des risques horizontaux qui nécessitent une attention soutenue.

La gestion intégrée du risque a été retirée du Cadre de responsabilisation de gestion (CRG) avant l'établissement de la portée de cet audit. L'absence d'évaluation de la gestion intégrée du risque dans le CRG, en plus de l'instabilité de l'environnement opérationnel et les exigences élevées en ressources de période de la COVID-19, peut avoir nui à l'attention accordée à la gestion des risques ainsi qu'à la mobilisation à cet égard au cours des dernières années.

Nos attentes

Nous nous attendions à ce qu'il y ait des cadres appropriés de gouvernance de la GRE dans l'ensemble de l'Agence, notamment des politiques et des normes établies, des rôles et des responsabilités clairement définis, et les entités convenables pour assurer la direction et la surveillance.

Principales constatations

Politique et directives

La Politique sur la gestion intégrée du risque de l'ASPC (la « Politique ») et les lignes directrices en matière d'intégration de la gestion des risques (les « Lignes directrices ») ont été élaborées pour mettre à jour ou remplacer la *Norme de gestion intégrée du risque* (2009) et la version antérieure de la *Politique sur la GIR* (2013). Les orientations fournies dans les nouveaux documents respectent le *Cadre stratégique de gestion du risque du SCT* et tiennent compte de ses principaux éléments. La Politique énonce les attentes générales liées à la gestion des risques et définit clairement les rôles et les responsabilités en matière de GRE et de risques pour la santé de la présidente et des responsables des directions générales, de l'ACSP, du CEIR, des principales unités organisationnelles et des comités de gouvernance, ainsi que des cadres supérieurs, des gestionnaires et des employés.

Pour améliorer davantage la Politique et les Lignes directrices, l'Agence devrait envisager de :

- identifier les attentes de base communes à l'ensemble des directions générales et des unités fonctionnelles pour les processus de gestion des risques, les livrables et leur documentation d'appui;
- attribuer la responsabilité concernant l'examen, l'évaluation et la communication des pratiques de GRE, ainsi que leur conformité avec les attentes en matière de politiques;
- fournir une orientation plus robuste sur les éléments clés et les points à prendre en considération dans l'élaboration de plans et de pratiques efficaces en matière de surveillance et de production de rapports sur les risques.

L'intégration des points ci-haut permettrait de favoriser une compréhension commune des attentes en matière de gestion des risques, d'établir des pratiques uniformes et de faciliter la surveillance et l'évaluation de la mise en œuvre de la Politique. De plus, elle permettrait à l'Agence de mieux consolider et intégrer l'information sur les risques dans tous les directions générales et les unités fonctionnelles.

Rôles et responsabilités

La Politique nouvellement élaborée définit clairement les rôles et les responsabilités en matière de gestion des risques à tous les niveaux de la gestion et pour les principaux organes de gouvernance. Comme indiqué ci-dessus, il a une possibilité de clarifier la responsabilité concernant la surveillance continue, l'évaluation et la communication des pratiques de gestion des risques, et leur alignement sur les exigences de la Politique. L'Agence serait ainsi en mesure d'évaluer rapidement le cadre de gestion des risques et de prendre les mesures correctives nécessaires.

La communication efficace de ces rôles et responsabilités devrait se faire par l'intermédiaire du Réseau de gestion du risque d'entreprise qui vient d'être constitué, et des initiatives de formation et de sensibilisation prévues dirigées par l'unité du REP.

Organismes de gouvernance

Dans l'ensemble, les comités de gouvernance de l'Agence sont mobilisés efficacement à l'examen et à la discussion concernant les risques à tous les niveaux de manière continue. Bien que les discussions sur la gestion des risques ne constituent pas un point permanent à l'ordre du jour, elles sont habituellement intégrées dans d'autres activités, y compris les présentations des plans et des priorités, les comptes rendus sur l'état d'avancement des initiatives, et diverses présentations ponctuelles sur des projets et des initiatives clés.

Il serait possible de normaliser davantage l'approche en matière de surveillance de la gestion des risques par les comités supérieurs au niveau des directions générales et de l'organisation. Il faudrait notamment identifier l'information clé liée aux risques et les outils de communications devant être présentés et discutés de façon périodique aux comités de gouvernance. Ces exigences devraient être clairement définies dans les plans de suivi et de communication des risques, et être conformes aux lignes directrices fournies par l'unité des REP. On s'attend à ce qu'une élaboration plus approfondie et une mise en œuvre complète de l'approche actuelle en matière de GRE abordent cette possibilité d'amélioration.

Conclusion

Comme prévu, l'approche mise à jour en matière de GRE devrait tenir compte de manière adéquate des principaux éléments de la gouvernance de la gestion des risques. Pour mieux appuyer la mise en œuvre de la nouvelle approche ainsi que de pratiques et de surveillance rigoureuses de la gestion des risques, l'Agence devrait envisager de clarifier les attentes de base en matière de gestion des risques et les processus de surveillance des risques pour les directions générales et les unités fonctionnelles.

Recommandation 1

Le DPF devrait s'assurer que la Politique sur la gestion intégrée du risque et les lignes directrices en matière d'intégration de la gestion des risques de l'Agence, qui sont en cours d'élaboration, respectent les critères suivants :

- elles établissent clairement les attentes de base et les produits livrables en matière de gestion des risques pour les directions générales et les unités fonctionnelles;
- elles clarifient les rôles et les responsabilités en matière de surveillance continue des pratiques de gestion des risques de l'Agence et de respect des attentes de la Politique, ainsi que la production de rapport à ce sujet.

Critère 2 – Processus de gestion des risques

Contexte

La gestion intégrée du risque, y compris la gestion du risque d'entreprise, soutient une approche continue, proactive et systématique de la gestion des risques à l'échelle de l'organisation. L'existence de processus uniformes de gestion des risques dans l'ensemble de l'organisation permet de regrouper l'information sur les risques au niveau organisationnel afin de mieux relever les défis qui se présentent.

Cette approche nécessite des évaluations continues à tous les niveaux de l'organisation, ainsi que la capacité de regrouper et de communiquer ces résultats de façon cohérente et uniforme.

Elle faciliterait ensuite la surveillance et la mise en œuvre des processus de gestion des risques au sein de l'Agence.

Nos attentes

Nous nous attendions à ce que la gestion des risques à tous les échelons soit soutenue par des processus, des orientations et des outils établis.

Principales constatations

Le PRO est le principal processus de gestion des risques utilisé pour identifier et documenter les risques stratégiques de l'organisation qui pourraient avoir une incidence sur la réalisation du mandat de l'Agence. Il permet d'identifier les risques sur des cycles de trois ans, au cours desquels des examens et des mises à jour annuels sont exigés. Bien que des preuves établissent que l'Agence avait antérieurement en place un processus d'examen et de renouvellement rigoureux, les dernières mises à jour du PRO ont eu lieu avant le début de la pandémie de COVID-19 et elles n'ont pas été approuvées par le Comité exécutif. Ceci peut s'expliquer par le contexte instable et exigeant en ressources de la pandémie, et par une fonction centrale de gestion des risques limitée durant cette période. Malgré l'absence d'un PRO à jour et approuvé au cours de la période visée par l'audit, il était établi que les risques organisationnels étaient pris en compte et que des mesures étaient prises pour y remédier au moyen d'activités de planification des secteurs fonctionnels, y compris les risques liés aux ressources humaines, à la continuité des activités, à la GI/TI ainsi qu'aux biens immobiliers et à la sécurité. Toutefois, il s'agit d'efforts de diverses équipes qui n'ont pas vraiment été coordonnés ni intégrés entre les directions générales ou dans l'ensemble de l'Agence. Même si des mesures étaient prises implicitement et explicitement pour remédier aux risques au moyen d'activités de planification, il n'y avait généralement pas de processus formel qui documentait l'identification et l'évaluation des risques à l'échelle de l'organisation. D'après nos observations, au moment de l'audit, le processus d'établissement du PRO pour la période de 2022 à 2025 était en cours et doit être soumis aux fins d'approbation vers la fin de l'hiver 2023.

Au niveau des directions générales, les pratiques de gestion des risques sont incluses dans les processus de planification opérationnelle et de production de rapports. Les personnes interrogées ont indiqué que la gestion des risques est aussi examinée de manière informelle dans le cadre de réunions bilatérales ou multilatérales périodiques et continues entre les DG, les directeurs et les gestionnaires. Bien que les risques soient pris en compte dans les processus de planification opérationnelle et d'établissement de rapports, il manque des preuves de l'existence de cadres ou de processus formels et systématiques à l'échelle des directions générales encadrant l'identification des risques, l'attribution des niveaux de risque, les réactions aux risques ou la surveillance des risques, notamment l'utilisation de modèles, de registres des risques, d'échelles des risques, de matrices des risques et de matrices de tolérance à l'égard du risque. Nous avons également constaté que le format et l'application des processus de planification opérationnelle qui étaient utilisés pour appuyer la gestion des risques variaient d'une direction générale à l'autre, et que ces processus n'étaient pas suivis de manière uniforme. Ce manque d'uniformité peut avoir entravé le regroupement et la prise en compte des risques touchant les directions générales dans l'ensemble de l'organisation. Toutefois, le plus récent cycle de planification et de production de rapports (2022-2023) comprend des étapes importantes pour formaliser et normaliser les processus de planification opérationnelle à l'échelle de l'Agence. Les données suggèrent l'utilisation d'un modèle de planification opérationnelle normalisé qui lie officiellement les activités et les priorités de planification opérationnelle aux risques à l'échelle de l'Agence, des directions générales et des directions.

L'Agence n'offre pas actuellement de formation officielle sur la gestion des risques, et les directives sur le site web sont limitées. Les personnes interrogées ont indiqué que la gestion des risques est pratiquée intuitivement et implicitement, et que toutes les décisions sont prises en tenant compte des risques. Toutefois, certaines personnes interrogées ont aussi exprimé leur intérêt à avoir une formation et des lignes directrices sur les attentes en matière de gestion des risques organisationnels, et souhaiteraient lier leur contexte de risque particulier et les décisions associées aux risques organisationnels stratégiques. Dans l'approche actuelle en matière de GRE, on s'engage à adopter une stratégie de communication et à réaliser des activités d'apprentissage et de développement selon les attentes de la Politique, y compris des ateliers de formation sur la GRE, des mises à jour de l'intranet de l'ASPC et le lancement d'un processus de registre des risques des directions générales. Le nouveau Réseau de gestion des risques organisationnels, dirigé par l'unité des ROP de la DGPFSG en collaboration avec les représentants des directions générales et des secteurs fonctionnels, devrait être un mécanisme efficace dans le soutien aux initiatives prévues de formation et de sensibilisation à la gestion des risques organisationnels.

L'absence de processus normalisés et systématiques, de méthodologies associées et d'outils pour des pratiques de gestion des risques efficaces accroît le risque :

- de nuire à la qualité et à l'exhaustivité de l'information sur les risques au niveau de l'organisation et des directions générales;

- de continuer de faillir à déterminer le risque de manière claire et objective pour faciliter l'attribution du niveau de risque ainsi que l'identification de l'efficacité des réactions aux risques;
- de restreindre la capacité d'intégrer et d'aligner efficacement l'information sur la gestion des risques verticalement et horizontalement au sein de l'Agence;
- d'élaborer des cadres et des pratiques de gestion des risques pour chaque direction générale et chaque unité fonctionnelle, ce qui rendrait inefficaces et multiplierait inutilement les efforts qui y seraient consacrés au sein de l'Agence.

L'absence d'initiatives de formation, ainsi que les indications restreintes ou obsolètes sur le site Web, peut également entraver la capacité des responsables de risques et du personnel à gérer les risques conformément aux attentes de la Politique.

Conclusion

Le manque généralisé de processus rigoureux et normalisés de gestion des risques durant la période d'audit était attribuable à la pandémie de COVID-19, qui a monopolisé l'attention de l'Agence, ainsi qu'à l'incidence des initiatives de restructuration organisationnelle et au changement des responsabilités au chapitre de la GRE.

Cependant, l'approche mise à jour en matière de GRE et les initiatives associées dirigées par l'unité des REP constituent une base solide pour les processus de GRE à venir. Le processus de planification opérationnelle qui vient d'être mis en œuvre, bien qu'il ne soit pas encore tout à fait établi et qu'il n'ait pas encore été mis à l'essai, est un volet important d'un processus global de GRE et doit permettre d'intégrer de manière formelle les risques dans les plans opérationnels à tous les niveaux. La version préliminaire de la Politique et celle des lignes directrices, auxquelles s'ajoutent les activités d'orientation, de formation et de communication prévues de l'unité des REP, sont prévues à fournir une formalisation suffisante et un niveau de normalisation pour les processus globaux de gestion des risques de l'Agence.

Recommandation

Aucune. Les recommandations 1 et 2 permettent d'identifier les possibilités qui ont été relevées d'améliorer les processus et les outils de GRE de l'Agence.

Critère 3 – Surveillance

Contexte

Une surveillance continue des risques est essentielle pour assurer que l'information connexe est toujours pertinente et que les changements apportés à l'environnement de risque sont pris en compte. Elle permet également de s'assurer que les mesures de réponse aux risques conçues pour remédier aux problèmes qui nuisent à l'organisation sont effectivement mises en œuvre et qu'elles produisent les résultats prévus.

De plus, les activités de surveillance permettent à cerner les nouvelles sphères et activités qui exigent une surveillance, et de soutenir l'amélioration continue de la gestion des risques dans l'ensemble de l'organisation.

Nos attentes

Nous nous attendions à ce que soient mis en place des processus systématiques pour surveiller les risques et les activités de gestion des risques, et pour en rendre compte, et à ce que ces processus intègrent et utilisent l'information relative aux risques pour la prise de décisions.

Principales constatations

À l'échelle de l'organisation, le Plan ministériel (PM) et le Rapport sur les résultats ministériels (RRM) présentent et examinent les principales priorités et les résultats associés. Ceci comprend les résultats prévus pour les secteurs fonctionnels des services internes comme les ressources humaines, la TI et les finances. Si le PM et le RRM présentent les principales initiatives et les projets majeurs à la haute direction, ils n'ont pas de lien avec l'incidence des risques sous-jacents dans le cadre de la GRE sur les priorités prévues.

À l'échelle des directions générales, les réponses aux risques et les risques sous-jacents sont surveillés dans le cadre de réunions et de discussions bilatérales informelles auxquelles participent les gestionnaires, les directeurs et les directeurs généraux, de même que dans le cadre des examens de mi-année et de fin d'année des plans opérationnels. Cependant, comme les processus de gestion des risques des directions générales ne sont pas suffisamment formalisés, il n'y a pas d'approche systématique pour surveiller la gestion des risques et évaluer l'efficacité des réponses aux risques. Plus précisément, les risques et l'évaluation des risques à l'échelle des directions générales ne sont pas documentés, et il n'y a pas d'indicateurs concrets qui permettent de vérifier si les mesures de réaction aux risques produisent les résultats prévus.

Rappelons que, même si toutes les directions générales ne les ont pas encore complètement adoptés, les processus de planification opérationnelle de l'Agence ont été considérablement renforcés au cours du cycle de planification 2022-2023. Une fois que ces processus sont pleinement mis en œuvre, l'unité des REP de la DGDPFSIG compte améliorer la surveillance des risques en mettant en place un processus normalisé pour examiner les questions liées aux risques à tous les niveaux de l'Agence.

Un manque d'approche formelle et systématique pour suivre les risques dans le cadre de la GRE nuit à la capacité de la direction d'effectuer les activités suivantes :

- déterminer et démontrer objectivement l'efficacité des réactions et des initiatives en matière de gestion des risques;
- évaluer l'évolution des risques au cours du temps et avoir une certaine visibilité sur les nouveaux risques;
- s'assurer que la surveillance est exercée au niveau approprié de gestion et à une fréquence qui permet d'intervenir de la bonne façon à l'égard des risques et d'apporter les modifications nécessaires en temps voulu.

Conclusion

Les processus et les mécanismes de surveillance et de communication des risques de l'Agence sont informels et manquent d'uniformité. L'Agence cherche à mettre en place des processus de surveillance des risques plus rigoureux lors de la mise à jour de son approche en matière de GRE. Les outils et les processus actuels de planification opérationnelle permettront de tenir compte des risques dans les processus de planification à l'Agence. Voici comment il serait possible de renforcer davantage les processus suivants de surveillance et de communication :

- Consigner officiellement l'identification et l'évaluation des risques, selon les attentes formulées dans la recommandation 1;
- Adopter des approches plus formelles et systématiques pour surveiller les risques de façon continue, afin de renforcer la capacité de la direction d'évaluer en quelle mesure les activités permettent l'atténuation des risques selon les seuils de tolérance établis;
- Mettre en œuvre la surveillance formelle de la gestion des risques par les comités de la haute direction en assurant une communication régulière et plus structurée de l'information sur le risque, et conforme aux lignes directrices qui seront élaborées selon la recommandation 1.

Recommandation 2

Le DPF, en consultation avec les chefs de direction générale et les responsables de secteur fonctionnel, devrait élaborer et fournir des conseils pour établir des processus plus rigoureux de surveillance et de communication des risques, ce qui consiste notamment à :

- effectuer l'évaluation continue et tenir compte de l'incidence des interventions sur les risques sous-jacents;
- s'assurer que les activités de surveillance et de production de rapports tiennent compte de la gravité des risques et des seuils de tolérance établis;
- définir les exigences relatives à l'information sur le risque à l'appui des plans et des processus de surveillance et de communication.

Annexe A – Grille d'évaluation

Audit de la gestion des risques organisationnels – Agence de la santé publique du Canada			
Critère	**Cote de risque[1]**	**Risques qui subsistent ou occasions ratées sans mise en œuvre des recommandations**	**Nº de rec.**
Gouvernance Il existe un cadre de gouvernance efficace pour soutenir la GRE dans l'ensemble de l'Agence.	**3**	• L'absence d'exigences à jour, pertinentes et claires relatives à la Politique et de lignes directrices associées augmente la possibilité que les attentes en matière de gestion des risques ne soient pas facilement comprises dans l'ensemble de l'Agence, et que la gestion des risques ne soit pas conforme à la Politique de l'Agence. De plus, elle nuit à la capacité de l'Agence d'évaluer efficacement si les pratiques de gestion des risques sont conformes aux attentes de l'Agence. • L'absence d'évaluation et de surveillance formelles, systématiques et continues des pratiques de gestion des risques qui soient conformes aux attentes de la Politique énoncées dans les structures de gouvernance de la haute direction peut miner l'importance perçue de la gestion des risques au sein de l'Agence. Elle peut aussi diminuer la responsabilité à l'égard de la gestion des risques, ainsi que la capacité de la haute direction de relever efficacement les risques et d'intervenir rapidement en réponse aux tendances ou aux nouveaux risques.	1
Processus La gestion des risques est soutenue à tous les échelons par des processus, des orientations et des outils établis.	**3**	L'absence de processus formels et structurés et de résultats connexes pour la gestion des risques accroît le risque : • de compromettre la qualité et l'exhaustivité de l'information sur les risques à l'échelle de l'organisation et des directions générales; • d'entraver la mise en place d'un processus de détermination objective des risques qui peut être répété et soutenu, ainsi que la capacité de mettre à jour les niveaux de risque et de faciliter la démonstration de l'efficacité des interventions et de leur incidence sur les risques; • de restreindre la capacité d'intégrer et d'aligner efficacement l'information sur la gestion des risques verticalement et horizontalement au sein de l'Agence; • d'élaborer des cadres et des pratiques de gestion des risques pour chaque direction générale et chaque unité fonctionnelle, ce qui rendrait inefficaces et multiplierait inutilement les efforts qui y seraient consacrés au sein de l'Agence. L'absence d'initiatives de formation, outre les indications restreintes ou obsolètes sur le site Web, peut entraver la capacité des responsables de risques à gérer les risques efficacement et conformément aux attentes de l'Agence. L'absence de formation peut aussi contribuer au manque d'uniformité dans les pratiques et les résultats, ce qui peut nuire à la bonne intégration de l'information sur les risques.	1
Surveillance Des processus systématiques sont en place pour surveiller les risques et les activités de gestion des risques et en rendre compte, ainsi que pour intégrer et utiliser efficacement l'information sur les risques dans le processus décisionnel.	**3**	L'absence de plans et de processus formels et systématiques de surveillance et de communication peut limiter la capacité de la direction à : • déterminer et démontrer objectivement l'efficacité des interventions et des initiatives en matière de gestion des risques; • évaluer l'évolution des risques au cours du temps et se faire une idée des nouveaux risques; • s'assurer que la surveillance est exercée à l'échelon de gestion approprié et à une fréquence qui permet d'intervenir de la bonne façon à l'égard des risques et d'apporter les modifications nécessaires en temps opportun.	2

1	2	3	4	5
Risque minime	Risque mineur	Risque modéré	Risque important	Risque majeur

[1] Risque résiduel si la recommandation n'est pas mise en œuvre.

Annexe B – À propos de l'audit

1. Objectif de l'audit

L'audit visait à déterminer si le cadre et les pratiques de gestion du risque d'entreprise (GRE) de l'Agence appuient adéquatement l'identification, l'évaluation et l'intégration de l'information sur les risques à des fins de planification, de surveillance et de prise de décisions. Il visait aussi à identifier les possibilités d'amélioration dans le cadre de l'initiative de renouvellement en cours de la gestion des risques.

2. Portée de l'audit

La portée de l'audit était axée sur les activités et les processus fondamentaux de GRE réalisés à l'échelle de l'organisation et des directions générales entre le 1er avril 2019 et le 31 mars 2022. L'audit portait en particulier sur les politiques et les cadres de gouvernance, les rôles et les responsabilités, les processus, les outils et les procédures mis en place pour identifier les risques, les évaluer et y répondre et les processus de suivi et de communication des risques et d'intégration de l'information dans les cycles de planification et de production de rapports de l'Agence. Il n'était pas question d'évaluer son approche en matière de gestion des risques pour la santé publique, la pertinence des risques ciblés, les niveaux ou les cotes de risques réels, ou les interventions déterminées par la direction. L'audit a également permis d'examiner certains documents antérieurs à 2019 concernant les activités et les processus établis en matière de GRE, dans le but de dégager les pratiques exemplaires pour les présenter à la DGDPFSIG en vue du renouvellement efficace des processus de gestion des risques.

3. Méthode de l'audit

L'audit s'est déroulé conformément à la *Politique sur l'audit interne du gouvernement du Canada*, qui exige l'examen d'éléments de preuve suffisants et pertinents ainsi que la collecte de données et d'explications suffisantes pour offrir un niveau raisonnable d'assurance à l'appui de sa conclusion. L'approche retenue comprenait :

- Des entrevues auprès de la direction, des membres des comités et des principaux intervenants de l'organisation et des unités organisationnelles des directions générales;
- L'examen des processus, des méthodes, des résultats et d'autres documents justificatifs pertinents;
- La mise en essai des contrôles au besoin.

Identifier les possibilités d'amélioration dans le cadre de l'initiative de renouvellement de la gestion des risques, on a aussi adopté une approche souple pour l'audit. Cette approche a permis à l'équipe d'audit de prendre connaissance des ébauches, de les commenter pendant la rédaction et de formuler des commentaires constructifs dans un délai raisonnable.

4. Énoncé de conformité

Cet audit a été réalisé conformément aux *Normes internationales pour la pratique professionnelle de l'audit interne* et est validé par les résultats du programme d'assurance et d'amélioration de la qualité du Bureau de l'audit et de l'évaluation.

5. Critères d'audit

Les critères d'audit sont tirés du Cadre stratégique de gestion du risque du SCT, du Guide de gestion intégrée du risque du SCT, des principes de gestion des risques de l'Organisation internationale de normalisation et du cadre de gestion du risque d'entreprise du COSO. Voici les critères qui ont été utilisés pour réaliser l'audit de la gestion des risques :

Audit de la gestion des risques organisationnels	
Critères d'audit	
1	Il existe un cadre de gouvernance approprié, conforme aux lignes directrices et aux principes du Conseil du Trésor, qui appuie la GRE dans l'ensemble de l'Agence.
2	La gestion du risque d'entreprise est soutenue à l'échelle de l'Agence, des directions générales et des directions par des processus, des orientations et des outils établis.
3	Des processus systématiques sont en place pour surveiller les risques organisationnels et les activités de gestion des risques, pour en rendre compte, ainsi que pour intégrer et utiliser efficacement l'information sur les risques dans le processus décisionnel et la planification.