10.2

Réglementation et lignes directrices

10.2. RÉGLEMENTATION ET LIGNES DIRECTRICES

10.2.1. Consultation

Aucune information.

10.2.2. Publication

DÉCISION N° 2022-PDG-0017

Ligne directrice applicable aux agents d'évaluation du crédit

Vu le pouvoir de l'Autorité des marchés financiers (l'« Autorité ») d'établir des lignes directrices destinées à tous les agents d'évaluation du crédit, conformément à l'article 53 de la *Loi sur les agents d'évaluation du crédit*, RLRQ, c. A-8.2 (la « LAÉC »);

Vu le pouvoir de l'Autorité d'établir une ligne directrice prévu à l'article 53 LAÉC, 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 18 novembre 2021 [(2021) vol. 18, n° 46, B.A.M.F., section 10.2] du projet de *Ligne directrice applicable aux agents d'évaluation du crédit* (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 53 LAÉC, selon lequel l'Autorité publie à son Bulletin les lignes directrices qu'elle établit après en avoir transmis une copie au ministre des Finances du Québec (le « Ministre »);

Vu le projet de ligne directrice 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 applicable aux agents d'évaluation du crédit*, 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 applicable aux agents d'évaluation du crédit* prend effet le 24 mars 2022.

Fait le 22 mars 2022.

Louis Morisset
Président-directeur général

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, en versions française et anglaise, la *Ligne directrice applicable aux agents d'évaluation du crédit* (la « Ligne directrice »).

Les attentes de la Ligne directrice couvrent notamment les mesures de protection suivantes découlant de la loi et destinées à mieux protéger le consommateur et ses renseignements personnels, à savoir : le gel de sécurité, l'alerte de sécurité, la note explicative, ainsi que l'accès à la cote de crédit.

La Ligne directrice prend effet à compter du 24 mars 2022.

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

Renseignements additionnels

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

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

Le 24 mars 2022

AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE APPLICABLE AUX AGENTS D'ÉVALUATION DU CRÉDIT

Mars 2022

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

Les pratiques commerciales ou la conduite des activités d'un AÉC réfèrent à 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 opportune, 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 (téléphones, adresse courriel, messagerie instantanée, etc.) et facilement repérables sur l'ensemble des plateformes (site Web, réseaux sociaux) de l'AÉC.

[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.

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 assurent la conformité à la *Loi sur la protection des renseignements personnels dans le secteur privé*[9] et tiennent compte des meilleures pratiques dans ce domaine.

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 une procédure simple et accessible pour les consommateurs.

En vertu de la Loi, l'AÉC doit tenir un registre des plaintes et adopter une politique portant sur le traitement des plaintes ainsi que sur le règlement des différends qui doit être conforme aux obligations prévues.

L'Autorité s'attend à ce que :

- les consommateurs aient accès à un résumé de la politique, sur le site Web de l'AÉC et par l'entremise de tout autre moyen propre à le rejoindre adéquatement, décrivant

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

les principales étapes du processus de traitement d'une plainte, les formalités à suivre et les délais de traitement;

- les consommateurs ne se heurtent pas à des contraintes ou des obstacles administratifs [10] lorsqu'il veut déposer une plainte;
- l'AÉC désigne un responsable du traitement des plaintes qui, notamment :
  - possède l'autorité et la compétence nécessaire à l'exécution de sa fonction;
  - assure la mise en œuvre et le respect de la politique;
  - développe une vision d'ensemble des plaintes reçues (p. ex. : nombre, motifs, causes) afin d'identifier les causes communes et résoudre les enjeux qu'elles soulèvent pour les consommateurs;
  - agit à titre de répondant officiel auprès des consommateurs et, le cas échéant, de l'Autorité dans les dossiers de plainte qui lui sont transmis.
- le processus de traitement des plaintes soit exempt de tout conflit d'intérêts;
- le registre des plaintes permette de colliger les informations pertinentes relatives aux plaintes, à leur reddition et aux mesures prises pour les résoudre;
- la classification des plaintes au registre soit détaillée et permette de bien cerner les motifs et les causes;
- les membres du personnel chargé du traitement des plaintes :
  - exercent ses fonctions avec indépendance;
  - connaissent et respectent la procédure de l'AÉC relative au traitement des plaintes, qu'il soit en mesure de divulguer une information appropriée aux consommateurs et de les assister adéquatement dans le dépôt de leurs plaintes et pendant tout le processus de traitement;
  - possèdent les compétences nécessaires pour traiter les plaintes qui lui sont assignées.

[10] P. ex., les consommateurs ne devraient pas avoir à soumettre leur plainte plus d'une fois, peu importe les paliers de traitement prévus au sein de l'organisation.

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 opérationnels 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

March 2022

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

The commercial practices, or conduct of business, of CAAs mean 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 timely, 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).

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.

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

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 ensure compliance with the *Act respecting the protection of personal information in the private sector*[9] and to take privacy best practices into account.

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 accessible for consumers.

The Act requires CAAs to keep a complaints register and adopt a complaint processing and dispute resolution policy that complies with established requirements.

The AMF expects:

- a summary of the policy, describing the main steps in the complaint process, the formalities to be completed and the processing timeframes, to be made available to consumers on the CAA's website and disseminated by any other appropriate means to reach them
- consumers not to be faced with constraints or administrative barriers[10] when they want to file a complaint
- CAAs to designate a complaints officer who, in particular:
    - has the authority and competence to perform the function

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

[10] For example, consumers should not have to submit their complaints more than once, regardless of how many complaint processing levels there are within the institution.

- ensures that the policy is implemented and complied with
- develops an overall picture of the complaints received (e.g., number, reasons, causes) in order to identify common causes and address the issues they raise for consumers
- acts as the person officially designated to respond to consumers, as well as to the AMF, where complaint files are sent to the AMF

- the complaint process to be free of any conflicts of interest
- the complaints register to be used to compile relevant information about complaints, complaints reporting and actions taken to resolve complaints
- complaints to be classified in the register in a detailed manner so that the reasons and causes are clearly identifiable
- staff responsible for processing complaints:
  - to be independent in the performance of their duties
  - to be familiar and comply with the CAA's procedure for processing complaints, be able to disclose appropriate information to consumers and properly assist them in filing a complaint and throughout the complaint process
  - to possess the necessary competencies to process the complaints assigned to them

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.