5.

Institutions financières

5.1 AVIS ET COMMUNIQUÉS

Aucune information.

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Ligne directrice applicable aux agents d'évaluation du crédit

Loi sur les agents d'évaluation du crédit, RLRQ, c. A-8.2

L'Autorité des marchés financiers (« l'Autorité ») publie pour consultation le projet de mise à jour de la *Ligne directrice applicable aux agents d'évaluation du crédit* publiée initialement en mars 2022.

Le projet de mise à jour tient compte des travaux effectués par l'Autorité en matière de traitement des plaintes et de règlement des différends dans le secteur financier, en reprenant essentiellement les attentes de la Ligne directrice sur les saines pratiques commerciales.

Les personnes intéressées à soumettre leurs commentaires sont invitées à les fournir au plus tard le **16 décembre 2022**. Il est à noter que les commentaires soumis seront rendus publics à défaut d'avis contraire à cet effet.

Soumission des commentaires

Les commentaires doivent être soumis à :

Me Philippe Lebel
Secrétaire et directeur général des affaires juridiques
Autorité des marchés financiers
Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1
Télécopieur : (514) 864-8381
consultation-en-cours@lautorite.qc.ca

Renseignements additionnels

Des renseignements additionnels peuvent être obtenus en s'adressant à :

Hélène Samson
Directrice de l'encadrement prudentiel des institutions financières
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4681
Numéro sans frais : 1 877 525-0337
helene.samson@lautorite.qc.ca

Le 17 novembre 2022

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE APPLICABLE AUX AGENTS D'ÉVALUATION DU CRÉDIT

Février 2023

TABLE DES MATIÈRES

Introduction

Les agents d'évaluation du crédit (les « AÉC ») collectent, utilisent, compilent, produisent et divulguent des données des consommateurs[1] conformément aux lois applicables.

Les entreprises qui ont recours aux AÉC, telles les institutions financières, utilisent ces données sur le crédit dans le cadre de leurs activités courantes.

En raison du rôle important que jouent les AÉC dans l'écosystème financier, l'Autorité des marchés financiers (l'« Autorité ») s'est vu confier, dans le cadre de La *Loi sur les agents d'évaluation du crédit*[2] (la « Loi »), le mandat de surveiller et de contrôler leurs pratiques commerciales ainsi que leurs pratiques de gestion et d'émettre en ce sens des attentes à leur égard[3], en sus de celles touchant les mesures de protection, les droits des personnes concernées, les recours et les plaintes[4].

Pour la mise en œuvre de ces attentes, l'Autorité privilégie une approche basée sur des principes et confère ainsi aux AÉC la latitude nécessaire leur permettant de déterminer les stratégies, politiques, procédures et processus, ainsi que de voir à leur application en regard de la nature, de la taille et de la complexité de leurs activités.

1. La gouvernance

Une saine gouvernance est cruciale et constitue la pierre angulaire d'une gestion appropriée de la part d'un AÉC assurant le respect des droits conférés aux consommateurs par la Loi.

Dans cette perspective, l'Autorité désire s'assurer que l'AÉC mette en place et suive des pratiques de gestion appropriées en s'appuyant notamment sur l'adoption et la promotion d'une culture d'entreprise fondée sur un comportement organisationnel éthique et sur la responsabilisation des instances décisionnelles.

Par culture d'entreprise, l'Autorité réfère aux valeurs et aux normes communes qui caractérisent une entreprise donnée et influencent sa façon de penser, sa conduite et les actions de l'ensemble de son personnel. Par conséquent, une bonne culture d'entreprise est essentielle pour maintenir la confiance des consommateurs, alors qu'à l'inverse, une culture déficiente peut nuire de manière importante à la réputation de l'entreprise et lui causer d'importants préjudices, ainsi qu'à ses différentes parties prenantes.

Une gouvernance efficace et efficiente implique la mise en place d'un cadre formel de fonctionnement, de supervision et de reddition de comptes par le biais de politiques, de procédures et de systèmes d'information qui contribuent à organiser la gestion de l'AÉC et à en assurer le contrôle. Ainsi, elle nécessite des dispositifs de gestion de risques et de

1 Désigné sous l'expression « personne concernée » dans la *Loi sur les agents d'évaluation du crédit*, le terme « consommateur » dans la présente ligne directrice renvoie à la personne qui fait l'objet du dossier de crédit ou son représentant.

2 *Loi sur les agents d'évaluation du crédit,* L.Q. 2020, c. 21.

3 Voir les articles 53 et 54 de la Loi.

4 Voir les articles 28 et suivants de la Loi.

contrôle répartis entre plusieurs secteurs et niveaux de l'organisation, ce qui requiert une approche rigoureuse et coordonnée.

Les AÉC interagissent notamment avec des institutions financières et gèrent les données personnelles des consommateurs. Vu la sensibilité et l'importance des données qu'ils détiennent, l'Autorité croit essentiel que les AÉC s'inspirent du modèle des trois lignes de défense afin de :

- favoriser une coordination rigoureuse entre les fonctions de gestion des risques et de contrôle;
- structurer la gestion des risques associés à leurs activités visées par la Loi;
- répondre aux mêmes standards que leurs principaux partenaires commerciaux.

Plus spécifiquement, l'Autorité émet les attentes suivantes en ce qui concerne le respect des dispositions de la Loi afin que les AÉC en assurent la conformité et garantissent aux consommateurs le plein exercice de leurs droits.

L'impartition des différentes fonctions identifiées ci-dessous devrait être divulguée à l'Autorité sur demande[5].

Première ligne de défense

Les directions opérationnelles des AÉC constituent la première ligne de défense responsable de la gestion quotidienne des risques puisque la conception et le pilotage des contrôles ainsi que leur intégration dans les systèmes et les processus s'effectuent sous leur supervision. À ce chapitre, leurs responsabilités devraient notamment consister à :

- identifier, évaluer, gérer et contrôler les risques en lien avec les exigences de la Loi;
- piloter l'élaboration et la mise en œuvre des procédures de contrôle interne;
- surveiller l'application de ces procédures par leurs collaborateurs;
- s'assurer que les activités soient compatibles avec les objectifs fixés;
- s'assurer que les activités soient exercées en conformité avec la Loi.

Les gestionnaires/directeurs opérationnels devraient également mettre en œuvre des mesures correctives permettant de pallier les contrôles et processus déficients.

Par ailleurs, le contrôle interne est également une composante essentielle d'une gouvernance efficace puisqu'il permet ainsi de détecter les déficiences fonctionnelles, lesquelles pourraient être des sources importantes de risques pour un AÉC. Par conséquent, les mécanismes de contrôle qui le composent devraient être conçus et opérés pour assurer l'efficacité des politiques et processus clés d'un AÉC assurant le respect des droits conférés aux consommateurs par la Loi.

[5] Voir les articles 50 et 51 de la Loi.

Ceux-ci devraient notamment couvrir les éléments suivants :

- La ségrégation appropriée des tâches, lorsque nécessaire;
- Les politiques d'approbation des décisions;
- La présence de contrôles adaptés à chacun des niveaux appropriés de l'organisation;
- La formation relative au contrôle interne, particulièrement pour les employés ayant d'importantes responsabilités;
- La cohérence du contrôle interne dans son ensemble et pour chacun des mécanismes individuels;
- Les vérifications et tests effectués par des parties indépendantes (auditeurs internes ou externes) quant à l'efficacité des mécanismes de contrôle en place.

Étant donné que le contrôle interne implique le personnel en place à tous les paliers de l'AÉC, celui-ci devrait être sensibilisé à l'importance des mécanismes le composant et recevoir, à cette fin, des communications claires de la part de la haute direction. Pour ce faire, il est essentiel que l'information pertinente soit identifiée, colligée et communiquée selon un format et dans les délais qui permettent aux personnes concernées d'assumer adéquatement leurs responsabilités.

Cet exercice d'identification, de collecte et de communication d'information devrait permettre de s'assurer que les mécanismes de contrôle interne répondent adéquatement aux objectifs visant à assurer la conformité à la Loi, dont l'obligation de suivre de saines pratiques commerciales plus précisément. L'évaluation de l'efficacité des contrôles internes devrait notamment inclure les aspects suivants :

- La stratégie adoptée relativement aux mécanismes de contrôle;
- Le cadre de référence utilisé en matière de contrôle;
- L'état d'avancement de leur implantation ou mise à jour;
- L'information sur les ressources nécessaires à son fonctionnement;
- La description des problèmes et des déficiences rencontrés.

Deuxième ligne de défense

Les fonctions de gestion des risques et de conformité ont pour rôle de s'assurer de la bonne conception, de l'efficacité et du fonctionnement adéquat du contrôle interne et de la conformité aux lois, règlements et normes applicables.

Pour être efficaces et assumer correctement leur rôle au sein de la deuxième ligne de défense, la fonction de gestion des risques et celle de conformité devraient avoir l'autorité suffisante, le positionnement hiérarchique adéquat, l'indépendance par rapport à la gestion des opérations, les ressources nécessaires à l'exercice de leurs rôles et le libre accès aux instances décisionnelles.

Une fonction de gestion des risques efficace au niveau de la deuxième ligne de défense est indépendante du niveau opérationnel lié à la prise de risques et assure un suivi rigoureux des risques importants ainsi qu'une veille des risques émergents.

Une fonction de conformité[6] indépendante des activités qu'elle supervise est une des composantes clés de la deuxième ligne de défense de l'AÉC et un fondement essentiel des pratiques de gestion appropriées en assurant le respect des droits conférés aux consommateurs par la Loi.

Troisième ligne de défense

Une fonction indépendante d'audit interne efficace et efficiente constitue la troisième ligne de défense du cadre de gouvernance dans la mesure où elle donne à l'AÉC, selon une approche axée sur les risques, une assurance quant au degré de maîtrise de ses opérations, lui apporte ses conseils pour renforcer leur efficacité et contribuer à créer de la valeur ajoutée.

En matière de pratiques de gestion appropriées et de saines pratiques commerciales, l'audit interne doit évaluer la conception, l'adéquation et l'efficacité opérationnelle des processus et formuler des recommandations appropriées en vue de leur amélioration. Le but étant de fournir une assurance objective aux instances décisionnelles que les processus sont conçus adéquatement, fonctionnent correctement et répondent aux objectifs de :

- promouvoir un comportement organisationnel éthique qui tient compte du traitement équitable des consommateurs;
- suivre les performances de l'organisation et d'en rendre compte;
- communiquer, aux services concernés de l'AÉC, l'information relative aux risques et aux contrôles;
- coordonner les activités et la communication des informations entre les instances décisionnelles, les auditeurs externes et les auditeurs internes[7].

De plus, l'audit interne devrait évaluer l'efficacité et la pertinence des processus de gestion des risques et de conformité et des mécanismes de contrôle interne et promouvoir leur amélioration continue, y compris l'atteinte des objectifs dans ces domaines par les fonctions composant les première et deuxième lignes de défense.

Pour que l'audit interne puisse jouer efficacement son rôle de troisième ligne de défense, un accès direct et sans restriction aux instances décisionnelles est souhaitable afin d'asseoir son indépendance et conforter son objectivité au sein de l'AÉC.

6 Une fonction de conformité n'est pas forcément une unité particulière au sein de l'AÉC. En effet, le personnel chargé de la conformité peut être impliqué dans des unités opérationnelles et rendre compte à la direction responsable de l'activité en question. Il importera toutefois que ces unités puissent, le cas échéant, rendre compte au chef de la conformité ou la personne responsable de cette fonction, lequel devrait être indépendant de la gestion des opérations.

7 INSTITUT DES AUDITEURS INTERNES. Norme de fonctionnement 2110.

Le modèle des trois lignes de défense pourrait toutefois être modulé en fonction de la répartition des rôles et responsabilités au sein du groupe corporatif auquel appartient l'AÉC, tout en ne limitant pas la responsabilité de l'AÉC à cet égard et conformément aux attentes de l'Autorité exprimées dans la section portant sur la gestion du risque d'impartition.

2. Les saines pratiques commerciales

L'AÉC a l'obligation légale de suivre de saines pratiques commerciales.

Les pratiques commerciales ou la conduite des activités d'un AÉC reflètent son comportement dans le cadre de sa relation avec les consommateurs, comportement qui devra se traduire par le traitement équitable de ces derniers.

Le traitement équitable des consommateurs s'inspire des orientations énoncées par diverses instances internationales[8]. Ce principe englobe des concepts comme le comportement éthique, la bonne foi et l'interdiction de pratiques abusives. Le traitement équitable des consommateurs consiste notamment à :

- offrir des services relatifs aux droits conférés aux consommateurs par la Loi répondant aux intérêts et aux besoins des consommateurs;
- communiquer aux consommateurs une information précise, claire et adéquate leur permettant de prendre des décisions éclairées;
- protéger la confidentialité des renseignements personnels des consommateurs;
- traiter les plaintes des consommateurs équitablement et avec diligence;
- mettre à leur disposition des ressources suffisantes, notamment humaines, afin de leur faciliter l'exercice en temps utile de leurs droits.

L'Autorité s'attend donc à ce que le traitement équitable du consommateur fasse partie intégrante de la culture d'entreprise de l'AÉC. L'établissement d'une culture de traitement équitable des consommateurs permettrait entre autres de placer l'intérêt des consommateurs au centre des décisions et de la conduite des activités et de s'assurer que l'ensemble du personnel agisse avec éthique et intégrité envers les consommateurs.

a. Communication avec les consommateurs

L'AÉC devrait communiquer les informations aux consommateurs, verbalement ou par écrit, dans un langage simple, clair et précis, peu importe le moyen utilisé. Ces communications devraient être en français ou en anglais selon la langue privilégiée par les consommateurs. De plus, l'AÉC devrait s'assurer que le personnel à son emploi soit en nombre suffisant et adéquatement formé pour répondre aux demandes et questions des consommateurs.

Par exemple, si un système de codes ou de notations est utilisé dans la documentation transmise ou qu'une terminologie technique est employée pour communiquer des informations, l'Autorité s'attend à ce que l'AÉC explique leur signification selon les bonnes pratiques énoncées à la présente sous-section.

L'AÉC devrait mettre à la disposition des consommateurs des moyens de communication permettant une prise de contact rapide et efficace. Ceux-ci devraient être variés

[8] Notamment, les énoncés relatifs à la protection des consommateurs en matière financière élaborés conjointement par l'Organisation de coopération et de développement économique et le Conseil de la stabilité financière.

(téléphones, adresse courriel, messagerie instantanée, etc.) et facilement repérables sur l'ensemble des plateformes (site Web, réseaux sociaux) de l'AÉC.

Par ailleurs, l'AÉC devrait prendre des mesures appropriées pour vérifier l'identité d'un consommateur avec lequel il interagit. À cet égard, l'AÉC ne devrait pas divulguer un rapport de crédit s'il n'est pas en mesure de vérifier adéquatement l'identité d'un consommateur.

L'Autorité s'attend à ce que la publicité relative aux produits et services soit exacte, claire et non trompeuse.

b. La gestion des informations contenues dans le dossier de crédit

L'AÉC devrait avoir une politique claire et à jour en ce qui concerne la gestion des informations contenues dans le dossier de crédit.

Compte tenu de la nature sensible de ces informations, l'AÉC devrait avoir en place des normes élevées de sécurité de l'information pour les données qu'il reçoit, utilise ou partage. L'AÉC devrait disposer de processus efficaces de révision périodique de la gestion desdites informations.

Par ailleurs, l'Autorité s'attend à ce que les politiques et procédures de l'AÉC en matière de protection des renseignements personnels s'inspirent des meilleures pratiques et lui permettent de s'acquitter de ses obligations en la matière, notamment celles qui découlent de la *Loi sur la protection des renseignements personnels dans le secteur privé*[9].

L'AÉC devrait établir et appliquer une méthode d'opération qui garantit que l'information qu'il communique est à jour et exacte. L'AÉC devrait à ce titre veiller à ce que des évaluations et examens réguliers soient effectués afin de déterminer si les ententes conclues avec les fournisseurs externes sont respectées et, le cas échéant, pallier les manquements présumés ou constatés aux termes de ces ententes.

L'AÉC devrait disposer d'un processus robuste de validation de toute modification apportée aux renseignements personnels des consommateurs (p. ex. adresse postale, numéro de téléphone, etc.).

c. Le traitement des plaintes

L'Autorité s'attend à ce que les plaintes soient traitées équitablement et avec diligence, selon un processus simple et facilement accessible pour les consommateurs.

Les plaintes reçues par un AÉC et le traitement qui en est effectué constituent, entre autres, des éléments importants permettant d'évaluer la performance de ce dernier en matière de traitement équitable des clients.

En vertu de la Loi, l'AÉC doit notamment tenir un registre des plaintes et adopter une politique portant sur le traitement des plaintes ainsi que sur le règlement des différends[10].

---

9 *Loi sur la protection des renseignements personnels dans le secteur privé*, R.L.R.Q., c. P-39.1

10 Voir l'article 35 de la Loi.

L'Autorité s'attend à ce que :

- Le processus de traitement des plaintes tient compte des intérêts des consommateurs et permet que les plaintes soient traitées de manière objective et cohérente;
- L'AÉC désigne un responsable du traitement des plaintes qui possède l'autorité et la compétence nécessaire à l'exercice de sa fonction et qui assure notamment la mise en œuvre, la diffusion et le respect de la politique de traitement des plaintes et de règlement des différends au sein de l'AÉC;
- Les membres du personnel chargés du traitement des plaintes possèdent les compétences nécessaires pour traiter les plaintes qui leur sont assignées;
- Les consommateurs sont adéquatement assistés tout au long du processus de traitement de leur plainte et sont informés en temps opportun du statut de leur plainte;
- Les consommateurs ne se heurtent pas à des contraintes ou obstacles administratifs et les compléments d'information requis par l'AÉC évitent d'entraver ou de retarder le processus de traitement d'une plainte;
- L'AÉC développe une vision d'ensemble des plaintes reçues afin d'identifier les causes communes et les enjeux à résoudre pour permettre un traitement équitable des consommateurs.

3. La gestion du risque opérationnel

L'Autorité s'attend à ce que l'AÉC gère adéquatement son risque opérationnel en lien avec son modèle d'affaires et la stratégie de gestion élaborée pour ce risque. Cette gestion devrait considérer l'exposition aux risques opérationnels inhérents aux personnes, processus, systèmes ou événements externes de l'AÉC de même que l'exposition des parties prenantes à ces risques.

La gestion du risque opérationnel devrait également mettre en lumière les situations où une activité, un processus ou un système en particulier n'assure pas le traitement équitable des consommateurs. À titre d'exemple, une brèche en matière de sécurité de l'information causée par une divulgation accidentelle de renseignements personnels de consommateurs ou une fuite d'informations confidentielles résultant d'un acte délibéré sont des situations susceptibles de nuire au traitement équitable des consommateurs, ce qui pourrait ultimement affecter la réputation de l'AÉC.

De plus, l'AÉC devrait faire preuve de diligence et prendre des mesures adéquates lorsqu'un ou des consommateurs font valoir qu'ils ont été ou croient être victimes d'une fraude ou d'un crime connexe, y compris le vol d'identité et ce, après avoir vérifié adéquatement l'identité de ceux-ci.

En ce qui a trait aux risques opérationnels, l'établissement d'une culture qui promeut la gestion adéquate des risques doit nécessairement émaner des instances décisionnelles et être modulé en fonction de l'ampleur de l'exposition aux risques opérationnels et, conséquemment, de l'engagement requis de tous les paliers de l'organisation, afin de bien gérer ces types de risques.

La sensibilisation devrait aussi viser les parties prenantes externes, notamment les fournisseurs de services découlant d'ententes d'impartition importantes[11], du fait que l'impartition expose l'organisation aux risques opérationnels (p. ex., l'exposition aux cyberrisques).

[11] Est considérée comme importante, toute entente d'impartition susceptible d'avoir un impact significatif sur la situation financière de l'institution, ses opérations et ultimement sa réputation.

4. Gestion des risques liés aux technologies de l'information et des communications

L'AÉC devrait s'assurer de mettre en place une gestion des risques liés aux technologies de l'information et des communications (« TIC ») qui soit robuste et appuyée sur les sources, les recommandations et les normes issues d'organismes reconnus tels que l'OCDE, le G7, le NIST, l'ISACA-COBIT ou l'ISO. De plus, l'AÉC devrait notamment s'assurer que les instances décisionnelles fassent la promotion d'une culture d'entreprise fondée sur un comportement éthique et sécuritaire dans l'exploitation des technologies.

À cette fin, l'AÉC devrait avoir en place un encadrement adéquat, basé sur les risques, pour la sécurité de l'information et la sécurité physique de l'ensemble de ses infrastructures technologiques et actifs informationnels.

L'AÉC devrait s'assurer de mettre en place une taxonomie qui lui est propre pour que tous les types de risques liés aux TIC soient répertoriés. La sécurité de l'information, l'infogérance et l'infonuagique, la continuité des activités, la gestion de crise, les ressources humaines, les opérations liées aux TIC et l'éthique sont quelques-unes des catégories de risques liées aux TIC qui devraient être considérées. Une fois développée, cette taxonomie devrait être communiquée à ceux qui participent directement aux activités d'évaluation des risques et aux contrôles, afin d'en assurer une utilisation cohérente dans l'identification et l'agrégation des risques TIC.

L'AÉC devrait délimiter clairement les responsabilités de la fonction de la sécurité de l'information, pour favoriser son indépendance et objectivité, notamment en la séparant des processus opérationnels TIC ou par la mise en place de contrôles compensatoires au besoin. Cette fonction ne devrait pas être responsable de travaux d'audit interne.

L'AÉC devrait veiller à l'assignation :

- d'un responsable à la haute direction, tel un chef de la sécurité de l'information, pour la surveillance du déploiement de l'encadrement relatif à la sécurité de l'information et à la sécurité physique des infrastructures technologiques de l'organisation;
- d'un responsable à la haute direction, tel un chef des données, lequel surveille l'encadrement approuvé à l'égard de la réception, l'emmagasinage et l'utilisation des données à travers l'organisation.

L'AÉC devrait maintenir des capacités adéquates pour anticiper, détecter et assurer le recouvrement lors d'incidents liés aux TIC qui incluent notamment les incidents de sécurité de l'information.

L'AÉC devrait notamment, à l'égard des droits conférés aux consommateurs par la Loi :

- définir dans sa politique de sécurité de l'information des principes et des règles à suivre pour protéger la confidentialité, l'intégrité et la disponibilité des informations des consommateurs;
- définir des objectifs de sécurité de l'information clairs pour les systèmes et les services en lien avec les TIC, les processus et les personnes;

- appliquer la politique de sécurité de l'information à toutes ses activités ,et ce, tout en s'assurant que cette politique encadre également l'information traitée chez les intervenants externes au périmètre de l'AÉC;
- déployer des contrôles pour les actifs (données, matériels et logiciels) informationnels qui soient proportionnels à la criticité et la sensibilité desdits actifs;
- effectuer des essais systématiques adéquats pour valider l'efficacité des contrôles mis en place.

Les activités préparatoires considérées par l'AÉC pour la gestion des risques TIC devraient notamment contribuer à la protection des données sensibles des consommateurs contre la divulgation, la fuite ou les accès non autorisés. Elle devrait aussi contribuer à la résilience de l'environnement TIC. Ces activités devraient couvrir, entre autres, les contrôles d'accès, l'authentification, l'intégrité et la confidentialité des données, l'enregistrement des activités et le suivi des événements de sécurité.

L'AÉC devrait considérer les activités nécessaires de préparation, de traitement et de suivi pour qu'en cas d'incident ou de crise réelle, les impacts négatifs pour les consommateurs puissent être rapidement mitigés.

L'AÉC devrait utiliser un processus rigoureux pour le recensement périodique des actifs informationnels et leurs vulnérabilités, afin d'y associer adéquatement les risques.

L'AÉC devrait exploiter un cadre de classification permettant de définir la criticité des données et des actifs informationnels (incluant ceux qui sont gérés par des parties intéressées externes) minimalement selon leurs exigences de disponibilité, d'intégrité et de confidentialité. Ce cadre de classification devrait refléter la mesure dans laquelle un incident de sécurité de l'information affectant un actif informationnel a le potentiel de nuire à l'AÉC, aux consommateurs ou aux autres parties intéressées.

L'AÉC devrait utiliser des processus de gestion d'incidents TIC, dotés d'objectifs de reprise et de recouvrement adéquats, assurer un suivi approprié et en temps opportun des activités de mitigation des risques présents au registre des risques TIC et suivre l'efficacité des mesures de mitigation, de même que le nombre d'incidents signalés afin de les corriger lorsque nécessaire. De plus, l'AÉC devrait effectuer des analyses spécifiques à la suite d'un incident majeur pour améliorer ses plans de réponse et de recouvrement.

L'AÉC devrait également établir et maintenir une documentation et l'information permettant la prise de décision éclairée à l'égard des risques TIC. La documentation devrait notamment comporter un registre, une description de l'impact des risques, une matrice des risques et contrôles et les processus et structures existantes pour la gestion de ces risques.

L'AÉC devrait aussi mettre en place des mécanismes robustes permettant d'assurer le respect des droits conférés aux consommateurs par la Loi. Parmi ceux à considérer, mentionnons notamment la gestion des identités et des accès, la formation et sensibilisation, la ségrégation des réseaux et la protection de leur intégrité, la sécurité des données, la protection des appareils de types « *endpoints* » (p. ex. : ordinateurs portatifs, tablettes, téléphones intelligents), la vérification de l'intégrité des logiciels et du microcode

et les solutions technologiques de protection contribuant à la résilience des systèmes et des actifs informationnels. De même, la détection et l'enregistrement d'événements et d'anomalies, la surveillance en continu des systèmes d'information et la mise à l'essai des processus de détection devraient être considérés.

L'AÉC devrait s'assurer que l'accès logique et physique aux actifs informationnels est restreint aux utilisateurs, processus, appareils et aux activités autorisées par la politique de sécurité établie de l'AÉC. Les privilèges d'accès octroyés devraient être établis sur la base des principes généralement reconnus tels que le « besoin de savoir », le « moindre privilège » et la « ségrégation des tâches », uniquement au personnel autorisé et de façon à prévenir les accès injustifiés à de larges ensembles de données et prévenir le contournement des contrôles de sécurité.

L'AÉC devrait soumettre ses contrôles à l'égard de la sécurité de l'information à différents types d'évaluation, de tests et des revues indépendantes périodiques, de même qu'à des tests d'intrusion.

L'AÉC devrait mettre en place les procédures et processus requis pour signaler selon les obligations en vigueur, les incidents de sécurité de l'information aux parties intéressées incluant l'Autorité et les consommateurs.

5. La gestion du risque lié à l'impartition

L'AÉC devrait identifier les différents risques liés à ses ententes d'impartition, notamment le risque TIC, afin d'être en mesure de les évaluer et de les gérer adéquatement.

L'impartition se définit comme étant une délégation à un fournisseur de services, sur une période définie, de l'exécution et de la gestion d'une fonction, d'une activité ou d'un processus, dont l'AÉC s'acquitte ou pourrait s'acquitter lui-même. Toute entente d'impartition conclue avec un fournisseur de services opérant à l'extérieur du Canada ou qui traite, emmagasine ou fait transiter des données à l'extérieur du Canada est considérée comme étant de la délocalisation. Ces ententes d'impartition ou de délocalisation relatives aux droits conférés aux consommateurs par la Loi doivent être divulguées à l'Autorité sur demande[12].

Avant de s'engager dans une entente d'impartition impliquant les mesures de protection et les droits conférés aux consommateurs par la Loi, il est essentiel pour l'AÉC d'évaluer les risques qui seraient engendrés par le recours à l'impartition. Cet exercice devrait également comprendre la capacité du fournisseur de services à assurer un service de qualité par le biais de volets portant, par exemple, sur les aspects financiers, opérationnels et de réputation.

L'Autorité s'attend à ce que les ententes d'impartition de l'AÉC soient rédigées afin d'y inclure les conditions gouvernant les relations, fonctions, obligations et responsabilités des parties à l'entente.

L'AÉC devrait assurer le suivi de ses ententes d'impartition afin de voir au respect des engagements. L'Autorité considère que l'AÉC demeure ultimement responsable des activités imparties, même si l'exécution et la gestion de ces activités sont assurées par des fournisseurs de services.

L'Autorité s'attend également à ce que l'AÉC gère adéquatement les risques liés aux ententes d'impartition importantes conclues avec les membres de son groupe, le cas échéant.

Enfin, la dépendance de l'AÉC à l'égard des fournisseurs de services ne devrait pas compromettre sa gestion de la continuité de ses activités.

Dans le contexte de l'infogérance et l'infonuagique, l'AÉC devrait notamment :

- assurer contractuellement son droit d'auditer et d'accès physique aux locaux des fournisseurs de services infonuagiques;
- mitiger les risques d'impartition en chaîne lorsque les fournisseurs impartissent eux-mêmes certaines activités à d'autres fournisseurs;
- s'assurer de la conformité des fournisseurs aux objectifs et mesures de sécurité et aux attentes de performance.

[12] Voir les articles 50 et 51 de la Loi.

L’utilisation des services de certaines parties prenantes pourrait ne pas constituer une forme d’impartition. Toutefois, plusieurs de ces services sont fournis à l’aide des TIC ou impliquent des informations potentiellement confidentielles. Ces parties prenantes peuvent aussi être exposées à des incidents de sécurité. L’AÉC devrait évaluer les risques de bris de confidentialité, d’intégrité et de disponibilité des informations traitées par ces services et les gérer adéquatement.

6. La continuité des activités

L'AÉC devrait disposer d'une stratégie lui permettant d'assurer la continuité des activités critiques et la reprise des activités perturbées ou interrompues, et ce, dans des délais raisonnables.

Dans cette perspective, l'AÉC devrait évaluer les impacts des incidents de nature opérationnelle sur ses ressources, son fonctionnement et son environnement et déterminer les mesures à prendre découlant de cette évaluation.

Le développement d'un plan de continuité des activités qui documente les actions à entreprendre en cas d'incident opérationnel ayant un impact sur les activités critiques est donc essentiel. Le plan de continuité des activités devrait par exemple définir les procédures et les systèmes nécessaires pour rétablir les opérations de l'AÉC en cas de perturbation de ses activités critiques. Il devrait être clair, facile d'utilisation, testé et mis à jour régulièrement. Il devrait également être accompagné d'un plan de communication. L'AÉC devrait dès que possible informer l'Autorité dès le moment où il active son plan de continuité des activités. L'AÉC devrait également informer toute autre partie intéressée susceptible d'être impactée par cette situation.

L'AÉC devrait également identifier ses activités critiques et les incidents opérationnels majeurs susceptibles de les perturber, de les ralentir ou de les interrompre. Il devrait également évaluer le niveau de concentration de ses activités critiques sur un même site, leur interdépendance, ainsi que leur dépendance aux mêmes ressources, notamment à l'égard des membres du personnel, des systèmes ou des fournisseurs de services.

L'AÉC devrait considérer un ensemble d'événements plausibles et de scénarios, incluant des événements de cybersécurité, dans la planification et la mise à l'essai des plans de recouvrement des opérations en cas de désastre et de continuité.

L'AÉC devrait identifier tous les points individuels de défaillance potentielle dans les systèmes TIC et les architectures de réseaux supportant les droits conférés aux consommateurs par la Loi afin que des mesures appropriées soient déployées pour mitiger les risques d'interruption.

L'AÉC devrait s'assurer de minimiser les risques d'interruption des opérations par la mise en place de processus adéquats pour la gestion des changements touchant les équipements TIC (matériels et logiciels) et les procédures liées au développement, l'exécution, le support et l'entretien des systèmes TIC.

Dans l'optique de réduire les risques d'interruption des opérations provenant par exemple de l'exploitation mal intentionnée de vulnérabilités des logiciels, l'AÉC devrait établir des pratiques et des standards sécurisés pour encadrer la programmation, la revue des codes sources et la mise à l'essai de la sécurité applicative de ses systèmes TIC supportant l'application des droits conférés aux consommateurs par la Loi. Lorsque l'application de ces pratiques soulève des enjeux de disponibilité, d'intégrité et de confidentialité de l'information et des systèmes TIC, ces derniers devraient être compilés, suivis et corrigés.

L'Autorité s'attend à ce que l'AÉC vérifie périodiquement la fiabilité de son plan de continuité des activités. Le processus de gestion de la continuité des activités devrait être

un processus dynamique prenant en charge les changements qui affectent l'AÉC, ses parties prenantes et son environnement. L'AÉC devrait s'assurer que ses fournisseurs de services disposent d'un plan de continuité des activités robuste qui respecte les objectifs de son propre plan et n'introduise pas de nouveaux risques non identifiés pour l'AÉC.

7. Surveillance des pratiques de gestion appropriées et des saines pratiques commerciales

En lien avec sa volonté de favoriser le déploiement de pratiques de gestion appropriées et des saines pratiques commerciales au sein des AÉC, l'Autorité entend procéder, dans le cadre de ses travaux de surveillance, à l'évaluation du degré d'observance des principes énoncés dans la présente ligne directrice.

En conséquence, l'efficacité et la pertinence des stratégies, politiques et procédures mises en place, la qualité de la supervision et le contrôle exercés par les instances décisionnelles seront évalués.

Les pratiques de gestion de même que les pratiques commerciales qui sont abordées dans cette ligne directrice évoluent constamment. L'Autorité s'attend à ce que les instances décisionnelles des AÉC s'enquièrent des meilleures pratiques en ces matières et les appliquent dans la mesure où celles-ci répondent à leurs besoins.

AUTORITÉ DES MARCHÉS FINANCIERS

GUIDELINE APPLICABLE TO CREDIT ASSESSMENT AGENTS

February 2023

TABLE OF CONTENTS

Introduction

Credit assessment agents ("CAAs") collect, use, compile, produce and disclose consumer[1] data in accordance with applicable legislation.

Businesses such as financial institutions use the consumer credit data provided by CAAs in the course of their day-to-day operations.

Given the significant role played by CAAs in the financial ecosystem, the Autorité des marchés financiers (the "AMF") has been empowered under the *Credit Assessment Agents Act*[2] (the "Act") to supervise and control the commercial practices and management practices of CAAs and to issue expectations regarding such practices,[3] protection measures, the rights of persons concerned, remedies and complaints.[4]

The AMF prefers a principles-based approach to implementing these expectations and therefore provides CAAs with the latitude necessary to determine the requisite strategies, policies, procedures and processes and apply them based on the nature, size and complexity of their activities.

1. Governance

Sound governance is crucial and constitutes the cornerstone of appropriate management by a CAA that ensures that consumers' rights under the Act are respected.

With this in mind, the AMF wants to ensure that CAAs implement and follow appropriate management practices while instilling and promoting a business culture based on ethical organizational behaviour and decision-making body accountability.

By business culture, the AMF means the common values and standards that characterize a business and influence its mindset and conduct and the actions of its personnel. A good business culture is therefore essential to maintaining consumer confidence, while a deficient corporate culture can cause significant damage to a business's reputation and serious harm to both the business and its various stakeholders.

For a CAA to be governed effectively and efficiently, a formal operating, supervisory and accountability framework must be implemented through policies, procedures and information systems that help to organize and monitor the way the CAA is managed. Effective and efficient governance also requires risk management and control processes to be implemented across the organization using a rigorous, coordinated approach.

CAAs interact, in particular, with financial institutions and manage consumers' personal data. Given the sensitivity and importance of the data held by CAAs, the AMF believes it is essential that they draw on the three lines of defence model to

1 Referred to as a "person concerned" in the *Credit Assessment Agents Act*, a "consumer" in this guideline means the person who is the subject of the credit report or the representative of that person.

2 *Credit Assessment Agents Act* (S.Q. 2020, c.21)

3 See sections 53 and 54 of the Act.

4 See section 28 *et seq.* of the Act.

- promote careful coordination among the risk management and control functions
- structure management of the risks associated with their activities subject to the Act
- meet the same standards as their main commercial partners

Specifically, the AMF is issuing the following expectations for observance of the provisions of the Act in order that CAAs may ensure compliance with those provisions and guarantee that consumers are able to fully exercise their rights.

The outsourcing of the various functions identified below should be disclosed to the AMF upon request.[5]

First line of defence

The first line of defence is a CAA's operational management. It is responsible for managing risks on a day-to-day basis because controls are designed, pilot-tested and integrated into systems and processes under its guidance. Its responsibilities should include:

- identifying, assessing, managing and controlling the risks related to the requirements of the Act
- guiding the development and implementation of internal control procedures
- overseeing the application of those procedures by their employees
- ensuring that activities are consistent with goals and objectives
- ensuring that activities are carried out in compliance with the Act

Operational managers should also take corrective actions to address process and control deficiencies.

Internal control is also a key component of an effective governance structure because it enables the detection of functional deficiencies that could be major sources of risk for a CAA. As a result, the constituent controls should be designed and operated to ensure that the CAA's key policies and processes are effective in ensuring that consumers' rights under the Act are respected.

These controls should, in particular, cover the following:

- The appropriate segregation of duties, where necessary
- Decision approval policies
- The presence of controls adapted to each appropriate level of the organization
- Internal control training, particularly for employees with key responsibilities
- Consistency of internal control overall and for each individual control

[5] Refer to sections 50 and 51 of the Act.

- Verifications and tests by independent parties (internal or external auditors) to determine the effectiveness of existing controls

Since staff at all levels of a CAA are involved in internal control, they should be made aware of the importance of the constituent controls and receive clear communications from senior management for that purpose. It is therefore essential to identify and compile the relevant information and provide it to the individuals concerned in a form and within a timeframe that allows them to properly fulfill their responsibilities.

The exercise of identifying, compiling and communicating information should help to ensure that internal controls adequately meet the objectives intended to ensure compliance with the Act, including the obligation to adhere to sound commercial practices. Specifically, the assessment of the effectiveness of internal controls should include the following:

- The control strategy adopted
- The control reference framework
- Completion status of the implementation or update
- Information regarding the resources needed to ensure internal control operating effectiveness
- A description of identified issues and deficiencies

Second line of defence

The risk management and compliance functions serve to ensure that internal controls are properly designed, effective and operating as intended and that the applicable laws, regulations and standards are complied with.

In order to be effective and properly fulfill their role in the second line of defence, the risk management and compliance functions should have sufficient authority, be appropriately positioned in the hierarchy, be independent from operational management, have the necessary resources to exercise their roles, and have unrestricted access to the decision-making bodies.

An effective risk management function in the second line of defence is independent from the risk-taking operational level and closely monitors material and emerging risks.

A compliance function[6] that is independent from the activities it oversees is one of the key components of a CAA's second line of defence and an essential foundation for appropriate management practices as it ensures that consumers' rights under the Act are respected.

Third line of defence

[6] A compliance function is not necessarily a specific unit within the CAA. The staff responsible for compliance may be involved in operational units and report to the management team responsible for the activity involved. However, where appropriate, it is important for those units to be able to report to the chief compliance officer or the individual responsible for that function, who should be independent from operational management.

An effective and efficient independent internal audit function constitutes the third line of defence of the governance framework, providing the CAA, using a risk-based approach, with independent, objective assurance and consulting services designed to add value and improve the organization's operations.

With respect to appropriate management practices and sound commercial practices, internal audit must assess the design, adequacy and operational effectiveness of processes and make appropriate recommendations to improve them. The goal is to provide the decision-making bodies with objective assurance that the processes are properly designed, operate as intended and achieve, in particular, the objectives of:

- promoting ethical organizational behaviour that reflects the fair treatment of consumers
- monitoring and reporting organizational performance
- communicating risk and control information to the appropriate areas of the CAA
- coordinating the activities of, and communicating information among, the decision-making bodies, the external auditors and the internal auditors[7]

Internal audit should also evaluate the effectiveness and relevance of risk management and compliance processes and internal controls and promote their continuous improvement, including the achievement of the organization's risk management, compliance and internal control objectives by the functions in the first and second lines of defence.

To effectively fulfil its role as the third line of defence, it is preferable that internal audit have direct and unrestricted access to the decision-making bodies in order to assert its independence and reinforce its objectivity within the CAA.

The three lines of defence model could, however, be adjusted to reflect how roles and responsibilities are allocated within the corporate group to which the CAA belongs, without limiting the CAA's responsibility in this regard and while satisfying the AMF's expectations set out in the section on outsourcing risk management.

[7] The INSTITUTE OF INTERNAL AUDITORS. Standard 2110.

2. Sound commercial practices

CAAs have a legal obligation to adhere to sound commercial practices.

The commercial practices, or conduct of business, of CAAs reflect their behaviour in their relationships with consumers—behaviour that should result in the fair treatment of consumers (FTC).

FTC draws on guidance issued by various international bodies.[8] It encompasses concepts such as ethical behaviour, acting in good faith and the prohibition of abusive practices. FTC involves, among other things:

- Offering services relating to consumers' rights under the Act in a way that pays due regard to the interests and needs of consumers
- Providing consumers with accurate, clear and sufficient information allowing them to make informed decisions
- Protecting the privacy of consumer information
- Processing consumer complaints in a fair and diligent manner
- Making sufficient resources available to consumers, including staff, to facilitate the timely exercise of their rights

Therefore, the AMF expects FTC to be an integral part of a CAA's business culture. Establishing an FTC culture would, among other things, help place consumers' interest at the centre of decisions and the conduct of business and ensure that all staff act ethically and with integrity in their dealings with consumers.

a. Communicating with consumers

CAAs should communicate information to consumers orally or in writing, in plain, simple and precise language, regardless of the means of communication. Such communications should be in French or English, according to each consumer's language preference. Moreover, CAAs should ensure that they have a sufficient number of employees who are properly trained to answer consumers' requests and questions.

For example, if a code or rating system is used in provided materials or technical terms are employed to communicate information, the AMF expects CAAs to explain what they mean in accordance with the good practices set out in this subsection.

A CAA should make means of communication available to consumers that enable them to contact the CAA quickly and efficiently. Such means of communication should be varied (telephone numbers, e-mail addresses, instant messaging, etc.) and easy to locate on all of the CAA's platforms (website, social networks).

[8] Including the principles on financial consumer protection developed jointly by the Organisation for Economic Co-operation and Development and the Financial Stability Board.

CAAs should also take appropriate measures to ascertain the identities of consumers they interact with. CAAs should not disclose a credit report if they are unable to properly ascertain a consumer's identity.

The AMF expects product and service advertising materials to be accurate, clear and not misleading.

b. Managing information in a credit report

CAAs should have a clear, up-to-date policy for managing information contained in a credit report.

Given the sensitive nature of such information, CAAs should have stringent information security standards in place for any data they receive, use and share. CAAs should also have effective processes for periodically reviewing the management of such information.

In addition, the AMF expects a CAA's privacy policy and procedures to draw on best practices and enable it to discharge its privacy obligations, including those under the *Act respecting the protection of personal information in the private sector.*[9]

CAAs should establish and apply an operating method that ensures that the information they communicate is up to date and accurate. To that end, CAAs should ensure that evaluations and reviews are conducted regularly to determine whether the agreements entered into with external providers are being complied with and, if necessary, to address any suspected or observed breaches of the terms of those agreements.

CAAs should have a robust process for validating any changes made to consumers' personal information (e.g., mailing address, telephone number).

c. Processing complaints

The AMF expects complaints to be processed fairly and diligently, following a process that is simple and readily accessible for consumers.

The complaints received by a CAA and the handling of those complaints are, among other things, key elements to consider in assessing the CAA's FTC performance.

The Act requires CAAs to do such things as keep a complaints register and adopt a complaint processing and dispute resolution policy.[10]

The AMF expects:

- the complaint process to take into account consumers' interests and ensure that complaints are handled in an objective and consistent manner
- the CAA to designate a complaints officer who has the authority and competence to perform the function and ensures, among other things, that the complaint processing

[9] *Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1

[10] *Credit Assessment Agents Act*, s. 35.

and dispute resolution policy is implemented, disseminated and complied with within the CAA

- staff responsible for processing complaints to have the necessary competencies to process the complaints assigned to them
- consumers to receive proper assistance throughout the processing of their complaint and be informed in a timely manner of the status of their complaint
- consumers not to be faced with constraints or administrative barriers and any need the institution has for additional information not to hinder or delay the complaint process
- the CAA to develop an overall picture of the complaints received in order to identify common causes and the issues to be resolved to ensure FTC

3. Operational risk management

The AMF expects a CAA to adequately manage operational risk related to its business model and the management strategy for such risk. Such management should take into account exposure to operational risks inherent in people, processes, systems or external events, as well as stakeholders' exposure to such risks.

Operational risk management should also identify situations where activities, processes or systems do not ensure FTC. For example, an information security breach caused by the accidental disclosure of consumers' personal information or a deliberate leak of confidential information could negatively affect FTC, which could ultimately harm a CAA's reputation.

Moreover, when a consumer reports that he or she has been, or believes he or she is, the victim of fraud or a related crime, including identity theft, a CAA should, after properly ascertaining the consumer's identity, demonstrate diligence and take appropriate action.

In terms of operational risk, the establishment of a culture that promotes sound risk management must necessarily emanate from the decision-making bodies and be adapted to reflect the extent of exposure to operational risks and, consequently, the requisite commitment of all levels of the organization to properly manage such risks.

Awareness-raising should also extend to external stakeholders, including service providers under material outsourcing arrangements,[11] since outsourcing exposes an organization to operational risks (e.g., exposure to cyber risk).

[11] An outsourcing arrangement that could have a significant impact on an institution's financial condition, its operations and, ultimately, its reputation is considered material.

4. Information and communications technology (ICT) risk management

CAAs should implement an ICT risk management approach that is robust and relies on sources, recommendations and standards emanating from recognized organizations such as the OECD, the G7, NIST, ISACA (COBIT) and ISO. In addition, CAAs should, among other things, ensure that the decision-making bodies promote a business culture based on ethical and secure conduct in using technology.

To that end, CAAs should have an appropriate risk-based framework ensuring information security and the physical security of all their technological infrastructures and information assets.

CAAs should implement their own taxonomies so that all types of ICT risks are identified. ICT risk categories that should be considered include information security, outsourcing, cloud computing, business continuity, crisis management, human resources, ICT operations and ethics. Once developed, this taxonomy should be communicated to those directly involved in risk assessment and control activities so that it may be used consistently in the identification and aggregation of ICT risks.

CAAs should clearly delineate the responsibilities of the information security function to ensure its independence and objectivity by, in particular, segregating it from ICT operational processes or implementing compensating controls where needed. This function should not be responsible for internal audit work.

CAAs should ensure that the following individuals are assigned:

- a member of senior management, such as a chief information security officer, to oversee the deployment of the framework ensuring information security and the physical security of the organization's technology infrastructures
- a member of senior management, such as a chief data officer, to oversee the approved framework for the collection, storage and use of data across the organisation

CAAs should maintain adequate capacity to anticipate, detect and recover from ICT-related operational incidents, including information security incidents.

Regarding consumers' rights under the Act, CAAs should, in particular:

- Define in their information security policy principles and rules for safeguarding the confidentiality, integrity and availability of consumers' information
- Define clear information security objectives for systems, ICT services, processes and people
- Apply the information security policy to all their activities while ensuring that the policy also covers information handled by external stakeholders within the CAA's scope
- Deploy controls for information assets (data, hardware and software) that are proportional to the criticality and sensitivity of those assets
- Conduct systematic testing to ensure that the controls in place are effective

The preparatory activities considered by CAAs for the management of ICT risks should, in particular, help to safeguard sensitive consumer data against disclosure, leaks or unauthorized access. They should also contribute to ICT environment resilience. These activities should cover, among other things, access controls, authentication, data integrity and confidentiality, activity recording and security event monitoring.

CAAs should take into account the preparation, processing and monitoring activities that need to be carried out to quickly mitigate negative impacts for consumers in the event of an incident or an actual crisis.

CAAs should use a rigorous process to periodically identify information assets and their vulnerabilities in order to appropriately associate risks with them.

CAAs should use a classification framework enabling the criticality of data and information assets (including those managed by external stakeholders) to be defined, as a minimum, according to their availability, integrity and confidentiality requirements. This classification framework should reflect the degree to which an information security incident affecting an information asset has the potential to adversely affect the CAA and consumers or other stakeholders.

CAAs should use ICT incident management processes with adequate resumption and recovery objectives, ensure appropriate and timely monitoring of activities to mitigate the risks recorded in the ICT risk register, and monitor the effectiveness of mitigation measures, along with the number of reported incidents in order to correct them when necessary. CAAs should also conduct specific analyses following a major incident to improve their response and recovery plans.

CAAs should also establish and maintain documentation and information enabling informed stakeholder decision-making regarding ICT risks. The documentation should include, in particular, a register, a description of the impact of ICT risks, a risk and control matrix and existing processes and structures for ICT risk management.

Moreover, CAAs should implement robust mechanisms enabling them to ensure that consumers' rights under the Act are respected. Activities to consider include identity and access management, training and awareness, network segregation and protection of network integrity, data security, protection of endpoint devices (e.g., laptops, tablets, smart phones), verification of software and microcode integrity, and technological protection solutions contributing to system and information asset resilience. Similarly, event and anomaly detection and logging, continuous information system monitoring and detection process monitoring should be considered.

CAAs should ensure that physical and logical access to information assets is restricted to users, processes, devices and activities authorized under their established security policies. Access rights should be granted based on such generally recognized principles as "need to know," "least privilege" or "segregation of duties" and only to authorized personnel and in such a manner as to prevent large data sets from being improperly accessed and security controls from being bypassed.

CAAs should subject their information security controls to various types of periodic independent assessments, tests and reviews as well as penetration testing.

CAAs should implement procedures and processes for reporting information security incidents to concerned parties, including the AMF and consumers, in accordance with existing requirements.

5. Outsourcing risk management

CAAs should identify the various risks related to outsourcing arrangements, particularly ICT risks, in order to be able to adequately assess and manage them.

Outsourcing is defined as delegating to a service provider, over a defined period, the performance and management of a function, activity or process that is or could be undertaken by the CAA itself. Any outsourcing arrangement entered into with a service provider operating outside Canada or that processes, stores or transfers data outside Canada is considered to be offshoring. Outsourcing or offshoring arrangements relating to consumers' rights under the Act must be disclosed to the AMF upon request.[12]

It is essential before entering into an outsourcing arrangement involving the protection measures and consumers' rights set out in the Act that CAAs assess the risks that could result from the use of outsourcing. This assessment should also cover the service provider's ability to provide quality service through components relating to financial, operational and reputational aspects.

The AMF expects CAAs' outsourcing arrangements to be drafted to include the terms governing the relationship, functions, obligations and responsibilities of the parties to the arrangement.

CAAs should monitor their outsourcing arrangements to ensure that commitments are met. In the AMF's view, ultimate responsibility for outsourcing arrangement compliance with the legal and regulatory requirements applicable to the outsourced activities remains with the CAAs even where those activities are performed and managed by service providers.

The AMF also expects CAAs to adequately manage the risks related to any material outsourcing arrangements entered into with the members of its group, if applicable.

Lastly, a CAA's reliance on service providers should not jeopardize its business continuity management.

In the context of outsourcing and cloud computing, CAAs should, in particular:

- Contractually secure their right to audit and their right to access the premises of the cloud computing service provider
- Mitigate supply chain outsourcing risks when suppliers outsource certain activities to other suppliers
- Ensure supplier compliance with security objectives and measures and performance expectations

While using the services of certain stakeholders may not constitute a form of outsourcing, many of those services are delivered using ICT or involve information that is potentially

[12] See sections 50 and 51 of the Act.

confidential. Such stakeholders may also be exposed to security incidents. CAAs should assess and appropriately manage the confidentiality breach, integrity breach and availability breach risks associated with the information processed by such third parties.

6. Business continuity

CAAs should adopt a strategy to ensure the continuity of critical business operations and the resumption of disrupted or interrupted business operations within reasonable time limits.

With this in mind, CAAs should assess the impact of operational incidents on their resources, operations and environment and determine the measures to be taken in light of this assessment.

It is therefore essential that CAAs develop a business continuity plan ("BCP") outlining the actions to be taken in the event of an operational incident that has an impact on critical operations. The BCP should, for example, define the procedures and systems required to restore the CAA's operations should its critical operations be disrupted. The BCP should be clear, easy to use, tested and updated regularly. It should also be accompanied by a communications plan. CAAs should notify the AMF as soon as possible when they activate their BCPs and also notify any other interested party that is likely to be affected by the situation.

CAAs should also identify their critical operations and major operational incidents that could disrupt, slow or interrupt them. They should also assess the extent to which critical operations are concentrated at a single site, their interdependence, and their reliance on the same resources, particularly with respect to staff, systems and service providers.

CAAs should consider a set of plausible events and scenarios, including cybersecurity events, in planning and testing disaster recovery and continuity plans.

CAAs should identify all potential individual points of failure in the ICT systems and the architecture of networks supporting consumers' rights under the Act in order to ensure that appropriate measures are taken to mitigate disruption risks.

CAAs should minimize business disruption risk by establishing appropriate processes to manage changes affecting ICT equipment (hardware and software) and procedures involved in ICT system development, delivery, support and maintenance.

To reduce business interruption risk stemming, for example, from the malevolent exploitation of software vulnerabilities, CAAs should establish a framework of secure practices and standards for programming, source code reviews and application security testing for their ICT systems supporting the application of consumers' rights under the Act. Any information and ICT system availability, integrity and confidentiality issues identified in applying such practices should be compiled, monitored and corrected.

The AMF expects a CAA to periodically verify the reliability of its BCP. The business continuity management process should be a dynamic one that takes into account any changes affecting the CAA, its stakeholders and its environment. The CAA should ensure that its service providers have robust BCPs aligned with the objectives of its own plan and do not introduce new unidentified risks for the CAA.

7. Supervision of appropriate management practices and sound commercial practices

In line with its wish to promote the establishment of appropriate management practices and sound commercial practices within CAAs, the AMF, in performing its supervisory activities, intends to assess the extent to which the principles in this guideline are being observed.

Consequently, the effectiveness and appropriateness of implemented strategies, policies and procedures and the quality of oversight and control exercised by the decision-making bodies will be assessed.

The management practices and commercial practices addressed in this guideline are constantly evolving. The AMF expects decision-making bodies of CAAs to inquire into best practices and apply them to the extent that they address their needs.

5.2.2 Publication

DÉCISION N° 2022-PDG-0053

Ligne directrice sur les saines pratiques commerciales

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») d'établir des lignes directrices destinées à tous les assureurs autorisés, à une catégorie seulement d'entre eux ou à une fédération dont de tels assureurs sont membres, conformément à l'article 463 de la *Loi sur les assureurs*, RLRQ, c. A-32.1 (la « LA »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les coopératives de services financiers, à une catégorie seulement d'entre elles, à des caisses, à une fédération dont de telles caisses sont membres ou à toutes les personnes morales faisant partie d'un groupe coopératif, conformément à l'article 565.1 de la *Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3 (la « LCSF »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les institutions de dépôts autorisées, à une catégorie d'entre elles seulement ou aux fédérations dont de telles institutions sont membres, conformément à l'article 42.2 de la *Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2 (la « LIDPD »);

Vu le pouvoir de l'Autorité d'établir des lignes directrices destinées à toutes les sociétés de fiducie autorisées ou à une catégorie d'entre elles seulement, conformément à l'article 254 de la *Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02 (la « LSFSÉ »);

Vu le pouvoir de l'Autorité d'établir une ligne directrice prévu aux articles 463 de la LA, 565.1 de la LCSF, 42.2 de la LIDPD et 254 de la LSFSÉ, qui appartient exclusivement à son président-directeur général, conformément à l'article 24 de la *Loi sur l'encadrement du secteur financier*, RLRQ, c. E-6.1;

Vu la publication pour consultation au Bulletin de l'Autorité (le « Bulletin ») le 21 octobre 2021 [(2021) vol. 18, n° 42, B.A.M.F., section 5.2.1] du projet de modification de la *Ligne directrice sur les saines pratiques commerciales* (la « ligne directrice »);

Vu les modifications apportées au projet de ligne directrice à la suite de cette consultation;

Vu le deuxième alinéa de l'article 463 de la LA, le troisième alinéa de l'article 565.1 de la LCSF, le deuxième alinéa de l'article 42.2 de la LIDPD et le deuxième alinéa de l'article 254 de la LSFSÉ qui prévoient que l'Autorité publie à son Bulletin les lignes directrices qu'elle établit après en avoir transmis une copie au ministre des Finances (le « Ministre »);

Vu le projet de la ligne directrice modifiée proposé par la Direction principale de l'encadrement des institutions financières, de la résolution et de l'assurance-dépôts ainsi que la recommandation du surintendant de l'encadrement de la solvabilité d'établir celle-ci;

En conséquence :

L'Autorité établit la *Ligne directrice sur les saines pratiques commerciales* modifiée, dans les versions française et anglaise, dont le texte est annexé à la présente décision, et en autorise la publication au Bulletin après en avoir transmis une copie au Ministre.

La *Ligne directrice sur les saines pratiques commerciales* modifiée prend effet le 17 novembre 2022.

Fait le 15 novembre 2022.

Louis Morisset
Président-directeur général

Ligne directrice sur les saines pratiques commerciales

(*Loi sur les assureurs*, RLRQ, c. A-32.1, art. 463 et 464)
(*Loi sur les coopératives de services financiers*, RLRQ, c. C-67.3, art. 565.1 et 566)
(*Loi sur les institutions de dépôts et la protection des dépôts*, RLRQ, c. I-13.2.2, art. 42.2 et 42.3)
(*Loi sur les sociétés de fiducie et les sociétés d'épargne*, RLRQ, c. S-29.02, art. 254 et 255)

L'Autorité des marchés financiers (l'« Autorité ») publie une mise à jour, en versions française et anglaise, de la *Ligne directrice sur les saines pratiques commerciales* (la « Ligne directrice ») publiée initialement en juin 2013. Cette Ligne directrice s'applique aux assureurs, coopératives de services financiers, sociétés de fiducie et autres institutions de dépôts autorisées.

Cette Ligne directrice modifiée fait suite à la consultation publique qui s'est déroulée du 21 octobre 2021 au 28 janvier 2022.

L'Autorité publie également ses réponses aux commentaires et observations reçus à l'égard des grands thèmes ci-après :

- l'éloignement de l'approche prudentielle basée sur les principes ;
- l'alourdissement de la charge en matière de conformité ;
- l'harmonisation souhaitée avec la Directive du Conseil canadien des responsables de la réglementation d'assurance et des Organismes canadiens de réglementation des services d'assurance;
- le partage des responsabilités entre les institutions financières et les intermédiaires.

Les réponses de l'Autorité aux commentaires et observations sur la base des grands thèmes ci-avant mentionnés sont disponibles sur le site Web de l'Autorité dans la section des consultations publiques.

La Ligne directrice modifiée prend effet immédiatement. Elle est publiée ci-après et est disponible sur le site Web de l'Autorité au www.lautorite.qc.ca.

Des renseignements additionnels peuvent être obtenus en s'adressant à :

François Dufour
Direction de l'encadrement prudentiel des institutions financières
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4673
Numéro sans frais : 1 877 525-0337
Courrier électronique : francois.dufour@lautorite.qc.ca

Le 17 novembre 2022

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE SUR LES SAINES PRATIQUES COMMERCIALES

Publication initiale : juin 2013
Mise à jour : novembre 2022

TABLE DES MATIÈRES

1. Les pratiques commerciales et le traitement équitable des clients

Les institutions financières ont l'obligation légale de suivre de saines pratiques commerciales[1].

Les pratiques commerciales ou la conduite des activités d'une institution financière[2] reflètent le comportement de l'institution dans le cadre de sa relation avec le client[3] avant la conclusion d'un contrat et jusqu'à la cessation de toutes les obligations contractuelles.

De saines pratiques commerciales contribuent notamment à une offre de produits[4] équitable et transparente. À l'inverse, lorsque les pratiques commerciales sont inadéquates, elles exposent les clients à des risques ou des situations susceptibles d'avoir un impact négatif sur ceux-ci. Suivre de saines pratiques commerciales implique de traiter les clients équitablement.

Le traitement équitable des clients s'inspire de principes fondamentaux et d'orientations énoncés par diverses instances internationales[5]. Il englobe des concepts comme le comportement éthique, la bonne foi et l'interdiction de pratiques abusives. Le traitement équitable des clients se manifeste à tous les stades du cycle de vie d'un produit et consiste notamment à :

- concevoir, commercialiser et offrir des produits en tenant compte des besoins et des intérêts des clients;
- communiquer au client, avant, pendant et après l'offre d'un produit une information précise, claire et adéquate lui permettant de prendre une décision éclairée;
- minimiser le risque que le produit offert ne soit pas adapté aux besoins et à la situation du client;
- traiter les demandes d'indemnité et les plaintes des clients équitablement et avec diligence;
- protéger la confidentialité des renseignements personnels des clients.

---

1 Loi sur les assureurs, RLRQ, c.- A-32.1, articles 50 et 51;
Loi sur les coopératives de services financiers, RLRQ, c.- C-67.3, articles 66.1 et 66.2;
Loi sur les sociétés de fiducie et les sociétés d'épargne, RLRQ, c.- S-29.02, articles 34 et 35;
Loi sur les institutions de dépôts et la protection des dépôts, RLRQ, c. I -13.2.2, articles 28.11 et 28.12.

2 Dans la présente ligne directrice, les termes « institution » et « institution financière » sont utilisés pour faire référence aux institutions financières visées par l'obligation légale de suivre de saines pratiques commerciales conformément aux lois précitées à la note 1. Par conséquent, ces termes n'incluent pas une fédération de sociétés mutuelles.

3 Bien que les lois habilitantes (précitées à la note 1) réfèrent précisément au concept de « clientèle », les termes « client » et « clients » sont utilisés dans le cadre de la présente ligne directrice. Il s'agit de concepts englobants qui visent tant le client actuel de l'institution financière que le client éventuel, et peuvent également inclure par exemple, une personne ayant un intérêt dans le produit vendu, tel que le bénéficiaire d'une police d'assurance, lorsque le contexte s'y prête.

4 Le terme « produit » utilisé dans la présente ligne directrice inclut également, lorsque le contexte s'y prête, un « service ».

5 Organisation de coopération et de développement économique, International Financial Consumer Protection Organisation, Conseil de stabilité financière, Association internationale des contrôleurs d'assurance, Comité de Bâle sur le contrôle bancaire, Organisation internationale des commissions de valeurs.

2. La culture d'entreprise

La culture d'entreprise est l'un des principaux vecteurs du comportement des membres du personnel au sein d'une institution. Elle réfère aux valeurs comme l'éthique et l'intégrité et aux normes communes qui caractérisent une entreprise et influencent la façon de penser ainsi que les actions des membres du personnel. Elle imprègne tant les décisions stratégiques de l'institution que la conduite des membres du personnel qui interagissent avec les clients.

Une culture d'entreprise axée sur le traitement équitable des clients crée un environnement qui favorise la confiance des clients et les relations à long terme avec ceux-ci. À l'inverse, une culture d'entreprise déficiente peut causer d'importants préjudices pour les clients et nuire à la réputation de l'institution jusqu'à un point où sa solvabilité pourrait être compromise.

L'institution financière dont la culture d'entreprise est axée sur le traitement équitable des clients :

- place l'intérêt des clients au centre de ses décisions et de la conduite de ses activités;
- identifie et gère les risques susceptibles de compromettre le traitement équitable des clients;
- veille à ce que les résultats en cette matière soient démontrés notamment au moyen d'indicateurs développés à cette fin;
- communique les résultats en cette matière aux personnes concernées par ceux-ci dans tous les paliers de l'organisation.

3. La responsabilité de l'institution financière

L'Autorité s'attend à ce que l'institution financière s'acquitte de son obligation de traiter équitablement les clients à tous les stades du cycle de vie des produits.

L'obligation qui incombe à l'institution financière de traiter équitablement les clients subsiste bien qu'il puisse y avoir des intermédiaires[6] qui interviennent dans l'offre des produits de l'institution financière et que ces derniers aient des obligations qui leur soient propres.

Ainsi, l'institution financière obtient l'assurance raisonnable que les actes posés par les intermédiaires et les autres personnes agissant pour son compte et intervenant dans l'offre de ses produits lui permettent de s'acquitter de son obligation de traiter équitablement les clients.

Par ailleurs, lorsque l'institution financière impartit certaines activités, elle en demeure entièrement responsable[7].

6 Les intermédiaires sont les personnes autorisées à offrir des produits et services financiers conformément à la Loi sur la distribution de produits et services financiers, RLRQ, c. D-9.2.

7 Autorité des marchés financiers, Ligne directrice sur la gestion des risques liés à l'impartition, avril 2010.

4. Les relations de l'institution financière avec les intermédiaires

L'Autorité s'attend à ce que l'institution financière établisse avec les intermédiaires des relations d'affaires qui lui permettent de s'acquitter de son obligation de traiter équitablement les clients.

Dans le cadre des relations de l'institution financière avec les intermédiaires, l'Autorité s'attend à ce que :

- les critères de sélection des intermédiaires permettent d'identifier ceux qui sont autorisés à agir et qui disposent des compétences et des ressources appropriées, et à ce qu'un suivi soit effectué pour s'assurer du maintien de ces critères;
- les ententes conclues définissent clairement les attentes de l'institution financière à l'égard des intermédiaires relativement au traitement équitable des clients;
- les redditions de compte, les indicateurs et les contrôles mis en place soient modulés en fonction des risques et des particularités propres à chaque intermédiaire[8] et permettent à l'institution financière d'obtenir l'assurance raisonnable que l'intermédiaire répond à ses attentes en matière de traitement équitable des clients.

  Entre autres, l'institution financière :

  - s'assure que l'intermédiaire dispose des moyens lui permettant de fournir aux clients, au moment opportun, l'information nécessaire à une prise de décision éclairée;
  - prévoit la mise en place de mesures permettant de garantir aux clients un niveau de service adéquat après la conclusion d'un contrat;
  - considère que les contrôles mis en place par l'intermédiaire lui permettent d'identifier les ventes, opérations et pratiques inadéquates envers les clients et se satisfait des correctifs apportés, lorsqu'ils s'avèrent requis;
  - obtient de l'intermédiaire l'information pertinente lui permettant de revoir, le cas échéant, la conception de ses produits, la définition des groupes de clients ciblés ou les stratégies de distribution utilisées;
  - obtient de l'intermédiaire l'information pertinente relative aux plaintes reçues quant à ses produits ou à leur distribution, et ce, afin d'avoir un portrait complet de l'expérience des clients et d'identifier les enjeux en matière de traitement équitable de ces derniers.

[8] Par exemple, les redditions de compte, les indicateurs et les contrôles tiennent compte de la responsabilité qui incombe à l'assureur relativement à un distributeur (art. 65 de la Loi sur les assureurs).

5. Résultats attendus en matière de traitement équitable des clients

5.1 Gouvernance

L'Autorité s'attend à ce que les instances décisionnelles de l'institution financière aient un leadership affirmé afin de faire du traitement équitable des clients un élément central de la culture d'entreprise.

Les risques de pratiques inadéquates envers les clients sont moins facilement quantifiables et sont plus difficiles à contrôler par des outils de conformité standards, d'où l'importance d'une culture d'entreprise axée sur le traitement équitable des clients.

Il appartient au conseil d'administration de promouvoir une culture d'entreprise axée sur le traitement équitable des clients et les saines pratiques commerciales, et à la haute direction de les intégrer dans le cadre de gestion des risques de l'institution financière.

Rôles et responsabilités du conseil d'administration[9]

- Veiller à l'établissement de comités pour surveiller l'évolution de la culture d'entreprise et les risques de pratiques inadéquates pouvant nuire au traitement équitable des clients;
- Veiller à ce que les programmes de rémunération et de gestion de la performance incluant les incitatifs octroyés par l'institution financière aux membres du personnel, aux intermédiaires ou aux autres personnes agissant pour le compte de l'institution et intervenant dans l'offre de ses produits tiennent compte du traitement équitable des clients;
- Veiller à ce que le code d'éthique de l'institution préserve et renforce la culture d'entreprise et permette de maintenir de hauts standards en matière d'éthique et d'intégrité, dès l'embauche et de façon continue;
- Examiner la performance de l'institution en matière de traitement équitable des clients en lien avec les objectifs et stratégies fixés et, le cas échéant, veiller à ce que les correctifs nécessaires soient apportés.

[9] Loi sur les assureurs, RLRQ, c.- A-32.1, article 94;
Loi sur les coopératives de services financiers, RLRQ, c- C-67.3, articles 66.1 et 99;
Loi sur les institutions de dépôts et la protection des dépôts, RLRQ, c. I-13.2.2, article 28.38;
Loi sur les sociétés de fiducie et les sociétés d'épargne, RLRQ, c.- S-29.02, article 75.

Rôles et responsabilités de la haute direction

- Voir au développement d'objectifs, de stratégies, de politiques, de processus et de procédures cohérents avec les valeurs de l'institution et permettant l'atteinte des résultats attendus en matière de traitement équitable des clients;
- Voir à l'établissement de mécanismes de contrôle pour :
  - repérer et traiter tout écart par rapport aux objectifs, stratégies, politiques, processus et procédures;
  - s'assurer que les membres du personnel agissent en cohérence avec les valeurs de l'institution en matière de traitement équitable des clients;
  - repérer et réagir promptement à tout risque ou situation susceptible de nuire au traitement équitable des clients;
  - générer une information à l'intention du conseil d'administration qui soutient le suivi, la mesure de la performance[10] et un processus d'amélioration continue de l'institution en matière de traitement équitable des clients.
- Voir à ce que les membres du personnel qui offrent des produits soient formés, périodiquement et selon les besoins, relativement aux politiques, processus et procédures établis en matière de traitement équitable des clients;
- Voir à ce que la gestion intégrée des risques de l'institution prenne en considération les risques et les pratiques commerciales susceptibles de nuire au traitement équitable des clients;
- Voir à ce que les actions appropriées soient prises pour corriger les pratiques des membres du personnel qui vont à l'encontre du traitement équitable des clients.

[10] Ainsi, au-delà du taux de satisfaction des clients ou du nombre de plaintes reçues, les indicateurs utilisés par l'institution devraient permettre de mesurer l'atteinte des résultats attendus en matière de traitement équitable des clients à tous les stades du cycle de vie des produits.

5.2 Traitement des conflits d'intérêts

L'Autorité s'attend à ce que tout conflit d'intérêts réel ou potentiel soit évité ou géré de façon à assurer le traitement équitable des clients.

Une situation de conflit d'intérêts peut notamment découler des programmes de rémunération et de gestion de la performance mis en place ou des relations établies entre l'institution financière et l'intermédiaire ou toute autre personne agissant pour son compte et intervenant dans l'offre de ses produits.

Une situation de conflit d'intérêts peut entraîner une vente, une opération ou une pratique inadéquate ou peut avoir une incidence sur la qualité des services fournis ou sur la prestation des conseils offerts, le cas échéant.

L'institution devrait donc identifier et évaluer régulièrement les risques de pratiques pouvant nuire au traitement équitable des clients qui peuvent résulter des situations de conflits d'intérêts.

Attentes pour parvenir à ce résultat

- Donner préséance à l'intérêt des clients;
- Prendre toutes les mesures raisonnables pour repérer les conflits d'intérêts réels ou potentiels;
- Éviter tout conflit d'intérêts réel ou potentiel ne pouvant pas être géré de façon à assurer le traitement équitable des clients;
- Démontrer que des contrôles ont été mis en place afin que les conflits d'intérêts puissent être gérés de façon à assurer le traitement équitable des clients;
- Divulguer par écrit au client concerné tout conflit d'intérêts réel ou potentiel qui pourrait raisonnablement avoir une incidence, dans les circonstances, sur l'offre de produits ou les décisions du client. Cette divulgation est effectuée au moment opportun et elle n'est pas suffisante à elle seule pour considérer que le conflit d'intérêts a été adéquatement géré;
- S'assurer, lorsqu'on s'appuie entre autres sur la divulgation du conflit d'intérêts, que cette divulgation permet au client d'apprécier la nature et la portée du conflit d'intérêts, son incidence potentielle sur les services fournis, le risque qu'il pourrait poser pour lui et la façon dont il est géré;
- Aviser le client de tout changement significatif qui survient relativement à la divulgation du conflit d'intérêts qui lui a déjà été transmise;
- Documenter chaque situation de conflit d'intérêts qui survient et la façon dont l'institution l'a gérée. L'information colligée devrait permettre d'illustrer l'importance du préjudice qu'un tel conflit d'intérêts peut poser au client.

5.3 Conception des produits

L'Autorité s'attend à ce que l'institution financière tienne compte des besoins et des intérêts communs des différents groupes de clients ciblés lors de la conception des produits.

La conception des produits inclut le développement de nouveaux produits et la modification importante à des produits existants. Le fait, pour l'institution financière, de ne pas tenir compte des besoins et des intérêts communs des différents groupes de clients ciblés lors de la conception des produits peut accroître le risque d'offres inadéquates.

Attentes pour parvenir à ce résultat

- La conception des produits s'appuie sur l'utilisation d'une information adéquate permettant d'identifier les besoins et les intérêts des clients;
- La conception des produits incluant la sélection de produits de tiers implique qu'il y ait une évaluation appropriée des principales caractéristiques du produit[11] ainsi que des documents d'information qui seront transmis aux clients, et ce, par des membres du personnel de l'institution[12] possédant les compétences nécessaires à une telle évaluation;
- Le processus d'approbation d'un produit permet :
    - de définir le groupe de clients ciblé auquel le produit est susceptible de convenir;
    - d'offrir un produit qui procure les avantages et caractéristiques raisonnablement attendus du groupe de clients ciblé;
    - d'identifier et de gérer les risques que le produit pourrait poser pour le groupe de clients ciblé;
    - de tenir compte des modifications aux lois et règlements applicables, des évolutions technologiques ou des changements aux conditions du marché;
- La définition du groupe de clients ciblé implique d'identifier les besoins et les intérêts communs desdits clients. Le niveau de détail des critères utilisés par l'institution pour définir un groupe de clients ciblé dépend du produit (p. ex. : nature, caractéristiques, complexité, niveau de risque) et permet de déterminer quels sont les clients qui appartiennent à ce groupe et quels sont ceux pour lesquels le produit est susceptible de ne pas convenir.

[11] P. ex. : Pour des produits de dépôts, l'évaluation des caractéristiques du produit pourrait tenir compte de critères tels que l'accessibilité, le rendement et la sécurité.

[12] P. ex. : Conformité, gestion intégrée des risques, finances, ventes, fiscalité, actuariat, affaires juridiques.

- Le contrôle exercé à l'égard d'un produit[13] :
  - permet de s'assurer que les principales caractéristiques du produit continuent de répondre aux besoins et intérêts du groupe de clients ciblé, et ce, en s'appuyant sur de l'information suffisante, pertinente et claire[14];
  - permet, s'il y a lieu, de prendre les mesures qui s'imposent :
    - pour adapter le produit aux besoins et intérêts changeants du groupe de clients ciblé[15];
    - pour s'assurer que les clients comprennent le produit et ses principales caractéristiques;
    - pour revoir la définition du groupe de clients ciblé.

13 S'applique également aux produits qui ne sont plus offerts, mais qui sont toujours détenus par des clients (par exemple, des investissements dans certains fonds distincts). Le contrôle exercé permet de s'assurer que les clients reçoivent une information continue nécessaire à une prise de décision éclairée.

14 P. ex. : information régulière en provenance des membres du personnel et des intermédiaires qui offrent le produit; information en provenance du service du contrôle de la qualité, du service de traitement des demandes d'indemnité, du service de traitement des plaintes, de l'analyse des produits concurrents et des méthodes d'évaluation de la satisfaction des clients. Par ailleurs, certains indicateurs dans le secteur de l'assurance tels qu'un taux élevé de refus des demandes d'indemnités ou un faible taux de demandes d'indemnités peuvent indiquer que le produit ne répond pas aux besoins et aux intérêts du groupe de clients ciblé.

15 P. ex. : voir à ce que les exclusions prévues à un contrat d'assurance demeurent pertinentes et soient rédigées de façon compréhensible pour le client. Considérer la conjoncture économique afin de prendre en compte l'évolution du taux d'endettement des clients.

5.4 Commercialisation des produits

L'Autorité s'attend à ce que les stratégies de distribution de l'institution financière tiennent compte des besoins et des intérêts des différents groupes de clients ciblés et soient adaptées aux produits.

L'institution financière est responsable des stratégies de distribution qu'elle utilise pour ses produits et en assure la surveillance.

Attentes pour parvenir à ce résultat

- Le choix des stratégies de distribution pour un produit s'appuie sur l'utilisation d'une information adéquate pour évaluer les besoins et intérêts du groupe de clients ciblé et est adapté au niveau de complexité du produit;
- Les membres du personnel, les intermédiaires et les autres personnes qui agissent pour le compte de l'institution et qui interviennent dans l'offre de ses produits reçoivent l'information pertinente sur ces derniers et les formations appropriées. Les caractéristiques des produits et des groupes de clients ciblés sont maîtrisées adéquatement;
- Les indicateurs utilisés et les contrôles exercés sur les stratégies de distribution permettent :
    - d'évaluer la performance des différentes stratégies de distribution par rapport aux résultats attendus en matière de traitement équitable des clients et de prendre les mesures correctives, lorsque requis;
    - de s'assurer que les stratégies de distribution utilisées pour un produit continuent de répondre aux besoins du groupe de clients ciblé et ne risquent pas de nuire à leurs intérêts.

5.5 Publicité relative aux produits

L'Autorité s'attend à ce que la publicité relative aux produits soit exacte, claire et non trompeuse.

Avant de diffuser une publicité, l'institution financière devrait prendre les mesures qui s'imposent pour s'assurer qu'elle soit exacte, claire et non trompeuse.

Attentes pour parvenir à ce résultat

- La publicité relative aux produits fait l'objet d'une révision par des personnes autres que celles qui l'ont conçue, et ce, avant d'être diffusée;
- La publicité :
  - est facile à comprendre;
  - identifie clairement l'institution financière;
  - reflète adéquatement les avantages que le groupe de clients ciblé peut raisonnablement attendre du produit;
  - met en évidence les informations ou les éléments essentiels à une prise de décision éclairée de la part des clients;
  - permet une bonne compréhension du produit et ne porte pas à confusion.
- La publicité est présentée dans un format qui en facilite la lecture et la compréhension;
- Les statistiques utilisées sont pertinentes au produit. La source des statistiques utilisées est mentionnée, le cas échéant;
- Les témoignages utilisés sont authentiques et si l'institution paie pour obtenir un témoignage, une mention à cet effet y apparaît;
- Si l'institution constate qu'une publicité est inexacte, qu'elle porte à confusion ou qu'elle s'avère trompeuse, elle la retire sans délai et prend toute autre mesure nécessaire, le cas échéant, pour corriger la situation.

5.6 Information destinée au client avant ou au moment de l'offre d'un produit

L'Autorité s'attend à ce que le client dispose d'une information qui lui permet, avant ou au moment de l'offre d'un produit, d'être adéquatement informé afin de prendre une décision éclairée.

L'information devrait permettre au client de comprendre le produit et ses principales caractéristiques et l'aider à évaluer s'il répond à ses besoins et intérêts.

Le degré de précision de l'information requise varie notamment en fonction de la nature et du niveau de complexité du produit.

Attentes pour parvenir à ce résultat

- L'information destinée au client :
  - est à jour et facilement accessible;
  - est rédigée dans un langage clair et simple de façon à ne pas l'induire en erreur[16] et est présentée dans un format qui en facilite la lecture et la compréhension;
  - met l'accent sur la qualité plutôt que sur la quantité d'information;
  - identifie clairement le nom de l'institution et fournit les coordonnées pour la joindre;
  - met en évidence et explique clairement les principales caractéristiques du produit[17] importantes pour la conclusion ou l'exécution du contrat, y compris les conséquences pour le client advenant le non-respect des conditions;
  - fait mention de ses droits et obligations, y compris tout droit de résiliation ou de résolution;
  - fait mention des coordonnées du service de traitement et de règlement des demandes d'indemnités[18] ;
  - fait mention des coordonnées du service de traitement des plaintes et de règlement des différends ainsi que la façon d'accéder au résumé de la politique de traitement des plaintes et de règlement des différends.

[16] Lorsque l'usage d'un vocabulaire technique, complexe ou difficile à comprendre ne peut pas être évité, rendre accessible des outils ou tout autre moyen afin d'aider le client à mieux comprendre l'information qui lui est transmise.

[17] P. ex. : pour les produits d'assurance, le type de contrat, les protections offertes, les conditions d'admissibilité, les risques couverts, les exclusions, les limitations, les franchises, le montant de la prime. Pour les produits de crédit, le taux d'intérêt, les frais et les charges, le coût total, la durée, les modalités de remboursement, la nature des garanties requises, etc.

[18] N'est applicable qu'aux assureurs autorisés en vertu de la Loi sur les assureurs.

5.7 Offre de produits d'une institution de dépôts[19]

L'Autorité s'attend à ce que l'institution de dépôts évalue si le produit offert convient au client.

Les politiques, processus, procédures et contrôles de l'institution de dépôts devraient permettre de s'assurer que le produit offert convient au client compte tenu de sa situation, notamment ses besoins financiers[20].

Attentes pour parvenir à ce résultat

- La nature des renseignements recueillis dépend de la situation du client[21] et du type de produit offert[22] ;
- L'analyse des renseignements recueillis permet de connaître le client, de comprendre sa situation et d'évaluer si le produit offert lui convient.

19 Coopératives de services financiers, sociétés de fiducie et autres institutions de dépôts autorisées.

Toute offre de produits encadrée par la Loi sur la distribution de produits et services financiers n'est pas visée par la présente section.

20 P. ex. : les politiques, processus, procédures, contrôles et systèmes d'information en matière d'octroi de crédit devraient permettre d'identifier, de contrôler ou d'atténuer les risques importants pour le client notamment en ce qui concerne les produits de crédit inadaptés et d'éviter, dans la mesure du possible, les problèmes de remboursement et leur corollaire, le surendettement.

21 L'évaluation de la situation du client, notamment ses besoins financiers peut nécessiter de prendre en considération différents éléments, par exemple : ses objectifs, sa situation financière, sa capacité de remboursement, sa tolérance au risque, son horizon de placement, ses autres engagements.

22 Caractéristiques, frais, risques et avantages pour les clients.

5.8 Information destinée au client après l'achat d'un produit

L'Autorité s'attend à ce que le client dispose d'une information qui lui permet d'être adéquatement informé, au moment opportun, afin de prendre des décisions éclairées quant au produit détenu.

L'information destinée au client après l'achat d'un produit lui est transmise au moment opportun et lui permet notamment de déterminer si le produit qu'il détient continue de répondre à ses besoins et intérêts.

Attentes pour parvenir à ce résultat

L'information destinée au client :

- est rédigée dans un langage clair et simple de façon à ne pas l'induire en erreur et est présentée dans un format qui en facilite la lecture et la compréhension;
- lui rappelle les options qu'il peut exercer;
- l'avise des changements au contrat ou des changements liés à l'exécution de celui-ci, des impacts de ces changements, de ses droits et obligations et obtient, lorsque requis, son consentement;
- l'avise de la survenance d'événements tels que :
    - la date de renouvellement du contrat ou la date de sa reconduction automatique;
    - la fin d'une période promotionnelle;
    - une date d'échéance de paiement au-delà de laquelle des frais lui seront imposés;
    - le remplacement du produit ou la résiliation anticipée du contrat;
    - un transfert de portefeuille;
    - des modifications à la législation applicable ou des changements aux conditions du marché qui pourraient influer sur les principales caractéristiques du produit;
    - tout changement organisationnel ou opérationnel de l'institution susceptible d'avoir un impact sur les produits qu'il détient ou les services qui lui sont fournis[23].

Les communications périodiques rappellent au client l'importance de revoir ses besoins en fonction de l'évolution de sa situation personnelle afin de s'assurer que le produit qu'il détient lui convient toujours.

L'institution prend les mesures nécessaires pour que le client reçoive un service continu et adéquat.

[23] P. ex. : advenant la fermeture ou la conversion de succursales ou de guichets automatiques, l'institution financière communique avec ses clients dans un délai préalable raisonnable et les informe des alternatives qui s'offrent à eux.

Lorsque le client souhaite remplacer ou substituer un produit, résilier un contrat, ou encore changer d'institution, les procédures en place au sein de l'institution facilitent de telles opérations.

5.9 Traitement et règlement des demandes d'indemnités[24]

L'Autorité s'attend à ce que les demandes d'indemnités soient traitées avec diligence et réglées équitablement, selon un processus simple et facilement accessible pour les clients.

Le traitement et le règlement des demandes d'indemnités sont des étapes importantes dans la relation d'un assureur avec ses clients.

Attentes pour parvenir à ce résultat

- Lors du dépôt d'une demande d'indemnités, le client est informé des principales étapes du traitement de celle-ci et des délais anticipés pour son règlement[25];
- Le client est informé de manière adéquate et en temps opportun du statut de sa demande d'indemnité;
- Les demandes d'informations additionnelles de la part de l'institution, associées au traitement d'une demande d'indemnité, sont cohérentes avec les risques couverts et évitent d'entraver ou de retarder le processus de traitement;
- Le client est informé, lorsque sa demande d'indemnités ne peut être traitée à l'intérieur du délai prévu, de la cause du délai additionnel et du moment où le traitement sera complété;
- Le client se voit expliquer clairement et avec diligence les facteurs déterminants dans l'établissement de l'indemnité (p. ex. : la dépréciation, la négligence) et, le cas échéant, les motifs de refus total ou partiel de sa demande d'indemnité. Le tout est confirmé par écrit au client et la possibilité de demander une révision de la décision lui est offerte;
- Les décisions relatives aux indemnités tiennent compte de l'intérêt des clients et sont rendues de manière objective et cohérente;
- Le processus de révision d'une décision relative à une indemnité est simple et sans lourdeur administrative;
- Le client est informé qu'il peut s'adresser au service de traitement des plaintes et de règlement des différends s'il est insatisfait du traitement de sa demande d'indemnités;
- Les membres du personnel chargé du traitement et du règlement des demandes d'indemnités connaissent et respectent la procédure de l'institution relative au traitement et règlement des demandes d'indemnités. Ils sont en mesure de fournir une information appropriée aux clients, de les assister adéquatement dans la présentation de leur demande d'indemnités pendant tout le processus de traitement et possèdent les compétences nécessaires selon le type de produit.

[24] Uniquement applicable aux assureurs autorisés en vertu de la Loi sur les assureurs.

[25] Le cas échéant, la procédure d'un assureur de dommages crée un environnement favorable à ce que l'expert en sinistre respecte les obligations qui lui sont imposées en vertu de la Loi sur la distribution de produits et services financiers.

5.10 Traitement des plaintes et règlement des différends

L'Autorité s'attend à ce que les plaintes soient traitées équitablement et avec diligence, selon un processus simple et facilement accessible pour les clients.

Les plaintes reçues par une institution financière et le traitement afférent effectué constituent, entre autres, des éléments importants permettant d'évaluer la performance de cette dernière en matière de traitement équitable des clients.

En vertu des dispositions législatives prévues aux lois administrées par l'Autorité, l'institution financière doit notamment tenir un registre des plaintes et adopter une politique de traitement des plaintes et de règlement des différends[26].

Attentes pour parvenir à ce résultat

- Le processus de traitement des plaintes tient compte des intérêts des clients et permet que les plaintes soient traitées de manière objective et cohérente;
- L'institution désigne un responsable du traitement des plaintes détenant l'autorité et la compétence nécessaires à l'exercice de ses fonctions et qui assure notamment la mise en œuvre, la diffusion et le respect de la politique de traitement des plaintes et de règlement des différends au sein de l'institution;
- Les membres du personnel chargés du traitement des plaintes possèdent les compétences nécessaires pour traiter les plaintes qui leur sont assignées;
- Les clients sont adéquatement assistés tout au long du processus de traitement de leur plainte et sont informés en temps opportun du statut de leur plainte;
- Les clients ne se heurtent pas à des contraintes ou obstacles administratifs et les compléments d'information requis par l'institution évitent d'entraver ou de retarder le processus de traitement d'une plainte;
- L'institution développe une vision d'ensemble des plaintes reçues afin d'identifier les causes communes et les enjeux à résoudre pour permettre un traitement équitable des clients.

[26] Loi sur les assureurs, articles 50, 52 à 58;
Loi sur les coopératives de services financiers, articles 66.1, 131.1 à 131.7;
Loi sur les sociétés de fiducie et les sociétés d'épargne, articles 34, 36 à 42;
Loi sur les institutions de dépôts et la protection des dépôts, articles 28.11, 28.13 à 28.19.

5.11 Protection des renseignements personnels

L'Autorité s'attend à ce que l'institution financière détermine et mette en place les mesures lui permettant de se conformer aux obligations qui lui incombent en matière de protection des renseignements personnels.

L'institution financière est responsable de la protection des renseignements personnels qu'elle détient.

La pérennité de ses opérations dépend, entre autres, de la confiance des clients à cet égard et ces derniers s'attendent à ce que leurs renseignements personnels, détenus par l'institution financière ou par une autre personne pour le compte de l'institution, demeurent confidentiels et soient protégés en conséquence.

Ainsi, les politiques, processus et procédures de l'institution en matière de protection des renseignements personnels s'inspirent des meilleures pratiques et lui permettent de s'acquitter de ses obligations en la matière, notamment celles qui découlent de la *Loi sur la protection des renseignements personnels dans le secteur privé*[27].

L'Autorité s'attend également à ce que l'institution financière évalue l'impact potentiel des risques nouveaux ou émergents pouvant menacer la confidentialité des renseignements personnels qu'elle détient et prend des mesures appropriées pour les atténuer.

[27] RLRQ, c. P-39.1.

AUTORITÉ DES MARCHÉS FINANCIERS

SOUND COMMERCIAL PRACTICES GUIDELINE

Initial publication: June 2013
Updated: November 2022

TABLE OF CONTENTS

1. Commercial practices and the fair treatment of clients

Financial institutions have a legal obligation to adhere to sound commercial practices.[1]

The commercial practices, or conduct of business, of financial institutions[2] reflect their behaviour in their relationships with clients,[3] from before a contract is entered into until all the institution's obligations under the contract are fulfilled.

Sound commercial practices help ensure, in particular, that a product offer[4] is fair and transparent. Conversely, unsound commercial practices expose clients to risks or situations that could negatively impact them. Adhering to sound commercial practices entails treating clients fairly.

The fair treatment of clients (FTC) is based on core principles and guidance published by various international bodies.[5] It encompasses concepts such as ethical behaviour, acting in good faith and the prohibition of abusive practices. FTC manifests itself at every stage of a product's life cycle and involves, among other things:

- Developing, marketing and offering products in a way that pays due regard to the needs and interests of clients
- Providing clients with accurate, clear and sufficient information, before, when and after a product is offered, allowing them to make an informed decision
- Minimizing the risk that the product offered is not suited to the client's needs and circumstances
- Examining client claims and complaints in a fair and timely manner
- Protecting the privacy of client information

1 Insurers Act, CQLR, c. A-32.1, sections 50 and 51

Act respecting financial services cooperatives, CQLR, c. C-67.3, sections 66.1 and 66.2

Trust Companies and Savings Companies Act, CQLR, c. S-29-02, sections 34 and 35

Deposit Institutions and Deposit Protection Act, CQLR, c. I-13.2.2, sections 28.11 and 28.12

2 In this guideline, the terms "institution" and "financial institution" refer to the financial institutions that are subject to the legal obligation to adhere to sound commercial practices in accordance with the statutes listed in Note 1. Consequently, these terms do not include a federation of mutual insurance associations.

3 Although the enabling statutes (supra note 1) refer specifically to the notion of "clientele," the terms "client" and "clients" are also used in this guideline. These broad notions cover both current and potential clients of the financial institution and may also include, for example, a person with an interest in the product sold, such as the beneficiary of an insurance policy, where appropriate for the context.

4 In this guideline, the term "product" also includes, where appropriate for the context, a "service".

5 The Organisation for Economic Co-operation and Development, the International Financial Consumer Protection Organisation, the Financial Stability Board, the International Association of Insurance Supervisors, the Basel Committee on Banking Supervision, the International Organization of Securities Commissions.

2. Business culture

Business culture is one of the main vectors of staff behaviour within an institution. It refers to the common values (e.g., ethics and integrity) and standards that characterize a business and influence the mindset and actions of its entire staff. It informs the institution's strategic decisions and the conduct of client-facing staff.

An FTC-centric business culture creates an environment that fosters client confidence and long-term client relationships. Conversely, a deficient business culture can cause serious harm to clients and damage the reputation of the institution to the point of compromising its solvency.

A financial institution with an FTC-centric business culture:

- Places clients' interests at the centre of its decisions and the conduct of its business
- Recognizes and manages risks that could compromise FTC
- Ensures that FTC outcomes are demonstrated, including through indicators developed for this purpose
- Communicates FTC outcomes to the persons concerned at all levels of the organization

3. Responsibility of the financial institution

The AMF expects financial institutions to fulfill their FTC obligation at all stages of the product life cycle.

A financial institution's FTC obligation continues to apply even though some intermediaries[6] involved in offering the financial institution's products may have their own obligations.

Financial institutions therefore obtain reasonable assurance that the actions of intermediaries and any other persons acting on its behalf who are involved in offering their products enable them to discharge their FTC obligation.

Moreover, financial institutions remain fully responsible for any activities that may be outsourced by them.[7]

6 Intermediaries are the individuals and firms authorized to offer financial products and services pursuant to the Act respecting the distribution of financial products and services, CQLR, c. D-9.2.

7 Autorité des marchés financiers, Outsourcing Risk Management Guideline, April 2010.

4. Financial institutions' relationships with intermediaries

The AMF expects financial institutions to establish business relationships with intermediaries that enable them to discharge their FTC obligation.

As part of financial institutions' relationships with intermediaries, the AMF expects:

- Criteria for selecting Intermediaries to enable the identification of intermediaries with the authorization to act and the appropriate competencies and resources, and follow-up to be performed to ensure the criteria are maintained
- Agreements entered into to clearly set out the financial institution's expectations for intermediaries with regard to FTC
- Reporting, indicators and controls put in place to be adjusted based on the risks specific to and characteristics of each intermediary[8] and to allow the financial institution to obtain reasonable assurance that the intermediary is meeting its expectations with regard to FTC

Among other things, the financial institution:

- Ensures that the intermediary has the means to provide clients with timely information necessary for enlightened decision-making
- Provides for the implementation of measures guaranteeing clients an appropriate level of service after they enter into a contract
- Considers the controls put in place by the intermediary sufficient to identify inappropriate sales, transactions and practices in respect of clients and is satisfied with any corrective action, where required
- Obtains relevant information from the intermediary enabling it to review, if necessary, its product designs, target client group definitions or distribution strategies
- Obtains relevant information from the intermediary about the complaints it has received regarding its products or their distribution so the financial institution can obtain a complete picture of the client experience and identify any FTC-related issues

[8] For example, reporting, indicators and controls include the insurer's liability with respect to a distributor (s. 65 of the Insurers Act).

5. Expected FTC outcomes

5.1 Governance

The AMF expects financial institutions' decision-making bodies to exercise strong leadership in making FTC a core component of their business culture.

Since risks of inappropriate practices with clients are harder to quantify and monitor using standard compliance tools, it is important to establish an FTC-centric business culture.

The board of directors is responsible for promoting an FTC-centric business culture and sound commercial practices, and senior management is responsible for ensuring that that culture and those practices are reflected in the financial institution's risk management framework.

Roles and responsibilities of the board of directors[9]

- Ensure that committees are established to monitor changes in the business culture and the risks of inappropriate practices that could adversely affect FTC
- Ensure that compensation and performance management programs, including incentives granted by the financial institution to staff, intermediaries or other persons acting on behalf of the institution who are involved in offering its products, take FTC into account
- Ensure that the institution's code of ethics preserves and strengthens the business culture and enables ongoing adherence to high standards of ethics and integrity from recruitment onward
- Review the institution's FTC performance on set objectives and strategies and, if necessary, ensure that the required remedial action is taken

[9] Insurers Act, CQLR, c. A-32.1, section 94
Act respecting financial services cooperatives, CQLR, c-C-67.3, sections 66.1 and 99
Deposit Institutions and Deposit Protection Act, CQLR, c. I-13.2.2, section 28.38
Trust Companies and Savings Companies Act, CQLR, c-S-29.02, section 75

Roles and responsibilities of senior management

- Ensure the development of objectives, strategies, policies, processes and procedures that are consistent with the institution's values and enable achievement of the expected FTC outcomes
- Ensure the implementation of controls to:
    - Identify and address any departure from the institution's objectives, strategies, policies, processes and procedures
    - Ensure that staff conduct is consistent with the institution's FTC-related values
    - Identify and react promptly to any risks or situations likely to adversely affect FTC
    - Generate information for the board of directors that supports the monitoring and measurement[10] of the institution's performance and a process for its continuing improvement in FTC
- Ensure that staff members who offer products receive training, periodically and as needed, on established FTC-related policies, processes and procedures
- Ensure that the institution's integrated risk management takes into account risks and commercial practices that could adversely affect FTC
- Ensure that appropriate action is taken to correct staff member practices that are contrary to FTC

[10] Accordingly, in addition to the client satisfaction rate or the number of complaints received, the indicators used by the institution should make it possible to measure the achievement of expected FTC outcomes at every stage of the product life cycle.

5.2 Handling conflicts of interest

The AMF expects any real or potential conflicts of interest to be avoided or managed in a manner that ensures FTC.

A conflict of interest situation may arise from, among other things, the compensation and performance management programs put in place or the relationships established between the financial institution and the intermediary and any other person acting on its behalf who is involved in offering its products.

A conflict of interest situation could result in an inappropriate sale, transaction or practice or have an impact on the quality of services provided or advice given to clients, as applicable.

The institution should therefore regularly identify and assess the risks of practices with a potentially adverse impact on FTC that may result from conflict of interest situations.

Expectations to achieve this outcome

- Put clients' interests first
- Take all reasonable steps to identify and avoid or manage real or potential conflicts of interest
- Avoid any real or potential conflict of interest that cannot be managed in a way that ensures FTC
- Demonstrate that controls have been put in place to ensure that conflicts of interest can be managed in a way that ensures FTC
- Disclose in writing to the client concerned any real or potential conflict of interest that might reasonably have an impact, given the circumstances, on the offer of products or the client's decisions. This disclosure is made in a timely manner, and it is not sufficient in and of itself for the conflict of interest to be considered to have been properly managed
- When relying on, among other things, disclosure of a conflict of interest, ensure that such disclosure allows the client to assess the nature and scope of the conflict of interest, its potential impact on the services provided, the potential risk it could pose for him or her and the way it is managed
- Notify the client of any significant change that occurs regarding the previously disclosed conflict of interest
- Document each conflict of interest situation that arises and how the institution managed it. The information collected should provide a basis for illustrating the extent of the harm that may be caused to the client by a such a conflict of interest

5.3 Product design

The AMF expects financial institutions to take the common needs and interests of the various target client groups into account when designing products.

Designing products includes developing new products and significantly altering existing ones. For the financial institution, not taking the common needs and interests of the various target client groups into account when designing products could increase the risk of inappropriate offers.

Expectations to achieve this outcome

- Product design relies on the use of adequate information enabling the identification of client needs and interests
- Product design, including the selection of products originating from third parties, involves an appropriate assessment of the main features of the product[11] and the disclosure documents provided to clients by institution staff who have the competencies to perform such an assessment[12]
- The process for approving a product enables the institution to:
    - Define the target client group that the product is likely to be appropriate for
    - Offer a product that delivers the benefits and features reasonably expected by the target client group
    - Identify and manage any risks that the product might present for the target client group
    - Take into account applicable statutory and regulatory amendments, technological developments or changes in market conditions
- Defining the target client group involves identifying the common needs and interests of the members of the group. The level of detail of the criteria used by the institution to identify a target client group is based on the type of product (e.g., nature, features, complexity, level of risk) and enables the institution to determine which clients belong to the group and those for whom the product may not be appropriate
- Product monitoring:[13]

[11] For example, for deposit products, the assessment of the product's features could take into account criteria such as accessibility, yield and security.

[12] For example, type, compliance, integrated risk management, finance, sales, taxation, actuarial services, legal affairs.

[13] Also applies to products no longer offered but still held by clients (e.g., investments in certain segregated funds). Product monitoring helps ensure that clients receive ongoing information supporting informed decision-making.

- Ensures, by relying on sufficient, relevant, clear information, that the product's main features continue to suit the target client group's needs and interests[14]
- Enables action to be taken, if necessary, to:
  - Tailor the product to the target client group's changing needs and interests[15]
  - Ensure that clients understand the product and its main features
  - Revisit the definition of the target client group

[14] For example, regular information from employees and intermediaries offering the product; information from the quality control department, the claims examination department, the complaint processing department, the analysis of competing products and client satisfaction assessment methods. Moreover, some insurance industry indicators such as a high claim denial rate or a low claim rate may indicate that the product is not suited to the needs and interests of the target client group.

[15] For example, ensure that the exclusions in the insurance contract are still relevant and drafted in a way that is clear to clients. Consider economic conditions in taking into account changes in clients' level of indebtedness.

5.4 Product marketing

The AMF expects financial institutions' distribution strategies to take into account the needs and interests of the target client groups and to be tailored to the products.

Financial institutions are responsible for the distribution strategies they use for their products and provide strategy oversight.

Expectations to achieve this outcome

- The distribution strategies for a product are chosen using appropriate information to assess the target client group's needs and interests and are tailored to the level of complexity of the product
- Staff, intermediaries or other persons acting on behalf of the institution who are involved in offering its products receive relevant information and appropriate training on the products. They have an adequate grasp of the product's features and the target client groups
- The indicators used and controls applied with respect to distribution strategies make it possible to:
    - Assess the performance of the various distribution strategies in terms of expected FTC outcomes and to take any remedial action, as required
    - Ensure that the distribution strategies used for a product continue to meet the target client group's needs and would not adversely affect clients' interests

5.5 Product advertising

The AMF expects product advertising materials to be accurate, clear and not misleading.

Before using advertising material, financial institutions should take the necessary steps to ensure that it is accurate, clear and not misleading.

Expectations to achieve this outcome

- Prior to being disseminated, product advertising materials are reviewed by persons other than those who prepared or designed them
- Advertising materials:
    - Are easy to understand
    - Clearly identify the financial institution
    - Adequately convey the benefits that the target client group may reasonably expect from the product
    - Highlight information or key elements required for informed decision-making by clients
    - Provide a clear understanding of the product and does not cause confusion
- Advertising materials are presented in a format that is easy to read and understand
- The statistics used are relevant to the product. The sources of the statistics used are indicated, if applicable
- Testimonials used are authentic, and, if paid for, mention is made of that fact
- If the institution notes that advertising material is inaccurate, misleading or is causing confusion, it withdraws it promptly and takes any other actions required to remedy the situation

5.6 Disclosure to clients before or when a product is offered

The AMF expects clients to have information, before or when a product is offered, that allows them to be properly informed in order to make an enlightened decision.

Such disclosure should enable clients to understand the product and its main features and help them determine whether the product suits their needs and interests.

The level of detail of disclosure will vary depending on, among other things, the nature and complexity of the product.

Expectations to achieve this outcome

- Disclosure to clients:
  - Is up-to-date and readily accessible
  - Is drafted in clear and plain language, in a manner that is not misleading,[16] and is presented in a format that facilitates reading and comprehension
  - Focuses on information quality, not quantity
  - Clearly identifies the name of the institution and provides its contact details
  - Gives prominence to and explains the main features of the product [17] that are important for finalizing or performing the contract, including the consequences for the client of not complying with the terms of the contract
  - Sets out the client's rights and obligations, including any right of cancellation or rescission
  - Gives the contact details for the claims examination and settlement department[18]
  - Gives the contact details for the complaint processing and dispute resolution department and the steps for accessing the summary of the complaint processing and dispute resolution policy

[16] When technical, complex or hard-to-understand language cannot be avoided, make tools or other means accessible to clients to help them clearly understand the information.

[17] Examples: For insurance products, the type of contract, the coverages offered, eligibility requirements, perils covered, restrictions, limitations, deductible, premium. For credit products, the interest rate, fees and charges, total cost, term, repayment terms, type of security required, etc.

[18] Applicable only to insurers authorized under the Insurers Act.

5.7 Offers of product by deposit institutions[19]

The AMF expects deposit institutions to assess whether the product that is offered is appropriate for the client.

The deposit institution's policies, processes, procedures and controls should ensure that the product that is offered is appropriate for the client, having regard for their circumstances, including their financial needs.[20]

Expectations to achieve this outcome

- The nature of the information collected varies depending on the client's circumstances[21] and the type of product that is offered[22]
- The Know Your Client (KYC) information that is collected is analyzed to understand the client's circumstances and assess the appropriateness of the product that is offered

19 Financial services cooperatives, trust companies and other authorized deposit institutions.

Product offers regulated by the Act respecting the distribution of financial products and services are not covered by this section.

20 For example, the policies, processes, procedures, controls and information systems relating to the granting of credit should enable the identification, control and mitigation of major risks to clients, including those related to mis-sold credit products, and to prevent, insofar as possible, repayment problems and what they logically lead to, i.e., debt overload.

21 The assessment of the client's circumstances, including their financial needs, may require consideration of a number of factors, such as the client's objectives, financial situation, repayment ability, risk tolerance, investment horizon and other commitments.

22 Features, charges, risks and benefits for clients.

5.8 Disclosure to clients after a product is purchased

The AMF expects clients to have information allowing them to be properly informed, in a timely manner, in order to make enlightened decisions about the products they hold.

Disclosure to clients after a product is purchased is timely and enables clients to determine whether the product they hold is still suited to their needs and interests.

Expectations to achieve this outcome

Disclosure to clients:

- Is drafted in clear and simple language so as not to cause misunderstanding and is presented in a format that is easy to read and understand
- Reminds them about the options they can exercise
- Informs them of changes to the contract or changes related to the performance of their contract, the impact of the changes, and their rights and obligations, and when necessary, obtains their consent
- Notifies clients of events such as:
    - Date of renewal or automatic renewal
    - Expiry of a promotional period
    - Payment due date after which time fees will be charged
    - Replacement of the product or early termination of the contract
    - A portfolio transfer
    - Amendments to applicable legislation or changes in market conditions that could affect the product's main features
    - Any organizational or operational change by the institution that could have an impact on the products held by and the services provided to the client[23]

Periodic communications remind clients of the importance of reviewing their needs based on changes in their personal situation to ensure that the product is still appropriate for them.

The institution therefore takes the necessary steps to ensure that clients receive ongoing and adequate service.

When clients wish to replace a product or switch products, cancel a contract or change institutions, the procedures in place facilitate such transactions.

[23] For example, if branches or automated teller machines are closed or converted, the financial institution contacts its clients within a reasonable period of time and informs them of available alternatives.

5.9 Claims examination and settlement[24]

The AMF expects claims to be examined diligently and settled fairly following a process that is simple and readily accessible for clients.

Claims examination and settlement are key steps in an insurer's relationship with its clients.

Expectations to achieve this outcome

- When filing a claim, the client is informed of the main steps in the examination of the claim and of the expected timeframes for settlement of the claim[25]
- The client is informed in a timely and appropriate manner of the claim's status
- Additional requests for information from the institution related to the examination of a claim are commensurate with the perils covered and do not hinder or delay the examination process
- The client is informed, when the claim cannot be examined within the expected timeframe, why additional time is required and when the process will be completed
- Claim-determinative factors (e.g., depreciation, negligence) and, when applicable, the reasons why the claim was wholly or partially denied are carefully and clearly explained to the client. Everything is confirmed in writing to the client, who is offered the opportunity to request a review of the decision
- Claim decisions take clients' interests into account and are made in an objective and consistent manner
- The claim decision review process is simple, without any red tape
- Clients are informed that they may contact the complaint processing and dispute resolution department if they are dissatisfied with the way their claim has been handled
- Staff responsible for claims examination and settlement:
    - Are familiar and comply with the institution's claims examination and settlement process. They are able to provide appropriate information to clients and properly assist them in making a claim and throughout the examination process
    - Possess the necessary competencies depending on the type of product

[24] Applicable only to insurers authorized under the Insurers Act.

[25] Where applicable, a damage insurer's procedure creates a favourable environment for a claims adjuster to meet the obligations set out in the Act respecting the distribution of financial products and services.

5.10 Complaint processing and dispute resolution

The AMF expects complaints to be processed fairly and diligently following a process that is simple and readily accessible for clients.

The complaints received by a financial institution and the handling of those complaints are, among other things, key elements to consider in assessing the financial institution's FTC performance.

The various laws administered by the AMF require financial institutions to do such things as keep a complaints register and adopt a policy for complaint processing and dispute resolution.[26]

Expectations to achieve this outcome

- The complaint process takes into account clients' interests and ensures that complaints are handled in an objective and consistent manner
- The institution designates a complaints officer who has the authority and competence to perform the function and ensures, among other things, that the complaint processing and dispute resolution policy is implemented, disseminated and complied with within the institution
- Staff responsible for processing complaints have the necessary competencies to process the complaints assigned to them
- Clients receive proper assistance throughout the processing of their complaint and are informed in a timely manner of the status of their complaint
- Clients are not faced with constraints or administrative barriers and any need the institution has for additional information does not hinder or delay the complaint process
- The institution develops an overall picture of the complaints received in order to identify common causes and the issues to be resolved to ensure FTC

[26] Insurers Act, CQLR, sections 50, 52 to 58
Act respecting financial services cooperatives, sections 66.1, 131.1 to 131.7
Trust Companies and Savings Companies Act, sections 34, 36 to 42
Deposit Institutions and Deposit Protection Act, sections 28.11, 28.13 to 28.19

5.11 Protection of personal information

The AMF expects financial institutions to establish and put in place measures enabling them to comply with their obligations with respect to the protection of personal information ("privacy obligations").

A financial institution is responsible for protecting the personal information it holds.

The sustainability of its operations depends, among other things, on its clients' trust in this respect, and clients expect personal information about them held by the financial institution or another person acting on the institution's behalf to remain private and protected accordingly.

Accordingly, the institution's policies, processes and procedures relating to the protection of personal information draw on best practices and enable it to discharge its privacy obligations, including those under the *Act respecting the protection of personal information in the private sector*.[27]

The AMF also expects the financial institution to assess the potential effects of new or emerging risks that could threaten the privacy of the personal information it holds and to take appropriate action to mitigate such risks.

[27] CQLR, c. P-39.1.

5.3 AUTRES CONSULTATIONS

Aucune information.

5.4 AVIS D'INTENTION DES ASSUJETTIS ET AUTRES AVIS

Aucune information.

5.5 SANCTIONS ADMINISTRATIVES

Aucune information.

5.6 PROTECTION DES DÉPÔTS

Aucune information.

5.7 AUTRES DÉCISIONS

Aucune information.