ARSF
Autorité ontarienne de réglementation des services financiers

Ligne directrice

☒ Interprétation | ☒ Approche | ☒ Information | ☐ Décisions

Date d'entrée en vigueur : à déterminer
Identifiant: No. GR0016INT

Proposition en matière de gestion des risques liés aux technologies de l'information (« TI »)

Ces lignes directrices s'applique à toutes les entités et personnes réglementées par l'ARSF. Le tableau 1 peut être utilisé pour naviguer les lignes directrices afin de déterminer quelles sections sont applicables à une entité ou à une personne réglementée.

Tableau 1 : Lignes directrices présentées par entité ou personne réglementée

Entité réglementée (ordre alphabétique)	Sections applicables	Aperçu de la section spécifique au secteur
Organismes d'accréditation pour les planificateurs et conseillers financiers	• Section Tous les secteurs • Approche sectorielle pour les organismes d'accréditation	• Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux

Entité réglementée (ordre alphabétique)	Sections applicables	Aperçu de la section spécifique au secteur
	des planificateurs et des conseillers financiers	technologies de l'information
Caisses populaires et credit unions (caisses)	• Section Tous les secteurs • Interprétation/approche sectorielle pour les caisses populaires et credit unions	• Interprétation de l'ARSF des exigences en matière de gestion des risques liés aux technologies de l'information en vertu de la règle *Pratiques commerciales et financières saines et de la Loi de 2020 sur les caisses populaires et les credit unions*. • Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information (conforme aux lignes directrices sur le risque et la résilience opérationnels)
Fournisseurs de services de santé	• Section Tous les secteurs	• Aucun contenu spécifique au secteur

Entité réglementée (ordre alphabétique)	Sections applicables	Aperçu de la section spécifique au secteur
Agents d'assurances, agences d'assurances, experts en sinistres et entreprises d'experts en sinistres	• Section Tous les secteurs • Spécifique au secteur : Approche pour les sociétés d'assurances, les agents d'assurances, les agences d'assurances, les experts en sinistres et les entreprises de redressement constituées ailleurs qu'en Ontario	• Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information
Sociétés de prêt et de fiducie	• Section Tous les secteurs	• Aucun contenu spécifique au secteur
Maisons de courtage d'hypothèques, agents en hypothèques, courtiers en hypothèques et administrateurs d'hypothèques	• Section Tous les secteurs • Spécifique au secteur : Approche/information pour les administrateurs d'hypothèques, les agents en hypothèques, les maisons de courtage d'hypothèques et les courtiers en hypothèques	• Information sur la façon dont les lignes directrices existantes MB0048INF Principes de préparation à la cybersécurité du Conseil canadien des autorités de s de réglementation des courtiers hypothécaires pour le secteur du courtage d'hypothèques s'alignent sur ces lignes directrices et sur la manière dont l'ARSF abordera la non-conformité.

Entité réglementée (ordre alphabétique)	Sections applicables	Aperçu de la section spécifique au secteur
Sociétés d'assurances et d'assurances réciproques constituées en Ontario	• Section Tous les secteurs • Spécifique au secteur : Interprétation/approche pour les sociétés d'assurances et d'assurances réciproques constituées en Ontario	• Interprétation par l'ARSF des exigences en matière de gestion des risques liés aux technologies de l'information en vertu de la *Loi sur les assurances*. • Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information
Sociétés d'assurances non constituées en Ontario	• Section Tous les secteurs • Spécifique au secteur : Approche pour les sociétés d'assurances, les agents d'assurances, les agences d'assurances, les experts en sinistres et les entreprises de redressement constituées ailleurs qu'en Ontario	• Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information
Administrateurs de régimes de retraite	• Section Tous les secteurs • Spécifique au secteur : Interprétation/Approche pour	• Interprétation de l'ARSF de la *Loi sur les régimes de retraite* en ce qui a trait aux TI

Entité réglementée (ordre alphabétique)	Sections applicables	Aperçu de la section spécifique au secteur
	les administrateurs de régimes de retraite	• Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information

Tous les secteurs

Objet et portée

Ces lignes directrices présentent :

- « Les pratiques[1] pour une gestion efficace des risques liés aux technologies de l'information. »
- Un processus permettant aux entités et aux personnes réglementées d'informer l'ARSF[2] en cas d'incident important découlant de risques liés aux technologies de l'information.
- Des lignes directrices sectorielles, y compris des interprétations des exigences pour les caisses, les sociétés d'assurances et d'assurances réciproques constituées en Ontario (« assureurs ») et les administrateurs de régimes de retraite.

Ces lignes directrices s'appliquent à toutes les entités et à tous les individus réglementés par l'ARSF. Elles décrivent les pratiques et les résultats souhaités pour les entités et les personnes réglementées, mais ne prescrivent pas la manière de les atteindre. Cette approche fondée sur des principes offre aux entités et aux personnes réglementées la souplesse nécessaire pour atteindre les résultats d'une manière qui convient à la taille et à la nature de leurs activités.

Ces lignes directrices comprennent des sections « Information », « Approche » et « Interprétation » :

- Ligne directrice pour l'information - Fournit des informations sur certains sujets tels que les pratiques sans créer d'obligations de conformité pour les entités et les personnes réglementées.

- Ligne directrice pour l'approche - Décrit les principes, les processus et les pratiques de l'ARSF pour les activités de surveillance et l'application du pouvoir discrétionnaire du directeur général de l'ARSF sans créer d'obligations de conformité pour les entités et les personnes réglementées.

- Ligne directrice pour l'interprétation - Énonce les exigences de l'ARSF dans le cadre de son mandat législatif (c'est-à-dire la législation, la réglementation et les règles). La non-conformité peut mener à des mesures d'application ou de surveillance.

Grandes lignes

Les lignes directrices sont divisées en deux sections principales :

- **Tous les secteurs**- Lignes directrices pour l'interprétation/information/approche applicables à toutes les entités et personnes réglementées par l'ARSF. Cette section contient :

    - Interprétation des exigences réglementaires existantes.

    - Information sur les pratiques pour une gestion efficace des risques liés aux technologies de l'information. »

    - Approche pour un « avis en cas d'incidents importants découlant des risques liés aux technologies de l'information » à l'ARSF.

- **Spécifique à un secteur**- Conseils applicables aux entités ou aux personnes réglementées dans un secteur spécifique.

En tant que régulateur fonctionnant selon des principes et des risques, l'approche réglementaire de l'ARSF varie selon la taille et la nature des entités et des individus réglementés. Bien que la section **« Tous les secteurs » de ces lignes directrices s'applique à toutes les entités et personnes réglementées** par l'ARSF, certaines entités et personnes réglementées suivent des lignes directrices supplémentaires spécifiques à un secteur. L'ARSF a fait cette détermination en se basant sur le risque posé aux consommateurs, et le risque pour l'entité/la personne

réglementée ou d'autres entités ou personnes dans le même secteur. Dans le cas de certaines entités et personnes réglementées, il n'y a pas de lignes directrices spécifiques à un secteur.

Justification et contexte

L'ARSF définit les « risques liés aux technologies de l'information » comme les risques de perte financière, de perturbation ou de dommage opérationnel, ou de perte de réputation résultant de l'inadéquation, de la perturbation, de la destruction, de la défaillance ou de l'endommagement, par quelque moyen que ce soit, des systèmes, de l'infrastructure et des données informatiques d'une entité ou d'une personne réglementée.

Les risques liés aux TI peuvent être externes ou internes à une entité ou à une personne réglementée. Les risques liés aux TI englobe, mais sans s'y limiter, le cyberrisque. Si le cyberrisque concerne spécifiquement les violations délibérées ou accidentelles de la sécurité (par exemple, une violation de données), les risques liés aux TI comprennent également tout risque lié à l'utilisation de l'informatique (par exemple, une infrastructure numérique vieillissante).

Les risques liés aux TI représentent une menace importante et croissante pour les activités, les opérations et la stabilité des secteurs réglementés par l'ARSF, et peuvent avoir des répercussions[3] négatives sur les consommateurs[4]. Cela peut perturber la confiance dans les secteurs des services financiers et des régimes de retraite.

L'accent mis par l'ARSF sur les risques liés aux TI est conforme à ses objectifs statutaires :[5]

- réglementer et superviser de manière générale les secteurs réglementés;
- contribuer à la confiance du public dans les secteurs réglementés;
- promouvoir des normes élevées de conduite professionnelles;
- protéger les droits et les intérêts des consommateurs;
- favoriser des secteurs de services financiers robustes, durables, compétitifs et innovants;
- promouvoir une bonne administration des régimes de retraite;
- protéger et sauvegarder les prestations de retraite et les droits des bénéficiaires de régimes de retraite; et

- promouvoir et contribuer autrement à la stabilité du secteur des caisses en Ontario.

Interprétation – Tous les secteurs

Conformité aux exigences existantes

Les entités et les personnes réglementées doivent se conformer aux exigences existantes en matière de risques liés aux TI et de protection des renseignements personnels. Cela comprend, sans s'y limiter, les exigences contenues dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRPDE ») du gouvernement fédéral[6].

Le non-respect de ces exigences est susceptible de causer un préjudice aux consommateurs. Par conséquent, l'ARSF considère la conformité aux exigences applicables existantes en lien avec les risques liés aux TI et à la protection des renseignements personnels comme un facteur pouvant avoir une incidence sur l'évaluation de l'aptitude d'un titulaire de licence à obtenir ou à renouveler une licence, à se constituer en société auprès de l'ARSF en tant que caisse ou société d'assurances, à s'enregistrer auprès de l'ARSF ou à être approuvé ou à conserver le statut d'organisme d'accréditation pour les planificateurs et les conseillers financiers.

Information – Tous les secteurs

Cette section s'applique à toutes les entités et personnes réglementées.

Pratiques pour une gestion efficace des risques liés aux technologies de l'information

Les « Pratiques pour une gestion efficace des risques liés aux technologies de l'information » suivantes décrivent les pratiques acceptées par l'industrie pour les entités et les personnes réglementées afin d'assurer une gestion efficace des risques liés aux technologies de l'information. L'ARSF s'attend à ce que toutes les entités et personnes réglementées suivent les pratiques de gestion efficace des risques liés aux technologies de l'information. L'ARSF tiendra compte de l'adhésion à ces pratiques et de leurs résultats souhaités lors de la supervision, ainsi que lors de la délivrance et du renouvellement des licences.

Note pour les personnes réglementées par l'ARSF :
Alors que certaines personnes réglementées sont responsables de la gestion des risques liés aux TI de leur entreprise, d'autres sont des employés ou des entrepreneurs d'une entité réglementée par l'ARSF qui est responsable en dernier ressort de la gestion des risques dans ce domaine (par exemple, les agents d'assurance/experts en sinistres employés par un assureur ou sous contrat avec lui, et les agents et courtiers en hypothèques travaillant pour une maison de courtage). Ces dernières personnes réglementées sont toujours responsables de se conduire d'une manière conforme à l'esprit des Pratiques pour une gestion efficace des risques liés aux technologies de l'information et aux résultats souhaités.

Par exemple, bien que les personnes réglementées qui sont des employés ou des entrepreneurs d'une entité réglementée ne soient pas responsables de l'élaboration d'une stratégie de gestion des risques, une bonne pratique serait de suivre la stratégie établie par l'entité réglementée.

Pratique 1 : Gouvernance - L'entité ou la personne réglementée dispose d'une gouvernance et d'une surveillance appropriées de ses risques liés aux TI.

Résultats souhaités :

- Les risques liés aux TI sont gouvernés efficacement par les entités et les personnes réglementées.
- Des responsabilités claires en matière de gestion des risques liés aux TI sont attribuées à une ou plusieurs personnes ayant suffisamment d'ancienneté et d'expertise.
- La responsabilité de la surveillance des risques liés aux TI incombe à la haute direction et au conseil d'administration.

Pratique 2 : Gestion des risques - L'entité ou la personne réglementée s'appuie sur des pratiques acceptées par l'industrie pour gérer efficacement les risques liés aux TI.

Résultats souhaités :

- Les entités et les personnes réglementées ont mis en place des politiques, des procédures et des contrôles pour protéger, détecter, répondre, récupérer et tirer des leçons des incidents découlant des risques liés aux TI.

- Les entités et les personnes réglementées qui dépendent fortement de la technologie pour fonctionner et fournir des produits et des services au public définissent leur appétit et leur tolérance en matière de risques liés aux TI.[7]

Pratique 3 : Gestion des données - L'entité ou la personne réglementée utilise des stratégies acceptées par l'industrie pour gérer et sécuriser efficacement les données confidentielles.

Résultats souhaités :

- Les données confidentielles supervisées par les entités et les personnes réglementées sont sécurisées.

- Les données confidentielles sont manipulées et stockées correctement de manière à préserver la qualité, l'intégrité, la disponibilité et la confidentialité des données.

Pratique 4 : Externalisation - L'entité ou la personne réglementée gère efficacement les risques liés aux TI associés à toute activité, fonction et service externalisé ou co-sourcé.[8]

Résultats souhaités :

- Les risques liés aux TI pour les activités, les fonctions et les services externalisés et co-sourcés sont identifiés, évalués et gérés correctement.
- La responsabilité et la propriété de toute fonction externalisée ou co-sourcée sont maintenues par les entités et les personnes réglementées.

Pratique 5 : Préparation aux incidents - L'entité ou la personne réglementée est prête à détecter, enregistrer, gérer, résoudre, récupérer, surveiller et signaler les incidents informatiques efficacement et en temps opportun.

Résultats souhaités :

- L'impact des incidents découlant des risques liés aux TI est minimisé.
- Les entités et les personnes réglementées tirent des leçons des incidents précédents pour mieux prévenir les incidents futurs.

Pratique 6 : Continuité et résilience - L'entité ou la personne réglementée est prête à assurer la continuité de ses actifs informatiques et sa capacité à fournir des services essentiels pendant et après un incident.

Résultats souhaités :

- Les entités et les personnes réglementées maintiennent la disponibilité des services financiers.
- Les entités et les personnes réglementées sont résilientes sur le plan opérationnel.

Pratique 7 : Avis en cas d'incidents importants découlant des risques liés aux technologies de l'information - L'entité ou la personne réglementée avise son ou ses organismes de réglementation en cas d'incident important découlant des risques liés aux TI (voir la section Avis en cas d'incidents importants découlant des risques liés aux technologies de l'information).

Résultats souhaités :

- Les entités et les personnes réglementées font preuve de transparence envers l'ARSF en ce qui concerne les incidents importants liés aux risques pour les TI.
- Les entités et les personnes réglementées aident l'ARSF à identifier les zones à haut risque en temps opportun, ce qui peut aider à prévenir de futurs incidents.

Approche – Tous les secteurs

Avis en cas d'incidents importants découlant des risques liés aux technologies de l'information

Les pratiques de gestion efficace des risques liés aux TI pour les entités et les personnes réglementées comprennent un avis aux autorités de réglementation dès que possible après avoir déterminé qu'un incident découlant de risques liés aux TI est important. L'ARSF maintiendra la confidentialité de tout incident signalé par les entités et les personnes réglementées dans la mesure permise par la loi.

Lorsque l'ARSF prend connaissance d'un incident découlant de risques liés aux TI, soit par un avis direct de l'entité ou de la personne réglementée, soit par d'autres canaux (par exemple, plainte, rapport des médias, etc.), elle déterminera s'il faut activer le **protocole de l'ARSF pour les incidents découlant de risques liés aux TI**. Dans certains cas, l'ARSF peut déterminer que l'activation du protocole pour les incidents découlant de risques liés aux TI n'est pas justifiée.

Lorsqu'ils signalent un incident découlant de risques liés aux TI, les entités ou les personnes réglementées peuvent en informer l'ARSF à l'adresse ITriskinbox@fsrao.ca en utilisant le « Rapport sur les incidents découlant des risques liés aux TI de l'ARSF ». Afin de réduire la charge de travail des entités ou des personnes réglementées qui doivent soumettre plusieurs rapports

d'incident, l'ARSF acceptera également d'être avisée au moyen d'un formulaire comparable émis par une autre autorité de réglementation des services financiers.

Une bonne pratique pour les personnes réglementées qui sont des employés ou des entrepreneurs d'une entité réglementée est de signaler tout incident à cette entité réglementée. Les entités réglementées peuvent déterminer si une violation est importante et en informer ensuite l'ARSF.

Pour le **secteur du courtage d'hypothèques**, ces lignes directrices, y compris les pratiques pour une gestion efficace des risques liés aux technologies de l'information, le Rapport sur les incidents découlant des risques liés aux TI et le Protocole relatif aux incidents liés aux risques liés aux TI, sont conformes aux principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH) pour le secteur du courtage d'hypothèques (lignes directrices du CCCPH). L'application de ces lignes directrices doit correspondre aux lignes directrices du CCARCH et, en cas d'incohérence, ces lignes directrices obtiendront la préséance.

Incidents importants découlant des risques liés aux TI

Ce qui constitue un incident important doit être déterminé par l'entité ou la personne réglementée en fonction de l'impact sur son activité, ses opérations et ses consommateurs.

Les indicateurs qu'un incident important s'est produit peuvent inclure, sans s'y limiter, les éléments suivants. Si l'incident :

- entraîne des perturbations opérationnelles importantes des systèmes et des fonctions de l'entreprise;
- perturbe de manière significative la capacité des consommateurs à accéder aux services essentiels pendant une période prolongée;
- affecte un fournisseur tiers dans la mesure où il a des répercussions importantes sur l'entité ou la personne réglementée;
- enfreint l'appétit ou les seuils de risque internes;
- nécessite des mesures ou des ressources non habituelles;

- entraîne l’exposition d’une grande quantité de données confidentielles;
- est récurrent et pourrait avoir un impact significatif sur une base cumulative;
- est signalé à la direction générale ou au conseil d’administration;
- est signalé à un autre organisme de réglementation, à un organisme d’application de la loi, au Commissariat à la protection de la vie privée, etc.;
- donne lieu à une demande d’indemnisation au titre de la cyberassurance;
- entraîne ou entraînera vraisemblablement une attention médiatique négative qui pourrait nuire à la réputation de l’entité ou de la personne réglementée ou du secteur dans lequel elle mène ses activités;
- pourrait potentiellement affecter d’autres entités ou personnes réglementées par l’ARSF, ou il s’agit d’un incident qui est susceptible de se reproduire avec d’autres entités ou personnes réglementées par l’ARSF.

L’ARSF a le pouvoir de demander des informations aux entités et aux personnes qu’elle réglemente par le biais des diverses lois qu’elle administre. L’ARSF peut demander de l’information aux entités et aux personnes réglementées, soit de façon ciblée, soit à l’échelle du secteur, afin de vérifier qu’elle reçoit en temps opportun de l’information sur les incidents importants liés aux TI.

Voir l’annexe 1 pour des exemples d’incidents de risques importants liés aux TI.

Activation du protocole de l’ARSF pour les incidents découlant de risques liés aux TI

Décision de l’ARSF d’activer son protocole pour les incidents découlant de risques liés aux TI

Lorsque l’ARSF prend connaissance d’un incident découlant de risques liés aux TI, soit par un avis direct de l’entité ou de la personne réglementée, soit par d’autres canaux (par exemple, plainte, rapport des médias, etc.), elle déterminera s’il faut activer le **protocole de l’ARSF pour**

les incidents découlant de risques liés aux TI. Dans certains cas, l'ARSF peut déterminer que l'activation du *protocole pour les incidents découlant de risques liés aux TI* n'est pas justifiée.

Le protocole décrit l'engagement attendu de l'ARSF avec l'entité ou la personne réglementée pour surveiller les actions prises dans l'enquête et l'intervention suite à l'incident. L'engagement est continu, jusqu'à ce que l'ARSF ait :

- une compréhension et une connaissance complètes de l'étendue de l'incident, y compris si des données confidentielles ont été violées et quelles informations ont été consultées;
- la confirmation que toute information corrompue a été restaurée et/ou que l'incident a été atténué ou contenu;
- la confirmation que tous les systèmes sont de nouveau en ligne et entièrement fonctionnels;
- la confirmation que toutes les parties prenantes concernées, y compris les clients et les autorités compétentes en matière de protection de la vie privée, ont été informées et que des mesures raisonnables ont été prises par l'entité réglementée ou le particulier pour limiter le préjudice subi par les consommateurs;
- une compréhension et une connaissance complètes des mesures de protection qui ont été mises en place pour garantir que l'entité ou le particulier réglementé est protégé contre des incidents similaires.

L'ARSF préservera la confidentialité des incidents signalés dans la mesure où la loi le permet.

Protocole pour les incidents découlant de risques liés aux TI - Protocole en trois phases

La réponse aux incidents se déroule généralement en phases similaires au schéma ci-dessous :

Phase 1 : Recevoir un avis de l'entité ou de la personne réglementée détaillant les informations immédiates concernant l'incident, y compris ce qui a été fait pour assurer le rétablissement et l'intervention, et quelles actions supplémentaires sont prévues.

Phase 2 : Une fois que l'ARSF a déterminé que le protocole de risques liés aux TI doit être activé, elle établit le contact avec l'entité ou la personne réglementée. L'entité ou la personne réglementée fournit à l'agence des mises à jour périodiques sur l'impact de l'incident sur les opérations, les services et les consommateurs. Les informations demandées par l'ARSF dépendront de la nature de l'incident.

Phase 3 : L'ARSF reçoit le plan de l'entité ou de la personne réglementée pour prévenir un incident similaire à l'avenir.

Le niveau et la fréquence d'intervention de l'ARSF auprès d'une entité ou d'une personne réglementée, et sa décision d'activer le protocole pour les incidents découlant de risques liés aux TI, reflètent la nature de l'incident de risque informatique, ainsi que la taille et la nature de l'entité ou de la personne réglementée.

Spécifique au secteur

Cette section contient des lignes directrices applicables aux entités ou aux personnes réglementées dans des secteurs spécifiques.

- Organisme d'accréditation
- Caisses populaires et credit unions (caisses)
- Courtiers en prêts hypothécaires, agents en hypothèques, administrateurs d'hypothèques et maisons de courtage d'hypothèques
- Approche pour les sociétés d'assurances, les agents d'assurances, les agences d'assurances, les experts en sinistres et les entreprises de redressement constituées ailleurs qu'en Ontario
- Sociétés d'assurances et d'assurances réciproques constituées en Ontario
- Administrateurs de régimes de retraite

Pour les entités et les personnes réglementées qui ne sont pas incluses dans cette section, veuillez consulter à la section Tous les secteurs qui s'applique à tous les secteurs réglementés par l'ARSF.

Organismes d'accréditation pour les planificateurs et conseillers financiers

Approche

En vertu des lignes directrices « Protection du titre des professionnels des finances - Administration des demandes » de l'ARSF[9], les organismes d'accréditation (« OA ») des planificateurs et des conseillers financiers doivent démontrer qu'ils respectent certaines normes prescrites. Les OA agréés doivent démontrer qu'ils ont :

- Des mesures de sûreté et de sécurité, qui garantissent la protection des systèmes informatiques et des données électroniques.

- Des processus et des procédures en place pour atténuer toute perturbation des opérations.

L'ARSF examine également si les organismes d'accréditation ont :

- Une stratégie informatique qui comprend des mesures de protection du matériel, des logiciels et des données, y compris :

    - des contrôles informatiques solides en place pour protéger ses données électroniques;

    - des politiques garantissant la mise en place de mots de passe forts pour les appareils électroniques, l'utilisation de logiciels antivirus et de pare-feu la sauvegarde des données électroniques et l'utilisation du stockage hors site/en nuage.

- un plan de continuité des activités pour minimiser toute interruption de service;

- la sauvegarde des données électroniques des TI;

- le stockage hors site/dans le nuage.

Les risques liés aux technologies de l'information font partie des principes et de l'approche basée sur les risques de l'ARSF pour la supervision des OA, comme indiqué dans le guide de l'ARSF intitulé « Protection du titre des professionnels des finances - Cadre de supervision »[10].

L'ARSF peut mener des examens thématiques basés sur les risques liés aux TI, et cette orientation sera utilisée pour évaluer si les OA ont rempli les conditions prescrites décrites dans les lignes directrices « Administration des demandes ».

La *Loi de 2019 sur la protection du titre des professionnels des finances* (LPTPF) et la règle no 2020-001 de l'ARSF - Protection du titre des professionnels des finances (« règle de PTPF ») permettent à l'ARSF de révoquer l'agrément d'un OA s'il ne respecte pas la LPTPF, la règle de PTPF ou les conditions de son agrément.

Caisses populaires et credit unions (caisses) – Interprétation et approche

Interprétation

Caisses populaires et credit unions (caisses) - Interprétation par l'ARSF des exigences en matière de gestion des risques liés aux TI en vertu de la règle de *Pratiques commerciales et financières saines (« règle de PCFS »)*

Les caisses doivent atteindre les résultats souhaités des pratiques pour une gestion efficace des risques liés aux technologies de l'information afin de satisfaire aux exigences de la règle *Pratiques commerciales et financières saines*. Cela comprend un avis à l'ARSF de tout incident important découlant des risques liés aux technologies de l'information dans les 48 heures.

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

Le conseil est chargé d'établir les stratégies et les structures de gouvernance nécessaires en matière de TI, de superviser et d'approuver le programme de gestion des risques liés aux TI de la caisse et de veiller à ce que les ressources soient suffisantes pour mener à bien ses activités de gestion des risques liés aux TI.[11] Le conseil d'administration est tenu d'examiner et d'approuver périodiquement un cadre de gestion des risques liés aux TI (CGRI) et des cadres de soutien (p. ex., cadre de gestion des risques d'un tiers) ou une structure similaire, selon la taille, la complexité et le profil de risque de la caisse, qui comprendra son appétit, sa tolérance et ses limites en matière de risques liés aux TI.[12]

La haute direction est responsable de ce qui suit :

- élaborer, mettre à jour et mettre en œuvre les politiques, les processus et les systèmes liés aux TI utilisés pour gérer efficacement les risques liés aux TI à tous les niveaux décisionnels et de veiller à ce qu'ils soient compris par le personnel, les tiers et les autres parties prenantes concernées.[13]

- établir et régir les rôles et responsabilités respectifs nécessaires pour identifier, évaluer, gérer et superviser efficacement les risques liés aux TI[14]

- mesurer le profil de risque de la caisse en matière de TI par rapport à l'appétit et à la tolérance pour le risque approuvés par le conseil et le présenter au conseil pour confirmer la conformité.[15]

La gestion des risques liés aux TI s'appuie sur des structures de gouvernance qui définissent clairement les obligations et les responsabilités, les voies hiérarchiques et les pouvoirs décisionnels. Les caisses doivent établir une structure organisationnelle dans laquelle les activités de gestion des risques liés aux TI sont menées par la Gestion opérationnelle des TI[16] (première ligne de défense), sont examinées et remises en question par la Gestion des risques liés aux TI[17] (deuxième ligne de défense), et une assurance indépendante est ensuite fournie par la Vérification interne[18] (troisième ligne de défense), facilitant ainsi une gouvernance, une surveillance et une gestion efficaces des risques en matière de TI.

La non-conformité à ces lignes directrices pourrait entraîner des mesures de surveillance ou d'application. Il peut s'agir d'exiger que la caisse prenne des mesures correctives et produise des rapports plus détaillés, d'émettre une ordonnance de conformité ou de placer la caisse sous

surveillance ou sous administration conformément à la *Loi de 2020 sur les caisses populaires et les credit unions* (LCPCU 2020)[19].

Le document « Lignes directrices sur les risques et la résilience opérationnels » de l'ARSF comprend une interprétation de la *règle SBFP* et des conseils relatifs aux risques liés aux TI. Ces lignes directrices et le document « Lignes directrices sur les risques et la résilience opérationnels » doivent être considérés ensemble lorsque les caisses élaborent leurs politiques, leurs processus et leurs procédures en matière de risques liés aux TI.

Approche

L'ARSF adopte une approche basée sur les risques pour la supervision des risques liés aux TI. Les activités de supervision de l'ARSF prennent en compte tous les résultats des pratiques pour une gestion efficace des risques liés aux technologies de l'information dans ses évaluations et elle exerce un jugement de supervision approprié lors de l'évaluation des politiques, des processus et des pratiques établis par l'entité réglementée pour gérer efficacement les risques liés aux TI.

Les lignes directrices du « Cadre de surveillance axée sur le risque » (« CSAR »)[20] de l'ASFR définissent ses processus et ses pratiques en matière de supervision des caisses et d'évaluation de leurs risques. Son objectif principal est de déterminer les impacts des événements actuels et futurs potentiels, tant internes qu'externes, sur les profils de risque des caisses.

L'ARSF utilise le CSAR pour évaluer le risque et identifier les pratiques commerciales imprudentes ou dangereuses et/ou les comportements répréhensibles qui peuvent avoir un impact sur les consommateurs, afin d'être en mesure d'intervenir en temps utile. Les risques liés aux TI sont un facteur dont l'ARSF tient compte dans l'élaboration de l'évaluation globale du risque des caisses en vertu du CSAR. Les caisses seront évaluées conformément au CSAR afin de déterminer leur cote globale de risque (CGR).

La gestion des risques liés aux TI est également un facteur à prendre en compte dans l'évaluation du risque opérationnel et de la résilience d'une caisse, comme décrit dans le document « Lignes directrices sur les risques et la résilience opérationnels » (lien lorsqu'il sera publié).

L'ARSF a la capacité de faire des enquêtes, d'effectuer des évaluations de surveillance et de recueillir des informations auprès des caisses concernant les risques liés aux TI. L'ARSF tiendra compte du fait que les caisses ont atteint les résultats souhaités décrits dans ce guide, y compris un avis à l'ARSF dans les 48 heures en cas d'incident important découlant des risques liés aux TI, lorsqu'elle évaluera si une entité a satisfait aux exigences décrites dans la section Interprétation.

L'ARSF doit se référer aux critères articulés dans cette approche lorsqu'elle évaluera l'application des pratiques pour une gestion efficace des risques liés aux technologies de l'information et leurs résultats souhaités. Les critères servent de guide aux évaluations prudentielles de l'ARSF et ne sont pas destinés à constituer une liste exhaustive ou prescriptive. L'ARSF doit tenir compte de la taille, de la complexité et du profil de risque de la caisse dans son évaluation.

Critères utilisés pour évaluer la pratique 1 : Gouvernance

- Le conseil d'administration a approuvé l'approche documentée de l'entité réglementée en matière de gestion des risques liés aux TI (par exemple, cadres, politiques, appétit pour le risque, tolérances et limites).

- La direction générale a veillé à ce qu'une stratégie informatique approuvée par le conseil d'administration soit documentée et mise en œuvre, et à ce qu'elle s'aligne sur la stratégie globale de l'entité réglementée et démontre que les investissements et l'affectation des ressources sont appropriés pour protéger les actifs informatiques de la caisse.

- Le conseil a veillé à ce qu'une structure organisationnelle appropriée soit établie et à ce que des ressources (humaines et financières) soient disponibles pour gérer efficacement les risques liés aux TI.

- La haute direction a veillé à ce qu'une formation adéquate soit dispensée afin de sensibiliser l'ensemble de l'entreprise aux risques liés aux technologies de l'information.

- Le conseil d'administration reçoit des informations appropriées et opportunes (p. ex., rapports de vérification, rapports trimestriels, rapports d'incidents) afin de superviser et d'évaluer efficacement la gestion des risques liés aux TI par la caisse.

Critères utilisés pour évaluer la pratique 2 : Gestion des risques

- La haute direction doit assurer l'établissement d'une fonction ou d'une personne indépendante chargée de surveiller les risques afin de s'assurer que les activités de la caisse soient conformes à l'approche approuvée par le conseil en matière de gestion des risques liés aux TI.

- La haute direction, qui possède l'expertise et les connaissances appropriées en matière de risques des TI, est responsable des activités informatiques de l'entité réglementée et de la mise en œuvre de la méthode de gestion des risques des TI approuvée par le conseil.

- La ou les personnes responsables de la surveillance des risques au sein de la caisse ont élaboré une approche de la gestion des risques liés aux TI à l'échelle de l'entreprise, qui comprend les éléments suivants :

    - l'appétit pour le risque informatique, les tolérances et les limites approuvées par le conseil d'administration de la caisse.

    - des politiques et des procédures qui permettent à l'entité réglementée de :

        - Identifier et mesurer - prendre des mesures de manière récurrente pour comprendre, analyser et évaluer efficacement les vulnérabilités aux risques liés aux TI.

        - Atténuer - déterminer les étapes appropriées pour se protéger contre les menaces identifiées, établir des contrôles (préventifs et de détection) et des mesures de sécurité, et transférer le risque lorsque cela est approprié (par exemple, par l'entremise d'une assurance).

        - Surveiller - élaborer et mettre en œuvre des processus pour surveiller régulièrement les menaces et fournir des rapports adéquats au conseil d'administration ou à la haute direction.

        - Réagir - élaborer des processus permettant aux entités de réagir de manière efficace et rapide en cas d'incident.

- Un processus permettant d'examiner et de répondre aux recommandations des vérificateurs ou d'autres examinateurs externes.

- Un processus permettant de rendre compte au conseil, de manière régulière et cohérente, du rendement de la caisse par rapport à son appétit pour les risques liés aux TI.

- La caisse a établi des politiques et des procédures de gestion des risques liés aux TI adaptées à la taille, à la complexité et au profil de risque de l'entité, notamment en ce qui concerne les aspects suivants :

    - gestion de l'information et des dossiers, le stockage et la maintenance des données;

    - classification et accès aux données;

    - gestion des risques liés aux tiers;

    - exigences spécifiques à l'infonuagique;

    - cybersécurité;

    - gestion des projets et des changements.

Critères utilisés pour évaluer la pratique 3 : Gestion des données

La caisse :

- suit des politiques et des procédures pour identifier et classer (selon le type d'information) les données de la caisse.

- a des politiques, des procédures et des contrôles pour garantir un accès autorisé aux sources de données et à l'environnement (par exemple, authentification multifactorielle, séparation des tâches et principes du moindre privilège).

- dispose de procédures de surveillance des incidents liés à la gestion des risques liés aux données (par exemple, des analyses de découverte).

- effectue des tests réguliers des contrôles de gestion des données et élabore un processus pour remédier aux déficiences et mettre en œuvre les recommandations.

- dispose de processus et de procédures de gouvernance des données adéquats et solides pour garantir que :

    - les données soient adaptées à leur usage;

    - les données sont collectées et stockées de manière transparente;

    - la qualité et l'intégrité des données sont maintenues;

    - la propriété des données est clairement définie.

- dispose d'un processus pour assurer la conformité aux exigences législatives pertinentes en plus des statuts du secteur (par exemple, la LPRPDE) et pour signaler les violations importantes de la conformité à la haute direction, au conseil d'administration, à l'ARSF et aux autres organismes de réglementation applicables.

Critères utilisés pour évaluer la pratique 4 : Externalisation

La caissse :

- possède des critères d'évaluation et de sélection des fournisseurs ainsi qu'un processus d'évaluation de la performance continue des contrôles informatiques des fournisseurs;

- effectue une évaluation des risques liés aux tiers avant de conclure un contrat ou de passer un marché;

- effectue une évaluation des risques liés aux tiers avant de conclure un contrat ou de passer un marché;

- inclut les droits d'audit et d'accès aux informations dans ses contrats avec les tiers;

- dispose d'un processus ou d'un mécanisme (par exemple, une attestation) pour garantir la responsabilité des fournisseurs et leur conformité aux politiques et aux procédures de gestion des risques liés aux TI de l'entité réglementée;

- dispose d'un processus de classification des fournisseurs critiques dans le cadre du plan plus large de continuité et de résilience technologiques de la caisse (voir la pratique 6);

- dispose d'exigences spécifiques à l'infonuagique qui s'alignent sur la stratégie informatique générale et l'appétit pour le risque de la caisse;

- évalue le risque d'incidents et de fuites de données en cas d'externalisation vers des fournisseurs de services d'informatique en nuage;

- décèle les incidents en lien avec ses prestataires tiers, effectue une enquête sur ceux-ci, en fait le suivi et en assure la correction.

- établit un plan de sortie dans le cas où le tiers subit un événement négatif majeur (par exemple, une faillite, une panne catastrophique ou la perte de personnes clés).

Critères utilisés pour évaluer la pratique 5 : Préparation aux incidents

La caisse :

- dispose d'un processus pour détecter, consigner, gérer, résoudre, récupérer, surveiller et signaler les incidents informatiques;

- définit et documente les rôles et les responsabilités des parties internes et externes concernées afin de soutenir une réponse efficace aux incidents;

- effectue des tests périodiques des processus de gestion des incidents avec des tiers;

- effectue des examens indépendants périodiques du processus de gestion des incidents et des contrôles pour garantir leur efficacité;

- priorise les incidents en fonction de leur impact sur l'entité de manière générale et sur les services informatiques en particulier;

- dispose d'indicateurs d'alerte précoce et identifie les zones de vulnérabilité informatique et les déclencheurs de perturbation du système;

- effectue des évaluations périodiques de la vulnérabilité de ses actifs informatiques à l'échelle du réseau, des systèmes et des applications; les vulnérabilités et les menaces sont évaluées et classées en fonction de leur gravité;

- dispose d'un processus de recours interne pour les incidents au niveau d'autorité approprié (par exemple, la direction générale ou le conseil d'administration) et développe des actions de communication interne et externe, le cas échéant;

- effectue des tests et des exercices périodiques (par exemple, des exercices sur table) pour évaluer les plans et les capacités de réponse aux incidents, y compris avec les PPT;

- dispose de processus pour s'assurer que les problèmes soient résolus en temps opportun et que des examens post-incident et des analyses des causes profondes soient effectués;

- identifie les menaces actuelles ou émergentes de manière proactive en utilisant des évaluations pour cerner les menaces et les risques liés aux TI;

- adopte des normes industrielles reconnues en matière de préparation aux incidents;

- a développé et mis en œuvre une politique sur les risques liés aux TI qui intègre une approche de détection, d'enregistrement, de gestion, de résolution, de rétablissement, de surveillance et de rapport;

- rend régulièrement et systématiquement compte à la direction et au conseil d'administration des incidents importants découlant des risques liés aux TI.

Critères utilisés pour évaluer la pratique 6 : Continuité et résilience

La caisse :

- tient à jour un inventaire de tous les actifs informatiques qui soutiennent les processus ou les fonctions commerciales;

- attribue une classification (p. ex., profil de risque, criticité pour l'entité) aux actifs TI et gère et surveille les actifs tout au long de leur cycle de vie;

- surveille en permanence l'actualité des logiciels et du matériel utilisés pour soutenir les processus opérationnels;

- atténue et gère de manière proactive les risques découlant de biens non corrigés, obsolètes ou non pris en charge, et remplace ou mettre à niveau les biens avant que la maintenance n'expire ou que la fin de vie ne soit atteinte;

- a conclut des accords de niveau de service internes et avec des fournisseurs tiers;

- dispose de politiques et de procédures de gestion de projet et de gestion du changement, qui garantissent l'achèvement en temps voulu des projets informatiques et limitent les perturbations de la prestation de services;

- dispose d'un plan de reprise après sinistre (« PRS »), qui s'aligne sur le plan de continuité des activités (« PCA ») plus large de l'entité, et qui explique comment l'entité continuera à fournir des services si les services essentiels sont interrompus :

    - établit les obligations et les responsabilités dans le cadre du PRS pour la disponibilité et la récupération des services informatiques, y compris les actions de récupération;

    - teste les scénarios de reprise après sinistre afin de promouvoir l'apprentissage, l'amélioration continue et la résilience des TI;

    - examine les pratiques du PRS d'un tiers critique et les résultats des tests.

Critères utilisés pour évaluer la pratique 7 : Avis en cas d'incidents importants découlant des risques liés aux TI

La caisse :

- a un processus pour évaluer ce qui constitue un risque important lié aux TI;

- avise l'ARSF tous les risques importants liés aux TI.

- apprend et améliore ses efforts d'atténuation des risques après un incident de risque important lié aux TI.

Courtiers en prêts hypothécaires, agents en hypothèques, administrateurs d'hypothèques et maisons de courtage d'hypothèques

Information/Approche

Les principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH)[21] pour le secteur du courtage d'hypothèques décrivent les résultats que les entités et les personnes réglementées doivent atteindre pour assurer la « préparation à la cybersécurité ». L'ARSF a publié des lignes directrices d'information[22] qui adoptent les principes de préparation à la cybersécurité du CCARCH dans le cadre réglementaire de l'ARSF. Elle a également établi le « protocole de surveillance des pratiques de l'industrie en matière de cybersécurité » que les maisons de courtage et les administrateurs d'hypothèques doivent suivre en cas d'incident de cybersécurité.

En vertu du principe 8 du Code de conduite pour le secteur du courtage hypothécaire (Code de conduite) du CCARCH[23], « les personnes et les entités réglementées doivent protéger les renseignements de leurs clients. Elles ne doivent les utiliser et les divulguer qu'aux fins pour lesquelles le client a donné son consentement ou lorsque la loi l'y oblige. » L'ARSF a adopté ce code dans son cadre de surveillance du secteur du courtage en hypothèques.

Le « code de conduite » et les « principes de préparation à la cybersécurité » du CCARCH, ainsi que les lignes directrices correspondantes de l'ARSF qui les intègrent à son cadre réglementaire, sont conformes aux pratiques pour une gestion efficace des risques liés aux technologies de l'information et aux résultats souhaités de ces lignes directrices. L'application de ces lignes directrices doit correspondre aux lignes directrices du CCARCH et, en cas d'incohérence, ces lignes directrices obtiendront la préséance.

L'ARSF peut prendre des mesures d'exécution en cas de non-conformité à ces lignes directrices qui correspondent aux exigences de la *Loi de 2006 sur les maisons de courtage d'hypothèques, les prêteurs hypothécaires et les administrateurs d'hypothèques* et de ses règlements. Les

exigences existantes qui s'appliquent aux pratiques pour une gestion efficace des risques liés aux technologies de l'information et aux résultats souhaités de ces lignes directrices comprennent l'obligation d'établir des politiques et des procédures pour les administrateurs d'hypothèques[24] et les maisons de courtage d'hypothèques[25], et l'obligation de prendre des précautions pour sécuriser les dossiers des administrateurs[26] et des maisons de courtage[27].

Ces lignes directrices s'appliquent aux courtiers, aux agents, aux maisons de courtage et aux administrateurs d'hypothèques. L'ARSF considère que les administrateurs d'hypothèques et les maisons de courtage d'hypothèques sont responsables en dernier ressort de veiller à ce que les risques liés aux TI soient gérés efficacement par leurs représentants et leur personnel titulaires d'un permis ou par toute fonction impartie à un tiers.

Le non-respect des pratiques pour une gestion efficace des risques liés aux technologies de l'information et de leurs résultats souhaités peut avoir une incidence sur l'aptitude à délivrer et à renouveler un permis.

Approche pour les sociétés d'assurances, les agents d'assurances, les agences d'assurances, les experts en sinistres et les entreprises de redressement constituées ailleurs qu'en Ontario

Approche

Cette section s'applique aux sociétés d'assurances constituées en vertu d'une loi fédérale et aux sociétés d'assurances constituées en vertu d'une loi d'une autre province, qui sont titulaires d'un permis en Ontario. Elle s'applique également aux agents d'assurances, aux experts en sinistres, aux cabinets d'experts en sinistres et aux agences d'assurances.

Voir cette section des lignes directrices pour les sociétés d'assurances et d'assurances réciproques constituées en Ontario.

Lignes directrices existantes d'autres organismes de réglementation

Les sociétés d'assurances constituées à l'extérieur de l'Ontario peuvent être assujetties à des lignes directrices similaires d'un autre organisme de réglementation, comme la ligne directrice en matière de gestion des risques liés aux technologies et du cyberrisque du Bureau du surintendant des institutions financières (« BSIF »)[28]. Les pratiques pour une gestion efficace

des risques liés aux technologies de l'information et les résultats souhaités de cette ligne directrice sont alignés sur la ligne directrice du BSIF et sur les lignes directrices similaires des autres organismes de réglementation provinciaux[29].

Harmonisation avec d'autres lignes directrices existantes

Les pratiques pour une gestion efficace des risques liés aux technologies de l'information et les résultats souhaités sont conformes aux lignes directrices publiées par l'ARSF, le Conseil canadien des responsables de la réglementation d'assurance (« CCRRA ») et les Organismes canadiens de réglementation en assurance (« OCRA »). Les présentes lignes directrices offrent plus d'informations sur les lignes directrices émises par le CCRRA et les OCRA et ne doivent pas être interprétées comme limitant ces lignes directrices. En cas d'incohérence entre les lignes directrices du CCRRA et des OCRA, les entités et les personnes réglementées doivent suivre les lignes directrices de l'ARSF.

Lignes directrices	Attentes pertinentes des lignes directrices
CCRRA et OCRA - Conduite des activités d'assurance et traitement équitable des clients (« Directive de TEC »)	Les assureurs et les intermédiaires ont mis en place des mesures de protection et ont adopté des politiques et des procédures relatives **à la protection des informations personnelles** qui « assurent la conformité avec la législation relative à la protection de la vie privée et reflètent les meilleures pratiques dans ce domaine ». L'ARSF a adopté ces lignes directrices[30] pour superviser le traitement équitable des clients.
Principes de conduite à l'intention des intermédiaires en assurance des OCRA[31] (« Principes des OCRA »)	Pour les intermédiaires d'assurance, comme les agents, les experts en sinistres et les agences d'assurances d'entreprise, la ligne directrice contient le principe de « protection des informations personnelles et confidentielles ».

Lignes directrices	Attentes pertinentes des lignes directrices
	L'ARSF a publié des lignes directrices de consultation[32] pour l'adoption des Principes des OCRA dans son cadre réglementaire qui décrit son approche en matière de surveillance et d'application.
Lignes directrices pour l'information de l'ARSF - Cadre de gestion du risque opérationnel (GRO) lors de la tarification et de la souscription de l'assurance automobile (« ligne directrice de GRO »)[33]	Applicable uniquement aux sociétés d'assurances qui offrent de l'assurance automobile. Ces lignes directrices, y compris les pratiques pour une gestion efficace des risques liés aux technologies de l'information et leurs résultats souhaités, sont cohérentes et ont pour but de développer les lignes directrices de GRO de l'ARSF. Les lignes directrices de GRO décrivent des pratiques fondamentales et saines pour l'application des trois lignes de défense afin d'aider les assureurs à respecter les obligations existantes en matière de protection des renseignements personnels (pratiques 1 et 2), pour la mise en place d'une gouvernance des données (pratique 3) ; et pour que les assureurs garantissent la surveillance de l'utilisation des données ou des services de tiers et en soient responsables (pratique 4).

Approche de surveillance

L'ARSF peut effectuer des examens thématiques des entités et des personnes titulaires d'un permis d'assurance de l'Ontario sur la gestion des risques liés aux TI en se fondant sur les présentes lignes directrices. Dans la mesure du possible, l'ARSF coordonnera les examens avec les autres organismes de réglementation du CCRRA.

L'ARSF peut prendre des mesures de surveillance ou d'exécution lorsque la non-conformité aux lignes directrices correspond à des exigences existantes en vertu de la *Loi sur les assurances* et de ses règlements. Ces mesures comprennent des solutions allant de l'éducation et de la remédiation à la discipline et à l'intervention réglementaires. La non-conformité à ces lignes directrices peut avoir une incidence sur l'aptitude d'un titulaire de permis individuel au moment du renouvellement.

Bien que cette ligne directrice s'applique également aux agents d'assurances, aux experts en assurances, aux experts en sinistres, aux cabinets d'experts en sinistres et aux agences d'assurances, l'ARSF considère que les assureurs sont en fin de compte responsables de veiller à ce que les risques liés aux TI soient gérés efficacement par l'intermédiaire de tous leurs canaux de distribution et de leurs fonctions externalisées.

Sociétés d'assurances et d'assurances réciproques constituées en Ontario – Interprétation et approche

Interprétation

Sociétés d'assurances et d'assurances réciproques constituées en Ontario - Interprétation de la *Loi sur les assurances* par l'ARSF en ce qui concerne les risques liés aux TI

Cette section décrit l'interprétation de la *Loi sur les assurances* selon l'ARSF en ce qui a trait aux principes de gestion efficace des risques liés aux technologies de l'information.

Le paragraphe 437 (3) de la *Loi sur les assurances* exige que chaque assureur « établisse et enregistre les procédures à suivre pour le traitement et la protection de ses placements et veille, en tout temps, au respect strict de ces procédures ».

Les sociétés d'assurances et d'assurances réciproques constituées en Ontario doivent atteindre les résultats des pratiques pour une gestion efficace des risques liés aux technologies de l'information afin de se conformer au paragraphe 437 (3) de la *Loi sur les assurances*. Cela comprend un avis à l'ARSF de tout incident important découlant des risques liés aux technologies de l'information dans les 48 heures.

L'ARSF surveille la conformité au paragraphe 437(3) de la *Loi sur les assurances* en ce qui concerne la gestion des risques liés aux TI. Les sociétés d'assurances et d'assurances réciproques constituées en Ontario qui ne démontrent pas qu'elles se conforment à ces lignes directrices en ce qui concerne leurs procédures de traitement et de protection des investissements peuvent faire l'objet de mesures de surveillance ou d'application.[34]

Approche

L'ARSF adopte une approche basée sur les risques pour la supervision des risques liés aux TI. Les activités de supervision de l'ARSF prennent en compte tous les résultats des pratiques pour une gestion efficace des risques liés aux technologies de l'information dans ses évaluations et elle exerce un jugement de supervision approprié lors de l'évaluation des politiques, des processus et des pratiques établis par l'entité réglementée pour gérer efficacement les risques liés aux TI.

Les lignes directrices du « Cadre de surveillance axée sur le risque pour les sociétés d'assurances et d'assurances réciproques constituées en Ontario » (« CSAR-A ») de l'ARSF (lien final nécessaire lors de la publication) définit les processus et les pratiques de l'ARSF pour la supervision des sociétés d'assurances et d'assurances réciproques constituées en Ontario et l'évaluation de leur risque. Son objectif principal est de déterminer les impacts des événements actuels et futurs potentiels, tant internes qu'externes, sur les profils de risque des sociétés d'assurances et d'assurances réciproques constituées en Ontario.[35]

L'ARSF utilise le CSAR-A pour évaluer le risque et identifier les pratiques commerciales imprudentes ou dangereuses et/ou les comportements répréhensibles qui peuvent avoir un impact sur les consommateurs, afin d'être en mesure d'intervenir en temps utile. Les risques liés aux TI sont un facteur dont l'ARSF tient compte dans l'élaboration de l'évaluation globale du risque des caisses en vertu du CSAR-A. Les entités réglementées seront évaluées conformément au CSAR-A afin de déterminer leur cote globale du risque (CGR).

L'ARSF a la capacité de faire des enquêtes, d'effectuer des évaluations de surveillance et de recueillir des informations auprès des sociétés d'assurances et d'assurances réciproques constituées en Ontario concernant les risques liés aux TI. L'ARSF tiendra compte du fait que les sociétés d'assurances et d'assurances réciproques constituées en Ontario ont atteint les résultats souhaités décrits dans ce guide, y compris un avis à l'ARSF dans les 48 heures en cas

d'incident important découlant des risques liés aux TI, lorsqu'elle évaluera si une entité a satisfait aux exigences décrites dans la section Interprétation.

L'ARSF doit se référer aux critères articulés dans cette approche lorsqu'elle évaluera l'application des pratiques pour une gestion efficace des risques liés aux technologies de l'information et leurs résultats souhaités. Les critères servent de guide aux évaluations prudentielles de l'ARSF et ne sont pas destinés à constituer une liste exhaustive ou prescriptive. L'ARSF doit tenir compte de la taille, de la complexité et du profil de risque de l'entité réglementée dans son évaluation.

Critères utilisés pour évaluer la pratique 1 : Gouvernance

- Le conseil d'administration a approuvé l'approche documentée de l'entité réglementée en matière de gestion des risques liés aux TI (par exemple, cadres, politiques, appétit pour le risque, tolérances et limites).

- La direction générale a veillé à ce qu'une stratégie informatique approuvée par le conseil d'administration soit documentée et mise en œuvre, et à ce qu'elle s'aligne sur la stratégie globale de l'entité réglementée et démontre que les investissements et l'affectation des ressources sont appropriés pour protéger les actifs informatiques de l'entité réglementée.

- Le conseil a veillé à ce qu'une structure organisationnelle appropriée soit établie et à ce que des ressources (humaines et financières) soient disponibles pour gérer efficacement les risques liés aux TI.

- La haute direction a veillé à ce qu'une formation adéquate soit dispensée afin de sensibiliser l'ensemble de l'entreprise aux risques liés aux technologies de l'information.

- Le conseil d'administration reçoit des informations appropriées et opportunes (p. ex., rapports de vérification, rapports trimestriels, rapports d'incidents) afin de superviser et d'évaluer efficacement la gestion des risques liés aux TI par l'entité réglementée.

Critères utilisés pour évaluer la pratique 2 : Gestion des risques

- La haute direction doit garantir l'établissement d'une fonction ou d'une personne indépendante chargée de surveiller les risques afin de s'assurer que les activités de

l'entité réglementée soient conformes à l'approche approuvée par le conseil en matière de gestion des risques liés aux TI.

- La haute direction, qui possède l'expertise et les connaissances appropriées en matière de risques des TI, est responsable des activités informatiques de l'entité réglementée et de la mise en œuvre de la méthode de gestion des risques des TI approuvée par le conseil.

- La ou les personnes responsables de la surveillance des risques au sein de l'entité réglementée ont élaboré une approche de la gestion des risques liés aux TI à l'échelle de l'entreprise, qui comprend les éléments suivants :

    - l'appétit pour le risque informatique, les tolérances et les limites approuvées par le conseil d'administration de l'entité.

    - des politiques et des procédures qui permettent à l'entité réglementée de :

        - identifier et mesurer - prendre des mesures de manière récurrente pour comprendre, analyser et évaluer efficacement les vulnérabilités aux risques liés aux TI.

        - atténuer - déterminer les étapes appropriées pour se protéger contre les menaces identifiées, établir des contrôles (préventifs et de détection) et des mesures de sécurité, et transférer le risque lorsque cela est approprié (par exemple, par l'entremise d'une assurance).

        - surveiller - élaborer et mettre en œuvre des processus pour surveiller régulièrement les menaces et fournir des rapports adéquats au conseil d'administration ou à la haute direction.

        - réagir - élaborer des processus permettant aux entités de réagir de manière efficace et rapide en cas d'incident.

    - Un processus permettant d'examiner et de répondre aux recommandations des vérificateurs ou d'autres examinateurs externes.

- Un processus permettant de rendre compte au conseil, de manière régulière et cohérente, du rendement de l'entité réglementée par rapport à son appétit pour les risques liés aux TI.

- L'entité réglementée a établi des politiques et des procédures de gestion des risques liés aux TI adaptées à la taille, à la complexité et au profil de risque de l'entité, notamment en ce qui concerne les aspects suivants :

    - gestion de l'information et des dossiers, le stockage et la maintenance des données;

    - classification et accès aux données;

    - gestion des risques liés aux tiers;

    - exigences spécifiques à l'infonuagique;

    - cybersécurité;

    - gestion des projets et des changements.

Critères utilisés pour évaluer la pratique 3 : Gestion des données

L'entité réglementée :

- suit des politiques et des procédures pour identifier et classer (selon le type d'information) les données de l'entité réglementée.

- a des politiques, des procédures et des contrôles pour garantir un accès autorisé aux sources de données et à l'environnement (par exemple, authentification multifactorielle, séparation des tâches et principes du moindre privilège).

- dispose de procédures de surveillance des incidents liés à la gestion des risques liés aux données (par exemple, des analyses de découverte).

- effectue des tests réguliers des contrôles de gestion des données et élabore un processus pour remédier aux déficiences et mettre en œuvre les recommandations.

- dispose de processus et de procédures de gouvernance des données adéquats et solides pour garantir que :

    - les données soient adaptées à leur usage;

    - les données sont collectées et stockées de manière transparente;

    - la qualité et l'intégrité des données sont maintenues;

    - la propriété des données est clairement définie.

- dispose d'un processus pour assurer la conformité aux exigences législatives pertinentes en plus des statuts du secteur (par exemple, la LPRPDE) et pour signaler les violations importantes de la conformité à la haute direction, au conseil d'administration, à l'ARSF et aux autres organismes de réglementation applicables.

Critères utilisés pour évaluer la pratique 4 : Externalisation

L'entité réglementée :

- possède des critères d'évaluation et de sélection des fournisseurs ainsi qu'un processus d'évaluation de la performance continue des contrôles informatiques des fournisseurs;

- effectue une évaluation des risques liés aux tiers avant de conclure un contrat ou de passer un marché;

- effectue une évaluation des risques liés aux tiers avant de conclure un contrat ou de passer un marché;

- inclut les droits d'audit et d'accès aux informations dans ses contrats avec les tiers;

- dispose d'un processus ou d'un mécanisme (par exemple, une attestation) pour garantir la responsabilité des fournisseurs et leur conformité aux politiques et aux procédures de gestion des risques liés aux TI de l'entité réglementée;

- dispose d'un processus de classification des fournisseurs critiques dans le cadre du plan plus large de continuité et de résilience technologiques de l'entité réglementée (voir la pratique 6);

- dispose d'exigences spécifiques à l'infonuagique qui s'alignent sur la stratégie informatique générale et l'appétit pour le risque de l'entité réglementée;

- évalue le risque d'incidents et de fuites de données en cas d'externalisation vers des fournisseurs de services d'informatique en nuage;

- décèle les incidents en lien avec ses prestataires tiers, effectue une enquête sur ceux-ci, en fait le suivi et en assure la correction.

- établit un plan de sortie dans le cas où le tiers subit un événement négatif majeur (par exemple, une faillite, une panne catastrophique ou la perte de personnes clés).

Critères utilisés pour évaluer la pratique 5 : Préparation aux incidents

L'entité réglementée :

- dispose d'un processus pour détecter, consigner, gérer, résoudre, récupérer, surveiller et signaler les incidents informatiques;

- définit et documente les rôles et les responsabilités des parties internes et externes concernées afin de soutenir une réponse efficace aux incidents;

- effectue des tests périodiques des processus de gestion des incidents avec des tiers;

- effectue des examens indépendants périodiques du processus de gestion des incidents et des contrôles pour garantir leur efficacité;

- priorise les incidents en fonction de leur impact sur l'entité de manière générale et sur les services informatiques en particulier;

- dispose d'indicateurs d'alerte précoce et identifie les zones de vulnérabilité informatique et les déclencheurs de perturbation du système;

- effectue des évaluations périodiques de la vulnérabilité de ses actifs informatiques à l'échelle du réseau, des systèmes et des applications; les vulnérabilités et les menaces sont évaluées et classées en fonction de leur gravité;

- dispose d'un processus de recours hiérarchique interne pour les incidents au niveau d'autorité approprié (par exemple, la direction générale ou le conseil d'administration) et développe des actions de communication interne et externe, le cas échéant;

- effectue des tests et des exercices périodiques (par exemple, des exercices sur table) pour évaluer les plans et les capacités de réponse aux incidents, y compris avec les PPT;

- dispose de processus pour s'assurer que les problèmes soient résolus en temps opportun et que des examens post-incident et des analyses des causes profondes soient effectués;

- identifie les menaces actuelles ou émergentes de manière proactive en utilisant des évaluations pour cerner les menaces et les risques liés aux TI;

- adopte des normes industrielles reconnues en matière de préparation aux incidents;

- a développé et mis en œuvre une politique sur les risques liés aux TI qui intègre une approche de détection, d'enregistrement, de gestion, de résolution, de rétablissement, de surveillance et de rapport;

- rend régulièrement et systématiquement compte à la direction et au conseil d'administration des incidents importants découlant des risques liés aux TI.

Critères utilisés pour évaluer la pratique 6 : Continuité et résilience

L'entité réglementée :

- tient à jour un inventaire de tous les actifs informatiques qui soutiennent les processus ou les fonctions commerciales;
- attribue une classification (p. ex., profil de risque, criticité pour l'entité) aux actifs TI et gère et surveille les actifs tout au long de leur cycle de vie;
- surveille en permanence l'actualité des logiciels et du matériel utilisés pour soutenir les processus opérationnels;
- atténue et gère de manière proactive les risques découlant de biens non corrigés, obsolètes ou non pris en charge, et remplace ou met à niveau les biens avant que la maintenance n'expire ou que la fin de vie ne soit atteinte;
- a conclut des accords de niveau de service internes et avec des fournisseurs tiers;
- dispose de politiques et de procédures de gestion de projet et de gestion du changement, qui garantissent l'achèvement en temps voulu des projets informatiques et limitent les perturbations de la prestation de services;
- dispose d'un plan de reprise après sinistre (« PRS »), qui s'aligne sur le plan de continuité des activités (« PCA ») plus large de l'entité, et qui explique comment l'entité continuera à fournir des services si les services essentiels sont interrompus :
    - établit les obligations et les responsabilités dans le cadre du PRS pour la disponibilité et la récupération des services informatiques, y compris les actions de récupération;
    - teste les scénarios de reprise après sinistre afin de promouvoir l'apprentissage, l'amélioration continue et la résilience des TI;
    - examine les pratiques du PRS d'un tiers critique et les résultats des tests.

Critères utilisés pour évaluer la pratique 7 : Avis en cas d'incidents importants découlant des risques liés aux TI

L'entité réglementée :

- a un processus pour évaluer ce qui constitue un risque important lié aux TI;
- avise l'ARSF de tous les risques importants liés aux TI.
- apprend et améliore ses efforts d'atténuation des risques après un incident de risque important lié aux TI.

Administrateurs de régimes de retraite – Interprétation et approche

Interprétation

Interprétation de l'ARSF de la *Loi sur les régimes de retraite* en ce qui a trait aux TI

Les administrateurs de régimes de retraite sont assujettis à des devoirs fiduciaires en vertu de la common law et des normes minimales prescrites par la *LRR*.

La *LRR* exige que les administrateurs agissent avec le soin, la diligence et la compétence dont ferait preuve une personne d'une prudence normale dans la gestion des biens d'une autre personne. Ils doivent également utiliser toutes les connaissances et compétences pertinentes qu'ils possèdent ou, en raison de leur profession, de leurs affaires ou de leur vocation, qu'ils devraient posséder.[36] Afin de protéger adéquatement les droits et les prestations des participants au régime et d'administrer efficacement le régime de retraite, les administrateurs doivent tenir compte des risques liés aux TI et les atténuer.

Comme l'indique la *LRR*, les administrateurs doivent veiller à ce que tout renseignement personnel envoyé par voie électronique utilise un « système d'information sécurisé qui :

a. exige que le destinataire s'identifie avant d'accéder au document;

b. est conforme à toute autre condition, exigence, limitation ou interdiction prescrite, y compris toute exigence concernant les méthodes d'identification aux fins de la clause (a) ».[37]

Le fait de ne pas suivre les pratiques pour une gestion efficace des risques liés aux technologies de l'information pour protéger adéquatement leurs actifs, leurs opérations et les renseignements confidentiels des participants au régime entraînera probablement une violation des articles 22 (1) et 30.1 (2) de la *LRR*.

Approche

L'ARSF a publié un document de lignes directrices sur les rôles et les responsabilités des administrateurs de régimes de retraite qui décrit leurs rôles et leurs responsabilités en détail.[38] Les lignes directrices sur les rôles et les responsabilités des administrateurs de régimes de retraite indiquent que les administrateurs sont responsables de la mise en œuvre de processus visant à garantir que les risques liés au régime soient compris et traités. Dans le cadre de ce processus, les administrateurs devront démontrer qu'ils ont tenu compte des risques liés aux TI.

Les administrateurs devront démontrer qu'ils se sont familiarisés avec les pratiques acceptées dans l'industrie en matière de gouvernance des régimes de retraite, notamment les lignes directrices sur la gouvernance des régimes de retraite de l'Association canadienne des organismes de contrôle des régimes de retraite (ACOR)[39] et les autres lignes directrices de l'ACOR, selon le cas. En outre, les administrateurs devront démontrer qu'ils ont tenu compte des pratiques de gestion efficace des risques liés aux TI et des résultats souhaités selon les présentes lignes directrices pour étayer leur réflexion sur la gestion des risques au sein de leur régime, conformément à la taille et à la nature du régime et à tout autre facteur pertinent.

Date d'entrée en vigueur et examen futur

Ces lignes directrices entrent en vigueur en **juin 2023** (à conf.)et feront l'objet d'un examen au plus tard en **juin 2027** (à conf.)**.**

À propos de ces lignes directrices

Ce document est conforme au Cadre de lignes directrices de l'ARSF.

La ligne directrice en matière d'information décrit le point de vue de l'ARSF sur certains sujets sans créer de nouvelles obligations de conformité pour les personnes réglementées.

La ligne directrice en matière d'interprétation décrit la vision de l'ARSF concernant les exigences en vertu de son mandat législatif (lois, règlements et règles) de sorte qu'un cas de non-conformité puisse mener à l'application de la loi ou à une mesure de surveillance.

La ligne directrice en matière d'approche décrit les principes, les processus et les pratiques internes de l'ARSF en matière de surveillance et d'application du pouvoir discrétionnaire du directeur général. La ligne directrice en matière d'approche peut faire référence à des obligations de conformité, mais ne crée pas en soi une obligation de conformité.

Annexe 1 - Exemples d'incidents découlant de risques liés au TI

Tableau 2 - Exemples d'incidents importants découlant de risques liés au TI (liste non exhaustive)

Scénario	Exemple
Cyberattaque	• Les systèmes informatiques de l'entité ou de la personne réglementée ont été compromis par un pirate externe et des données confidentielles peuvent/peuvent avoir été exposées.
Violation interne des données	• Un employé ou un entrepreneur a volontairement ou involontairement provoqué l'exposition de données confidentielles.
Attaque par logiciel de rançon	• L'entité ou la personne réglementée est incapable d'accéder à un système interne à moins de payer une rançon à un extorqueur.

Scénario	Exemple
Défaillance des systèmes internes	• Une mise à jour informatique, une infrastructure numérique vieillissante ou un autre incident entraîne l'arrêt de l'un des systèmes clés de l'entité ou de la personne réglementée pendant une période prolongée; la capacité à fournir des services essentiels aux consommateurs peut/ne peut pas être affectée.
Incident de tiers	• Un incident découlant de risques liés aux TI se produit chez un tiers et l'entité ou la personne réglementée est informée que des données confidentielles ont été compromises ou qu'il peut y avoir une interruption prolongée des services.

Annexe 2 - Formulaire d'avis en cas de risques liés aux TI

Le formulaire d'avis en cas de risques liés aux TI de l'ARSF fournit aux entités et aux personnes réglementées des indications sur les informations utiles à fournir à l'ARSF en cas d'incident important découlant de risques liés aux TI.

Formulaire d'avis en cas de risques liés aux TI
Coordonnées
Nom de l'entité ou de la personne réglementée :
Type d'entité ou de personne réglementée (menu déroulant) :

Formulaire d’avis en cas de risques liés aux TI

Où l’incident s’est produit (menu déroulant, incluant l’entité/la personne réglementée, l’intermédiaire, le tiers, autre (veuillez préciser))

Nom du responsable de l’incident :

Poste du responsable de l’incident :

Adresse courriel du responsable de l’incident :

Numéro de téléphone du responsable de l’incident :

Nom/identifiant de l’incident :

Date et heure où l’incident s’est produit (calendrier) :

Date et heure de la découverte/détection de l’incident (calendrier) :

Date et heure de l’évaluation de l’incident comme étant important (calendrier) :

Informations sur l’incident

Type d’incident (liste de vérification, cochez tout ce qui s’applique) :

Exemples : cyberviolation, violation de données interne, attaque par logiciel de rançon, défaillance des systèmes internes, incident de tiers, autre (veuillez préciser).

L’incident a-t-il été résolu?

Si oui, indiquez quand l’incident a été résolu (calendrier).

Si non, veuillez estimer la date à laquelle l’incident devrait être résolu (calendrier)

L’incident a-t-il entraîné l’exposition de données confidentielles? Oui/Non/Incertain(e)

Formulaire d'avis en cas de risques liés aux TI

Si oui, veuillez fournir des détails sur la gravité de l'exposition des données confidentielles, y compris le nombre de personnes touchées, la nature des données confidentielles (indiquez si la gravité totale n'est pas connue pour le moment, auquel cas fournissez une meilleure estimation) :

Sur une échelle de 1 à 10, veuillez évaluer la gravité de l'incident (liste déroulante) :

L'incident a-t-il entraîné des perturbations opérationnelles importantes des systèmes et fonctions de l'entreprise? Oui/Non

Si oui, les opérations sont-elles revenues à la normale? Oui/Non	Si non ou si vous n'êtes pas sûr, veuillez indiquer quand le retour à la normale est prévu (calendrier).

Veuillez fournir tous les détails sur l'incident découlant de risques liés aux TI (y compris l'état actuel de l'incident, les impacts directs/indirects, le type de systèmes touchés, la méthode principale utilisée pour identifier l'incident, la procédure et les étapes utilisées (ou prévues) pour intervenir et se rétablir, les causes connues ou soupçonnées, le plan pour prévenir les incidents futurs).

Date d'entrée en vigueur : [à determiner]

---

[1] Les pratiques de gestion efficace des risques liés aux technologies de l'information ont été élaborées par l'ARSF en fonction des normes nationales et internationales.

[2] Le directeur général de l'ARSF et l'ARSF peuvent tous deux exercer un pouvoir réglementaire en vertu de la législation qu'ils administrent. Toutefois, aux fins du présent guide, on fera uniquement référence à l'ARSF, car le directeur général peut déléguer des pouvoirs au personnel de l'ARSF, comme le permet l'article 10(2.3) de la *Loi de*

2016 sur l'Autorité ontarienne de réglementation des services financiers.

[3] Les impacts négatifs pour les consommateurs peuvent inclure des pertes financières, une violation de la vie privée et/ou des informations confidentielles, et un manque de capacité à accéder aux services essentiels.

[4] Aux fins des présentes lignes directrices, le terme « consommateurs » comprendra également le public, les titulaires de polices, les membres de caisse, les bénéficiaires de régimes de retraite, les investisseurs et d'autres parties prenantes.

[5] *Loi de 2016 sur l'Autorité ontarienne de réglementation des services financiers* art. 3 (Loi de l'ARSF)

[6] *La Loi sur la protection des renseignements personnels et les documents électroniques*

[7] L'appétit pour le risque désigne le type et le montant du risque qu'une organisation est prête à accepter pour atteindre ses objectifs. Les entités et les personnes réglementées sont censées utiliser leur propre jugement pour déterminer si elles dépendent fortement des technologies.

[8] Cela englobe toutes les activités, tous les services et tous les arrangements entrepris par une partie externe à l'entreprise de l'entité ou de la personne réglementée. Cela comprend tous les services fournis par des tiers et les activités co-sourcées.

[9] Ligne directrice d'approche de l'ARSF : Protection du titre des professionnels des finances - Administration des demandes

[10] Ligne directrice d'interprétation/d'approche de l'ARSF : Protection du titre des professionnels des finances - Cadre de supervision

[11] Règle 2021-001 Pratiques commerciales et financières saines, art. 5(4) [RÈGLE SBFP].

[12] Ibid., art. 5(2), 5(3)(h).

[13] Ibid., art. 6(1)(i), art. 6(2)(iii).

[14] Ibid., art. 6(1)(i).

[15] Ibid., art. 5(3)(i)(g).

[16] Ibid., art. 15(2)(iv), s. 15(2)(v).

[17] Ibid., art. 10(9)(i)(a)-(b), s. 10(11) et s. 12(1)(i).

[18] Ibid., art. 11(2).

[19] *Loi de 2020 sur les caisses populaires et les credit unions* L.O. 2020, chap. 36, annexe 7, par. 230 et 233 (LCPCU 2020).

[20] Ligne directrice d'approche de l'ARSF : Cadre de surveillance axée sur le risque

[21] Principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH)

[22] Ligne directrice d'information de l'ARSF : Principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH) pour le secteur du courtage d'hypothèques

[23] Code de conduite pour le secteur du courtage hypothécaire du Conseil canadien des autorités de réglementation des courtiers hypothécaires (CCARCH)

[24] Règl. de l'Ont. 189/08, paragraphe 25 (1)

[25] Règl. de l'Ont. 188/08, paragraphe 40 (1)

[26] Règl. de l'Ont. 189/08, art. 30-31

[27] Règl. de l'Ont. 188/08, art. 47-48

[28] Ligne directrice en matière de gestion des risques liés aux technologies et du cyberrisque du Bureau du surintendant des institutions financières

[29] Cela comprend la ligne directrice sur la sécurité de l'information de la BC Financial Services Authority et la Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications de l'Autorité des marchés financiers.

[30] Ligne directrice d'approche de l'ARSF : Traitement équitable des clients en assurance

[31] Organismes canadiens de réglementation en assurance (OCRA) - Principes de conduite à l'intention des intermédiaires en assurance.

[32] Ligne directrice d'interprétation/d'approche de l'ARSF : Principes proposés de conduite à l'intention des intermédiaires en assurance

[33] Ligne directrice d'information de l'ARSF : Cadre de gestion du risque opérationnel (GRO) lors de la tarification et de la souscription de l'assurance automobile

[34] *Loi sur les assurances*, L.R.O. 1990, chap. I.8. par. 441 et 447 (Loi sur les assurances).

[35] Ligne directrice d'approche de l'ARSF - Cadre proposé de surveillance prudentielle en matière d'assurance

[36] *Loi sur les régimes de retraite*, L.R.O. 1990, chap. P.8, art. 22 (1) (LRR)

[37] Ibid., art. 30.1 (2)

[38] Consulter les responsabilités des administrateurs de régimes de retraite dans la Ligne directrice sur l'interprétation de l'ARSF - Rôles et responsabilités des administrateurs de régimes de retraite.

[39] Consulter la Ligne directrice 4 de l'ACOR sur la gouvernance des régimes de retraite.