Bureau du surintendant des institutions financières Canada
Office of the Superintendent of Financial Institutions Canada

Bureau du surintendant des institutions financières

Rapport d'audit interne sur le Bureau de l'actuaire en chef - Gestion de l'information et protection de la vie privée

Juin 2015

BSIF
OSFI

Canada

Table des matières

1. Le contexte

Introduction

Le Bureau de l'actuaire en chef (BAC) a été mis sur pied pour fournir des services, actuariels et autres, au gouvernement du Canada et aux gouvernements provinciaux qui participent au Régime de pensions du Canada (RPC). Le BAC constitue une entité distincte au sein du Bureau du surintendant des institutions financières Canada (BSIF) et, même si l'actuaire en chef relève du surintendant, il a l'entière responsabilité du contenu des rapports préparés par le BAC et des opinions actuarielles qui y sont formulées. Cette structure préconise l'indépendance et garantit du coup que l'actuaire en chef porte un jugement professionnel impartial dans l'exécution de son mandat.

L'équipe d'audit interne du BSIF effectue périodiquement des travaux d'assurance pour déterminer si la gestion des risques, les processus de contrôle et la gouvernance du BAC, tels que conçus et présentés par la direction, sont adéquats et fonctionnent de manière à ce que les risques soient bien identifiés et pris en charge, et pour veiller au respect des politiques et procédures applicables.

Le Comité d'audit du BSIF a recommandé que l'audit du BAC soit inscrit au Plan d'audit interne 2014-2015 du BSIF et le surintendant a approuvé sa recommandation. Le présent rapport présente les résultats des travaux d'audit achevés en mars 2015.

Ce rapport a été présenté au Comité d'audit du BSIF le 19 juin 2015, et a par la suite été approuvé par le surintendant. La direction du BAC a revu ce rapport et a fourni des réponses accompagnées de plans d'action.

Importance de l'audit

Le BAC contribue à la santé financière et à la viabilité du système de revenu de retraite canadien en fournissant des services d'évaluation actuarielle et des conseils d'expert au gouvernement du Canada et aux gouvernements provinciaux qui participent au Régime de pensions du Canada (RPC). Le BAC effectue les évaluations actuarielles prévues par la loi de divers régimes de retraite. Lorsque le Parlement est saisi d'un projet de loi qui a d'importantes répercussions sur la situation financière d'un régime de retraite public ou d'un programme social à l'égard duquel la loi confère des responsabilités à l'actuaire en chef, le BAC doit soumettre au ministre approprié un rapport actuariel qui évalue l'impact du projet de loi en question. Le BAC fournit aussi aux ministères visés des conseils actuariels sur la conception, la capitalisation et l'administration de leurs régimes.

Le BAC reçoit des données de diverses sources, y compris de d'autres ministères et organismes gouvernementaux. Certains fichiers contiennent des renseignements tels que l'âge, l'état civil, le salaire ou les renseignements médicaux de particuliers. Il incombe au BAC de recueillir, d'analyser, de conserver, de protéger et de correctement éliminer ces données.

2. L'audit

Objectif

L'objectif de l'audit était d'évaluer l'adéquation des pratiques en matière de gestion de l'information et de protection de la vie privée.

Étendue

L'audit a couvert les activités opérationnelles en matière de gestion et de protection des renseignements de niveaux protégé et classifié ayant trait au mandat du BAC et relevant directement de lui. Il s'agit, entre autres, de la formation et de la sensibilisation, des politiques, directives et procédures applicables, de la conception et de l'efficacité des contrôles internes ainsi que des activités de surveillance et de supervision.

Stratégie

Les critères d'évaluation retenus pour l'audit du BAC s'appuient sur le cadre intégré de gestion du risque d'entreprise du Committee of Sponsoring Organizations of the Treadway Commission (COSO), qui est reconnu internationalement.

Les auditeurs ont eu des entretiens avec les membres de l'équipe du BAC et leur ont demandé d'expliquer les processus, ils ont mis à l'essai les contrôles des pratiques en matière de gestion de l'information et ils ont examiné divers documents, tels que du matériel de formation et des politiques et procédures applicables au BSIF.

Déclaration de conformité

L'audit s'est déroulé en pleine conformité avec les *Normes internationales pour la pratique professionnelle de l'audit interne* définies par l'Institut des auditeurs internes, et en accord avec la *Politique sur la vérification interne* du Conseil du Trésor ainsi qu'avec les normes d'audit interne du gouvernement du Canada, dont la qualité est attestée par les résultats du Programme d'assurance et d'amélioration de la qualité.

3. Les conclusions

Conclusion

Les contrôles et les activités de surveillance ayant trait à la gestion de l'information doivent être améliorés. Le BAC exerce ses activités sous les politiques et procédures de gestion de l'information et de protection de la vie privée du BSIF. Toutefois, il arrive que certains employés ne s'y conforment pas, et certains autres ne les connaissent tout simplement pas. La plupart des employés n'ont su nommer les politiques et procédures applicables à la gestion de l'information et ont indiqué qu'il leur serait utile de recevoir plus de formation à ce sujet.

Dans les rares occasions où le BAC reçoit des renseignements classifiés, ils sont conservés sur un réseau homologué pour le stockage d'information dont la cote ne dépasse pas Protégé B. Quelques employés qui utilisent ces renseignements n'ont pas la cote de sécurité nécessaire, et certains employés ont accès à de l'information de programmes dont ils ne sont pas responsables. Le BAC doit améliorer ses pratiques liées à l'accès aux données, à leur transmission, à leur conservation et à leur élimination afin d'atténuer le risque de fuite de données.

Le BAC est une petite unité indépendante du BSIF. Le BSIF lui fournit gratuitement les services de soutien dont il a besoin pour mener la plupart de ses activités de gestion de l'information. Cependant, les responsabilités de chacune des parties ne sont pas très clairement définies, sauf en ce qui concerne la gestion du cycle de vie des appareils informatiques. La gestion de l'information et la protection de la vie privée sont complexes. Le BAC doit se conformer à un grand nombre de politiques et directives du Secrétariat du Conseil du Trésor, ce pour quoi il bénéficie d'un soutien très limité et a très peu de connaissances. Le BAC manifeste la volonté de bien agir et s'engage à régler les problèmes lorsqu'il en prend connaissance.

Nous tenons à souligner l'excellent appui que nous ont accordé tous ceux qui ont participé à l'audit et la qualité des échanges que nous avons eus avec eux. Leur collaboration et leur apport ont contribué de façon inestimable à la réussite de l'audit.

4. La réponse de la direction

Réponse et commentaires de la direction

Le présent rapport a été examiné par l'actuaire en chef et le directeur général du BAC, qui reconnaissent le bien-fondé des observations et des recommandations qui y sont formulées.

L'équipe de direction reconnaît la nécessité de donner suite sans attendre aux observations et aux recommandations des auditeurs. Grâce à ces recommandations, le BAC sensibilisera ses employés aux politiques et procédures en matière de gestion de l'information et de protection de la vie privée et atténuera le risque de fuite d'information en améliorant ses pratiques liées à l'accès aux données, à leur conservation, à leur transmission et à leur rétention.

Dans l'ensemble, la direction comprend bien l'esprit du rapport, et elle est d'accord avec ses observations et ses recommandations. Le BAC y donnera suite, tel qu'il est expliqué ci-après.

Le BAC aimerait remercier l'équipe d'audit interne, qui a examiné de façon exhaustive les pratiques en matière de gestion de l'information et les politiques sur la protection de la vie privée. Il est capital que le BAC prenne toutes les mesures nécessaires pour protéger la vie privée des Canadiens, qui doivent avoir la certitude que leurs renseignements administratifs ne sont jamais exposés à un risque d'atteinte à la sécurité.

5. Les observations et les recommandations

Observation 1 Information de nature délicate

Les politiques, les directives et les guides du BSIF ont pour objet de répondre aux exigences du Secrétariat du Conseil du Trésor. À titre d'organisme gouvernemental, le BAC doit respecter ces exigences. Le BAC ne possède pas ses propres politiques, directives et guides; il se réfère à ceux du BSIF. Il arrive que des renseignements de nature délicate que reçoit le BAC ne soient pas traités et conservés conformément aux exigences en matière de sécurité de l'information du BSIF.

Seuls les employés détenant la cote de sécurité voulue et dont les fonctions le justifient doivent avoir accès à certains renseignements. La cote « Fiabilité » permet de consulter des renseignements protégés, alors qu'il faut une cote de niveau « Confidentiel », « Secret » ou « Très secret » pour avoir accès à des renseignements classifiés. Or, quelques employés du BAC n'ont pas fait l'objet d'une enquête de sécurité au niveau requis pour être habilités à utiliser les renseignements dont ils ont besoin pour s'acquitter de leurs fonctions. Certains ont accès à des répertoires réseau dont ils n'ont pas besoin dans le cadre de leurs fonctions.

Recommandations

Le BAC doit consulter la Division de la gestion de l'information et de la technologie de l'information (GI-TI) et la Division des services de la sécurité et de l'administration (SSA) dans le but de mieux comprendre les politiques et procédures du SCT et du BSIF, plus particulièrement le *Guide sur la sécurité de l'information* et la *Politique sur la mise en commun de l'information* du BSIF.

Le BAC doit également s'employer à améliorer les pratiques liées à la réception de renseignements classifiés, à leur conservation et à leur accès. Il doit veiller à ce que seuls les employés ayant la cote de sécurité nécessaire puissent accéder aux renseignements classifiés.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC consultera la Division de la gestion de l'information et de la technologie de l'information (GI-TI) et la Division des services de la sécurité et de l'administration afin de mieux comprendre les politiques et procédures applicables du BSIF. Le BAC remédiera au manque de sensibilisation des employés en rédigeant des instructions claires sur la gestion de la sécurité et de la mise en commun de l'information. Le BAC concevra également des outils qui aideront la direction à répondre aux exigences en matière de stockage et de transmission et à contrôler l'accès des employés à l'information classifiée.

Directeur général; achèvement : Mars 2016.

Suite à la page suivante

5. Les observations et les recommandations, suite

Observation 2 Catégories d'information et formation du personnel

Lors des quatre inspections de sécurité menées entre le 14 mai 2014 et le 16 février 2015, les inspecteurs ont relevé 71 dérogations (ce qui représente un taux de dérogation de 42 %). À noter toutefois que le nombre d'incidents a diminué progressivement au cours de la période.

Les employés n'ont pas tous la même interprétation de ce que sont des renseignements classifiés et protégés. La plupart n'ont pu nommer une politique ou procédure en matière de gestion de l'information ou de protection de la vie privée, et ont indiqué qu'ils aimeraient recevoir plus de formation à ce sujet. Lorsque les employés ne reçoivent pas de formation appropriée et ne sont pas suffisamment sensibilisés en matière de sécurité, il se peut qu'ils ne puissent distinguer les catégories d'information et les protéger adéquatement, ce qui pourrait entraîner des fuites d'information.

Des rappels sur la gestion de l'information sont publiés régulièrement sur le site intranet du BSIF, mais ce n'est généralement qu'au moment de leur entrée en fonction que les employés reçoivent de la formation. La formation est de nature générale et porte principalement sur les données des institutions financières et pas nécessairement sur celles du BAC. Par conséquent, les employés du BAC sont incertains de la façon de catégoriser certaines données du BAC et des pratiques adéquates en matière de gestion de l'information et de la protection de la vie privée.

Recommandations

L'équipe de direction doit s'entendre sur la catégorisation des renseignements que reçoit le BAC. Les renseignements personnels doivent être protégés conformément à la *Loi sur la protection des renseignements personnels*. Lorsque les intéressés auront convenu de la catégorisation des renseignements reçus, les employés peuvent avoir accès à de la formation sur mesure et à des cours de recyclage périodiques. Le BAC peut également adapter sa formation aux résultats des inspections de sécurité.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC profitera des assemblées générales du personnel et des réunions de service pour mieux renseigner les employés et leur rappeler de suivre les instructions claires (dont l'élaboration est prévue en réponse à l'observation 1) sur les politiques et procédures applicables en matière de gestion et de mise en commun de l'information, et de protection de la vie privée. Le BAC obtiendra également les résultats des rondes de sécurité effectuées par les SSA- pour aider dans le développement de ses instructions.

Directeur général; achèvement : Mars 2016.

Suite à la page suivante

Observation 3 Conservation des données

Le BAC n'a pas de politique sur la conservation des documents. Actuellement, toutes les données sont conservées tant qu'il y a suffisamment d'espace de stockage. Il y a de vieux documents papier. Il y a aussi des fichiers contenant des renseignements de nature délicate sur le réseau. Garder de l'information pendant une période de temps plus longue que nécessaire utilise la capacité de stockage inutilement et augmente le risque de fuite d'information. Ceci présente des inquiétudes, particulièrement en ce qui concerne les renseignements de nature délicate.

Recommandations

Le BAC doit établir une politique de conservation de l'information qui traite notamment de l'archivage des documents électroniques et papier, et il doit en contrôler l'application. La période de conservation doit respecter les prescriptions de la loi (s'il y a lieu), les politiques du SCT et du BSIF, la *Loi sur la Bibliothèque et les Archives du Canada*, et tenir compte des besoins opérationnels du BAC.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC examinera les politiques en vigueur et en rédigera une sur la conservation de l'information qui satisfera aux prescriptions de la loi, aux politiques du SCT et du BSIF, à la *Loi sur la Bibliothèque et les Archives du Canada* et à ses besoins.

Actuaire en chef; achèvement : Mars 2016

Suite à la page suivante

5. Les observations et les recommandations, suite

Observation 4 Administration des accès et profil d'accès

Des contrôles doivent être mis en place pour surveiller l'autorisation des accès (octroi, modification et révocation de droits) et l'adéquation des profils d'accès. Par exemple, nous avons appris qu'en 2014, un employé avait demandé oralement qu'un collègue ait accès aux dossiers du BAC et que des droits d'accès lui avaient été accordés, même si certains directeurs croient plutôt que des droits d'accès ne devraient être accordés qu'avec leur autorisation écrite. De plus, quelques employés du BSIF qui n'ont plus besoin de consulter les dossiers du BAC y avaient toujours accès mais leurs droits ont été révoqués depuis.

Généralement, les employés sont autorisés à consulter en mode lecture et parfois en mode lecture-écriture les autres programmes. Toutefois, dans certains cas, ils n'ont pas besoin d'accéder à ces données. Les fichiers de certains programmes contiennent des renseignements classifiés.

Recommandations

- Le BAC doit décider des droits d'accès dont les employés ont besoin en tenant compte des avantages et des inconvénients d'une approche de « confiance universelle des utilisateurs » et d'une approche axée sur le « besoin de savoir ».

- Le BAC doit établir un processus d'autorisation des accès de concert avec la Division de la GI-TI. Il doit également informer la GI-TI des mutations d'employés pour que les droits d'accès soient révisés. Une surveillance périodique des profils d'accès permettrait également de relever les privilèges d'accès inappropriés.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC examinera les privilèges d'accès de chaque employé et concevra, en collaboration avec la Division de la gestion de l'information et de la technologie de l'information (GI-TI), un outil ou une procédure qui aidera la direction à surveiller et à contrôler à intervalles réguliers les profils d'accès des employés.

Directeur général; achèvement : Mars 2016

Suite à la page suivante

5. Les observations et les recommandations, suite

Observation 5 Évaluation des facteurs relatifs à la vie privée

Les évaluations des facteurs relatifs à la vie privée (ÉFVP) permettent de relever les risques d'atteinte à la vie privée des programmes et des activités du gouvernement et de ramener ces risques à un niveau acceptable. Une ÉFVP consiste à examiner la façon dont les renseignements personnels sont protégés lors de leur collecte, de leur utilisation, de leur divulgation, de leur conservation et, finalement, de leur élimination.

Un seul programme du BAC a fait l'objet d'une ÉFVP, et aucune mesure n'a été prise pour déterminer si d'autres devaient l'être.

La seule ÉFVP effectuée par le client a débouché sur la conclusion que les fichiers du programme devaient être enregistrés sur un serveur sécurisé réservé à cet usage. Actuellement, ces fichiers sont stockés sur le même serveur que ceux des autres programmes du BAC, bien que seulement un petit nombre d'employés y aient accès. Cette pratique est peut-être contraire à la conclusion de l'ÉFVP. De plus, le BAC doit respecter les délais de conservation prévus par la politique du BSIF en la matière jusqu'à ce qu'il ait finalisé ses propres exigences.

Recommandations

De concert avec ses clients, la GI-TI et la Division des services juridiques, le BAC doit décider si d'autres programmes devraient faire l'objet d'une ÉFVP et s'assurer de respecter la conclusion de l'ÉFVP à laquelle un programme a déjà été soumis.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC se conformera aux exigences de l'ÉFVP en vigueur pour un de ses programmes et consultera ses clients afin de déterminer si d'autres programmes requièrent une ÉFVP. Dans le passé, des ÉFVPs n'étaient pas effectuées comme elles le sont présentement. Toutefois, les exigences en matière de protection des données du BAC étaient examinées de près par les Services juridiques de leurs clients.

Directeur général; achèvement : Mars 2016

Suite à la page suivante

5. Les observations et les recommandations, suite

Observation 6 ***Politiques, procédures et lignes directrices sur la gestion de l'information et la protection de la vie privée***

Le BAC ne possède pas de politiques, procédures ou lignes directrices sur la gestion de l'information et la protection de la vie privée. Il applique celles du BSIF. Toutefois, certains employés du BAC ne connaissaient pas les politiques du BSIF ou ne les respectaient pas, notamment celle qui porte sur le traitement des renseignements classifiés.

À titre d'organisme gouvernemental, le BAC doit connaître les lois, directives et lignes directrices sur la gestion de l'information et la protection de la vie privée, et s'y conformer. Le BAC doit identifier les politiques et procédures applicables du BSIF et rédiger des lignes directrices complémentaires qui répondront à ses besoins particuliers. Par exemple, le processus d'autorisation des accès du BAC et son processus d'archivage différeront de ceux du BSIF, puisque les employés du BAC n'utilisent pas le système de gestion des documents électroniques (SGDE) du BSIF. Le BAC doit veiller à ce que les politiques et procédures qu'il adopte répondent à ses besoins et respectent les exigences en vigueur.

Recommandations

Le BAC doit identifier les politiques et procédures sur la gestion de l'information et la protection de la vie privée qui lui sont présentement applicables, et développer des lignes directrices complémentaires qui répondront à ses besoins particuliers.

Mesures préconisées

Pour donner suite aux recommandations formulées, le BAC examinera toutes les politiques et procédures applicables en matière de gestion de l'information et de protection de la vie privée et développera, au besoin, des instructions additionnelles (comme le prévoit la réponse à l'observation 1).

Directeur général; achèvement : Mars 2016

Suite à la page suivante

5. Les observations et les recommandations, suite

Observation 7 **Rôles et responsabilités du BSIF en ce qui concerne la gestion de l'information et la protection de la vie privé au BAC**

Aucun protocole d'entente n'a été établi entre le BSIF et le BAC, à l'exception d'une entente concernant la gestion du cycle de vie des appareils informatiques. Les responsabilités de chacun ne sont pas très claires, ce qui expose le BAC à des risques inutiles s'il présume à tort que l'atténuation des risques est prise en charge par le BSIF. Le BAC n'est pas tout à fait au courant de la portée du soutien accordé par le BSIF, de ses niveaux de service et de ses mesures de rendement. Le BAC se fie aux politiques et procédures sur la gestion de l'information du BSIF, mais il semble qu'il règne une certaine incertitude concernant l'ampleur de la participation du BSIF à la gestion de l'information du BAC.

Recommandations

Le surintendant doit clarifier les responsabilités du BSIF par rapport au BAC en ce qui concerne la gestion de l'information et la protection de la vie privée. Il doit également envisager de conclure avec le BAC une entente sur les niveaux de services qui engloberait la gestion de l'information et la protection de la vie privée.

Mesures préconisées

Une étude est en cours afin de déterminer la nature et l'ampleur des mesures de sécurité de l'information qui doivent être mises en place pour le BAC, puisqu'il « fait partie du BSIF ».

Les besoins du BAC seront évalués en fonction des résultats de l'étude. Les modifications qui peuvent être effectuées à peu de frais et aisément et qui nécessitent la collaboration de la GI-TI seront mise en œuvre sans attendre. L'affectation définitive des ressources sera décidée en tenant compte du plan d'action en matière de sécurité de la TI. Un accord de service biennal sera négocié avec le BAC en vue d'effectuer des travaux supplémentaires, s'il y a lieu.

Directeur général, Finances et planification intégrée, et directeur, Sécurité de la technologie de l'information; achèvement : décembre 2015.