ARSF
Autorité ontarienne de réglementation des services financiers

Ligne directrice

☒ Interprétation | ☒ Approche | ☒ Information | ☐ Décisions

Date d'entrée en vigueur : à déterminer
Identifiant : Nº. CU0088APP

Ligne directrice proposée sur les risques opérationnels et résilience

Objet

La ligne directrice sur les risques opérationnels et la résilience (la « ligne directrice ») de l'Autorité de réglementation des services financiers[1] (ARSF) fournit :

i. L'interprétation de l'ARSF des exigences en matière de risques opérationnels et de résilience pour les caisses populaires et credit unions de l'Ontario (les « caisses ») en vertu de la *Loi de 2020 sur les caisses populaires et credit unions* (la « Loi ») et de la *Règle 2021 – 001, Pratiques commerciales et financières saines* (la « *Règle* »)

ii. L'approche de l'ARSF pour évaluer la façon dont les caisses respectent efficacement les principes et atteignent les résultats identifiés dans la section Interprétation de la présente ligne directrice

iii. L'information sur les directives 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 caisses

Cette ligne directrice vise à améliorer l'identification, l'évaluation et la gestion des risques opérationnels, ainsi que la résilience non financière[2], en améliorant la capacité des caisses 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 section Interprétation de la présente ligne directrice énonce l'interprétation de l'ARSF des exigences applicables en vertu de la *Loi* et de la *Règle* afin de déterminer où la non-conformité peut mener à des mesures de supervision ou d'application de la loi. Cela pourrait comprendre l'obligation des caisses d'apporter des mesures correctives et de produire un rapport ou l'émission d'ordonnances et, dans les certains cas, le placement d'une caisse sous supervision ou administration conformément aux dispositions de la *Loi*[3].

La section Approche de la présente ligne directrice décrit les processus et les pratiques de l'ARSF pour évaluer les risques opérationnels et la résilience des caisses conformément au Cadre de surveillance axée sur le risque (CSAR) et peut avoir des répercussions sur la cote de risque globale des caisses. L'incidence sur la cote de risque globale est double : (1) l'identification, l'évaluation et la gestion des risques opérationnels seront prises en compte lors de l'évaluation du risque inhérent et de la qualité des contrôles et de la surveillance dans le cadre de la détermination du sommaire du risque résiduel prudentiel (SRRP); et (2) la résilience des caisses sera évaluée et reflétée dans la cote de résilience, qui sera utilisée pour modifier la cote sommaire de risque résiduel (SRR) afin de déterminer la cote de risque globale.

L'ARSF appliquera la présente ligne directrice et tiendra compte des répercussions potentielles découlant de la non-conformité, de manière proportionnelle, en fonction de la taille, de la complexité et du profil de risque des caisses populaires et credit unions.

Portée

La présente ligne directrice concerne les entités suivantes réglementées par l'ARSF :

- Les caisses populaires et les credit unions constituées en vertu de la Loi.

La présente ligne directrice complète d'autres lignes directrices de l'ARSF et publications connexes sur le site Web de l'ARSF, aux pages « Lignes directrices – Credit unions et caisses populaires » et « Règles », et doit être lue conjointement avec ces lignes directrices et publications.

Justification et contexte

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

Le risque opérationnel est le risque de perte résultant de carences ou de défauts attribuables à des procédures, au personnel et aux systèmes internes ou à des événements extérieurs. 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[4] des risques opérationnels par les caisses en temps normal ou en situation de crise, et contribue à la sécurité et à la solidité des caisses. Les caisses qui ont un niveau élevé de résilience sont plus susceptibles de subir des pannes plus courtes de leurs activités et de subir des pertes moins importants suite à des perturbations opérationnelles, ce qui réduit l'impact des incidents sur les activités essentielles et les services, fonctions et systèmes connexes. Pour atteindre la résilience opérationnelle, les caisses 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.

La présente ligne directrice appuie les objectifs statutaires de l'ARSF, tels qu'ils sont énoncés aux paragraphes 3(1), 3(2) et 3(4) de la *Loi de 2016 sur l'Autorité ontarienne de réglementation des services financiers* (la « *Loi sur l'ARSF* »), notamment :

- réglementer les secteurs réglementés et les superviser de manière 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 innovateurs

- promouvoir la stabilité du secteur des caisses en Ontario et y contribuer, en tenant compte de la nécessité de permettre aux caisses de soutenir efficacement la concurrence tout en prenant des risques raisonnables

- poursuivre les objets à l'avantage des déposants des caisses et de manière à minimiser les risques de perte que court le Fonds de réserve d'assurance-dépôts (FRAD)

Interprétation

La présente section expose le point de vue de l'ARSF sur les exigences relatives à la détermination, à l'évaluation et à la gestion efficaces des risques opérationnels des caisses, ainsi que sur la résilience opérationnelle énoncée dans les documents suivants :

- Dispositions particulières contenues dans les articles 4, 5, 6, 10, 11, 12 et 15 de la *Règle*, qui décrivent les exigences axées sur les principes et les résultats en ce qui concerne :

    - la composition et les responsabilités du conseil;

    - les responsabilités de la haute direction;

    - le statut, l'autorité et l'indépendance des fonctions de surveillance des caisses;

    - la fonction de vérification interne des caisses;

    - la fonction de gestion des risques des caisses;

    - la gestion opérationnelle des caisses;

- Le paragraphe 109(1) de la Loi, qui énonce les exigences sur la façon dont les pouvoirs et les fonctions des administrateurs, des dirigeants et des membres des comités des caisses doivent être exercés et satisfaits.

Le respect des principes énoncés ci-dessous est dans l'intérêt des caisses et de leurs membres et aide à démontrer à quel point les caisses se conforment efficacement aux dispositions de la *Règle* et de la *Loi* susmentionnées. Les principes décrivent les résultats attendus de l'ARSF, qui

doivent être atteints par les caisses de l'Ontario afin de démontrer une détermination, une évaluation et une gestion efficaces des risques opérationnels, ainsi que la résilience au moment de la concrétisation des événements liés aux risques opérationnels. L'ARSF surveillera le respect de ces principes dans le cadre de son approche de surveillance, tel qu'indiqué dans 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[5] et à la haute direction[6] des caisses.

La saine gestion des risques opérationnels et la résilience témoignent de l'efficacité du Conseil d'administration et de la haute direction des caisses dans l'administration du portefeuille de produits, d'activités, de processus et de systèmes, ce qui entraîne une réduction de la fréquence et de l'incidence des événements liés aux risques opérationnels.

Le conseil d'administration, composé d'administrateurs possédant les compétences et l'expertise appropriées[7], est chargé d'établir les stratégies et les structures de gouvernance nécessaires, de superviser et d'approuver le programme de gestion des risques opérationnels de la caisse ainsi que de veiller à ce qu'il y ait suffisamment de ressources[8] pour mener à bien les activités de gestion des risques opérationnels[9] et protéger les dépôts des membres. Le conseil est tenu d'examiner et d'approuver périodiquement le cadre de gestion des risques opérationnel (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 la caisse ce, qui comprendra sa propension à prendre des risques opérationnels, sa tolérance et ses limites[10]. Le conseil est également tenu d'examiner le plan de continuité des activités[11] et le plan de reprise après sinistre[12]. Le conseil doit énoncer clairement la nature, les types et les niveaux de risque opérationnel que la caisse est disposée à assumer[13].

La haute direction est responsable de l'élaboration, de la mise à jour et de la mise en œuvre des politiques, des processus et des systèmes utilisés pour gérer les risques opérationnels, y compris 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[14]. La haute direction

établit et régit les rôles et responsabilités respectifs nécessaires pour identifier, évaluer, gérer et superviser efficacement les risques opérationnels[15]. Comme le conseil est responsable de la supervision et de l'approbation de la gestion des risques, le profil de risque opérationnel de la caisse par rapport à la propension à prendre des risques et à la tolérance aux risques approuvées par le conseil doit être mesuré par la haute direction et présenté au conseil pour confirmer l'harmonisation[16].

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 des caisses. Les caisses doivent établir une structure organisationnelle où les activités de gestion des risques opérationnels sont menées par la Gestion opérationnelle[17] (première ligne de défense), puis examinées et remises en question par la Gestion des risques[18] (deuxième ligne de défense), et une assurance indépendante est ensuite fournie par la Vérification interne[19] (troisième ligne de défense), facilitant une gouvernance, une surveillance et une gestion des risques efficaces[20].

Principe 2 : Identification et évaluation du risque opérationnel

Les caisses sont tenues 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'atténuation des risques correspondantes puissent être calque et mises en œuvre[21].

L'exécution régulière d'analyses de l'environnement des activités des caisses appuie leur capacité de cerner, d'évaluer et de gérer de façon exhaustive le risques opérationnel inhérent à l'ensemble de leurs produits, activités, personnes, processus et systèmes, ainsi qu'à ceux de l'environnement externe. Les activités, les processus et les systèmes peuvent comprendre les technologies de l'information utilisées pour appuyer les activités opérationnelles des caisses. La compréhension de ces risques inhérents facilitera la prise de décisions éclairées et permettra une gestion efficace des risques.

Principe 3 : Gestion du risque opérationnels

Les caisses 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 minimiser le risque de pertes pour leurs déposants[22].

Un solide programme de gestion du risque opérationnel réduit la fréquence de la concrétisation des risques et l'impact des événements liés aux risques opérationnels. L'approche des caisses en matière de gestion du risque opérationnel doit être soigneusement examinée, adéquatement documentée[23] et périodiquement mise à jour afin de tenir compte des changements dans l'environnement opérationnel des caisses, de leur propension à prendre des risques et de leur tolérance aux risques, ou des progrès réalisés dans les capacités de gestion des risques[24].

En fonction de la taille, de la complexité et du profil de risque des caisses, celles-ci doivent élaborer 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[25]. Le cadre de gestion des risques opérationnels et tout cadre de soutien ou structure semblable doivent être harmonisés et intégrés à leur programme de gestion des risques à l'échelle de l'organisation[26].

Principe 4 : Résilience

Le conseil[27] et la haute direction[28] doivent se préparer en cas de scénarios défavorables et s'assurer que la caisse est prête à faire face à une crise. À ce titre, les caisses doivent atteindre la résilience en temps normal en améliorant leur préparation en cas de crise et leur capacité de surveiller et de prévoir toute escalade des risques[29]. Lors de la concrétisation d'un risque opérationnel, les caisses doivent réagir et s'adapter en prenant des mesures réalisables et opportunes, en tirant parti des processus et des protocoles prédéterminés, afin de faciliter un rétablissement rationalisé et efficace[30]. Les caisses sont également tenues d'examiner et de réévaluer les processus et les protocoles à la lumière des échecs et des réussites passés, dans le but d'améliorer continuellement la résilience[31].

La résilience opérationnelle est un résultat du traitement efficace des risques opérationnels par les caisses en temps normal ou en situation de crise, et elle contribue à la sécurité et à la solidité des caisses. Pour atteindre la résilience opérationnelle, les caisses devront peut-être adopter un nouvel état d'esprit avec une perspective élargie, se sensibiliser, et mettre en œuvre des stratégies efficaces lorsqu'elles passeront 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 des caisses à atteindre ce résultat. Les caisses résilientes sur le plan opérationnel sont en mesure d'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 caisses résilientes sont plus susceptibles de connaître des défaillances plus courtes de leurs activités et de subir des pertes moins importantes en raison de perturbations, ce qui réduit l'impact des l'incidents sur les activités essentielles et les services, fonctions et systèmes connexes.

Approche

Processus et pratiques

La présente section de la ligne directrice décrit les processus et les pratiques que l'ARSF utilisera pour évaluer le respect par les caisses des dispositions de la *Règle* et de la Loi qui sont mentionnées ci-dessus, en s'appuyant sur les principes définis dans la section Interprétation du présent document. Pour plus de détails sur le processus d'évaluation des risques, veuillez consulter la Ligne directrice relative au Cadre de surveillance axée sur le risque (no CU0083APP).

L'ARSF utilise le CSAR intégré pour repérer les pratiques commerciales imprudentes ou dangereuses qui peuvent avoir une incidence sur les membres, les clients et les déposants des caisses, et pour intervenir en temps opportun, au besoin. L'ARSF exercera son jugement de surveillance et évaluera les risques les plus importants que posent les caisses par rapport aux objectifs de surveillance ainsi que la mesure dans laquelle elles peuvent cerner, évaluer et gérer ces risques et atteindre la résilience.

Évaluation de l'ARSF du risque opérationnel des caisses en tant que catégorie de risque inhérent

Lors de l'évaluation de la conformité des caisses à la *Règle* selon l'interprétation du **Principe 2 : Identification et évaluation des risques opérationnels** dans la section Interprétation de la présente ligne directrice, l'ARSF évaluera le risque opérationnel en tant que catégorie de risque inhérent intrinsèque à l'activité importante[32] des caisses (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 des caisses.

Le risque opérationnel peut provenir des produits, des activités, du personnel, des processus, des systèmes et de l'environnement externe des caisses. Entre autres choses, l'ARSF tiendra compte de la complexité des produits et des services des caisses, des canaux de prestation et du niveau d'automatisation lors de l'évaluation du niveau de risque opérationnel des caisses.

Le risque opérationnel est vaste et comprend divers sous-risques, notamment, mais sans s'y limiter, le risque lié aux tiers, le cyber-risque et le risque lié aux données :

- Le risque lié aux tiers survient lorsque les caisses embauchent un tiers pour la fourniture d'un produit ou d'un service et que le tiers ne livre pas le produit ou le service conformément à l'accord contractuel.

- Le cyber-risque 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 des caisses.

- 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 des caisses, 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 cyber-risque, le risque lié aux tiers et l'analyse avancée. Le risque lié aux données peut se produire lorsque les caisses disposent de processus et de contrôles de cybersécurité inadéquats pour protéger les données confidentielles des consommateurs contre une éventuelle atteinte à la vie privée.

Voici quelques exemples d'événements pouvant présenter un risque opérationnel pour illustrer la façon dont les risques opérationnels peuvent se matérialiser et les résultats connexes. Ces exemples ne constituent pas une liste exhaustive. Ces événements peuvent entraîner des pertes réelles ou des quasi-échecs et représenter plusieurs types de risques opérationnels (comme illustré entre parenthèses).

- **Exemple 1 :** Une cyberattaque a compromis le cœur bancaire d'une caisse et a également entraîné une atteinte à la sécurité des données dans l'entrepôt de données hébergé par un fournisseur tiers. Des données ont été corrompues. Le système a été arrêté par le fournisseur tiers aux fins d'enquête afin de nettoyer et de restaurer les données, ce qui a causé d'importantes perturbations opérationnelles pour la caisse.

(*Événement de risque opérationnel illustrant un cyber-risque, un risque lié aux tiers et un risque lié aux données.*)

- **Exemple 2 :** Une caisse ne parvient pas à identifier, à saisir et à enregistrer adéquatement les détails pour différents types de comptes de dépôt, en partie en raison de son système bancaire désuet. Dans certains cas, des renseignements sur les bénéficiaires de certains comptes de fiduciaire étaient manquants. Les membres étaient insatisfaits après avoir découvert de nombreux problèmes et ont décidé de retirer leurs dépôts. (*Événement de risque opérationnel illustrant un risque lié aux technologies de l'information et un risque lié aux données.*)

- **Exemple 3 :** Une caisse a transféré par erreur des informations confidentielles sur un membre dans le cadre d'un appel au sujet de l'interface de programmation d'application (API) à une entreprise de technologie financière sans d'abord obtenir le consentement du membre. L'atteinte à la vie privée a entraîné une responsabilité juridique et des dommages à la réputation de la caisse. (*Événement de risque opérationnel illustrant un risque lié aux données et un risque juridique.*)

- **Exemple 4 :** Une caisse fait appel à un conseiller tiers sans comprendre les hypothèses sous-jacentes du modèle. Par conséquent, la caisse a pris de mauvaises décisions en matière de gestion des risques, ce qui a fini par entraîner des pertes financières. (*Événement de risque opérationnel illustrant un risque lié aux tiers et un risque lié au modèle.*)

- **Exemple 5 :** Une caisse n'intègre pas les risques émergents liés au climat dans ses stratégies opérationnelles ou ses cadres de gouvernance d'entreprise et de contrôle interne, ce qui entraîne des pertes financières et des pertes de réputation futures. (*Événement de risque opérationnel illustrant un risque d'ESG.*)

L'ARSF considère l'informatiques des caisses comme une activité importante pour ces dernières.

L'utilisation de technologies de l'information est un facteur clé de la fourniture efficace des produits et des services des caisses, mais elle peut également entraîner des risques opérationnels importants. Les risques opérationnels associés à l'informatique 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 une autre caisse) 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 dans les caisses.

En tirant parti des technologies de l'information pour appuyer la numérisation et mieux répondre à l'évolution des demandes des membres, les caisses comptent de plus en plus sur des fournisseurs tiers, y compris des fournisseurs de services infonuagiques, dans leurs modèles d'affaires. Ces partenariats ont créé de nouvelles possibilités pour les caisses, mais les ont aussi exposées à des risques et à des vulnérabilités.

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

L'ARSF évaluera dans quelle mesure le niveau de contrôle et de surveillance des caisses est adéquat et permet d'atténuer les risques inhérents. L'évaluation de l'ARSF permettra de déterminer dans quelle mesure les pratiques des caisses sont conformes aux exigences législatives et réglementaires (p. ex., celles énoncées dans la *Règle* et la *Loi*) et à l'interprétation de ces exigences par l'ARSF (en particulier celles établies en vertu du **Principe 2 : Identification et évaluation des risques opérationnels** et du **Principe 3 : Gestion du risque opérationnel** dans la section Interprétation de la présente ligne directrice). Pour chacune des activités importantes des caisses, 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 des caisses.

Lors de l'évaluation de la gestion du risque opérationnel des caisses, L'ARSF évaluera la mesure dans laquelle la gestion opérationnelle 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 des caisses (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 leurs risques opérationnels. L'ARSF évaluera également les fonctions de surveillance des caisses (c.-à-d. les fonctions 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 opérationnelle, et de déterminer si les activités des caisses et l'exposition aux risques sont conformes à leur propension à prendre des risques opérationnels et à leur tolérance à ceux-ci. Dans le cadre de cette évaluation, l'ARSF tiendra également compte de l'efficacité avec laquelle les caisses adhèrent au **Principe 1 : Gouvernance** dans la section Interprétation de la présente ligne directrice. Pour les caisses 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 technologies de l'information des caisses (y compris les cyber-risques)

En évaluant les fonctions de contrôle et de surveillance des caisses en ce qui a trait à la gestion des risques liés aux technologies de l'information (TI), l'ARSF évaluera la mesure dans laquelle les risques liés aux technologies de l'information et les cyber-risques des caisses 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 des caisses soient proportionnels à leur taille, à leur complexité et à leur profil de risque.

L'ARSF évaluera la capacité des caisses 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 décrits dans la section Interprétation de la présente ligne directrice, ainsi que dans **la ligne directrice sur la gestion des risques liés aux TI** de l'ARSF. L'ARSF tiendra également compte de la mesure dans laquelle les caisses ont adopté des pratiques de gestion des risques fondées sur les cadres et les normes de l'industrie. L'ARSF évaluera dans quelle mesure le programme de gestion des risques liés aux TI des caisses comprend (sans nécessairement s'y limiter) les éléments suivants :

- 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

- contrôles adéquats dans l'environnement de contrôle informatique pour prévenir, détecter et gérer les accès non autorisés au réseau et aux systèmes des caisses (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);

- identification, classification et entretien des biens technologiques pour en assurer l'intégrité

- surveillance, consignation, gestion, résolution et 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 à prendre des risques des caisses. Il est important que les caisses 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.

- surveillance et 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

- gestion et mise en œuvre efficace des projets de TI et des changements ou mises à jour technologiques avec des processus suffisants pour réduire au minimum les perturbations potentielles

- mise en œuvre d'une formation de sensibilisation à la cybersécurité

L'ARSF évaluera dans quelle mesure les caisses protègent la confidentialité, l'intégrité et la disponibilité de leurs propres ressources informatiques et comprennent 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 des caisses 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 les caisses externalisent ces activités, l'ARSF évaluera comment les caisses examinent et comprennent les contrôles mis en place par leurs fournisseurs tiers pour gérer ces risques. De plus, il est important que les caisses améliorent leurs caractéristiques de résilience et leur performances en préparation et en cas de perturbations des services technologiques.

L'ARSF évaluera la mesure dans laquelle les caisses examinent et mettent à jour périodiquement leur plan de continuité des activités/plan de reprise après catastrophe pour refléter leurs 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 les activités opérationnelles essentielles des caisses, 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 des caisses articulent les rôles et les responsabilités, définit les seuils et les déclencheurs pour l'activation des plans, intègrent des évaluations quantitatives et qualitatives des impacts ou l'analyse 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 des tiers des caisses

Les caisses 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 caisses à des risques supplémentaires. Indépendamment de l'entente, les caisses conservent la responsabilité et la propriété de tous les risques, y compris ceux présentés par l'embauche de tierces parties. Par conséquent, il est essentiel d'établir un cadre de gestion des risques pour les tiers, ou une structure semblable, et de veiller à ce que des ressources adéquates possédant les compétences et l'expertise nécessaires à la mise en œuvre du cadre soient affectées 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 des caisses appuie une approche cohérente et saine de la gestion des risques liés aux tiers tout au long du cycle de vie de ces derniers. Entre autres choses, l'ARSF évaluera dans quelle mesure les caisses 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 implicatons 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 les caisses 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 de risque et de performances établies. L'ARSF évaluera également la mesure dans laquelle les caisses surveillent et déclarent continuellement leurs 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 avec la propension à prendre des risques des caisses (**Principe 2 :**

Identification et évaluation des risques opérationnels et au **Principe 3 : Gestion du risque opérationnel**).

En ce qui concerne le plan de continuité des activités/plan de reprise après catastrophe des caisses, l'ARSF cherchera également des preuves démontrant que les caisses ont pris en compte le risque de concentration ainsi que les liens et les interdépendances de leurs fournisseurs tiers. L'ARSF évaluera la pertinence des plans et des mesures des caisses (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 des caisses

L'ARSF évaluera dans quelle mesure la gouvernance des données des caisses est appuyée par des structures de responsabilisation et de rapport hiérarchique claires. L'ARSF évaluera le cadre de gouvernance des données des caisses ou une structure similaire afin de déterminer dans quelle mesure ils définissent clairement les rôles et les responsabilités (**Principe 1 : Gouvernance**) et identifient, évaluent et gèrent suffisamment les risques liés aux données (**Principe 2 : Identification et évaluation des risques opérationnels** et **Principe 3 : Gestion des risques opérationnels**).

L'ARSF évaluera l'approche des caisses en matière de gestion et de protection de leurs données et la mesure dans laquelle elles ont mis en œuvre des processus et des contrôles pour gérer leurs risques liés aux données tout au long du cycle de vie des données (de la création/collecte des données à la suppression) et protéger la vie privée des consommateurs. De plus, l'ARSF cherchera des preuves que l'architecture de données et l'infrastructure informatique des caisses soutiennent adéquatement leurs capacités d'agrégation[33] et de rapport des données sur les risques, ainsi que des preuves de l'identification, de la classification, de la propriété et de l'autorisation d'utilisation appropriée des données. Des processus et des procédures robustes avec une formation adéquate du personnel pour sensibiliser les gens peuvent contribuer à assurer l'exactitude, l'exhaustivité, l'uniformité, l'actualité, la disponibilité, la confidentialité, la traçabilité, la non-répudiation et l'adéquation des données. Pour les caisses qui utilisent des analyses avancées (c.-à-d. des techniques d'analyse de données complexes comme l'intelligence artificielle) afin d'obtenir des renseignements approfondis, améliorer les prévisions et d'orienter la prise des décisions, l'ARSF évaluera la mesure dans laquelle des

mécanismes appropriés sont en place pour assurer une gouvernance robuste des données et atténuer les risques de préjudice et de partialité dans leurs modèles.

L'ARSF évaluera si les caisses disposent de capacités de données suffisantes pour appuyer la prise de décisions éclairées, non seulement en temps normal, mais aussi dans des situations de crise (p. ex., produire des rapports hors cycle et plus détaillés sur les actifs et les dépôts, produire des rapports ad hoc) (**Principe 4 : Résilience**).

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

Lorsque des caisses entreprennent une nouvelle activité commerciale, soit par elles-mêmes, soit par l'intermédiaire d'une filiale, qui implique des innovations technologiques et de nouvelles utilisations, ou le partage de données ou d'informations sur les clients (p. ex., la participation à un système bancaire ouvert, la création d'une filiale de courtage d'assurance), l'ARSF évaluera dans quelle mesure les caisses disposent d'une gouvernance solide et un processus de détermination, d'évaluation et de gestion efficace des risques opérationnels dans le cadre de la réalisation de nouvelles activités commerciales.

L'ARSF évaluera également dans quelle mesure les caisses ont :

- 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 les directives sur l'approche ci-dessus)

- 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 consommateurs sont adéquatement indemnisés et protégés contre les pertes futures

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

- veillé à ce que les données fournies par un consommateur à une fin ne soient pas utilisées à une autre fin, à moins d'obtenir un consentement éclairé

Évaluation de la résilience des caisses de l'ARSF

L'ARSF évaluera la résilience des caisses par rapport à leur adhésion au **Principe 4 : Résilience** dans la section Interprétation de la présente ligne directrice, qui interprète les exigences énoncées dans la *Règle*. La résilience peut être classée comme financière ou non financière. Selon les lignes directrices de l'ARSF sur le CSAR, la cote de résilience des caisses est fondée sur des considérations non financières et opérationnelles, car la résilience financière est reflétée dans les cotes de capital (y compris les bénéfices) et de liquidité des caisses.

Lors de l'évaluation de la résilience des caisses, l'ARSF tiendra compte de la manière dont elles fonctionnent à la fois en temps normal et lorsqu'elles sont forcées de vivre une situation de crise. L'ARSF tiendra compte de la capacité des caisses 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 de performance. Les caractéristiques de résilience sont démontrées en temps normal, où les caisses améliorent leur préparation en cas de crise en améliorant leur capacité de **surveiller** et de **prévoir** toute escalade des risques. La performance des caisses en matière de résilience est démontrée en fonction de leur capacité de **réagir à la pression et de 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 les caisses **tirent des leçons** des échecs et des réussites du passé en vue d'améliorer continuellement leur résilience.

Voici quelques volets précis sur lesquels l'ARSF concentrera son évaluation des caractéristiques de résilience et de performance en matière de résilience des caisses. Ces volets reflètent les principes énoncés dans la section Interprétation de la présente ligne directrice.

- gouvernance
- préparation aux crises et aux incidents par la planification de mesures d'urgence, de la continuité et du rétablissement[34]
- gestion du risque opérationnel, notamment la gestion des risques liés aux TI, aux tiers et aux données

- considérations environnementales, sociales et de gouvernance (voir la section Information ci-dessous)

Lors de l'évaluation de la cote de résilience des caisses, l'ARSF cherchera des preuves de la capacité des caisse à surveiller et à prévoir l'escalade des risques en temps normal, en démontrant leurs **caractéristiques de résilience**, ce qui comprend, sans toutefois s'y limiter, dans quelle mesure :

- le conseil a examiné périodiquement les rapports sur les indicateurs réels des caisses, mesurés par rapport aux déclencheurs de l'équipe de direction/du conseil, décrivant l'état global de la santé financière de la caisse

- il existe des preuves de communications périodiques entre le conseil et la haute direction

- la qualité des plans de circonstance opérationnels des caisses est adéquate, compte tenu de leur taille, de leur complexité et de leur profil de risque

L'ARSF cherchera des preuves de la capacité des caisses à réagir aux périodes de crise et à en tirer des leçons, démontrant ainsi leur résilience. Par exemple, l'ARSF tiendra compte de la mesure dans laquelle :

- des mesures ont été prises par la haute direction et le conseil d'administration en fonction des protocoles et des critères décrits dans le plan de rétablissement ou les plans de circonstance des caisses, au moment de l'activation de ces plans, et de l'efficacité de ces mesures

- il y a eu des améliorations continues des pratiques des caisses fondées sur les leçons apprises

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

Information

Au cours de la dernière décennie, il y a eu des développements importants et une sensibilisation aux enjeux ESG dans les industries des économies mondiales. Les Objectifs de développement

durable (ODD) ont été présentés par les Nations Unies comme un élément important de son Programme de développement durable à l'horizon 2030. De plus en plus de données probantes provenant d'études ont également été recueillies sur la menace croissante des changements climatiques et l'incidence qu'ils pourraient avoir sur la sécurité et la solidité des institutions financières, y compris les caisses.

Certaines caisses ont déjà commencé à travailler à l'élaboration et à l'atteinte d'objectifs ESG. L'ARSF reconnaît ces efforts et encourage les caisses à continuer de progresser vers l'intégration d'objectifs ESG à leurs stratégies d'entreprise et leurs activités commerciales. Il est important que les caisses travaillent de manière proactive pour appuyer les objectifs du Canada en matière d'ESG et d'ODD, qui peuvent être abordés en parallèle.

À l'avenir, l'ARSF envisagera l'intégration d'objectifs ESG dans ses cadres de réglementation et de surveillance, ce qui pourrait comprendre la publication de lignes directrices supplémentaires sur les risques liés au climat, des aspects liés aux droits de la personne et aux droits sociaux, et des pratiques de gouvernance qui sont alignés sur la Règle. Dans l'intervalle, les caisses sont encouragées à élaborer et à mettre en œuvre des plans qui tiennent compte des facteurs ESG dans leurs stratégies d'entreprise et leurs activités commerciales afin de contribuer positivement à l'atteinte d'objectifs ESG.

D'autres administrations et organismes de normalisation ont publié des directives et des normes sur la gestion des risques ESG, en particulier dans les domaines suivants :

- les risques physiques et de transition liés au climat qui nécessitent des cadres, des politiques, des divulgations, des indicateurs, des cibles ainsi qu'une compréhension complète de la chaîne d'approvisionnement

- les risques sociaux nécessitant de mettre l'accent sur les droits de la personne et du travail, la diversité, la collectivité et les clients

- les risques de gouvernance nécessitant des cadres d'atténuation appropriés

À l'heure actuelle, l'ARSF évalue les initiatives ESG des caisses (en particulier en matière de risque climatique) dans le cadre du CSAR comme partie intégrante de leur cote de résilience. L'ARSF peut émettre des observations aux caisses dans le cadre de son processus de supervision, mais les observations sur les facteurs ESG ne contribueront pas de façon punitive à

la cote de risque globale des caisses jusqu'à ce que des lignes directrices soient publiées à l'avenir.

Date d'entrée en vigueur et examen futur

La présente ligne directrice entrera en vigueur le (date à déterminer – au moment de l'émission) et sera révisée au plus tard le (date à déterminer).

À propos de la présente ligne directrice

Le présent document est conforme au Cadre de lignes directrices de l'ARSF. À titre d'orientation en matière d'interprétation, elle établit la vision de l'ARSF concernant les exigences en conformité avec son mandat prévu par la loi (lois, règlements et règles) afin qu'une non-conformité puisse mener à l'application de la loi ou à une mesure de surveillance. À titre d'orientation en matière d'approche, il décrit les principes, les processus et les pratiques internes de l'ARSF concernant les activités de surveillance, ainsi que l'application du pouvoir discrétionnaire du directeur général le cas échéant. La section Approche de la présente ligne directrice peut faire référence à des obligations de conformité, mais ne crée pas en soi une obligation de conformité. 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 : à déterminer

---

[1] La présente ligne directrice est publiée sous forme de lignes directrices combinées en matière d'interprétation, d'approche d'information en vertu du cadre de lignes directrices de l'ARSF. Chaque section est clairement indiquée.
[2] La résilience globale des caisses 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 financiers comprennent le capital (y compris les bénéfices) et les liquidités; les facteurs non financiers sont généralement liés à la gouvernance et aux activités opérationnelles et mettent l'accent sur la préparation aux crises. Aux fins de la présente ligne directrice, la résilience fait référence à la résilience non financière.
[3] Loi de 2020 sur les caisses populaires et les credit unions, L.O. 2020, chap. 36, annexe 7, articles 230 et 233 [LCPCU 2020].
[4] Aux fins de la présente ligne directrice, le traitement des risques opérationnels comprend l'identification,

l'évaluation et la gestion des risques opérationnels (tel que décrit aux Principes 2 et 3 de la section Interprétation). La gestion des risques opérationnels peut comprendre l'atténuation, la surveillance et la déclaration de risques opérationnels (tel que décrit au Principe 3 dans la section Interprétation).

[5] *Règle* 2021-001, Pratiques commerciales et financières saines, sous-alinéa 5(3)(i)(g) [*RÈGLE PCFS*].

[6] Ibidem alinéas 6(2)(ii) et 6(2)(iii).

[7] Ibidem paragraphe 4(1).

[8] Ibidem alinéa 5(4)(ii).

[9] Ibidem sous-alinéa 5(3)(i)(g).

[10] Ibidem.

[11] Règl. de l'Ont. 105/22, article (18) du paragraphe 36(1).

[12] Ibidem.

[13] *RÈGLE* PCFS, sous-alinéa 5(3)(i)(g).

[14] Ibidem sous-alinéa 6(1)(i)(b), alinéa 6(2)(iii).

[15] Ibidem sous-alinéa 6(1)(i)(b).

[16] Ibidem sous-alinéa 5(3)(i)(g).

[17] Ibidem alinéas 15(2)(iv) et 15(2)(v).

[18] Ibidem sous-alinéa 10(9)(i)(a)-(b), paragraphe 10(11) et alinéa 12(1)(i).

[19] Ibidem paragraphe 11(2).

[20] Conformément au paragraphe 10(1) de la Règle, une caisse doit établir et maintenir des fonctions de surveillance de sorte que ces fonctions aient suffisamment de ressources, de statut, d'autorité et d'indépendance pour s'acquitter de leurs rôles et responsabilités, proportionnellement à la taille, à la complexité et au profil de risque de la caisse.

[21] Ibidem sous-alinéa 5(3)(i)(g), sous-alinéa 6(1)(i)(b), alinéa 6(2)(ii), alinéa 6(2)(iii), paragraphe 11(2), alinéa 12(1)(i), alinéa 12(1)(i), alinéa 15(2)(iv) et alinéa 15(2)(v).

[22] Ibidem alinéa 12(1)(i).

[23] Ibidem alinéa 12(1)(ii).

[24] Ibidem alinéa 12(1)(i).

[25] Ibidem alinéa 12(1)(i) et 12(1)(ii).

[26] Ibidem alinéa 12(1)(i).

[27] Ibidem sous-alinéa 5(3)(i)(g).

[28] Ibidem alinéas 6(2)(ii) et (iii).

[29] Ibidem alinéa 12(1)(i).

[30] Ibidem alinéa 12(1)(ii).

[31] Ibidem.

[32] Comme défini dans le Cadre de surveillance axée sur le risque de l'ARSF (no CU0083APP).

[33] L’agrégation des données sur les risques permet de définir, de recueillir et de traiter les données sur les risques en fonction des exigences de déclaration des risques des caisses afin de leur permettre de mesurer leur rendement par rapport à leur propension à prendre des risques et à leur tolérance aux risques.

[34] Se reporter à la Ligne directrice pour la planification de la reprise des activités (CU0069INT).