AUTORITÉ DES MARCHÉS FINANCIERS

LIGNE DIRECTRICE APPLICABLE AUX AGENTS D'ÉVALUATION DU CRÉDIT

Novembre 2021

TABLE DES MATIÈRES

Introduction

Les agents d'évaluation du crédit (les « AÉC ») collectent, utilisent, compilent, produisent et divulguent des données sur le crédit 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, en sus de celles touchant les mesures de protection, les droits des personnes concernées, les recours et les plaintes[3].

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 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[4].

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.

[4] 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.

<u>Deuxième ligne de défense</u>

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[5] 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[6].

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.

5 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.

6 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[7]. 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.

[7] 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.

Les réponses aux demandes des consommateurs concernant l'exercice d'un droit leur étant conféré par la Loi doivent être communiquées par écrit et transmises dans les trois jours ouvrables suivant la réception de ces demandes. Lorsque l'AÉC acquiesce aux demandes des consommateurs, il devrait donner suite à celles-ci au plus tard le jour qui suit la transmission des réponses écrites.

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*[8] et tiennent compte des meilleures pratiques dans ce domaine.

L'AÉC devrait prendre toutes les mesures nécessaires afin de garantir que, eu égard à la finalité pour laquelle elles sont détenues, les informations sont exactes et à jour. L'AÉC devrait en tout temps veiller à l'intégrité et l'exactitude des données, tant celles en sa possession que celles qui lui sont transmises par les fournisseurs de crédit. L'AÉC devrait à ce titre veiller à ce que des audits réguliers soient effectués par une personne indépendante afin de déterminer si les ententes conclues avec lesdits fournisseurs sont respectées et, le cas échéant, traiter 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.) afin de prévenir le vol d'identité.

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.

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

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 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 [9] 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.

[9] 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[10], du fait que l'impartition expose l'organisation aux risques opérationnels (p. ex., l'exposition aux cyberrisques).

[10] 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. Les 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 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, 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 et 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 inclure 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 celles 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 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[11].

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 réputationnels.

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.

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

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

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 immédiatement informer l'Autorité dès le moment où il active son plan de continuité des activités.

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.