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

Audit des régimes de retraite privés

BSIF
OSFI

Canada

N° de cat. : IN4-37/2024F-PDF

ISBN : 978-0-660-71747-0

Bureau du surintendant des institutions financières
255 rue Albert – 12ième étage
Ottawa, ON K1A 0H2
Téléphone : 1-800-385-8647
Courriel : information@osfi-bsif.gc.ca

Also available in English

Audit des régimes de retraite privés

Type de publication : Audit
Date : 30 avril 2023

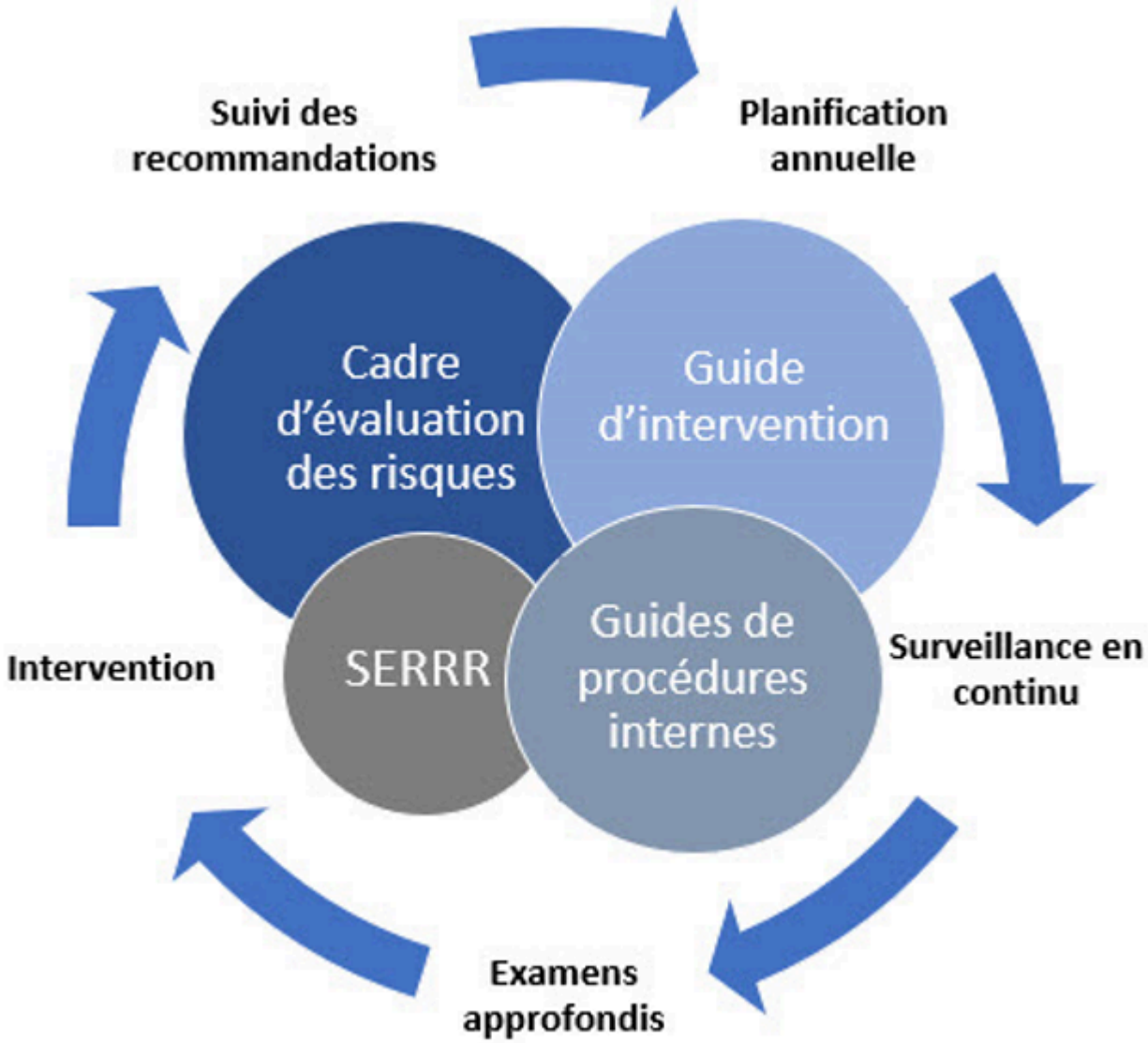
Table des matières

1. Contexte

Les régimes de retraite privés (RRP) parrainés par l'employeur sont des ententes volontaires qui forment une importante source de revenus de retraite pour les employés et leurs familles. Une fois qu'un régime de retraite est mis en place, il doit être financé et administré conformément aux lois et règlements en vigueur en matière de fiscalité et de retraite.
Il existe différents types de régimes de retraite, qui relèvent généralement d'une autorité du gouvernement fédéral ou provincial. Parmi les exemples de régimes de retraite relevant de la compétence fédérale, citons ceux des banques, des entreprises de transport transfrontalier et du secteur des communications. Le BSIF surveille plus de 1 200 RRP fédéraux afin de s'assurer qu'ils répondent aux exigences minimales de capitalisation et qu'ils sont conformes aux lois et règlements en vigueur; ainsi, le BSIF vise à protéger les droits et l'intérêt des bénéficiaires des régimes de retraite.

La surveillance des RRP s'appuie sur une approche fondée sur le risque, dans le cadre de laquelle l'ampleur des activités de surveillance et la fréquence des interventions dépendent du risque net du régime de retraite. Les principaux cadres et consignes de surveillance des RRP comprennent le Cadre d'évaluation des risques visant les régimes de retraite privés fédéraux et le Guide d'intervention des régimes de retraite privés fédéraux, deux outils du BSIF. En outre, l'équipe de Surveillance des RRP a rédigé des guides de procédures de surveillance pour appuyer le Cadre et assurer la cohérence des travaux de

surveillance. Les processus de surveillance consistent en une planification annuelle, des activités de suivi en continu, des examens approfondis, des interventions et des travaux de suivi des recommandations. Ces activités de surveillance sont facilitées par le Système d'évaluation des risques des régimes de retraite (SERRR).



Description texte - Surveillance des RRP

Structure opérationnelle

Après la restructuration organisationelle en mars 2022, la Division des RRP d'origine a été divisée en deux équipes distinctes : l'équipe de Surveillance des RRP est désormais intégrée au groupe de surveillance des sociétés d'assurance et des régimes de retraite, alors que l'équipe des Politiques et des approbations des RRP fait partie du Secteur de l'innovation stratégique et des relations avec les intervenants. L'audit a porté sur l'équipe de Surveillance des RRP, qui comprend une équipe de systèmes qui soutient l'utilisation et les fonctionnalités du SERRR, ainsi que l'équipe de l'Actuariat, qui offre un soutien spécialisé.

Au sein de l'équipe de Surveillance des RRP, le gestionnaire des relations (GR), récemment devenu chargé de surveillance (CS), est le principal point de contact pour les RRP et est responsable des activités de surveillance que peuvent soutenir les équipes de spécialistes (c.-à-d. les équipes des Politiques, de l'Actuariat et des approbations), au besoin. Les gestionnaires, Surveillance agissent à titre de contrôleurs pour l'équipe de Surveillance afin de s'assurer que les travaux de surveillance répondent aux exigences définies dans les guides de procédures et aux attentes de la direction; les risques cernés sont communiqués et acheminés aux intervenants internes et externes au besoin.

Portée des audits antérieurs

Le dernier audit dans ce domaine a été celui de 2014, mené par la Division des régimes de retraite privés, qui avait formulé deux recommandations liées à l'amélioration du Sommaire d'évaluation du risque et à l'attribution des accès aux systèmes. Les deux recommandations ont été closes avant le début de la présente mission d'audit.

2. L’audit

2.1 Objectif

L’audit visait à évaluer la suffisance, l’efficacité et l’efficience des activités de contrôle liées aux processus de surveillance du BSIF pour les RRP.

2.2 Portée

L’audit portait sur l’équipe de Surveillance des RRP et sur ses activités de surveillance menées entre le 1er avril 2020 et le 31 juillet 2022. L’accent a été mis sur l’évaluation des éléments suivants :

- La conception et l’efficacité opérationnelle des principaux processus de surveillance, notamment la planification annuelle, les activités de suivi en continu, les examens approfondis, les interventions et les travaux de suivi des recommandations;
- Le respect du Cadre de surveillance ainsi que des normes et politiques applicables.

2.3 Approche et méthodologie

L’audit a été réalisé en appliquant les procédures suivantes :

- examens des cadres, normes et politiques applicables en matière de RRP;
- démonstrations et entrevues avec des membres de la direction et de l’équipe de Surveillance;
- contrôle d’échantillonnage statistique et fondé sur le jugement pour les principales activités de contrôle et de surveillance.

Les résultats de cet audit aideront la direction à cerner les lacunes en matière de conception et d’efficacité opérationnelle dans les activités de contrôle et les processus de surveillance importants de l’organisation.

2.4 Déclaration de conformité

L'audit s'est déroulé conformément aux Normes internationales pour la pratique professionnelle de l'audit interne de l'Institut des auditeurs internes et à la *Politique sur l'audit interne* du Conseil du Trésor, comme en témoignent les résultats du programme d'assurance et d'amélioration de la qualité.

3. Vue d'ensemble des résultats de l'audit

3.1 Sommaire des résultats

De façon générale, les activités de surveillance menées par l'équipe de Surveillance des RRP étaient conformes aux processus formels en place et étaient fondées sur les risques, en plus d'être adéquatement documentées pour étayer l'analyse. Cependant, l'audit a mis en lumière quelques éléments des activités de contrôle et des processus de surveillance importants qui peuvent être renforcés, notamment : formaliser les processus de planification annuelle et de suivi des recommandations; améliorer la supervision et la production de rapports, par la direction, sur les principaux risques et les indicateurs de rendement des RRP; améliorer les preuves d'examen et d'approbation des principales activités de surveillance; et renforcer les contrôles d'accès pour les utilisateurs.

Bien que les recommandations de ce rapport d'audit concernent la surveillance des RRP, toutes les équipes de Surveillance du BSIF sont invitées à en examiner les conclusions pour voir si elles s'appliquent à leurs activités.

Depuis la période visée par l'audit, des changements importants ont eu lieu dans le Secteur de la surveillance, notamment la transformation du plan directeur et le projet de renouvellement du Cadre de surveillance. Par conséquent, de nombreux processus ont été revus et peuvent avoir été supprimés depuis la période de l'audit. Les résultats de l'audit peuvent renseigner la direction sur les lacunes observées dans certains processus opérationnels et appuyer les changements déjà en cours.

3.2 Réponse de la direction

La direction accepte les conclusions. Elle a défini des plans d'action de la direction pour chaque recommandation, comme indiqué dans les sections connexes, et prévoit de mettre en œuvre toutes les recommandations d'ici le deuxième trimestre de l'exercice 2024-2025.

4. Observations et recommandations

4.1 Planification annuelle

> Le processus de planification annuelle a été mené de concert avec les membres de l'équipe de Surveillance des RRP. Il devrait être optimisé afin d'accroître la surveillance des capacités des ressources et de favoriser la souplesse dans un environnement de risque dynamique.

Le processus de planification annuelle fait appel à une approche fondée sur le risque pour cerner les travaux de surveillance à effectuer au cours de l'année suivante. Il consiste à déterminer pour quels RRP des examens approfondis sont justifiés, en fonction des préoccupations soulevées au cours de la surveillance en continu tout au long de l'année. Tous les membres de l'équipe de Surveillance participent au processus de planification annuelle; ils discutent des principaux risques et de l'établissement des priorités à l'égard des travaux.

Supervision de la planification des ressources et suivi des modifications apportées au plan

Conformément au guide de procédures *Selecting Plans to Examine*, il existe des principes et des critères établis qui orientent l'équipe de Surveillance en matière de sélection des régimes à examiner et d'établissement des priorités à l'égard de ces régimes. De plus, le chargé de surveillance doit déterminer le type d'examen approfondi à réaliser (c.-à.-d. un

examen administratif ou un examen réalisé sur place) en consultant le gestionnaire, Surveillance. L'audit a permis de constater qu'il existe un nombre cible d'examens approfondis fondés sur le risque qui sont planifiés en fonction des ressources accessibles pendant l'année. Toutefois, le processus existant ne comprenait pas de documentation de l'écart entre les ressources nécessaires pour les travaux de surveillance fondés sur les risques et les ressources disponibles. En outre, rien n'attestait de l'existence de documentation sur l'avancement lié à l'utilisation des ressources pour les activités de surveillance (p. ex., révisions d'examen, interventions, etc.) Compte tenu du grand nombre de régimes de retraite que surveillent les chargés de surveillance, une supervision inadéquate de l'utilisation des ressources et des contraintes liées à ces dernières peut restreindre la capacité de la direction à prendre rapidement des décisions éclairées en matière de ressources.

Par railleurs, le tableur de planification est conçu pour consigner les renseignements clés sur l'avancement des activités de surveillance. La direction s'attend à ce que les chargés de surveillance fassent le suivi de l'avancement des examens et des changements au plan et documentent le tout dans le tableur, pour ensuite obtenir l'approbation du directeur. Pour les deux années auditées, le bien-fondé du plan initial était documenté dans ces tableurs. Toutefois, en raison de l'évolution rapide des risques pendant la pandémie, les changements et leur justification, y compris tout compromis en matière de ressources qui découlait de décisions fondées sur le risque, n'ont pas été documentés. Cette lacune a nui à la capacité de faire le suivi au chapitre de la continuité et d'assurer la réalisation des travaux prévus en fonction des priorités en matière de risque. Qui plus est, l'audit a révélé que les approbations des régimes initiaux ou des changements subséquents n'ont pas été appuyées par des documents justificatifs pendant ces deux années, ce qui pourrait entraîner des changements non autorisés aux travaux de surveillance.

Bien que la pratique actuelle exige que le directeur approuve à la fois le plan initial et les changements ultérieurs, il n'existe aucune exigence définie concernant la divulgation à la haute direction du plan et de toute modification à celui-ci concernant les besoins en ressources pour les travaux planifiés. Enfin, pour les deux années auditées, rien ne fait état d'une supervision de la haute direction pour les ressources prenant part à la planification annuelle. En l'absence d'une supervision adéquate des ressources

nécessaires pour la réalisation des activités planifiées, la direction pourrait ne pas être en mesure de comprendre l'harmonisation des contraintes en matière de ressources à la tolérance au risque et aux priorités définies pour l'exercice.

Recommandation 1 (risque élevé)

La direction devrait mettre en place et documenter un processus qui permet de définir et de superviser les capacités en ressources pour les activités de surveillance planifiées et de produire des rapports sur ces capacités. En outre, la direction devrait réexaminer les exigences actuelles en matière de suivi et d'approbation des changements apportés au plan en cours d'exercice.

4.2 Suivi des recommandations

Les lacunes et les recommandations font l'objet d'un suivi et sont closes, justification à l'appui, par le chargé de surveillance responsable. Toutefois, le processus de suivi relatif aux recommandations pourrait être renforcé afin que le suivi, la clôture et l'approbation des reports de dates cibles se fassent au moment opportun.

Les travaux de surveillance permettent de cerner des préoccupations précises à l'égard des RRP et de les communiquer à l'administrateur de régime en tant que « constatations ». Les recommandations servent à communiquer officiellement le point de vue du BSIF sur la façon dont les RRP peuvent remédier aux risques décelés pendant les activités de surveillance. Il est essentiel que les recommandations fassent l'objet d'un suivi et soient closes en temps opportun, afin de garantir que les préoccupations découlant de la surveillance soient réglées de façon appropriée.

Création de recommandations d'examen dans le SERRR

En vertu du manuel d'examen de la DRRP, les chargés de surveillance doivent créer une recommandation d'examen distincte dans le SERRR pour permettre la surveillance et le suivi des recommandations. La création d'une recommandation d'examen a généralement lieu après l'envoi de la lettre de recommandations, et au moment de la réception de la lettre d'accusé de réception, qui, en général, survient dans les 30 jours suivant l'envoi de la lettre de recommandations. Pour sept des douze échantillons audités, les recommandations d'examen n'ont pas été créées dans le SERRR en temps utile; la création a eu lieu entre 97 et 623 jours après l'envoi des lettres de recommandations. Par conséquent, parmi ces sept échantillons, six ne disposaient pas de preuves du suivi des recommandations ou n'ont pas fait l'objet d'un suivi. En outre, une recommandation provenant d'une lettre de recommandations de 2020 n'a pas été saisie dans le SERRR. Cette entrée manquante dans le système découle du fait qu'une intervention sans recommandation avait déjà été créée pour le même contexte.

La saisie tardive et incomplète des recommandations dans le SERRR pourrait conduire à l'absence de suivi des mesures correctives avant les dates d'échéance cibles et ainsi exposer plus longtemps l'organisation aux risques associés aux lacunes cernées dans les régimes de retraite.

Recommandation 2 (risque modéré)

La direction devrait réexaminer la communication auprès du personnel et la formation de celui-ci sur les exigences en place en matière de création adéquate et opportune des recommandations.

Suivi de la lettre d'accusé de réception et des preuves de clôture

Le manuel d'examen de la DRRP stipule que les chargés de surveillance doivent s'assurer que l'administrateur de régime fait parvenir une lettre d'accusé de réception au BSIF dans les 30 jours suivant la date d'envoi de la lettre de recommandations. Si l'administrateur de régime n'accuse pas réception des constatations et des recommandations dans le délai imparti, les chargés de surveillance doivent faire un suivi. Pour deux les douze

échantillons audités, les chargés de surveillance ont fait un suivi 17 jours après la date d'échéance de remise de l'accusé de réception. Même si les accusés de réception ont finalement été reçus, un suivi tardif peut retarder l'atténuation des risques, puisque l'administrateur de régime peut ne pas avoir compris les risques soulevés par le BSIF ou ne pas avoir pris les mesures appropriées pour y remédier.

La lettre de recommandations présente également les dates cibles de mise en œuvre des recommandations par l'administrateur de régime. La direction s'attend à ce que les chargés de surveillance fassent un suivi avant et après la date limite de l'envoi de l'accusé de réception lorsque les preuves de clôture n'ont pas été envoyées à temps. Les neuf échantillons pour lesquels des preuves de clôture avaient été soumises après la date limite ou n'avaient pas encore été soumises au moment de la date des présents travaux d'audit sur place ne faisaient état d'aucun suivi dans les délais requis.

En l'absence d'accusé de réception des lacunes indiquées dans la lettre de recommandations et de suivi en temps utile pour l'obtention de preuves de clôture, il y a un risque que les administrateurs de régime ne prennent pas de mesures rapides et appropriées pour remédier aux risques ciblés.

Report de la date cible

Comme l'indiquent les lettres de recommandations adressées aux RRP, il incombe aux administrateurs de régime de fournir au BSIF des preuves de clôture en fonction de l'échéancier convenu. Si les administrateurs de régime ne sont pas en mesure de respecter les échéances, ils peuvent demander au BSIF de repousser les dates de présentation cibles. Les demandes de report de date sont généralement envoyées par courriel et doivent être approuvées par l'autorité officielle (c.-à-d. le gestionnaire, Surveillance et le directeur).

L'audit a porté sur cinq échantillons pour lesquels les dates cibles de présentation ont été reportées. Bien que les cinq échantillons comportaient tous une documentation appropriée qui justifiait le report, un échantillon ne comprenait pas de preuve

d’approbation. Les reports non autorisés des dates initiales de présentation peuvent accroître l’exposition au risque de l’administrateur de régime au-delà du niveau de tolérance au risque du BSIF.

Clôture des recommandations

La direction s’attend à ce que les chargés de surveillance évaluent les preuves, obtiennent l’approbation du gestionnaire, Surveillance pour l’évaluation et répondent à l’administrateur de régime au sujet des résultats de l’évaluation dans les 45 jours suivant la réception des preuves de clôture envoyées par l’administrateur de régime. Sur les douze échantillons audités, des preuves de clôture avaient été présentées pour six échantillons; l’évaluation des preuves de ces six échantillons s’accompagnait de documents à l’appui. Toutefois, un seul échantillon avait été évalué et clôturé dans les délais prévus. À la date des travaux d’audit sur place, pour les cinq autres échantillons, certains n’avaient pas fait l’objet d’une évaluation ou avaient fait l’objet d’une évaluation/approbation tardive, soit entre 50 et 282 jours suivant la réception des preuves de clôture fournies par les administrateurs de régime.

La direction a indiqué que ce retard dans le suivi et la clôture des recommandations a découlé du roulement de personnel au sein de l’équipe de Surveillance, ainsi que du suivi insuffisant des étapes relatives aux principales recommandations (décrit plus en détail ci-dessous à la section 4.4 Indicateurs de rendement clés).

En l’absence d’un processus défini visant à favoriser la gestion cohérente et opportune des lacunes, les administrateurs de régime pourraient se voir exposés à des risques prolongés.

Recommandation 3 (risque modéré)

La direction devrait établir et documenter un processus permettant de suivre et de contrôler les dates des étapes clés par rapport aux dates cibles et veiller à ce que des preuves de l’approbation du report des dates cibles soient obtenues et conservées.

4.3 Surveillance du profil de risque des régimes de retraite privés

> L'équipe de Surveillance fait un suivi continu et dynamique des risques au sein du secteur. Toutefois, ce processus peut être renforcé pour garantir qu'une surveillance constante est effectuée et intégrée aux rapports existants utilisés pour la surveillance du risque.

L'équipe de Surveillance des RRP fait un suivi continu des risques au sein du secteur afin de déceler et d'évaluer les risques qui ont une incidence sur le profil de risque global des RRP. Ces activités aident à cerner les préoccupations en matière de surveillance et les tâches d'intervention connexes.

Jusqu'à l'exercice de 2019, l'équipe de Surveillance des RRP réalisait des évaluations de surveillance et de notation au sein du secteur au moins deux fois par année. Toutefois, après avoir constaté que la fréquence du contrôle ne permettait pas toujours l'obtention opportune de rétroaction et d'observations, la direction a révisé le processus pour adopter une approche de suivi continu et dynamique des risques au sein du secteur. Dans le cadre de cette approche, les chargés de surveillance ont été invités à mettre en place des avis de nouvelles pertinentes pour leur portefeuille et à évaluer rapidement les répercussions de ces nouvelles sur les portefeuilles de retraite. Toutefois, cette tâche ne se voulait pas une exigence formelle, et aucune consigne n'a été donnée sur les paramètres utilisés pour générer des avis de nouvelles ou sur la façon d'intégrer les résultats de ces avis à l'évaluation des risques des RRP. Cette situation peut restreindre la capacité des chargés de surveillance à cerner et à évaluer les risques pertinents au sein du secteur de manière constante et opportune.

En outre, aucun rapport n'est produit sur les tendances et résultats cumulatifs ou sectoriels du profil de risque global des RRP. Cette absence de rapports peut restreindre les perspectives et la surveillance globales des tendances en matière de risque et des

risques macro-environnementaux qui s'appliquent aux RRP, perspectives et surveillance qui favorisent une prise de décisions appropriées en temps utile en ce qui a trait aux mesures supplémentaires de surveillance à mettre en place.

Recommandation 4 (risque élevé)

La direction devrait mettre en place et documenter un processus qui permet d'évaluer et d'intégrer systématiquement les risques de surveillance au sein du secteur dans une optique de supervision efficace des RRP. Les résultats des profils de risque des RRP devraient faire l'objet, en continu, d'une surveillance et d'une reddition de comptes auprès de la direction.

4.4 Supervision des activités de surveillance

Le rendement de certaines activités de surveillance fait l'objet d'un suivi régulier de la part de la direction. Toutefois, les rapports peuvent être améliorés pour inclure des paramètres qui assurent une surveillance complète des activités de surveillance, ainsi que des contrôles liés aux données utilisées pour ces mesures.

Indicateurs de rendement clés

L'équipe de Surveillance des RRP a défini des indicateurs de rendement clés (IRC) internes pour surveiller le rendement mensuel de certaines activités et opérations de surveillance comme les demandes externes en suspens relatives aux régimes, les alertes relatives aux seuils de déclenchement et les réponses aux administrateurs externes.

Même si ces indicateurs de rendement clés sont présentés chaque mois au directeur, ils ne tiennent pas compte du progrès des autres grandes activités de surveillance, comme l'état d'avancement des examens et des recommandations par rapport aux calendriers

cibles. Le manque de rapports adéquats sur l'avancement de toutes les activités de surveillance pourrait entraîner une supervision inefficace et des retards dans l'achèvement des examens et dans la clôture des recommandations.

En outre, des activités d'intervention sont nécessaires pour garantir que les profils de risque globaux des RRP restent à jour afin que les activités de surveillance en aval, y compris des interactions accrues avec les RRP, soient adéquates et aient lieu en temps utile. Les activités d'intervention sont entreprises en fonction des résultats de la surveillance en continu des seuils de déclenchement liés au SERRR. Dans le SERRR, l'équipe de Surveillance des RRP crée et consigne des renseignements sur les mesures d'intervention, comme celles concernant un promoteur à risque ou un versement en retard. Toutefois, le rapport mensuel sur les indicateurs de rendement clés ne rend pas compte de l'état d'avancement de ces activités à la direction. Par conséquent, la direction pourrait ne pas avoir de contrôle sur les calendriers et le caractère adéquat de ces activités d'intervention.

Un autre paramètre qui fait l'objet d'une surveillance est le tri des demandes des administrateurs de régime externes et l'envoi des réponses en temps opportun, soit dans les 15 jours suivants, comme le stipule la norme de service du BSIF. Ces demandes peuvent à la fois nécessiter la collaboration de l'équipe de Surveillance et, au besoin, un soutien additionnel de l'équipe des Politiques dans le cas des demandes complexes. Toutefois, le délai cible de réponse de l'équipe des Politiques, soit 30 jours, entre en conflit avec la norme de service de 15 jours du BSIF. Les échantillons audités démontrent qu'environ 54 % des demandes en retard nécessitaient une analyse de la part de l'équipe des Politiques, et que toutes les demandes étaient en retard. Toutefois, ces résultats ont été attribués à l'équipe des Politiques, et non à l'équipe de Surveillance, ce qui a entraîné une disparité sur le plan de la responsabilisation. Cette incohérence au niveau de la responsabilisation, ainsi que les disparités dans les délais cibles de réponse aux demandes provenant des régimes externes, pourrait accroître le risque d'atteinte à la réputation du BSIF, et prolonger l'exposition aux risques et le traitement des questions non résolues pour les participants aux régimes.

Validation des données utilisées pour les indicateurs de rendement clés

Actuellement, le principal système de surveillance utilisé, le SERRR, comporte des champs qui permettent de saisir les dates des étapes clés, par exemple, la date d'examen, la date de rencontre de récapitulation et la date d'envoi de la lettre de recommandations. Ces champs de date peuvent être utilisés pour produire des IRC et d'autres rapports sur le risque pour l'équipe de Surveillance des RRP. Toutefois, il n'y a aucun contrôle de validation permettant de garantir l'exactitude et l'exhaustivité des données. Pour les quatre examens audités, des disparités ont été remarquées entre les dates saisies dans le SERRR et les dates indiquées dans les documents justificatifs. Si les données utilisées dans les rapports de surveillance ne sont pas validées, elles risquent d'être inexactes et incomplètes et de mener à une prise de décision mal éclairée.

En outre, l'audit a permis de constater que pour certains des échantillons d'IRC présentés dans les rapports mensuels, il n'y avait aucun document justifiant les résultats de ces IRC. Plus précisément, aucun document de référence n'a été conservé pendant 3 des 8 mois pour les données à l'égard des catégories d'indicateurs de risque nécessitant un suivi afin d'étayer l'avancement de la surveillance en continu. Si aucun document de référence n'est conservé, l'exactitude des paramètres présentés dans les rapports remis à la direction risque d'être compromise.

Recommandation 5 (risque modéré)

La direction devrait réexaminer régulièrement les paramètres et les seuils afin qu'ils restent pertinents pour le suivi du rendement des activités de surveillance et qu'ils soient conformes aux objectifs attendus. Le cas échéant, des contrôles de validation des données doivent être mis en place pour garantir l'exactitude et l'exhaustivité des rapports.

4.5 Examen et approbation

> Les principaux documents et activités de surveillance font l'objet d'un examen et d'une approbation pour garantir la qualité des travaux. Toutefois, le processus et les contrôles existants qui servent à prouver qu'il y a eu examen et approbation peuvent être améliorés afin de soutenir les activités de surveillance et l'évaluation adéquate des risques liés aux RRP.

L'examen et l'approbation appropriés des principaux travaux de surveillance par la direction garantissent que les activités et documents de surveillance respectent les normes et consignes établies et répondent aux attentes de la direction. Ils garantissent également que la surveillance en continu des alertes est efficace et que les profils de risque des RRP sont exacts et exhaustifs. Les preuves d'examen et d'approbation sont directement consignées dans le SERRR ou dans des courriels conservés dans eSpace.

Sommaire de l'évaluation des risques

Le sommaire de l'évaluation des risques dans le SERRR fait état de la justification des cotes de risque et d'intervention des RRP. Conformément à la matrice des pouvoirs de surveillance des RRP, le sommaire d'évaluation des risques doit être approuvé par le directeur et/ou le directeur général avant tout changement de cote si la cote d'intervention est supérieure à zéro. Pour l'un des huit échantillons audités, le sommaire d'évaluation des risques, qui comportait une cote d'intervention de 1 avant le changement, n'a pas été approuvé par le directeur comme il se doit.

En outre, conformément au manuel d'examen de la DRRP, un sommaire d'évaluation des risques doit être réalisé et révisé après l'examen afin qu'il reflète tout changement par rapport aux résultats de l'examen. Pour les trois examens audités, les résultats généraux d'examen ont été révisés et approuvés, mais le sommaire d'évaluation des risques post-examen n'a pas été réalisé. Une corroboration auprès de la direction a fait ressortir que ces examens ne nécessitaient pas de mise à jour immédiate du sommaire d'évaluation des risques, étant donné que les résultats des examens n'avaient entraîné aucun

changement de cote. Toutefois, si les sommaires d'évaluation des risques ne sont pas mis à jour rapidement après l'examen, les évaluations des risques liés aux RRP pourraient être désuètes, ce qui pourrait entraîner des répercussions sur les futures activités de surveillance prévues.

Examen annuel des contrôles des seuils de déclenchement

Le SERRR facilite la mise en œuvre des processus de surveillance en effectuant une révision initiale des relevés annuels de rendement des RRP en fonction d'un ensemble de critères et de formules prédéterminés. Lorsqu'un régime de retraite dépasse ces critères, le SERRR envoie une alerte à l'équipe de Surveillance des RRP pour qu'elle puisse analyser et confirmer le tout. Afin de veiller à ce que le SERRR fonctionne efficacement et comme prévu, et qu'il appuie l'analyse et la surveillance, des contrôles annuels sont en place pour réviser les seuils de déclenchement et les critères du système.

Le guide de procédures *Annual Review Criteria for Waiving RAS Requirement and Appropriateness of TRIs Triggering RAS Requirements* énumère les exigences de révision et détaille le processus qui régit l'actualisation et l'examen annuel des critères de risque qui déclenchent les avertissements. Lorsque ces seuils de déclenchement des sommaires d'évaluation des risques sont franchis, il est possible que les superviseurs doivent analyser et mettre à jour le profil de risque des RRP, ce qui peut ensuite déclencher d'autres activités de surveillance en aval (c.-à-d. une intervention ou un suivi continus). Plus précisément, le guide stipule que les seuils de déclenchement des sommaires d'évaluation des risques doivent être actualisés annuellement et approuvés par le directeur avant le 15 août de chaque année.

Pour l'un des trois exercices audités, soit 2022-2023, l'examen et l'approbation annuels n'ont pas été faits. La direction a confirmé qu'elle avait décidé d'omettre cet examen annuel en raison de l'examen des seuils de déclenchement de l'exercice précédent qui présentait un chevauchement avec l'exercice de 2022-2023. Toutefois, rien ne démontre que cette décision a été approuvée par le directeur ou par une personne d'un échelon supérieur. Par conséquent, il est possible que certaines décisions ne soient pas

autorisées ou que certains seuils de déclenchement des sommaires d'évaluation des risques ne fassent pas l'objet d'une supervision adéquate, alors que ces deux éléments permettent de soutenir les analyses et les suivis de surveillance.

Un autre contrôle annuel est la révision des critères et formules des catégories d'indicateurs de risques qui déclenchent les alertes dans le SERRR. Afin de garantir que les critères des catégories d'indicateurs de risque sont intégrés au SERRR conformément aux critères approuvés, des contrôles relatifs aux essais d'acceptation par l'utilisateur sont en place. Conformément au guide de procédures *RASP Change Management Process*, les changements de seuil de déclenchement liés aux catégories d'indicateurs de risque dans le SERRR nécessitent l'approbation du directeur lorsque ces changements sont apportés par l'équipe de Surveillance, ou l'approbation du directeur général si ces changements sont apportés par l'équipe de GI-TI. Des documents à l'appui doivent être conservés pour chacun des changements apportés. Des essais d'acceptation par l'utilisateur ont été réalisés et documentés pour cinq des neuf échantillons; cependant, il n'y avait aucune preuve d'approbation des changements de seuil de déclenchement liés aux catégories d'indicateurs de risque par le directeur ou le directeur général.

En l'absence de supervision adéquate des seuils de déclenchement, il y a un risque que les changements apportés aux critères définis dans le SERRR soient inappropriés pour le déclenchement des activités de surveillance en aval liées aux analyses et aux évaluations.

Recommandation 6 (risque modéré)

La direction devrait revoir les guides de procédures actuels du Secteur de la surveillance afin qu'ils reflètent les processus existants et qu'une formation appropriée soit dispensée au personnel pour favoriser le respect de ces exigences.

4.6 Accès des utilisateurs

> L'équipe de Surveillance des RRP gère et surveille l'accès des utilisateurs au SERRR. Les contrôles d'accès des utilisateurs peuvent être renforcés pour assurer que les changements apportés aux accès soient repérés et supervisés en temps utile.

Le SERRR est un outil important que l'équipe de Surveillance des régimes de retraite utilise pour faciliter son travail de surveillance. Il contient un vaste ensemble de renseignements sur les régimes et les travaux de surveillance, notamment les détails relatifs aux différents régimes, les cotes de risque et d'intervention, les dates importantes, etc. De plus, grâce à l'utilisation de critères précis, ce système déclenche également des activités de surveillance en aval, comme des analyses et des activités de suivi. Outre les équipes de RRP, d'autres équipes du BSIF (p. ex., les Services des applications, l'équipe des communications, les Finances, etc.) ont besoin d'accéder au système pour s'acquitter de leurs rôles de soutien. Comme les besoins d'accès changent de temps à autre, il est essentiel de veiller à ce que les accès soient autorisés, accordés seulement en cas de nécessité absolue et mis à jour en temps utile.

Demandes d'accès ponctuel des utilisateurs

En vertu du guide de procédures *Risk Assessment System Access Management*, l'agent principal, Système de régimes de retraite est responsable du traitement des demandes d'accès des utilisateurs au SERRR après avoir obtenu une autorisation à cet effet et avoir consigné les demandes dans eSpace. Le processus actuel exige également que le gestionnaire, Surveillance approuve ces demandes une fois que l'agent principal en a fait l'examen. Toutefois, les dix échantillons audités ne présentaient aucune preuve d'approbation du gestionnaire, Surveillance, et 50 % de ces échantillons ne comprenaient pas de preuve d'approbation initiale de la demande. En outre, les demandes d'accès n'ont pas toutes été adéquatement consignées dans eSpace, comme exigé; cependant, elles ont été fournies une fois qu'elles ont été demandées aux fins de l'audit.

L’absence d’approbation adéquate peut entraîner des accès inappropriés au SERRR et aux données sensibles et critiques qu’il contient.

Examen des accès au système

En vertu du guide de procédures *Risk Assessment System Access Management*, l’agent principal, Système de régimes de retraite est également responsable de la surveillance périodique des accès des utilisateurs au SERRR, afin de s’assurer que ces accès sont adéquats et que les documents à l’appui (c.-à-d. la liste des accès des utilisateurs) sont consignés dans eSpace.

Le suivi périodique comprend un examen mensuel de la liste des accès des utilisateurs pour confirmer qu’elle est adéquate dans l'ensemble, ainsi qu’un examen trimestriel subséquent de tous les changements d’accès apportés d’un trimestre à l’autre. Pour 16 des 28 échantillons de l’examen mensuel des accès, aucune preuve de la mise en œuvre du suivi n’avait été conservée. En outre, pour l’un des deux examens mensuels audités, des changements aux accès ont été décelés. Toutefois, les examens ne comportaient aucune preuve de l’approbation de ces changements.

Même si la direction a récemment commencé à réviser le processus de conservation des preuves des examens et des approbations des accès, ce processus n’avait pas été mis en œuvre au moment de la période visée par l’audit.

L’équipe de l’audit interne a procédé à un nouvel examen mensuel de la liste des accès des utilisateurs au SERRR en août 2022 et a constaté que dans douze cas, l’accès à un utilisateur devait être supprimé; l’équipe a également repéré quatre exceptions dans lesquelles des utilisateurs s’étaient vu attribuer des rôles en double, exceptions que l’examen annuel de la direction n’avait pas mises en lumière. Même si ces exceptions ont finalement été résolues au cours du cycle d’examen trimestriel suivant, en septembre, elles n’ont pas été repérées et corrigées en temps utile.

Si le suivi des accès des utilisateurs n’est pas fait efficacement et en temps utile, certains utilisateurs pourraient avoir un accès inapproprié et prolongé à des renseignements sensibles et confidentiels au sujet des RRP.

Recommandation 7 (risque modéré)

La direction devrait revoir les contrôles d'accès des utilisateurs, y compris les contrôles d'accès ponctuels et périodiques, afin de superviser en temps utile l'accès aux renseignements sensibles et confidentiels contenus dans le SERRR.

Annexe A – Notation des recommandations

Les recommandations sont notées afin d'aider la direction à affecter les ressources nécessaires pour combler les lacunes relevées ou améliorer les contrôles internes ou l'efficience opérationnelle. Ces notes ne sont fournies qu'à titre informatif. La direction doit les évaluer selon sa propre expérience et sa propension à prendre des risques.

Les recommandations sont notées en fonction des définitions suivantes :

- **Risque élevé :** une attention immédiate est requise 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.
- **Risque modéré :** lacune à combler sur le plan d'un contrôle ou amélioration opérationnelle à apporter à court terme.
- **Risque faible :** recommandation non essentielle à laquelle on peut donner suite pour renforcer un contrôle interne ou en améliorer l'efficience, normalement à peu de frais et d'efforts. Les notes individuelles ne doivent pas être considérées seules; il faut tenir compte aussi de leur effet sur d'autres objectifs.

Liens utiles

- Audit des régimes de retraite privés – Plan d’action de la direction (/fr/propos-du-bsif/rapports-publications/audit-regimes-retraite-prives/audit-regimes-retraite-prives-plan-daction-direction)

Date de modification :

2023-07-31