ARSF
Autorité ontarienne de réglementation des services financiers

Ligne directrice

☒ Interprétation ☒ Approche ☒ Information ☐ Décision

Date d'entrée en vigueur : 8 juin 2026
Identifiant : Nº PC0050APP

Ligne directrice sur les risques opérationnels et la résilience pour les compagnies d'assurance constituées en Ontario et les bourses d'assurance réciproque

Objectif

La ligne directrice sur les risques opérationnels et la résilience (la « **ligne directrice** ») de l'Autorité ontarienne de réglementation des services financiers (**ARSF**) pour les compagnies d'assurance constituées en Ontario et les bourses d'assurance réciproques (collectivement les « **assureurs** ») présente ce qui suit :

i. Approche de l'ARSF en matière d'évaluation des risques opérationnels et de la résilience pour les assureurs selon l'approche nº PC0045APP, *Cadre de surveillance axée sur le risque pour les compagnies d'assurance constituées en Ontario et les assureurs réciproques* (« **CSAR-I** »).

Ontario

ii. Des renseignements sur les lignes directrices et les normes de gestion des risques environnementaux, sociaux et de gouvernance (**ESG**) qui ont été élaborées par d'autres administrations et organismes de normalisation, et les répercussions potentielles sur les assureurs.

La présente ligne directrice vise à améliorer l'identification, l'évaluation et la gestion des risques opérationnels, ainsi que la résilience non financière, en améliorant la capacité des assureurs à surveiller leur environnement actuel, à prévoir les menaces et les possibilités futures, à réagir efficacement aux situations de crise et à tirer des leçons des échecs et des réussites du passé.

La présente ligne directrice décrit les processus et les pratiques de l'ARSF pour évaluer les risques opérationnels et la résilience des assureurs. Si les processus et pratiques présentés ne sont pas obligatoires, ils peuvent, selon les circonstances propres à un dossier, témoigner du respect ou non des obligations par l'assureur.

La section Information de la présente ligne directrice reconnaît que certains assureurs ont commencé à prendre en compte des facteurs ESG dans leurs pratiques de gestion des risques. Elle résume quelques-unes des directives et des normes sur la gestion des risques ESG élaborés par d'autres administrations et organismes de normalisation, et décrit les répercussions potentielles sur les assureurs.

Portée

La ligne directrice concerne les entités suivantes, réglementées ou enregistrées par l'ARSF :

- Les assureurs constitués en personne morale aux termes de la *Loi sur les personnes morales* (Ontario) et titulaires d'un permis octroyé par l'ARSF aux termes de la *Loi sur les assurances (la « Loi »).*

- Les bourses d'assurance réciproque titulaires d'un permis octroyé par l'ARSF aux termes de la *Loi.*

La présente ligne directrice complète la ligne directrice de l'ARSF en matière d'approche et d'interprétation nº PC0051INT, Gouvernance d'entreprise pour les compagnies d'assurance *constituées en Ontario et les bourses d'assurance réciproques* et les autres lignes directrices de l'ARSF et publications connexes figurant sur sa page Web. Elle doit être lue conjointement avec ces documents.

Justification et contexte

Les assureurs s'appuient de plus en plus sur la technologie, les données et des tiers dans leurs activités quotidiennes. Par conséquent, l'ARSF accorde une grande importance à l'identification, à l'évaluation et à la gestion des risques opérationnels, ainsi qu'à la résilience opérationnelle.

Le **risque opérationnel** représente le risque de subir des pertes découlant de lacunes ou de défauts attribuables aux ressources humaines et matérielles, comme des procédures et des systèmes internes, ou résultant d'événements déclencheurs. Cette définition inclut le risque juridique, mais exclut les risques stratégiques et de réputation. Le risque de réputation est une conséquence qui peut découler de la concrétisation du risque opérationnel.

La **résilience opérationnelle** est un résultat du traitement efficace des risques opérationnels par les assureurs en temps normal ou en situation de crise, et elle contribue à la sécurité et à la solidité des assureurs. Les assureurs qui ont un niveau élevé de résilience sont plus susceptibles de subir des interruptions plus courtes de leurs activités et d'enregistrer des pertes moins importantes découlant de perturbations opérationnelles, ce qui réduit les effets des incidents sur leurs activités essentielles et les services, fonctions et systèmes connexes. Pour atteindre la résilience opérationnelle, les assureurs devront peut-être adopter un nouvel état d'esprit avec une perspective élargie, élaborer des plans de préparation et de sensibilisation, et mettre en œuvre des stratégies efficaces lorsqu'elles passeront d'une période d'activités courantes à une période de crise.

Objets de l'ARSF

La présente ligne directrice appuie les objets législatifs de l'ARSF énoncés aux paragraphes 3(1) et 3(2) de la *Loi de 2016 sur l'Autorité ontarienne de réglementation des services financiers*, notamment :

- réglementer les secteurs réglementés et les superviser de façon générale
- contribuer à la confiance du public dans les secteurs réglementés
- promouvoir des normes de conduite professionnelle élevées
- favoriser le développement de secteurs des services financiers solides, durables, concurrentiels et novateurs

L'ARSF supervise les assureurs pour évaluer leur efficacité à considérer et à gérer leurs risques opérationnels, et à mettre en œuvre des mesures de résilience pour promouvoir des normes élevées de conduite professionnelle. L'ARSF aide ainsi les assureurs à exercer leurs activités de façon durable en cas de risques opérationnels et d'événements défavorables (notamment des catastrophes naturelles et des sinistres catastrophiques), ce qui contribue à renforcer la confiance du public à l'égard du secteur de l'assurance.

Définitions

Les termes employés dans la ligne directrice, à moins qu'ils ne soient définis autrement aux présentes, ont le sens qui leur est conféré dans la *Loi*. Dans la présente ligne directrice :

« **conseil d'administration »** s'entend du conseil d'administration d'un assureur ou du conseil consultatif d'une bourse d'assurance réciproque.

« haute direction » s'entend d'un dirigeant défini au sens du paragraphe 1(2), mais n'inclut pas les particuliers exclus de cette définition dans le paragraphe 1(3) du Règlement de l'Ontario 123/08, *Gouvernance d'entreprise – Partie II.2* de la *Loi*.

Approche

Cette section de la ligne directrice décrit l'approche utilisée par l'ARSF pour évaluer le cadre de gestion du risque opérationnel de l'assureur ainsi que ses pratiques en matière de résilience. Elle décrit également les processus et pratiques que l'ARSF utilisera pour évaluer l'adoption par l'assureur des principes indiqués dans la section Interprétation de la présente ligne directrice en vue d'obtenir les résultats souhaités. Pour plus de précisions sur le processus d'évaluation des risques, se reporter au CSAR-I.

Les principes exposent les résultats escomptés par l'ARSF, qui peuvent démontrer une identification, une évaluation et une gestion efficaces des risques opérationnels, ainsi qu'une résilience face à la concrétisation d'événements de risque opérationnel. Leur adoption n'est pas obligatoire, mais l'ARSF les prendra en considération dans son approche de supervision.

Les principes définissent les objectifs auxquels l'ARSF s'attend des assureurs. Une fois atteints, ces objectifs attestent d'une gestion efficace des risques opérationnels et d'une résilience appropriée en cas de concrétisation de tels événements. L'ARSFS surveillera et évaluera l'efficacité avec laquelle les assureurs adoptent ces principes dans le cadre de son approche de supervision, comme indiqué à la section « Approche » de la présente ligne directrice.

Principes

Principe 1 : Gouvernance

La responsabilité ultime de la surveillance des risques opérationnels incombe au conseil d'administration et à la haute direction des assureurs.

Une saine gestion des risques liés aux TI reflète l'efficacité du conseil d'administration et de la haute direction d'un assureur à administrer son portefeuille de produits, d'activités, de processus et de systèmes, ce qui permet de réduire la fréquence et l'incidence des événements en lien avec des risques liés aux TI.

Le conseil d'administration est chargé d'établir les stratégies et les structures de gouvernance nécessaires, de superviser et d'approuver le programme de gestion des risques opérationnels des assureurs ainsi que de veiller à ce qu'il y ait suffisamment de ressources pour mener à bien les activités de gestion des risques opérationnels et répondre à leurs obligations à l'égard des titulaires de police. Le conseil d'administration est tenu de respecter son obligation d'examiner et d'approuver périodiquement l'approche à l'égard des risques opérationnels, qui peut comprendre le cadre de gestion des risques opérationnels (**CGRO**) et les cadres de soutien (p. ex., le cadre de gestion des risques de tiers, le cadre des technologies de l'information, le cadre de gestion des incidents) ou une structure similaire en fonction de la taille, de la complexité et du profil de risque de l'assureur, ce qui comprendra sa propension à prendre des risques opérationnels, sa tolérance et ses limites. Le conseil d'administration examine aussi le plan de continuité des activités (**PCA**) et le plan de reprise après sinistre (**PRS**) de l'assureur. Pour définir la propension de l'assureur à prendre des risques et vérifier que le CGRO en tient compte, le conseil d'administration expose clairement la nature, le type et le niveau de risque opérationnel que l'assureur est prêt à endosser. Le conseil d'administration doit également veiller à ce qu'il fasse preuve d'une surveillance adéquate et efficace compte tenu de ces éléments.

La haute direction est responsable d'élaborer, de mettre à jour et de mettre en œuvre des politiques, des processus et des systèmes utilisés pour gérer les risques opérationnels et rehausser la résilience opérationnelle, de façon efficace à tous les niveaux décisionnels, et de veiller à ce que le personnel, les tiers et les autres intervenants pertinents les comprennent, selon leur degré de participation à la gestion des risques. La haute direction

établit les rôles et responsabilités respectifs nécessaires pour identifier, évaluer, gérer et superviser efficacement les risques opérationnels. Comme le conseil d'administration est responsable de la surveillance et de la gouvernance des risques, le profil de risque opérationnel de l'assureur par rapport à la propension à prendre des risques et à la tolérance aux risques approuvées par le conseil d'administration est mesuré par la haute direction et présenté au conseil d'administration pour confirmer l'harmonisation.

Des structures de gouvernance avec des responsabilités bien définies, des liens hiérarchiques et des pouvoirs décisionnels appuient la gestion des risques opérationnels et la résilience de l'assureur. Les assureurs sont responsables d'établir une structure organisationnelle où les activités de gestion des risques opérationnels sont menées par la gestion opérationnelle (première ligne de défense), puis examinées et remises en question par la gestion des risques (deuxième ligne de défense), et une assurance indépendante est ensuite fournie par la vérification interne (troisième ligne de défense), facilitant une gouvernance, une surveillance et une gestion des risques efficaces. Si les trois lignes de défense constituent une pratique établie dans l'industrie, l'ARSF évaluera également, dans le cadre de son analyse des risques opérationnels, d'autres structures de gouvernance caractérisées par des responsabilités et des comptes à rendre clairement délimités.

Principe 2 : Identification et évaluation du risque opérationnel

Les assureurs sont tenus d'identifier, d'évaluer et de comprendre de façon exhaustive le risque opérationnel inhérent à l'ensemble de leurs produits, activités, personnes, processus et systèmes, ainsi qu'à leur environnement externe, afin que des stratégies d'intervention correspondantes puissent être conçues et mises en œuvre.

L'assureur doit régulièrement procéder à des analyses de l'environnement de ses activités pour soutenir sa capacité à établir, évaluer et gérer de façon exhaustive les risques opérationnels inhérents à l'ensemble de ses produits, activités, personnes, processus et systèmes, ainsi qu'à ceux de l'environnement externe. Les activités, les processus et les systèmes visés par cette analyse de l'environnement comprennent les technologies de l'information utilisées pour appuyer les activités opérationnelles de l'assureur. La compréhension de ces risques inhérents facilitera la prise de décisions éclairées et permettra une gestion efficace des risques.

Principe 3 : Gestion du risque opérationnel

Les assureurs doivent élaborer et mettre en œuvre un cadre efficace de gestion du risque opérationnel afin de favoriser un environnement opérationnel stable pour leurs activités, de réduire la probabilité de perturbation et de limiter le risque de pertes pour les titulaires de police.

L'assureur met en œuvre un solide programme de gestion du risque opérationnel pour réduire la fréquence de la concrétisation des risques et l'impact des événements liés aux risques opérationnels sur ses titulaires de police et les autres intervenants. L'approche utilisée par un assureur pour gérer les risques opérationnels doit être soigneusement examinée, adéquatement documentée et périodiquement mise à jour afin de tenir compte des changements dans l'environnement opérationnel de l'assureur, de sa propension à prendre des risques et de sa tolérance aux risques, ou des progrès réalisés dans sa capacité à gérer les risques.

L'assureur doit créer et mettre en œuvre des cadres et des politiques et procédures à l'appui pour faciliter un traitement raisonnable, y compris la détermination, l'évaluation, l'atténuation, la surveillance et la déclaration de l'exposition aux risques opérationnels, compte tenu de la taille, de la complexité et du profil de risque de l'assureur. Le cadre de gestion des risques opérationnels d'un assureur et tout cadre de soutien ou structure semblable sont harmonisés et intégrés à son programme de gestion des risques à l'échelle de l'entreprise.

Principe 4 : Résilience

Le conseil d'administration et la haute direction se préparent en cas de scénarios défavorables et font en sorte que l'assureur soit prêt à faire face à une crise. À ce titre, l'assureur atteint la résilience en temps normal en améliorant sa préparation en cas de crise et sa capacité à surveiller et à prévoir toute escalade des risques. Lors de la concrétisation d'un risque opérationnel, l'assureur répond et s'adapte en prenant des mesures réalisables et opportunes, et en tirant parti des processus et des protocoles prédéterminés, afin de faciliter un rétablissement rationalisé et efficace. L'assureur examine aussi et réévalue les processus et protocoles à la lumière des échecs et des réussites passés, dans le but d'améliorer continuellement sa résilience.

La résilience opérationnelle est une composante clé d'un cadre efficace de gestion du risque opérationnel et un résultat du traitement efficace des risques opérationnels par l'assureur en

temps normal ou en situation de crise. La résilience opérationnelle contribue à la sécurité et à la solidité de l'assureur. Pour atteindre la résilience opérationnelle, l'assureur pourra être tenu d'adopter une nouvelle perspective, de se sensibiliser, et de mettre en œuvre des stratégies efficaces lorsqu'il passera d'une période d'activités courantes à une période de crise. Une gouvernance efficace (principe 1) ainsi qu'une identification et une évaluation solides (principe 2) et une gestion (principe 3) du risque opérationnel améliorent la capacité de l'assureur à atteindre ce résultat.

Les assureurs résilients sur le plan opérationnel peuvent exécuter des activités essentielles en cas de perturbation et sont moins susceptibles de subir des événements de risques opérationnels. Dans l'éventualité où un risque opérationnel se concrétiserait, les assureurs résilients sont plus susceptibles de connaître des interruptions plus courtes de leurs activités et de subir des pertes moins importantes découlant de perturbations, ce qui réduit les effets des incidents sur leurs activités essentielles et les services, fonctions et systèmes connexes.

Évaluation par l'ARSF des processus et pratiques en matière de risque opérationnel et de résilience

L'ARSF utilise le CSAR-I pour repérer les pratiques commerciales imprudentes ou dangereuses qui peuvent avoir des répercussions sur les titulaires de police, les souscripteurs et les clients des assureurs, et être en mesure d'intervenir en temps utile. L'ARSF exercera un jugement de supervision et évaluera les risques les plus importants que pose l'assureur par rapport à ses objectifs de supervision, et la mesure dans laquelle l'assureur peut repérer, évaluer et gérer ces risques, et faire preuve de résilience.

Évaluation de l'ARSF du risque opérationnel de l'assureur en tant que risque inhérent

Lors de l'évaluation d'un assureur en vertu du Principe 2 : Identification et évaluation des risques opérationnels, l'ARSF évaluera le risque opérationnel en tant que risque inhérent[1] intrinsèque aux activités importantes de l'assureur (p. ex. un secteur d'activité, une unité opérationnelle ou un processus à l'échelle de l'entreprise comme une technologie de l'information). L'ARSF évalue le risque inhérent avant toute atténuation et tient compte de la probabilité et de l'incidence d'un événement défavorable sur le capital et les bénéfices de l'assureur.

[1] Comme défini dans le CSAR-I de l'ARSF, le « risque inhérent » fait référence au niveau de risque intrinsèque à une activité importante et découle de l'exposition à des événements à venir potentiels et de l'incertitude qui s'y rapporte. Il est évalué avant toute atténuation et en tenant compte de la probabilité d'une incidence négative sur le capital ou les bénéfices d'un assureur et, en fin de compte, sur ses titulaires de police.

Le risque opérationnel peut provenir des produits, des activités, du personnel, des processus, des systèmes et/ou de l'environnement externe de l'assureur. L'assureur tient compte de la complexité de ses produits et services, de ses canaux de prestation de services et de son degré d'automatisation lors de l'établissement de la nature et de la complexité des risques opérationnels au sein de l'entreprise.

Le risque opérationnel est un concept général qui comprend divers sous-risques, y compris, mais sans s'y limiter, le risque lié aux tiers, le cyberrisque, le risque lié aux données et le risque climatique (physique et transition) :

- Le risque lié aux tiers survient lorsqu'un assureur embauche un tiers pour la fourniture d'un produit ou d'un service et que le tiers ne livre pas le produit ou le service en raison des risques inhérents à ses propres activités.
- Le cyberrisque est le risque de perte financière, de perturbation opérationnelle ou de dommages causés par l'accès non autorisé, l'utilisation, la divulgation, la perturbation, la modification ou la destruction de systèmes informatiques et/ou des données de l'assureur.
- Le risque lié aux données survient lorsque la gouvernance et l'infrastructure des données sont inadéquates pour assurer l'intégrité et la disponibilité des données à l'appui des activités quotidiennes d'un assureur, des rapports internes sur les risques et de la prise de décisions. Le risque lié aux données recoupe souvent d'autres secteurs de risque comme le cyberrisque, le risque lié aux tiers et l'analyse avancée. Le risque lié aux données peut se produire lorsque les assureurs disposent de processus et de contrôles de cybersécurité inadéquats pour protéger les données confidentielles des consommateurs contre une éventuelle atteinte à la vie privée.
- Le risque climatique physique découle de changements climatiques qui augmentent la fréquence et la gravité des feux de forêt, des inondations, des tempêtes, des vents violents et de la montée du niveau de la mer, entre autres. Les phénomènes climatiques pourraient perturber les activités essentielles quand les actifs physiques détenus par l'assureur ou ses fournisseurs de services tiers sont endommagés, comme les biens immobiliers et les infrastructures. Les risques physiques peuvent également accroître le risque lié à la souscription en raison d'une hausse potentielle

des demandes d'indemnisation pour des dommages matériels concernant un vaste éventail d'actifs, notamment les biens immobiliers, les infrastructures et les ressources naturelles.

Prise en compte par l'ARSF des technologies de l'information des assureurs comme une activité importante pour ceux-ci

L'utilisation de technologies de l'information (TI) est un facteur clé de la fourniture efficace des produits et des services d'un assureur, mais elle peut également entraîner des risques opérationnels importants. Les risques opérationnels associés aux TI proviennent d'un large éventail de services de soutien et d'activités commerciales. Les systèmes et l'infrastructure pourraient devenir inadéquats (en raison, par exemple, de l'obsolescence, de mises à niveau insuffisantes, de mauvaises conversions de systèmes ou d'une intégration infructueuse ou inefficace entre les systèmes après une fusion avec un autre assureur) ou pourraient être mal utilisés (en raison, par exemple, d'une mauvaise adaptation ou d'un accès non autorisé), ce qui peut contribuer aux risques opérationnels de l'assureur.

En tirant parti des TI pour appuyer la numérisation et mieux répondre à l'évolution des demandes des titulaires de police, les assureurs comptent de plus en plus sur des fournisseurs tiers, y compris des fournisseurs de services infonuagiques, dans leurs modèles d'affaires. Cette relation a ouvert de nouvelles possibilités pour les assureurs, mais les ont aussi exposés à de nouveaux risques et vulnérabilités.

Évaluation par l'ARSF de la qualité des contrôles et de la surveillance de l'assureur pour la gestion du risque opérationnel

L'ARSF évaluera dans quelle mesure le niveau de contrôle et de surveillance de l'assureur est adéquat et permet d'atténuer les risques inhérents. Elle évaluera notamment dans quelle mesure l'assureur adopte les pratiques énoncées dans le Principe 2 : Identification et évaluation du risque opérationnel et le Principe 3 : Gestion du risque opérationnel dans la présente ligne directrice. Pour chacune des activités importantes de l'assureur, l'ARSF tiendra compte des caractéristiques et du rendement des contrôles et de la surveillance dans le contexte de la taille, de la complexité et du profil de risque de l'assureur.

Lors de l'évaluation de la gestion du risque opérationnel de l'assureur, L'ARSF évaluera la mesure dans laquelle la gestion opérationnelle de l'assureur a identifié le potentiel de pertes importantes découlant des activités et si des processus et des contrôles adéquats sont en place pour atténuer ces risques opérationnels dans le cas où ils se concrétiseraient. Cela comprendrait, entre autres, une évaluation de l'efficacité des outils de gestion des risques opérationnels d'un assureur (p. ex. la taxonomie des risques opérationnels, les évaluations des risques et des contrôles et la collecte de données sur les pertes) pour déterminer, évaluer et gérer ses risques opérationnels. L'ARSF évaluera également les fonctions de surveillance d'un assureur (c.-à-d. les fonctions d'actuariat, de conformité, de gestion des risques et de vérification interne, la haute direction et le conseil d'administration) afin d'évaluer dans quelle mesure elles fournissent une surveillance indépendante efficace à l'échelle de l'entreprise de la gestion des risques opérationnels, et de déterminer si les activités de l'assureur et son exposition aux risques sont conformes à sa propension à prendre des risques opérationnels et à sa tolérance à ceux-ci. Dans le cadre de cette évaluation, l'ARSF tiendra également compte de l'efficacité avec laquelle les assureurs adoptent les pratiques décrites en vertu du Principe 1 : Gouvernance dans la section Interprétation de la présente ligne directrice. Pour les assureurs de petite taille, l'indépendance peut être atteinte par la séparation des tâches fonctionnelles entre les personnes et l'examen indépendant des processus et des fonctions.

Approche de l'ARSF en matière d'évaluation de la gestion des risques liés aux TI de l'assureur (y compris les cyberrisques)

En évaluant les fonctions de contrôle et de surveillance de l'assureur en ce qui a trait à la gestion des risques liés aux TI, l'ARSF évaluera la mesure dans laquelle les risques liés aux TI et les cyberrisques d'un assureur sont gérés au moyen de responsabilités et de structures redditionnelles claires (Principe 1 : Gouvernance). Il est important que les stratégies technologiques et les plans de cybersécurité d'un assureur soient proportionnels à sa taille, à sa complexité et à son profil de risque.

L'ARSF évaluera la capacité de l'assureur à cerner, à évaluer et à gérer les risques liés aux TI par rapport au Principe 2 : Identification et évaluation du risque opérationnel et au Principe 3 : Gestion du risque opérationnel comme énoncé dans la présente ligne directrice, ainsi que la ligne directrice de l'ARSF numéro GR0016INT, Gestion des risques liés aux technologies de l'information (TI). L'ARSF évaluera dans quelle mesure le programme de gestion des risques liés aux TI des assureurs comprend (sans nécessairement s'y limiter) les éléments suivants :

- des processus d'identification et d'évaluation des risques importants en matière de TI en fonction de la probabilité et de l'incidence des événements liés aux risques en matière de TI
- des contrôles adéquats dans l'environnement de contrôle informatique pour prévenir, détecter et gérer les accès non autorisés au réseau et aux systèmes de l'assureur (p. ex. en établissant des contrôles de gestion des identités et des accès, une piste de vérification, le chiffrement, des pare-feu et le renforcement des serveurs)
- des mécanismes d'identification, de classification et d'entretien des biens technologiques pour en assurer l'intégrité
- des processus de surveillance, de consignation, de gestion, de résolution et de signalement des incidents de TI afin de s'assurer que les normes de service et les objectifs opérationnels sont respectés, et que les risques connexes sont suffisamment atténués dans les limites de la propension de l'assureur à prendre des risques. Il est important que les assureurs informent l'ARSF en temps opportun des incidents importants liés aux risques informatiques, comme le décrit la **ligne directrice sur la gestion des risques liés aux TI** de l'ARSF.
- la surveillance et la gestion de l'actualité des technologies (y compris l'élimination sécuritaire des actifs technologiques en fin de vie utile) pour soutenir un environnement opérationnel robuste, sûr et résilient pour les activités commerciales
- une gestion et une mise en œuvre efficaces des projets de TI et des changements ou mises à jour technologiques avec des processus suffisants pour réduire au minimum les perturbations potentielles
- la mise en œuvre d'une formation de sensibilisation à la cybersécurité

L’ARSF évaluera dans quelle mesure l’assureur protège la confidentialité, l’intégrité et la disponibilité de ses propres ressources informatiques et comprend l’ampleur et l’incidence des faiblesses de l’environnement de contrôle des TI qui pourraient être exploitées par les auteurs de menaces internes et externes. À cette fin, l’ARSF cherchera des preuves démontrant que les contrôles de sécurité informatiques de l’assureur sont adéquats pour se protéger contre des incidents de TI, détecter ces derniers, intervenir, rétablir les activités et tirer des leçons. Dans les cas où l’assureur externalise ces activités, l’ARSF évaluera comment il examine et comprend les contrôles mis en place par ses fournisseurs tiers pour gérer ces risques. De plus, il est important que l’assureur améliore ses caractéristiques de résilience et son rendement en préparation des perturbations des services technologiques et dans l’éventualité de celles-ci.

L’ARSF évaluera la mesure dans laquelle l’assureur examine et met à jour périodiquement son plan de continuité des activités/plan de reprise après catastrophe pour refléter ses activités, les risques et les menaces actuels, en plus de tester régulièrement ces plans par rapport à des scénarios graves, mais plausibles qui pourraient avoir une incidence sur ses activités opérationnelles essentielles, de manière à s’assurer que les plans demeurent efficaces. L’ARSF tiendra compte de la mesure dans laquelle le plan de continuité des activités et le plan de reprise après catastrophe de l’assureur articulent les rôles et les responsabilités, définissent les seuils et les déclencheurs pour l’activation des plans, intègrent des évaluations quantitatives et qualitatives des impacts ou les analyses des impacts sur les activités, établissent des objectifs de rétablissement, et comprennent des plans d’intervention et de communication en cas d’incident (Principe 4 : Résilience).

Approche de l’ARSF en matière d’évaluation de la gestion des risques de l’assureur

Les assureurs comptent de plus en plus sur des fournisseurs tiers pour innover, fournir des services technologiques et répondre aux besoins opérationnels. Bien que ces fournisseurs tiers puissent accroître l’efficacité organisationnelle et réduire les coûts, ils peuvent aussi exposer les assureurs à des risques supplémentaires. Indépendamment de l’entente, l’assureur conserve la responsabilité de tous les risques, y compris ceux présentés par l’embauche de tierces parties. Par conséquent, l’assureur devrait établir un cadre de gestion des risques pour les tiers, ou une structure semblable, et veiller à mobiliser des ressources adéquates possédant les compétences et l’expertise nécessaires pour mettre en œuvre le cadre. Ces éléments sont essentiels pour appuyer une gestion efficace des risques découlant de l’embauche de ces fournisseurs tiers (Principe 1 : Gouvernance).

L’ARSF évaluera dans quelle mesure le cadre de gestion des risques liés aux tiers de l’assureur concourt à une approche uniforme et saine de la gestion des risques liés aux tiers tout au long du cycle de vie des tiers. Entre autres, l’ARSF évaluera dans quelle mesure les assureurs font preuve de diligence raisonnable avant d’intégrer un tiers et de façon continue par la suite. Cela inclut la compréhension du risque de concentration et des implications en cas de perturbation importante chez un fournisseur tiers dominant (p. ex., le risque de contagion). De plus, l’ARSF évaluera l’efficacité des processus d’approvisionnement et d’établissement de contrats et la pertinence des dispositions contractuelles pour gérer les risques associés à l’entente. Cela peut comprendre l’obligation d’aviser l’assureur des incidents importants ou du recours à des sous-traitants, les droits d’accès à l’information et à la vérification, ou les obligations de fonctionner dans le cadre des limites des mesures établies de risque et de rendement. L’ARSF évaluera également la mesure dans laquelle l’assureur surveille et déclare continuellement ses risques liés aux tiers afin de s’assurer que les produits et services sont fournis conformément aux ententes contractuelles, et si les risques sont gérés de façon appropriée et alignés sur la propension à prendre des risques de l’assureur (Principe 2 : Identification et évaluation du risque opérationnel et Principe 3 : Gestion du risque opérationnel).

En ce qui concerne le plan de continuité des activités/plan de reprise après catastrophe de l'assureur, l'ARSF cherchera également des preuves démontrant que l'assureur a pris en compte le risque de concentration ainsi que les liens et les interdépendances de ses fournisseurs tiers. L'ARSF évaluera la pertinence des plans et des mesures de l'assureur (mise à l'essai de scénarios, établissement de redondances) pour assurer la continuité des activités en cas de panne ou de perturbation chez un tiers (Principe 4 : Résilience).

Approche de l'ARSF en matière d'évaluation de la gestion et de la gouvernance des données de l'assureur

L'ARSF évaluera dans quelle mesure la gouvernance des données de l'assureur est appuyée par des structures claires de responsabilisation et de rapport hiérarchique. L'ARSF évaluera le cadre de gouvernance des données de l'assureur ou une structure similaire afin de déterminer dans quelle mesure il définit clairement les rôles et les responsabilités (Principe 1 : Gouvernance) et dans quelle mesure il identifie, évalue et gère le risque lié aux données de façon suffisante (Principe 2 : Identification et évaluation du risque opérationnel et Principe 3 : Gestion du risque opérationnel).

L'ARSF évaluera dans quelle mesure l'assureur possède des capacités suffisantes en matière de données pour appuyer une prise de décisions éclairée, non seulement en temps normal, mais également dans des situations de crise (Principe 4 : Résilience).

Approche de l'ARSF en matière d'évaluation du risque opérationnel et de la résilience pour l'assureur qui entreprend de nouvelles activités commerciales

Lorsque l'assureur entreprend une nouvelle activité commerciale, soit par lui-même, soit par l'intermédiaire d'une filiale ou d'une société affiliée, qui implique des innovations technologiques et de nouvelles utilisations, ou le partage de données ou d'informations sur les titulaires de police, l'ARSF évaluera dans quelle mesure l'assureur dispose d'une gouvernance solide et un processus efficace de détermination, d'évaluation et de gestion des risques opérationnels dans le cadre de la réalisation de nouvelles activités commerciales. L'ARSF évaluera également dans quelle mesure l'assureur :

- a établi des politiques, des procédures et des pratiques pour gérer les risques introduits par de nouvelles activités commerciales, comme le risque lié aux données et le risque lié aux TI (voir la section Approche plus haut)

- a fait preuve de diligence raisonnable dans le traitement des données financières des consommateurs avec des mesures de sécurité suffisantes, y compris la façon dont les données confidentielles et de nature délicate sont protégées et la façon dont les titulaires de police sont adéquatement indemnisés et protégés contre les pertes futures

- a envisagé les problèmes possibles de responsabilité, de protection des renseignements personnels et de sécurité lors du traitement des données des titulaires de police

Évaluation par l'ARSF de la résilience de l'assureur

L'ARSF évaluera la résilience de l'assureur en vertu du Principe 4 : Résilience. L'ARSF évaluera également si un assureur adhère aux pratiques de marché quant à la manière dont les assureurs devraient se préparer à des scénarios défavorables et à la réalisation des risques opérationnels. Dans le cadre de sa surveillance prudentielle, l'ARSF peut adresser une demande de renseignements à l'assureur pour qu'il présente son PCA, son PRS ou tout rapport pertinent qui démontre ses exercices de simulation de crise et de mise à l'essai de scénarios, ainsi que sa résilience générale dans des situations de crise [2].

La résilience globale de l'assureur est évaluée de façon holistique au moyen de facteurs financiers et non financiers et tient compte des conditions de travail en temps normal et après une période de crise. Les facteurs de résilience financière comprennent le capital et les liquidités dans la situation actuelle et sur une base prospective. Les facteurs non financiers sont généralement liés à la gouvernance et aux activités, mais ils requièrent également des ressources d'appui adéquates et un capital humain suffisant, aux fins de la préparation aux crises. Parmi les indicateurs clés des caractéristiques et du rendement en matière de

[2] Para. 442.1(1) 1 de la Loi.

résilience figure la solidité d'une politique de gestion du capital d'un assureur, la suffisance et la mise en œuvre de son plan de reprise, de son plan de financement d'urgence, de son PCA et de son PRS en cas de crise.

Lors de l'évaluation de la résilience d'un assureur, l'ARSF tiendra compte de la manière dont il fonctionne à la fois en temps normal et lorsqu'il est forcé de vivre une situation de crise. L'ARSF tiendra compte de la capacité de l'assureur à réagir et à se remettre efficacement d'une perturbation après la concrétisation d'un risque opérationnel ou d'une crise.

L'ARSF évaluera la résilience du point de vue des caractéristiques et du rendement. Les caractéristiques de résilience sont démontrées en temps normal, où l'assureur améliore sa préparation en cas de crise en améliorant sa capacité de surveiller et de prévoir toute escalade des risques. Le rendement de l'assureur en matière de résilience est démontré par sa capacité à réagir à la pression et à s'y adapter en prenant des mesures réalisables et opportunes, et en tirant parti de processus prédéterminés dans le cadre de protocoles préétablis pour faciliter un rétablissement rationalisé et efficace. L'ARSF tiendra également compte de la mesure dans laquelle l'assureur tire des leçons des échecs et des réussites du passé en vue d'améliorer continuellement sa résilience.

Voici quelques volets précis sur lesquels l'ARSF concentrera son évaluation des caractéristiques et du rendement d'un assureur en matière de résilience. Ces volets reflètent les principes énoncés dans la présente ligne directrice :

- Gouvernance
- Préparation aux crises et aux incidents au moyen de la planification d'urgence, de la continuité et de la reprise
- Gestion des risques opérationnels, en particulier la gestion des risques liés aux technologies de l'information, aux tiers et aux données
- Facteurs environnementaux, sociaux et de gouvernance (voir la ligne directrice en matière d'information ci-dessous).

Pour évaluer la cote de risque d'un assureur, l'ARSF cherchera à réunir des preuves sur sa capacité à surveiller et à prévoir l'escalade des risques en temps normal, ce qui démontre ses caractéristiques de résilience. Cela inclut, sans s'y limiter, la mesure dans laquelle :

- le conseil d'administration a examiné périodiquement les rapports sur les indicateurs réels de l'assureur, comparativement aux déclencheurs de la direction/du conseil d'administration, décrivant la situation globale de la santé financière de l'assureur
- il existe des preuves d'une communication régulière entre le conseil d'administration et la haute direction
- la solidité et la suffisance de la gestion du capital de l'assureur, notamment le nombre, la gravité et la qualité générale des scénarios de crise qui ont été utilisés pour évaluer la suffisance du capital
- la qualité des plans opérationnels d'urgence de l'assureur, et leur convenance, compte tenu de sa taille, de sa complexité et de son profil de risque.

L'ARSF cherchera des preuves de la capacité de l'assureur à réagir aux périodes de crise et à en tirer des leçons, démontrant ainsi sa résilience. Par exemple, l'ARSF évaluera ce qui suit :

- la haute direction et le conseil d'administration ont pris des mesures en se fondant sur les protocoles et les critères décrits dans les PCA, les PRS et les plans d'urgence de l'assureur, et lorsque ces plans ont été activés, ces mesures ont été efficaces
- des améliorations ont été apportées en continu aux activités et aux pratiques de l'assureur à la lumière des leçons apprises.

Les exemples ci-dessus ne sont pas exhaustifs et n'ont été fournis qu'à titre d'illustration.

Chaque assureur est libre d'adopter une approche de gouvernance organisationnelle adaptée à sa taille, à sa complexité et à son profil de risque, démontrant ainsi sa conformité aux dispositions législatives et réglementaires susmentionnées. Néanmoins, si cette approche s'écarte des pratiques reconnues en gestion des risques et en gouvernance, ou si son efficacité soulève des interrogations, l'ARSF peut demander à l'assureur d'expliquer pourquoi une telle approche est retenue et de démontrer comment elle satisfait aux exigences pertinentes.

Information

Le changement climatique et la réponse mondiale aux menaces qu'il représente ont le potentiel d'avoir une incidence importante sur la sécurité et la solidité des assureurs et sur le système financier en général. Les « risques liés au climat » sont généralement regroupés sous deux catégories : les risques physiques et les risques de transition. Les risques physiques et les risques de transition peuvent également mener à des risques en matière de responsabilité civile, comme le risque de demandes d'indemnité liées au climat en vertu de polices de responsabilité civile, ainsi que des procédures et des actions directes intentées à l'encontre des institutions financières pour avoir omis de gérer les risques liés au climat. Les risques liés au climat peuvent se traduire par des risques financiers pour les assureurs, comme des risques de crédit, de marché, d'assurance et d'illiquidité. Ils peuvent également mener à des risques stratégiques et opérationnels, et à des risques d'atteinte à la réputation. Dans les cas graves, les risques liés au climat peuvent menacer la viabilité à long terme du modèle d'entreprise d'un assureur et la stabilité du secteur.

Au cours des dernières années, les organismes de réglementation du monde entier et les organismes de normalisation comme le Conseil de stabilité financière[3], les Normes internationales d'information financière (IFRS) et l'Association internationale des contrôleurs d'assurance[4] ont mis au point des réponses réglementaires face aux risques physiques et aux risques de transition associés au changement climatique.

En juin 2023, l'International Sustainability Standards Board (ISSB) a publié ses deux premières normes IFRS d'information sur la durabilité : IFRS S1 Obligations générales en matière d'informations financières liées à la durabilité (anglais seulement) *(*et IFRS S2 Informations à fournir en lien avec les changements climatiques (anglais seulement). L'IFRS S2 énonce les obligations pour les entreprises de communiquer des informations sur les risques et les possibilités en lien avec les changements climatiques, tout en s'appuyant sur les obligations avancées dans l'IFRS S1. L'IFRS S2 intègre les recommandations du Groupe de travail sur l'information financière relative aux changements climatiques, et s'appuie sur ces recommandations.

---

[3] le Conseil de stabilité financière (anglais seulement)
[4] l'Association internationale des contrôleurs d'assurance (anglais seulement)

Cette norme exige également la communication d'informations sur les risques et les possibilités en lien avec les changements climatiques. Dans cette lignée, le Conseil canadien des normes d'information sur la durabilité a proposé les premières normes canadiennes d'information sur la durabilité le 13 mars 2024, marquant une nouvelle référence en la matière, et facilitant une approche plus uniforme et plus cohérente [5].

Certains assureurs ont déjà commencé à travailler à l'élaboration et à l'atteinte d'objectifs ESG. L'ARSF reconnaît ces efforts et encourage les assureurs à continuer de progresser vers l'intégration d'objectifs ESG et de la gestion des risques climatiques à leurs stratégies d'entreprise et leurs activités commerciales.

À l'avenir, l'ARSF envisagera d'intégrer les objectifs ESG dans ses cadres de réglementation et de surveillance, ce qui pourrait l'amener à publier des lignes directrices supplémentaires sur les risques liés au climat, les risques liés aux catastrophes naturelles et aux sinistres catastrophiques, et des pratiques de gouvernance conformes à la *Loi sur l'ARSF* et à la *Loi sur les assurances*. Dans l'intervalle, les assureurs sont encouragés à élaborer et à mettre en œuvre des plans qui tiennent compte des facteurs ESG dans leurs stratégies d'entreprise, leurs plans d'activités et leurs activités commerciales afin de contribuer positivement à l'atteinte d'objectifs ESG.

D'autres organismes canadiens de réglementation des services financiers ont publié des lignes directrices et des normes sur la gestion des risques ESG, en particulier dans les domaines suivants :

- les risques physiques et les risques de transition liés aux changements climatiques qui exigent des cadres, des politiques, des déclarations, des indicateurs, des cibles et une compréhension complète de la chaîne d'approvisionnement
- les risques sociaux exigeant de mettre l'accent sur les droits de la personne et des travailleurs, la diversité, la communauté et les consommateurs
- le risque de gouvernance exigeant de mettre en place des cadres adaptés d'atténuation.

[5] Normes canadiennes d'information sur la durabilité

À l'heure actuelle, l'ARSF évalue les initiatives ESG des assureurs (en particulier en matière de risque climatique) dans le cadre du CSAR-I comme partie intégrante de leur cote de résilience.

Date d'entrée en vigueur et prochain examen

La présente ligne directrice entrera en vigueur le 8 juin 2026 et sera révisée au plus tard le 8 juin 2031.

À propos de la présente ligne directrice

Ce document est conforme au cadre de lignes directrices de l'ARSF. En tant que ligne directrice en matière d'approche, elle décrit les principes, les processus et les pratiques internes de l'ARSF en matière de supervision et d'application du pouvoir discrétionnaire de l'ARSF. La section Information de la présente ligne directrice décrit les points de vue de l'ARSF sur certains sujets sans créer de nouvelles obligations de conformité pour les personnes réglementées.

Date d'entrée en vigueur : 8 juin 2026