ARSF
Autorité ontarienne de réglementation des services financiers

Ligne directrice

☑ Interprétation | ☑ Approche | ☑ Information | ☐ Décision

Date d'entrée en vigueur : 1er avril 2024
Identifiant : No GR0016INT

Gestion des risques liés aux technologies de l'information (« TI »)

Le tableau 1 présente les parties applicables de la ligne directrice, organisées par entité ou personne réglementée.

Tableau 1 : Ligne directrice présentée par entité ou personne réglementée

Entité réglementée	Parties applicables	Aperçu des parties spécifiques au secteur applicables
Organismes d'accréditation pour les planificateurs et conseillers financiers	• Partie Tous les secteurs • Approche sectorielle pour les organismes d'accréditation des planificateurs et des conseillers financiers	• Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information
Caisses	• Partie Tous les secteurs	• Interprétation de l'ARSF des exigences en matière de gestion

	• Spécifique au secteur : Interprétation/approche pour les caisses	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 à la ligne directrice sur les risques opérationnels et la résilience)
Fournisseurs de services de santé	• Partie Tous les secteurs	• Aucun contenu spécifique au secteur
Agents d'assurance, agences d'assurance, experts d'assurance et sociétés d'experts d'assurance	• Partie Tous les secteurs • Spécifique au secteur : Approche pour les compagnies d'assurance constituées ailleurs qu'en Ontario, les agents d'assurance, les agences d'assurance, les experts d'assurance et les sociétés d'experts d'assurance	• 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	• Partie Tous les secteurs	• Aucun contenu spécifique au secteur

Maisons de courtage d'hypothèques, agents en hypothèques, courtiers en hypothèques et administrateurs d'hypothèques	• Partie 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.
Compagnies d'assurance constituées en Ontario et assureurs réciproques	• Partie Tous les secteurs • Spécifique au secteur : Interprétation/approche pour les compagnies d'assurance constituées en Ontario et les assureurs réciproques	• 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
Compagnies d'assurance non constituées en Ontario	• Partie Tous les secteurs • Spécifique au secteur : Approche pour les compagnies d'assurance constituées ailleurs qu'en Ontario, les agents d'assurance, les agences d'assurance, les experts d'assurance et les sociétés d'experts d'assurance	• 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	• Partie Tous les secteurs • Spécifique au secteur : Interprétation/Approche pour les administrateurs de régimes de retraite	• Interprétation de l'ARSF de la *Loi sur les régimes de retraite* en ce qui a trait aux TI • Approche en matière de supervision de l'ARSF pour évaluer la gestion des risques liés aux technologies de l'information

Objet et portée

La ligne directrice sur la gestion des risques liés aux technologies de l'information (la « ligne directrice ») de l'Autorité ontarienne de réglementation des services financiers (ARSF) présente :

- Les pratiques de gestion efficace des risques liés aux technologies de l'information[1], sous la section 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, sous la section Approche.
- Des lignes directrices sectorielles, y compris des interprétations des exigences pour les caisses, les compagnies d'assurance constituées en Ontario et les assureurs réciproques (les « assureurs ») ainsi que les administrateurs de régimes de retraite.

La présente ligne directrice s'applique à toutes les entités et personnes réglementées par l'ARSF. La présente ligne directrice décrit les pratiques et les résultats souhaités pour les entités et les personnes réglementées, mais ne prescrit pas la manière de les atteindre. Cette approche

[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*.

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.

La présente ligne directrice[3] comprend des sections **Interprétation**, **Information** et **Approche** :

- La ligne directrice pour l'interprétation établit la vision de l'ARSF à l'égard des exigences applicables dans le cadre de son mandat prévu par la loi (c.-à-d. la législation, les règlements et les règles). La non-conformité peut mener à des mesures d'application ou de surveillance.

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

- La 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.

[3] La présente ligne directrice est publiée en tant que ligne directrice combinant les sections Interprétation, Approche et Information, conformément au cadre de lignes directrices de l'ARSF. Chaque section est clairement indiquée.

Description

La présente ligne directrice est divisée en deux grandes parties :

- **Tous les secteurs** – Ligne directrice en matière d'interprétation, d'information et d'approche applicable à toutes les entités et personnes réglementées par l'ARSF. Cette partie contient :
    - Interprétation des exigences réglementaires existantes.
    - Information sur les pratiques pour une gestion efficace des risques liés aux technologies de l'information.
    - Approche pour la transmission à l'ARSF d'un avis en cas d'incidents importants découlant des risques liés aux technologies de l'information.
- **Spécifique à un secteur –** Conseils applicables aux entités ou aux personnes réglementées par l'ARSF dans un secteur spécifique.

En tant qu'organisme de réglementation 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 partie **« Tous les secteurs » de la présente ligne directrice s'applique à toutes les entités et personnes réglementées** par l'ARSF, certaines doivent suivre une ligne directrice propre à leur secteur. L'ARSF a fait cette détermination en se basant sur le risque posé aux consommateurs, aux membres des caisses et aux participants des régimes de retraite[4] 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 ligne directrice spécifique à un secteur.

[4] Aux fins de la présente ligne directrice, ce groupe comprendra également le public, les titulaires de police, les investisseurs et d'autres intervenants.

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 englobent, mais sans s'y limiter, le cyberrisque. Si le cyberrisque concerne spécifiquement les violations délibérées ou accidentelles de la sécurité (p. ex. une violation de données), les risques liés aux TI comprennent également tout risque lié à l'utilisation de l'informatique (p. ex. 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. Les incidents peuvent avoir des répercussions négatives[5] sur les consommateurs, les membres des caisses et les participants des régimes de retraite, au risque d'effriter la confiance envers 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, comme le stipule la *Loi de 2016 sur l'Autorité ontarienne de réglementation des services financiers*, notamment : [6]

- 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 professionnelle;

[5] Les répercussions négatives peuvent inclure des pertes financières, une violation de la vie privée ou des informations confidentielles, et un manque de capacité à accéder aux services essentiels.
[6] Autorité ontarienne de réglementation des services financiers (Loi de 2016 sur l'), L.O. 2016, chap. 37, annexe 8

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

Tous les secteurs

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, le cas échéant. Le non-respect de ces exigences est susceptible de causer un préjudice aux consommateurs, aux membres des caisses et aux participants des régimes de retraite.

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;
- la capacité à se constituer en société auprès de l'ARSF en tant que caisse ou compagnie d'assurance;
- la capacité à s'enregistrer auprès de l'ARSF; ou

- la capacité à être approuvé ou à conserver le statut d'organisme d'accréditation pour les planificateurs et les conseillers financiers.

Information – Tous les secteurs

Cette partie 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 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 qui exercent leurs activités au sein d'une entité réglementée (courtiers en assurance et en hypothèques uniquement) :

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 (p. ex. les agents/experts d'assurance employés par un assureur ou sous contrat avec lui, et les agents et courtiers en hypothèques travaillant pour une maison de courtage). Ces 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 direction principale (dans certains cas, au titulaire de licence) et au conseil d'administration (le cas échéant).

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 :

- Pour les entités réglementées applicables, la surveillance assurée par le conseil d'administration de l'entité à l'égard de ses activités de gestion des risques liés aux TI est efficace.

- Les entités et les personnes réglementées ont mis en place des cadres et des stratégies visant à assurer une gestion efficace des risques liés aux TI.

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 en préserver la qualité, l'intégrité, la disponibilité et la confidentialité.

Pratique 4 : Externalisation – L'entité ou la personne réglementée gère efficacement les risques liés aux TI associés aux activités, aux fonctions et aux services externalisés ou co-sourcés. [7]

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 et la probabilité des incidents découlant des risques liés aux TI sont limités au minimum.
- Les entités et les personnes réglementées tirent des leçons des incidents précédents pour mieux prévenir les incidents futurs.

[7] 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.

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 partie intitulée « 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.
- Au moyen d'avis, 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 TI

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, soit dans un délai maximal de 72 heures normalement[8], 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 (à l'aide du formulaire d'avis d'incident découlant de risques liés aux TI, par exemple), soit par d'autres canaux (p. ex. 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** (voir plus bas). Dans certains cas, l'ARSF peut déterminer que l'avis d'incident est suffisant et que l'activation du protocole pour les incidents découlant de risques liés aux TI n'est pas justifiée.

Lorsqu'elles signalent un incident découlant de risques liés aux TI, les entités ou les personnes réglementées peuvent en informer l'ARSF :

- en envoyant par courriel le formulaire d'avis d'incident découlant de risques liés aux TI à l'adresse ITriskinbox@fsrao.ca;

- en téléchargeant le formulaire d'avis d'incident découlant de risques liés aux TI et tout autre document justificatif sur le portail de signalement des incidents;

[8] Pour les caisses et les compagnies d'assurance constituées en Ontario, un délai de 72 heures est considéré comme le délai maximal pour aviser l'ARSF.

- en communiquant directement avec le responsable de la gestion des relations (le cas échéant) ou l'agent/analyste des régimes de retraite.

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, le cas échéant, en informer ensuite l'ARSF.

Pour le **secteur du courtage d'hypothèques**, la présente ligne directrice, y compris les pratiques pour une gestion efficace des risques liés aux technologies de l'information, le formulaire d'avis d'incident découlant de risques liés aux TI et le protocole pour les incidents découlant de risques liés aux TI, est conforme 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 la présente ligne directrice doit correspondre aux lignes directrices du CCARCH et, en cas d'incohérence, la présente ligne directrice prévaut.

Pour les **administrateurs de régimes de retraite**, la présente ligne directrice, y compris les pratiques pour une gestion efficace des risques liés aux technologies de l'information, le formulaire d'avis d'incident découlant de risques liés aux TI et le protocole pour les incidents découlant de risques liés aux TI, est conforme à la ligne directrice de l'Association canadienne des organismes de contrôle des régimes de retraite (ACOR), intitulée « Le cyberrisque pour les régimes de retraite ». L'application de la présente ligne directrice doit correspondre à la ligne directrice de l'ACOR et, en cas d'incohérence, la présente ligne directrice prévaut.

Incidents importants découlant des risques liés aux TI

Les entités et les personnes réglementées doivent aviser l'ARSF uniquement quand un incident découlant de risques liés aux TI est « important ». Ce qui constitue un incident important doit être déterminé par l'entité ou la personne réglementée en fonction de l'impact sur son activité et ses opérations, ainsi que les consommateurs, les membres des caisses ou les participants des régimes de retraite.

Entités et personnes réglementées (à l'exception des administrateurs de régimes de retraite)

Les indicateurs qu'un incident important s'est produit peuvent inclure, sans s'y limiter, les éléments suivants (pour toutes les entités et les personnes réglementées, à l'exception des administrateurs de régimes de retraite). Si l'incident :

- entraîne des perturbations opérationnelles importantes des systèmes et des fonctions de l'entreprise;
- perturbe de manière significative la capacité des consommateurs ou des membres/participants 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; ou

- affectera probablement de façon négative 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.

Administrateurs de régimes de retraite

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

- perturbe les activités du régime de retraite au point qu'il n'est plus possible d'administrer le régime de façon efficace;

- affectera probablement de façon négative 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;

- compromet les données confidentielles des participants du régime de retraite; ou

- a une incidence sur la capacité de l'administrateur à verser des prestations.

Toutes les entités et les personnes réglementées

Si l'entité ou la personne réglementée n'est pas sûre qu'un incident soit important, elle peut communiquer avec l'ARSF à l'adresse courriel ltriskinbox@fsrao.ca, avec son responsable de la gestion des relations (le cas échéant) ou l'agent/analyste des régimes de retraite.

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.

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

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[9], jusqu'à ce que l'ARSF ait :

- une compréhension adéquate de l'étendue de l'incident, y compris si des données confidentielles ont été violées et quelles informations ont été consultées;

- la confirmation que les répercussions ont été prises en compte, ce qui comprend, sans s'y limiter :

    - la confirmation que toute information corrompue a été restaurée 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

[9] Il peut également être établi en amont du processus que l'incident ne nécessite pas de renseignements complémentaires, auquel cas l'ARSF désactivera le protocole.

ou le particulier pour limiter le préjudice subi par les consommateurs, les membres des caisses et les participants des régimes de retraite;

- une compréhension adéquate 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.

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 (p. ex. plainte, rapport des médias, etc.), elle déterminera s'il faut activer son protocole 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.

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

L'ARSF suivra, en général, l'approche suivante pour donner suite aux incidents :

Phase 1 : L'ARSF reçoit un avis de l'entité ou de la personne réglementée détaillant les informations disponibles 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 pour les incidents découlant 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 lui fournit des mises à jour périodiques sur l'impact de l'incident sur les opérations et les services, ainsi que sur les consommateurs, les membres de la caisse ou les participants du régime de retraite. 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.

Sa décision d'activer le protocole, et le niveau et la fréquence de son intervention auprès d'une entité ou d'une personne réglementée, reflètent la nature de l'incident, ainsi que la taille et la nature de l'entité ou de la personne en question.

Spécifique au secteur

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

- Organismes d'accréditation
- Credit Unions et caisses populaires
- Courtiers en prêts hypothécaires, agents en hypothèques, administrateurs d'hypothèques et maisons de courtage d'hypothèques
- Approche pour les compagnies d'assurance constituées ailleurs qu'en Ontario, les agents d'assurance, les experts d'assurance, les sociétés d'experts d'assurance et les agences d'assurance
- Compagnies d'assurance constituées en Ontario et assureurs réciproques
- Administrateurs de régimes de retraite

Pour les entités et les personnes réglementées qui ne sont pas incluses ici, veuillez consulter à la partie 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[10], les organismes d’accréditation des planificateurs et des conseillers financiers doivent démontrer qu’ils respectent certaines normes prescrites. Les organismes d’accréditation 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;

[10] Protection du titre des professionnels des finances – Administration des demandes d'approbation

- un plan de continuité des activités pour minimiser toute interruption de service;
- sauvegarde des données électroniques;
- 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 organismes d'accréditation, comme indiqué dans le guide de l'ARSF intitulé « Protection du titre des professionnels des finances – Cadre de supervision » [11].

L'ARSF peut mener des examens thématiques basés sur les risques liés aux TI, et cette orientation sera utilisée pour évaluer si les organismes d'accréditation 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 organisme d'accréditation s'il ne respecte pas la LPTPF, la règle de PTPF ou les conditions de son agrément.

11 Protection du titre des professionnels des finances - Cadre de supervision

Caisses

Interprétation

Interprétation par l'ARSF des exigences en matière de gestion des risques liés aux TI en vertu de la Règle 2021-001, Pratiques commerciales et financières saines (la « règle 2021-001 »).

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 2021-001. Ces pratiques prévoient notamment l'envoi d'un avis à l'ARSF en cas d'incident important **dès que possible, et au plus tard 72 heures après avoir déterminé qu'un incident découlant des risques liés aux TI était survenu.**

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[12]. Le conseil d'administration est tenu d'examiner et d'approuver périodiquement un cadre de gestion des risques liés aux TI et d'autres 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[13].

[12] Règle 2021-001 Pratiques commerciales et financières saines, par. 5(4) [RÈGLE 2021-001].
[13] Ibid., par. 5(2) et alinéa 5(3)(h).

La haute direction a pour responsabilité de mettre en œuvre le cadre relatif aux risques liés aux TI approuvé par le conseil d'administration. Notamment :

- Élaborer, mettre à jour et mettre en œuvre les politiques relatives aux TI utilisées pour gérer les risques liés aux TI, notamment les rôles et responsabilités clairement définis de la direction, du personnel et des tiers, et veiller à ce que ces politiques soient comprises par tous les autres intervenants concernés [14]

- Mettre en œuvre des systèmes et des processus qui permettent de détecter, de mesurer et de gérer avec efficacité les risques liés aux TI[15]

- Contrôler le profil de risque de la caisse en matière de TI par rapport à l'appétit pour le risque approuvé par le conseil et en rendre compte régulièrement au conseil pour confirmer la conformité. [16]

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[17] (première ligne de défense), sont 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).

La non-conformité aux exigences stipulées dans 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

[14] Ibid., par. 6(1)(i) et alinéa 6(2)(iii).
[15] Ibid., alinéa 6(1)(i).
[16] Ibid., sous-alinéa 5(3)(i)(g).
[17] Ibid., alinéas 15(2)(iv) et 15(2)(v).
[18] Ibid., sous-alinéas 10(9)(i)(a)-(b), par. 10(11) et alinéa 12(1)(i).
[19] Ibid., par. 11(2).

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) [20].

La gestion des risques liés aux TI est également un facteur pour évaluer le risque et la résilience d'une caisse sur le plan opérationnel. Le document « Lignes directrices sur les risques et la résilience opérationnels » de l'ARSF comprend une interprétation de la règle 2021-001 ainsi que des conseils relatifs aux risques liés aux TI. Les présentes lignes directrices et le document « Directives 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

Processus et pratiques

Le Cadre de surveillance axée sur le risque pour les caisses populaires et les credit unions (le « CSAR-CP ») de l'ARSF présente son approche pour assurer la supervision et la surveillance des caisses 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-CP pour repérer les pratiques commerciales imprudentes ou dangereuses qui peuvent avoir des répercussions sur les clients, les membres et les déposants des caisses, et être en mesure d'intervenir en temps utile. L'ARSF exercera un jugement de supervision et évaluera les risques les plus importants que posent les caisses par rapport à ses objectifs de supervision, et la mesure dans laquelle les caisses sont en mesure de repérer, d'évaluer et de gérer ces risques, et de faire preuve de résilience.

Dans le cadre de ses activités de supervision, elle tiendra compte du fait que les résultats décrits plus bas ont été obtenus ou non, après avoir évalué le cadre de gestion des risques liés aux TI d'une caisse. Elle évaluera également la mesure dans laquelle la direction a mis en œuvre ce cadre de façon efficace à l'aide de politiques, de processus, de systèmes et de contrôles

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

connexes. Les critères qui accompagnent chaque résultat constituent des indicateurs d'efficacité que l'ARSF utilise comme guide dans le cadre de ses évaluations de supervision. Il ne s'agit pas d'une liste exhaustive ou contraignante.

Pratique 1 : Gouvernance

Résultats

- La caisse assure la gouvernance des risques liés aux TI avec efficacité.
- Le conseil d'administration de la caisse est responsable de la gestion efficace des risques liés aux TI.
- La responsabilité de la gestion des risques liés aux TI fait l'objet d'une délégation adéquate au sein de la caisse.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

- Le conseil a approuvé une stratégie informatique documentée qui s'aligne sur la stratégie globale de la caisse et démontre que les investissements et l'affectation des ressources sont appropriés pour protéger les actifs informatiques de la caisse.
- Le conseil a approuvé l'approche générale de la caisse en matière de gestion des risques liés aux TI (p. ex. cadres, politiques, appétit pour le risque, tolérances et limites).
- Le conseil a établi une structure organisationnelle appropriée et veillé à ce que des ressources (financières et autres) soient disponibles pour gérer efficacement les risques liés aux TI.
- Le conseil a approuvé les seuils qui déclenchent la procédure d'intervention par paliers et le signalement des risques liés aux TI, notamment une définition claire et raisonnable de ce qui constitue un incident important.

Pratique 2 : Gestion des risques

Résultats

- Le conseil d'administration de la caisse assure une surveillance efficace de ses activités de gestion des risques liés aux TI.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ce résultat :

- La haute direction a mis en œuvre des politiques, des processus, des systèmes et de contrôle qui sont proportionnels à la taille et à la complexité de la caisse, aux fins de la gestion opérationnelle, de la gestion des risques et de la vérification interne. Le but est que la caisse fonctionne conformément à l'approche approuvée par le conseil concernant la gestion des risques liés aux TI. Ce qui comprend, sans s'y limiter :
    - 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.
- Le conseil reçoit régulièrement des rapports concernant la conformité des activités de la caisse avec son cadre de gestion des risques liés aux TI, notamment le degré de son exposition par rapport à l'appétit pour le risque qui a été approuvé. Il existe des processus permettant de transmettre aux paliers supérieurs tout risque, problème et événement qui surviennent en dehors des rapports réguliers.

- La ou les personnes/fonctions 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'approche générale de la caisse en matière de gestion des risques liés aux TI définit l'appétit, les tolérances et les limites approuvés par le conseil dans ce domaine.

    - Des politiques et des procédures qui permettent à la caisse de gérer ses risques liés aux TI :

        - **Repérer 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 (p. ex. par l'entremise d'une assurance), lorsque cela est approprié.

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

        - **Réagir** – élaborer des processus qui permettent à la caisse 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 tiers 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 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.

Pratique 3 : Gestion des données

Résultats

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

- Les données sont manipulées et stockées correctement de manière à préserver la qualité, l'intégrité, la disponibilité et la confidentialité des données ainsi que le respect de la vie privée.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

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 (p. ex. authentification multifactorielle, séparation des tâches et principes du moindre privilège);

- dispose de procédures pour détecter les incidents liés à la gestion des risques liés aux données (p. ex. des analyses de découverte);

- effectue des tests réguliers de ses 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 sont 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 (p. ex. 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.

Pratique 4 : Externalisation

Résultats

- Le conseil demeure responsable de la gestion des risques en cas d'externalisation des fonctions ou des processus.

Les risques liés aux TI pour les activités, les fonctions et les services externalisés et co-sourcés sont établis, évalués et gérés correctement.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

La caisse :

- possède des critères d'évaluation et de sélection des fournisseurs tiers ainsi qu'un processus d'évaluation de la performance continue des contrôles informatiques des fournisseurs tiers;
- effectue une évaluation des risques liés aux tiers avant de conclure un contrat ou de passer un marché;

- a mis en place une méthodologie pour évaluer le niveau de risque et la criticité des dispositions tierces/fournisseurs tiers.

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

- possède un processus ou un mécanisme pour confirmer l'obligation qui incombe au fournisseur tiers de respecter les politiques et procédures de la caisse en matière de gestion des risques liés aux TI;

- possède un processus ou un mécanisme pour tester périodiquement le respect par le fournisseur tiers des politiques et procédures de la caisse en matière de gestion des risques liés aux TI;

- dispose d'exigences spécifiques à l'infonuagique, s'il y a lieu, 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;

- au besoin, a établi un plan de sortie (s'il y a lieu) dans le cas où le tiers subit un événement négatif majeur (p. ex. une faillite, une panne catastrophique ou la perte de personnes clés).

Pratique 5 : Préparation aux incidents

Résultats

- Les rôles et responsabilités en cas d'incident lié aux TI sont uniformément compris.

- L'impact et la probabilité des incidents découlant des risques liés aux TI sont limités au minimum.

- Les entités et les personnes réglementées tirent des leçons des incidents précédents pour mieux prévenir les incidents futurs.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

La caisse :

- dispose d'un processus documenté, au titre de ses politiques sur les risques liés aux TI, 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 régulièrement des tests concernant les processus de gestion des incidents, notamment des exercices sur maquette, et fait participer des tiers à ces exercices, comme il convient;

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

- 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;

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

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

Pratique 6 : Continuité et résilience

Résultats

- Les caisses ont fait preuve de résilience opérationnelle et leurs services restent accessibles en cas de crise.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ce résultat :

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. niveau de risque, criticité) 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 instauré des accords de niveau de service entre les intervenants clés à l'interne et avec des fournisseurs tiers;

- dispose de politiques et de procédures de gestion de projet et de gestion du changement, lesquelles garantissent que les risques liés aux projets sont gérés de manière adéquate et que les changements sont mis en œuvre efficacement, en temps opportun, en limitant 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 la caisse, et qui explique comment l'entité continuera à fournir des services si les services essentiels sont interrompus. Le PRS, entre autres :

    - 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.

Pratique 7 : Avis en cas d'incidents importants découlant des risques liés aux TI

Résultats

- Ce qui constitue un incident important lié aux TI est uniformément compris au sein de la caisse.

- Au moyen d'avis, les entités et les personnes réglementées aident l'ARSF à identifier les zones à haut risque en temps opportun, pour prévenir de futurs incidents.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

La caisse :

- a un processus et des seuils clairs pour évaluer ce qui constitue un risque important lié aux TI;

- a documenté un processus et attribué des responsabilités garantissant que l'ARSF soit informée en cas d'incident important découlant de risques liés aux technologies de l'information;

- apprend et améliore de manière systématique 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

[21] Mortgage Broker Regulator's Council of Canada (MBRCC) Principles for Cybersecurity Preparedness
[22] Principes de préparation à la cybersécurité du Conseil canadien des autorités de réglementation des courtiers hypothécaires pour le secteur du courtage d'hypothèques
[23] Mortgage Broker Regulators' Council of Canada (MBRCC) Code of Conduct for the Mortgage Brokering Sector

réglementaire, sont conformes aux pratiques pour une gestion efficace des risques liés aux technologies de l'information et aux résultats souhaités de la présente ligne directrice. L'application de la présente ligne directrice doit correspondre aux lignes directrices du CCARCH et, en cas d'incohérence, la présente ligne directrice prévaut.

L'ARSF peut prendre des mesures d'exécution en cas de non-conformité à la présente ligne directrice 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 la présente ligne directrice 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]

La présente ligne directrice s'applique 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.

---

[24] Règl. de l'Ont. 189/08, par. 25 (1)
[25] Règl. de l'Ont. 188/08, par. 40 (1)
[26] Règl. de l'Ont. 189/08, art. 30-31
[27] Règl. de l'Ont. 188/08, art. 47-48

Approche pour les compagnies d'assurance constituées ailleurs qu'en Ontario, les agents d'assurance, les experts d'assurance, les sociétés d'experts d'assurance et les agences d'assurance

Approche

Cette partie s'applique aux compagnies d'assurance constituées en vertu d'une loi fédérale et aux compagnies d'assurance 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'assurance, aux experts d'assurance, aux sociétés d'experts d'assurance et aux agences d'assurance.

Voir cette section de la ligne directrice pour les compagnies d'assurance constituées en Ontario et les assureurs réciproques.

Lignes directrices existantes d'autres organismes de réglementation

Les compagnies d'assurance constituées à l'extérieur de l'Ontario peuvent être assujetties à des lignes directrices semblables d'un autre organisme de réglementation, comme la ligne directrice sur la gestion du risque lié 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]

---

[28] Gestion du risque lié aux technologies et du cyberrisque

[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.

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.

Ligne directrice	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	Pour les intermédiaires d'assurance, comme les agents, les experts en sinistres et les agences d'assurances d'entreprise, la ligne directrice[32] contient le principe de « protection des informations personnelles et confidentielles ».

[30] Traitement équitable des clients du secteur de l'assurance
[32] Organismes canadiens de réglementation en assurance (OCRA) - Principes de conduite à l'intention des intermédiaires en assurance.

OCRA[31] (« Principes des OCRA »)	L'ARSF a publié des lignes directrices de consultation[33] 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 ») [34]	Applicable uniquement aux compagnies d'assurance 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

[31] Organismes canadiens de réglementation en assurance (OCRA). Principes de conduite à l'intention des intermédiaires en assurance.
[33] Principes de conduite proposés pour les intermédiaires en assurance
[34] Cadre de gestion du risque opérationnel lié aux activités de tarification et de souscription de l'assurance automobile

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 la présente ligne directrice s'applique également aux agents d'assurance, aux experts d'assurance, aux sociétés d'experts d'assurance et aux agences d'assurance, l'ARSF considère que les assureurs ont la responsabilité ultime de veiller à ce que les clients bénéficient d'un traitement équitable. Ils sont tenus notamment de s'assurer que les risques liés aux TI sont gérés efficacement dans tous les canaux de distribution et les fonctions externalisées qui interviennent dans l'exercice de leurs activités. Cette responsabilité de l'assureur ne saurait décharger les intermédiaires de leurs propres responsabilités.

Compagnies d'assurance constituées en Ontario et assureurs réciproques

Interprétation

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.*

Les compagnies d'assurance constituées en Ontario et les assureurs réciproques (les « assureurs ») doivent obtenir les résultats souhaités qui accompagnent chacune des pratiques pour une gestion efficace des risques liés aux technologies de l'information, afin de satisfaire aux exigences stipulées dans la *Loi sur les assurances*. 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 ».

Cela inclut l'envoi d'un avis à l'ARSF en cas d'incident important dès que possible, mais au plus tard 72 heures après avoir déterminé qu'un incident découlant des risques liés aux TI était survenu.

Les assureurs qui omettent de se conformer à la présente ligne directrice s'exposent à des mesures d'application ou de supervision.[35]

Approche

Processus et pratiques

Le Cadre de surveillance axée sur le risque (CSAR-I) pour les compagnies d'assurance constituées en Ontario et les assureurs réciproques établit l'approche de l'ARSF pour la supervision et l'évaluation des assureurs. Son objectif principal est de déterminer les impacts des événements actuels et futurs potentiels, tant internes qu'externes, sur le profil de risque de chaque assureur.[36]

L'ARSF utilise le CSAR- I pour repérer les pratiques commerciales ou les inconduites imprudentes ou dangereuses se répercutant sur les titulaires de police, les bénéficiaires, les consommateurs et les intervenants (notamment les participants et les abonnés) et être en mesure d'intervenir en temps utile. L'ARSF exercera un jugement de supervision et évaluera les risques les plus importants que posent les assureurs, par rapport à ses objectifs de supervision, et la mesure dans laquelle les assureurs sont en mesure de repérer, d'évaluer et de gérer ces risques, et de faire preuve de résilience.

Dans le cadre de ses activités de supervision, elle tiendra compte du fait que les résultats décrits plus bas ont été obtenus ou non, après avoir évalué le cadre de gestion des risques liés aux TI d'un assureur. Elle évaluera également la mesure dans laquelle la direction a mis en œuvre ce cadre de façon efficace à l'aide de politiques, de processus, de systèmes et de contrôles connexes. Les critères qui accompagnent chaque résultat constituent des indicateurs d'efficacité que l'ARSF utilise comme guide dans le cadre de ses évaluations de supervision. Il ne s'agit pas d'une liste exhaustive ou contraignante.

---

[35] *Loi sur les assurances*, L.R.O. 1990, chap. I.8. par. 441 et 447 (Loi sur les assurances).
[36] Cadre de surveillance axée sur le risque (CSAR-I) pour les compagnies d'assurance constituées en Ontario et les assureurs réciproques

Pratique 1 : Gouvernance

Résultats

- L’assureur effectue la gouvernance des risques liés aux TI avec efficacité.
- Le conseil d’administration de l’assureur est responsable de la gestion efficace des risques liés aux TI.
- La responsabilité de la gestion des risques liés aux TI fait l’objet d’une délégation adéquate au sein de l’assureur.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l’obtention de ces résultats :

- Le conseil a approuvé une stratégie informatique documentée qui s’aligne sur la stratégie globale de l’assureur et démontre que les investissements et l’affectation des ressources sont appropriés pour protéger les actifs informatiques de l’assureur.
- Le conseil a approuvé l’approche générale de l’assureur en matière de gestion des risques liés aux TI (p. ex. cadres, politiques, appétit pour le risque, tolérances et limites).
- Le conseil a établi une structure organisationnelle appropriée et veillé à ce que des ressources (financières et autres) soient disponibles pour gérer efficacement les risques liés aux TI.
- Le conseil a approuvé les seuils qui déclenchent la procédure d’intervention par paliers et le signalement des risques liés aux TI, notamment une définition claire et raisonnable de ce qui constitue un incident important.

Pratique 2 : Gestion des risques

Résultats

- Le conseil d'administration de l'assureur effectue une surveillance efficace de ses activités de gestion des risques liés aux TI.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ce résultat :

- La haute direction a mis en œuvre des politiques, des processus, des systèmes et de contrôle qui sont proportionnels à la taille et à la complexité de l'assureur, aux fins de la gestion opérationnelle, de la conformité, de la gestion des risques et de la vérification interne. Le but est que l'assureur fonctionne conformément à l'approche approuvée par le conseil concernant la gestion des risques liés aux TI. Ce qui comprend, sans s'y limiter :
    - 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.
- Le conseil reçoit régulièrement des rapports concernant la conformité des activités de l'assureur avec son cadre de gestion des risques liés aux TI, notamment le degré de son exposition par rapport à l'appétit pour le risque qui a été approuvé. Il existe des processus permettant de transmettre aux paliers supérieurs tout risque, problème et événement qui surviennent en dehors des rapports réguliers.

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

    - Une définition claire et approuvée par le conseil d'administration de l'appétit, de la tolérance et des limites de l'assureur en matière de risque.

    - Les politiques et procédures qui permettent à l'assureur de gérer ses risques liés aux TI sont suffisamment complètes pour orienter l'approche suivante :

        - **Repérer et mesurer** – repérer et évaluer les risques et les vulnérabilités.

        - **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 (p. ex. par l'entremise d'une assurance), lorsque cela est approprié.

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

        - **Réagir** – élaborer des processus qui permettent à l'assureur 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 tiers externes.

    - Un processus permettant de rendre compte au conseil, de manière régulière et cohérente, du rendement de l'assureur par rapport à son appétit pour 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.

Pratique 3 : Gestion des données

Résultats

- Les données confidentielles supervisées par l'assureur sont sécurisées.
- Les données sont manipulées et stockées correctement de manière à préserver la qualité, l'intégrité, la disponibilité et la confidentialité des données ainsi que le respect de la vie privée.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

L'assureur :

- suit des politiques et des procédures pour identifier et classer les données de l'assureur;
- a des politiques, des procédures et des contrôles pour garantir un accès autorisé aux sources de données et à l'environnement (p. ex. authentification multifactorielle, séparation des tâches et principes du moindre privilège);
- dispose de procédures permettant de détecter le mauvais usage des données;
- effectue des tests réguliers des contrôles de gestion des données et élabore un processus pour remédier aux déficiences;
- dispose de processus et de procédures de gouvernance des données adéquats et solides pour garantir que :
    - les données sont 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 (p. ex. 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.

Pratique 4 : Externalisation

Résultats

- Le conseil demeure responsable en cas d'externalisation des fonctions ou des processus.

- Les risques liés aux TI pour les activités, les fonctions et les services externalisés et co-sourcés sont identifiés, évalués et gérés de façon adéquate.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

L'assureur :

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

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

- a mis en place une méthodologie pour évaluer le niveau de risque et la criticité des dispositions tierces/fournisseurs tiers.

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

- possède un processus ou un mécanisme pour confirmer l'obligation qui incombe au fournisseur tiers de respecter les politiques et procédures de l'assureur en matière de gestion des risques liés aux TI;

- possède un processus ou un mécanisme pour tester périodiquement le respect par le fournisseur tiers des politiques et procédures de l'assureur en matière de gestion des risques liés aux TI;

- dispose d'exigences spécifiques à l'infonuagique, s'il y a lieu, qui s'alignent sur la stratégie informatique générale et l'appétit pour le risque de l'assureur;

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

- s'assure que les fournisseurs tiers ont un processus établi pour gérer les incidents découlant des risques liés aux TI, notamment le signalement des incidents à l'assureur;

- au besoin, a établi un plan de sortie, comme il convient, dans le cas où le fournisseur tiers subit un événement négatif majeur (p. ex. une faillite, une panne catastrophique ou la perte de personnes clés).

Pratique 5 : Préparation aux incidents

Résultats

- Les rôles et responsabilités en cas d'incident lié aux TI sont uniformément compris.

- L'impact et la probabilité des incidents découlant des risques liés aux TI sont limités au minimum.

- Les assureurs tirent des leçons des incidents précédents pour mieux prévenir les incidents futurs.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

L'assureur :

- dispose d'un processus documenté, au titre de ses politiques sur les risques liés aux TI, pour détecter, consigner, gérer, résoudre, récupérer, surveiller et signaler les incidents informatiques;

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

- effectue régulièrement des tests concernant les processus de gestion des incidents, notamment des exercices sur maquette, et fait participer des tiers à ces exercices, comme il convient;

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

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

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

- 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;

- se reporte à des normes pertinentes et reconnues par l'industrie pour orienter son programme de gestion des incidents;

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

Pratique 6 : Continuité et résilience

Résultats

- Les assureurs font preuve de résilience opérationnelle et leurs services restent accessibles en cas de crise.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ce résultat :

L'assureur :

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

- attribue une classification (p. ex. niveau de risque, criticité) 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 instauré des accords de niveau de service entre les intervenants clés à l'interne et avec des fournisseurs tiers;

- dispose de politiques et de procédures de gestion de projet et de gestion du changement, lesquelles garantissent que les risques liés aux projets sont gérés de manière adéquate et que les changements sont mis en œuvre efficacement, en temps opportun, en limitant 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'assureur

continuera à fournir des services si les services essentiels sont interrompus : Le PRS, entre autres :

- 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.

Pratique 7 : Avis en cas d'incidents importants découlant des risques liés aux TI

Résultats

- Ce qui constitue un incident important lié aux TI est uniformément compris par l'assureur.

- Au moyen d'avis, les entités et les personnes réglementées aident l'ARSF à identifier les zones à haut risque en temps opportun, pour prévenir de futurs incidents.

Voici des exemples, et non une liste exhaustive, de caractéristiques qui appuient l'obtention de ces résultats :

L'assureur :

- a un processus et des seuils clairs pour évaluer ce qui constitue un risque important lié aux TI;

- a documenté un processus et attribué des responsabilités garantissant que l'ARSF soit informée en cas d'incident important découlant de risques liés aux technologies de l'information;

- apprend et améliore de manière systématique 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 par l'ARSF de la *Loi sur les régimes de retraite* (LRR) 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.[37]

Comme le stipule la LRR, l'administrateur « ne doit pas envoyer par voie électronique un document qui contient des renseignements personnels ou des renseignements prescrits, à moins de l'envoyer au moyen d'un système d'information sécurisé qui :

(a) oblige le destinataire à s'identifier avant d'accéder au document;

(b) respecte les autres conditions, exigences, restrictions ou interdictions prescrites, y compris les exigences concernant les modes d'identification pour l'application de l'alinéa a) ».[38]

[37] *Loi sur les régimes de retraite*, L.R.O. 1990, chap. P.8, par. 22(1) (LRR)
[38] Ibid., art. 30.1 (2)

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

Approche

L'ARSF a publié une ligne directrice sur les rôles et responsabilités des administrateurs de régimes de retraite qui décrit leurs rôles et leurs responsabilités en détail. [39] Cette ligne directrice stipule que les administrateurs sont tenus de mettre en œuvre des processus visant à garantir que les risques liés au régime soient compris et traités. En tant qu'organisme de réglementation qui suit une approche fondée sur les risques, l'ARSF peut prendre en compte les risques liés aux TI dans son évaluation des risques susceptibles de toucher les régimes de retraite.

Dans le cadre de ce processus, l'ARSF détermine si les administrateurs peuvent démontrer :

- qu'ils se sont familiarisés avec les pratiques acceptées dans l'industrie en matière de gouvernance des régimes de retraite, notamment la ligne directrice sur la gouvernance des régimes de retraite de l'Association canadienne des organismes de contrôle des régimes de retraite (ACOR) [40] et les autres lignes directrices de l'ACOR, selon le cas;

- qu'ils ont tenu compte des pratiques de gestion efficace des risques liés aux TI et des résultats souhaités selon la présente ligne directrice 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.

[39] Consulter les responsabilités des administrateurs de régime de retraite au Rôles et rsponsabiités des administrateurs de régimes de retraite
[40] Voir la ligne directrice nº 4 de l'ACOR sur la gouvernance des régimes de retraite au Ligne directrice no 4 : Ligne directrice sur la gouvernance des régimes de retraite

La présente ligne directrice, y compris les pratiques pour une gestion efficace des risques liés aux technologies de l'information, le formulaire d'avis d'incident découlant de risques liés aux TI et le protocole pour les incidents découlant de risques liés aux TI, est conforme à la ligne directrice de l'ACOR, intitulée « Le cyberrisque pour les régimes de retraite ». L'application de la présente ligne directrice doit correspondre à la ligne directrice de l'ACOR et, en cas d'incohérence, la présente ligne directrice prévaut.

Date d'entrée en vigueur et examen futur

La présente ligne directrice entre en vigueur le **1er avril 2024** et fera l'objet d'une révision au plus tard en **juin 2028**.

À propos de la présente ligne directrice

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 d'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. Cette dernière peut également faire référence à des obligations de conformité, mais ne crée pas en soi une obligation de conformité.