

**LIGNE DIRECTRICE SUR LA  
GESTION DES RISQUES LIÉS À LA  
CRIMINALITÉ FINANCIÈRE**

Novembre 2011

## TABLE DES MATIÈRES

<b>Préambule</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>4</b>
<b>Champ d'application</b> .....	<b>6</b>
<b>Entrée en vigueur et processus de mise à jour</b> .....	<b>7</b>
<b>Risques liés à la criminalité financière</b> .....	<b>8</b>
<b>Gouvernance en matière de risques liés à la criminalité financière</b> .....	<b>9</b>
Principe 1 : Rôles et responsabilités du conseil d'administration et de la haute direction .....	9
<b>Encadrement de la gestion des risques liés à la criminalité financière</b> .....	<b>10</b>
Principe 2 : Gestion des risques liés à la criminalité financière .....	10
Principe 3 : Gestion intra-groupe .....	12
Principe 4 : Vigilance auprès de la clientèle .....	13
Principe 5 : Vigilance auprès des employés, dirigeants et relations d'affaires .....	15
Principe 6 : Examens sur des activités suspectes .....	16
Principe 7 : Communication de renseignements .....	17
<b>Surveillance des pratiques de gestion saine et prudente et des saines pratiques commerciales</b> .....	<b>18</b>

## Préambule

Une ligne directrice est une indication des attentes de l'Autorité des marchés financiers (l'« Autorité ») à l'égard de l'obligation légale des institutions financières de suivre des pratiques de gestion saine et prudente et de saines pratiques commerciales. Elle porte donc sur l'exécution, l'interprétation et l'application de cette obligation imposée aux institutions financières.

Dans cette optique, l'Autorité privilégie une approche basée sur des principes plutôt que d'édicter des règles précises. Ainsi, du fondement même d'une ligne directrice, l'Autorité confère aux institutions financières la latitude nécessaire leur permettant de déterminer elles-mêmes les stratégies, politiques et procédures pour la mise en œuvre de ces principes et de voir à leur application en regard de la nature, de la taille et de la complexité de leurs activités.

L'Autorité considère la gouvernance, la gestion intégrée des risques et la conformité (GRC) comme les assises sur lesquelles doivent reposer les pratiques de gestion saine et prudente et les saines pratiques commerciales, et conséquemment, les bases sur lesquelles l'encadrement prudentiel donné par l'Autorité s'appuiera.

La présente ligne directrice s'inscrit dans cette perspective et énonce les attentes de l'Autorité à l'égard des pratiques de gestion saine et prudente et des saines pratiques commerciales, en matière de gestion des risques liés à la criminalité financière.

## Introduction

Dans le cours normal de leurs activités, les institutions financières pourraient, à leur insu ou non, être utilisées pour faciliter des activités associées à la criminalité financière ou encore en être la cible.

Le cas échéant, en plus des pertes pouvant être subies par une institution, le manque de diligence dans sa gestion des risques liés à la criminalité financière pourrait entacher sa réputation. Dans certains cas, cette situation pourrait entraîner une perte de confiance du public, tant envers cette institution que pour l'ensemble du secteur financier.

Ainsi, l'ampleur de la criminalité financière et la menace grandissante que constituent les risques, tant pour les consommateurs de produits et de services financiers que pour les institutions, interpellent l'Autorité à promouvoir la mise en place par une institution financière, d'un encadrement lui permettant d'assurer une gestion efficace des risques liés à la criminalité financière.

Dans cette perspective et en vertu de l'habilitation<sup>1</sup> de l'Autorité prévue aux diverses lois sectorielles qu'elle administre, l'Autorité précise, relativement à la gestion des risques liés à la criminalité financière, ses attentes à l'égard de l'obligation légale des institutions financières de suivre des pratiques de gestion saine et prudente et de saines pratiques commerciales<sup>2</sup>. La ligne directrice privilégie *a priori*, la nécessité pour une institution financière d'exercer une gouvernance efficace et de mettre en œuvre des pratiques de gestion des risques afin de prévenir et détecter les activités associées à la criminalité financière.

Les principes énoncés dans cette ligne directrice privilégient une approche proactive visant à atténuer les risques qu'une institution financière soit impliquée dans des activités de criminalité financière. Leur application et leur respect par les institutions financières devraient, par conséquent, se conjuguer aux efforts soutenus de l'Autorité et d'autres intervenants, notamment les corps policiers et le Centre d'analyse des opérations et déclarations financières du Canada (« CANAFE »), dans la lutte à la criminalité financière pour mieux promouvoir l'intégrité des marchés financiers et pour une meilleure protection du public.

---

<sup>1</sup> *Loi sur les assurances*, L.R.Q., c. A-32, articles 325.0.1 et 325.0.2;  
*Loi sur les coopératives de services financiers*, L.R.Q., c. C-67.3, article 565;  
*Loi sur les sociétés de fiducie et les sociétés d'épargne*, L.R.Q., c. S-29.01, article 314.1.

<sup>2</sup> *Loi sur les assurances*, L.R.Q., c. A-32, article 222.2;  
*Loi sur les coopératives de services financiers*, L.R.Q., c. C-67.3, article 66.1;  
*Loi sur les sociétés de fiducie et les sociétés d'épargne*, L.R.Q., c. S-29.01, article 177.3.

Enfin, les attentes de l'Autorité s'inspirent des principes fondamentaux et des orientations des organismes internationaux<sup>3</sup> énoncés notamment par le Comité de Bâle sur le contrôle bancaire (« CBCB »), le Groupe d'Action financière (« GAFI ») et l'Association internationale des contrôleurs d'assurance (« AICA »).

---

<sup>3</sup> Comité de Bâle sur le contrôle bancaire, Devoir de diligence des banques au sujet de la clientèle, octobre 2001;

Comité de Bâle sur le contrôle bancaire, Méthodologie des principes fondamentaux, octobre 2006;

Comité de Bâle sur le contrôle bancaire, Saines pratiques pour la gestion et la surveillance du risque opérationnel, février 2003;

Basel Committee on Banking Supervision, Due Diligence and Transparency Regarding Cover payment messages related to Cross-border Wire transfers, May 2009;

Financial Action Task Force, Guidance on the Risk-Based Approach to combating money laundering and Terrorist Financing, June 2007;

Groupe d'action financière, Les quarante recommandations du GAFI, octobre 2003. Les IX recommandations spéciales, octobre 2004;

International Association of Insurance Supervisors, Countering Fraud in Insurance (Insurance Core Principle 21 and Application Paper), October 2011 ;

International Association of Insurance Supervisors, Anti-Money Laundering and Combating the Financing of Terrorism (Insurance Core Principle 22), October 2011;

International Association of Insurance Supervisors, Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism, October 2004;

International Association of Insurance Supervisors, Insurance Core principles, Standards, Guidance and Assessment Methodology, October 2011.

## Champ d'application

La ligne directrice sur la gestion des risques liés à la criminalité financière est applicable aux assureurs de personnes, aux assureurs de dommages, aux sociétés de gestion de portefeuille contrôlées par un assureur, aux sociétés mutuelles d'assurance, aux coopératives de services financiers, aux sociétés de fiducie et aux sociétés d'épargne, régis par les lois suivantes :

- *Loi sur les assurances*, L.R.Q., c. A-32
- *Loi sur les coopératives de services financiers*, L.R.Q., c. C-67.3
- *Loi sur les sociétés de fiducie et les sociétés d'épargne*, L.R.Q., c. S-29.01.

Enfin, cette ligne directrice s'applique tant à une institution financière qui opère de façon autonome qu'à celle qui fait partie d'un groupe financier<sup>4</sup>. Dans le cas des coopératives de services financiers et des sociétés mutuelles d'assurance de dommages membres d'une fédération, les normes ou politiques adoptées à leur intention par la fédération doivent être cohérentes, voire convergentes, avec les principes en vue de suivre des pratiques de gestion saine et prudente et de saines pratiques commerciales tel que prescrit par la loi et précisés à la présente ligne directrice.

Les expressions génériques « institution financière » ou « institution » sont utilisées pour faire référence à toutes les entités financières visées par le champ d'application.

---

<sup>4</sup> Aux fins d'application de la présente, est considéré comme « groupe financier », tout ensemble de personnes morales formé d'une société mère (institution financière ou *holding*) et de personnes morales qui lui sont affiliées.

## **Entrée en vigueur et processus de mise à jour**

La ligne directrice sur la gestion des risques liés à la criminalité financière est effective à compter du xx mois 201X.

En regard de l'obligation légale des institutions de suivre des pratiques de gestion saine et prudente et de saines pratiques commerciales, l'Autorité s'attend à ce que chaque institution s'approprie les principes de la présente ligne directrice en élaborant des stratégies, politiques et procédures adaptées à sa nature, sa taille, la complexité de ses activités et son profil de risque, et qu'elle les mette en œuvre d'ici le (2 ans après la mise en vigueur). Dans la mesure où une institution a déjà mis en place un tel encadrement, l'Autorité pourra vérifier si cet encadrement permet à l'institution de rencontrer les exigences prescrites par la loi.

Cette ligne directrice sera actualisée en fonction des développements en matière de gestion des risques liés à la criminalité financière et à la lumière des constats effectués dans le cadre des travaux de surveillance menés auprès des institutions financières.

## Risques liés à la criminalité financière

Dans les secteurs des assurances et des dépôts, les institutions financières peuvent être la cible d'activités associées à la criminalité financière de toutes formes et de toute importance, impliquant diverses parties, tant des clients, des employés, des dirigeants que des relations d'affaires, par exemple des fournisseurs.

Aux fins de la présente ligne directrice, l'Autorité entend comme principales activités associées à la criminalité financière, la fraude à l'interne et la fraude à l'externe<sup>5</sup>, le recyclage des produits de la criminalité (blanchiment d'argent), le détournement de fonds, le transfert illégal de capitaux dans des paradis financiers ou fiscaux<sup>6</sup>, l'évitement illicite d'impôt (évasion fiscale), ainsi que le financement du terrorisme. Certaines activités sont fréquemment médiatisées, notamment les réclamations frauduleuses d'assurance, les fraudes liées aux prêts hypothécaires, aux cartes de débit et de crédit et à l'utilisation frauduleuse de renseignements confidentiels sur les clients.

La criminalité financière peut exposer une institution financière à différents risques, dont le risque opérationnel, le risque juridique, le risque réglementaire et le risque de réputation. L'ampleur de ces risques, indépendants ou souvent interreliés, est surtout considérable lorsque les auteurs tirent avantage de déficiences de la gestion exercée par l'institution ou de la complicité de ses employés ou de ses dirigeants.

L'institution financière devrait avoir une vision globale des risques liés à la criminalité financière. Elle devrait mettre en place des mesures pour prévenir la criminalité financière et détecter les activités qui peuvent y être associées. Ces mesures devraient également faciliter les examens, les inspections et les enquêtes relatives à la criminalité financière.

---

<sup>5</sup> De façon générale, la fraude à l'interne correspond à la fraude commise par un dirigeant, un administrateur, ou par un employé, en collusion ou non avec une personne à l'interne ou à l'externe (par exemple, un détournement de fonds par un employé).

De façon générale, la fraude à l'externe correspond à la fraude commise par un client ou un tiers (par exemple, une falsification de signature sur un chèque, une réclamation d'assurance dont la valeur d'un bien réclamé a été volontairement surévaluée).

<sup>6</sup> L'Organisation de Coopération et de Développement Économiques (OCDE) définit notamment un paradis fiscal comme un pays ou un territoire dont les impôts sont inexistantes ou insignifiants. Un paradis financier est un pays ou territoire où prédomine le secret bancaire. Référence : [www.oecd.org](http://www.oecd.org).



## Gouvernance en matière de risques liés à la criminalité financière

### Principe 1 : Rôles et responsabilités du conseil d'administration et de la haute direction

L'Autorité s'attend à ce que la gestion des risques liés à la criminalité financière soit soutenue par une gouvernance efficace.

L'Autorité considère que le conseil d'administration<sup>7</sup> et la haute direction demeurent ultimement responsables d'instaurer des pratiques de gestion saine et prudente et de saines pratiques commerciales en matière de gouvernance des risques liés à la criminalité financière.

En considérant les rôles et responsabilités qui leur sont respectivement dévolus au sein de la Ligne directrice sur la gouvernance<sup>8</sup>, le conseil d'administration et la haute direction devraient entre autres :

- élaborer, approuver et mettre en œuvre des stratégies, politiques et procédures.

Afin que l'institution gère les risques liés à la criminalité financière de façon efficace et efficiente, ces stratégies, politiques et procédures devraient être axées principalement sur la prévention et la détection des activités associées à la criminalité financière et porter sur la vigilance de l'institution à l'égard de sa clientèle, de ses employés, de ses dirigeants et de ses relations d'affaires. À cette fin, l'institution devrait tenir compte de la vulnérabilité de l'institution à ces risques notamment à l'égard des éléments suivants :

- les clients et la nature de leurs opérations;
- les employés, les dirigeants et les fournisseurs de services;
- les produits et services financiers offerts;
- les systèmes d'information et le contrôle interne de l'institution;
- les méthodes utilisées par les auteurs d'activités de la criminalité financière et la possibilité d'incidents opérationnels et leurs impacts potentiels.

Les stratégies, politiques et procédures devraient être documentées et régulièrement révisées, notamment en fonction de l'évolution de la clientèle, de la mise en marché de nouveaux produits et de la complexité grandissante des activités associées à la criminalité financière;

---

<sup>7</sup> Lorsqu'il est fait mention du conseil d'administration, il peut s'agir d'un comité de ce dernier formé, par exemple, à des fins d'examen de points particuliers.

<sup>8</sup> Autorité des marchés financiers, Ligne directrice sur la gouvernance, avril 2009.

- promouvoir une culture qui encourage un comportement éthique à tous les niveaux de l'institution;
- s'assurer que le personnel et les dirigeants aient une formation appropriée et que les personnes affectées à la gestion des risques liés à la criminalité financière sont expérimentées<sup>9</sup>.

Dans cette optique, la responsabilité relative au développement et à l'implantation de la stratégie de gestion des risques liés à la criminalité financière devrait être confiée au chef de la gestion des risques<sup>10</sup>. Compte tenu de la taille de l'institution et de l'ampleur des risques liés à la criminalité financière, un responsable de la gestion des risques liés à la criminalité financière pourrait également être désigné;

- effectuer un suivi approprié des activités de criminalité financière qui sont soupçonnées ou décelées. Ils devraient également s'assurer du signalement de ces activités aux autorités compétentes, de la communication de tous les renseignements pertinents et des résultats des examens et des enquêtes, le cas échéant;
- s'assurer de la conformité de l'institution aux lois, règlements et lignes directrices<sup>11</sup>. À ce titre, ils devraient notamment s'assurer que les rapports, documents et déclarations sont complétés et transmis à l'Autorité et aux autres autorités compétentes, selon la forme et dans les délais prévus.

## **Encadrement de la gestion des risques liés à la criminalité financière**

### **Principe 2 : Gestion des risques liés à la criminalité financière**

L'Autorité s'attend à ce que la gestion des risques liés à la criminalité financière fasse partie intégrante de la gestion intégrée des risques de l'institution financière.

L'institution financière devrait effectuer la gestion des risques liés à la criminalité financière à l'intérieur de son cadre de gestion intégrée des risques. Elle devrait par conséquent tenir compte des interrelations et des interdépendances entre les risques. Cette façon de faire implique pour cette institution :

- l'identification des risques liés à la criminalité financière, leur évaluation et leur quantification;

---

<sup>9</sup> Autorité des marchés financiers, Ligne directrice sur les critères de probité et de compétence (projet), octobre 2011.

<sup>10</sup> Autorité des marchés financiers, Ligne directrice sur la gestion intégrée des risques, avril 2009.

<sup>11</sup> Autorité des marchés financiers, Ligne directrice sur la conformité, avril 2009.

- la mise en place de mesures d'atténuation des risques afin de diminuer la probabilité d'incidents qui peuvent affecter l'institution.

Dans cette optique, l'approche de gestion intégrée des risques devrait permettre à l'institution d'identifier les incidents de nature opérationnelle qui sont associés à la criminalité financière, de mettre en place des mesures pour diminuer l'occurrence de ces incidents et leurs impacts potentiels sur l'institution.

Ainsi, l'institution devrait prendre en compte, notamment :

- les facteurs internes tels que :
  - sa structure organisationnelle, la nature de ses activités, ses orientations stratégiques, ses politiques;
  - la qualité de son contrôle interne, dont la séparation des tâches et la délégation de pouvoirs;
  - la nature et les caractéristiques de ses produits;
  - le profil de risque de ses clients, leurs activités professionnelles et le volume de leurs opérations, tant locales que transfrontalières;
  - les technologies de l'information utilisées;
  - ses relations d'affaires, y incluant l'impartition qui peut être effectuée;
  - la polyvalence et le taux de rotation de son personnel, le niveau de connaissance des employés en matière de criminalité financière, la qualité de leurs relations de travail.
- les facteurs externes tels que :
  - les exigences légales, réglementaires et normatives relatives à la lutte contre la criminalité financière, notamment la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (2000, ch.17) (« LRPCFAT »), et les modifications apportées aux personnes désignées sur la liste dressée par les Nations Unies<sup>12</sup>.

---

<sup>12</sup> Référence : *Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme*. Des renseignements additionnels sont disponibles sur le site de l'Autorité : [www.lautorite.qc.ca/fr/lutte-terrorisme.html](http://www.lautorite.qc.ca/fr/lutte-terrorisme.html).

L'institution devrait notamment participer à un système de traçabilité des télévirements. L'Autorité s'attend à ce qu'elle remplisse son obligation de déclarer au CANAFE<sup>13</sup> certains télévirements effectués par ses clients;

- ❑ le contexte économique et social, les nouvelles menaces et opportunités en matière de criminalité financière ainsi que l'évolution des techniques et des méthodes utilisées<sup>14</sup>;
- ❑ l'évolution des orientations internationales en matière de lutte contre la criminalité financière.

### **Principe 3 : Gestion intra-groupe**

L'Autorité s'attend à ce que l'institution financière gère les risques liés à la criminalité financière en adéquation avec le cadre de gestion applicable au groupe auquel elle appartient.

Les activités associées à la criminalité financière effectuées par l'entremise d'une institution financière faisant partie d'un groupe sont susceptibles d'avoir des répercussions importantes sur les autres entités du groupe et nuire à leur solvabilité et ultimement entacher la réputation du groupe tout entier.

Par conséquent, il est important d'adopter une approche globale de la gestion des risques liés à la criminalité financière à l'échelle du groupe, tant au niveau local, national qu'international.

Il s'avère donc essentiel que des normes cohérentes soient adoptées au sein du groupe et que des échanges d'information aient lieu entre les entités qui en font partie, notamment pour identifier et évaluer les différentes vulnérabilités et atténuer les risques liés à la criminalité financière.

---

<sup>13</sup> *Ligne directrice 8B : Déclaration à CANAFE des télévirements SWIFT*, publiée par le CANAFE en juin 2011.

<sup>14</sup> L'Autorité émet régulièrement des mises en garde à la suite des renseignements recueillis par ses enquêteurs, entre autres en cybersurveillance. Les renseignements peuvent également provenir d'investisseurs et de régulateurs de différentes juridictions. [www.lautorite.qc.ca/fr/mises-en-garde](http://www.lautorite.qc.ca/fr/mises-en-garde).

## Principe 4 : Vigilance auprès de la clientèle

L'Autorité s'attend à ce que l'institution financière exerce une vigilance constante auprès de sa clientèle grâce à une connaissance suffisante de ses clients et à des procédures appropriées afin de détecter les opérations susceptibles d'être associées à la criminalité financière.

L'institution financière devrait être vigilante auprès de sa clientèle en tenant compte de l'ampleur des risques liés à la criminalité financière, notamment à l'égard des opérations monétaires, des produits d'assurance et des produits d'investissement.

### *Connaissance de la clientèle*

La connaissance de la clientèle constitue une composante essentielle de la gestion des risques liés à la criminalité financière. Elle contribue à réduire la probabilité d'incidents de nature opérationnelle par l'entremise d'une institution financière.

La connaissance de clients, incluant leurs relations avec d'autres clients de l'institution et, le cas échéant, des autres entités du groupe auquel appartient l'institution, devrait également permettre de mesurer le risque de concentration d'une institution. Une vigilance accrue devrait être exercée surtout en présence de contreparties liées ou de prêts apparentés.

L'institution devrait mettre en place des procédures adéquates d'identification, établir un profil de risque et des critères d'acceptation de ses clients, notamment pour des catégories de clients qui sont susceptibles de présenter un risque plus grand. Par conséquent, elle devrait exiger tous les documents justificatifs appropriés selon la nature du client et les particularités de certains comptes, tels que corporatifs, institutionnels ou en fidéicommiss. Elle devrait également s'assurer que le client ne figure pas sur les listes des personnes et organisations présumément associées à des activités terroristes<sup>15</sup>.

Dans la mesure du possible, un surcroît de diligence est requis notamment à l'égard des clients :

- dont la structure de l'entité ou la nature des affaires rend difficile l'identification du propriétaire ou des intérêts qui la contrôlent;
- qui agissent comme des intermédiaires financiers, courtiers, conseillers ou représentants en valeurs mobilières, gardiens de valeurs, fiduciaires et des professionnels;

---

<sup>15</sup> Voir la note 12.

- dont le contexte semble anormal, par exemple un client qui change souvent d'adresse, qui refuse de fournir des preuves d'identité ou qui s'intéresse plus au rachat anticipé d'une police d'assurance plutôt qu'à répondre à ses besoins de protection;
- qui sont des déposants ou des emprunteurs importants, des groupes d'emprunteurs liés, des « étrangers politiquement vulnérables »<sup>16</sup>;
- qui sont des mandataires d'un client ou des bénéficiaires d'un contrat d'assurance<sup>17</sup>.

L'institution devrait tenir et maintenir à jour un registre de ses clients et des transactions qu'ils effectuent. Elle demeure également responsable de protéger les renseignements personnels de ses clients<sup>18</sup>, notamment afin de prévenir l'utilisation inappropriée de ces derniers.

### *Suivi des opérations des clients*

En tenant compte du profil de risque de ses diverses catégories de clients, l'institution devrait prendre des mesures adéquates de vigilance, notamment :

- déterminer des critères pour contrôler, suivre et surveiller les opérations de ses clients, en outre, à l'égard de l'origine des fonds, de la nature des transactions, des liens entre plusieurs opérations, du type de devises et du pays du destinataire;
- procéder à un examen pour toute opération qui n'a pas d'objet économique ou licite apparent ou à l'égard de laquelle, elle a des motifs de croire que l'opération est susceptible d'être associée à la criminalité financière.
- procéder à un examen plus approfondi du contexte et de l'objet :
  - pour toute opération complexe ou dont l'origine des fonds est douteuse ou inconsistante avec le profil de risque de cette personne;
  - pour toute opération inhabituelle notamment si le volume des transactions est anormal par rapport à l'historique d'un client et à la nature de ses affaires;
  - pour les transactions fréquentes en espèces (ou en équivalent) ou celles effectuées dans des circonstances inhabituelles en regard du profil de ce client, et pour des opérations avec des mouvements importants de fonds sans cause apparente pour un client précis;

---

<sup>16</sup> *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (2000, ch.17), article 9.3.

<sup>17</sup> L'identification et la vérification du bénéficiaire devraient être effectuées, au plus tard, lors de la prestation de la police d'assurance.

<sup>18</sup> Autorité des marchés financiers, Ligne directrice sur les pratiques commerciales (projet), mars 2011.

- ❑ pour les virements électroniques<sup>19</sup> faits par un client via une autre institution financière en vue de mettre une somme d'argent importante à la disposition d'un bénéficiaire (le client lui-même ou une autre personne);
- ❑ pour toute opération avec certains pays représentant un risque plus grand de criminalité financière.

Pour les réclamations d'assurance, un processus adéquat devrait être mis en place par l'institution en vue de minimiser les cas de fraude par ses clients. Des mesures supplémentaires, notamment relatives à la validation des sommes réclamées, devraient être mises en œuvre, au besoin et suivant l'importance des réclamations.

Finalement, les résultats du suivi des opérations des clients devraient être consignés dans des rapports de gestion.

## **Principe 5 : Vigilance auprès des employés, dirigeants et relations d'affaires**

L'Autorité s'attend à ce que l'institution financière exerce une vigilance constante auprès de ses employés, dirigeants et relations d'affaires grâce à des contrôles internes efficaces et à des procédures appropriées afin de détecter les situations susceptibles d'être associées à la criminalité financière.

L'institution devrait mettre l'accent sur la prévention des activités associées à la criminalité financière auprès de ses employés et dirigeants. Elle devrait cependant être vigilante face à des individus qui pourraient exercer des activités criminelles et surveiller de près ses relations d'affaires, notamment avec ses fournisseurs.

### *Identification des vulnérabilités*

Dans cette perspective, l'institution devrait identifier ses vulnérabilités aux incidents de nature opérationnelle ou de stratagèmes qui pourraient impliquer des employés dans le cadre de leur travail ou des dirigeants à l'égard de leurs rôles et responsabilités, tels que :

- le vol par des employés de sommes d'argent ou de biens appartenant à l'institution;
- l'utilisation non autorisée de renseignements personnels sur les clients;
- la corruption, les pots de vin, les ristournes ou les commissions d'un fournisseur;
- le paiement à un fournisseur fictif pour un service non rendu à l'institution;
- la falsification de documents, l'absence de comptabilisation d'opérations et la présentation volontairement erronée d'information financière.

---

<sup>19</sup> Incluant aussi les virements de fonds, virements transfrontaliers, et virements nationaux.

## *Contrôle*

L'institution devrait mettre en place des contrôles internes pour traiter ces sources de vulnérabilité à des risques liés à la criminalité financière. À cette fin, elle devrait instaurer notamment :

- des contrôles axés sur la répartition des responsabilités et la séparation des tâches relatives aux opérations des clients et à la protection des actifs de l'institution;
- des mécanismes de sécurité au niveau des technologies de l'information, incluant ceux impartis pour contrer l'utilisation inappropriée de renseignements personnels sur des clients par des employés;
- un processus rigoureux et documenté d'octroi des contrats.

Finalement, l'institution devrait être attentive aux indices ou signaux qui pourraient conduire à déceler un stratagème associé à une activité de la criminalité financière, par exemple, des déficiences soulevées sur des contrôles, le non-respect des processus, l'employé qui reporte souvent ses vacances ou celui qui a un comportement inhabituel, des plaintes de la clientèle et des actifs manquants suite à un inventaire.

Elle devrait aussi tenir compte de la collusion possible impliquant plusieurs individus dans le but de passer outre aux contrôles internes mis en place par l'institution en vue de se prémunir contre les risques liés à la criminalité financière.

## **Principe 6 : Examens sur des activités suspectes**

L'Autorité s'attend à ce que l'institution financière procède à des examens lorsque des activités associées à la criminalité financière sont suspectes ou détectées.

L'institution financière devrait réagir promptement à toute situation où des activités associées à la criminalité financière sont suspectées ou détectées. Les examens pourraient nécessiter des compétences dans plusieurs domaines d'expertise, par exemple légal, fiscal ou des technologies de l'information. L'institution devrait documenter les résultats de ses travaux et veiller à réaliser les différents examens conformément au cadre législatif lui étant applicable

Lorsqu'elle a été la cible d'une activité associée à la criminalité financière, l'institution devrait utiliser l'incident afin de tirer des leçons et, le cas échéant, d'ajuster ses politiques et ses procédures pour en atténuer la probabilité de récurrence.



L'institution pourrait également être appelée à collaborer avec l'Autorité lors des inspections et des enquêtes autorisées en vertu des lois sectorielles auxquelles elle est assujettie, la portée de cette collaboration serait limitée aux fins permises par les lois applicables. À cet effet, l'Autorité peut, lors de ces inspections ou enquêtes, avoir accès aux renseignements relatifs aux directives et aux mécanismes mis en œuvre par une institution dans le cadre de la partie 1 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, et pourrait alors les communiquer au CANAFE<sup>20</sup>. Le cas échéant, la collaboration de l'institution pourrait également être requise lors d'examens et d'enquêtes effectuées par des autorités compétentes en matière de lutte à la criminalité financière, dont la Sûreté du Québec, la Gendarmerie royale du Canada et le CANAFE.

## Principe 7 : Communication de renseignements

L'Autorité s'attend à ce que l'institution financière communique à toute autorité compétente, sous réserve des lois applicables, les renseignements relatifs aux activités associées à la criminalité financière.

Pour favoriser l'application ou l'exécution d'une loi en matière de fiscalité, en matière pénale ou criminelle ou d'une loi étrangère en semblables matières, l'Autorité rappelle l'obligation légale pour une institution financière de communiquer tout renseignement concernant des activités associées à la criminalité financière à toute autre autorité compétente, notamment à l'Autorité, au CANAFE<sup>21</sup>, à la Sûreté du Québec et à l'Agence du Revenu du Québec.

Une institution a également l'obligation de vérifier et de rendre compte à l'Autorité<sup>22</sup>, de l'existence de biens qui sont en sa possession ou à sa disposition et qui appartiennent à une entité inscrite sur la liste établie par le *Règlement établissant une liste d'entités*<sup>23</sup>.

---

<sup>20</sup> Article 2.1 b) de l'entente entre le CANAFE et l'Autorité signée en juin 2006.

<sup>21</sup> Le 19 juin 2006, une entente concernant l'échange d'information est intervenue entre l'Autorité et le CANAFE. Cette entente vise aussi à éviter le chevauchement des interventions du CANAFE et de l'Autorité tout en atténuant leurs conséquences pour les institutions et représentants visés. Site Web du CANAFE : [www.canafe.ca](http://www.canafe.ca).

<sup>22</sup> En vertu du paragraphe 2 de l'article 83.11 du Code criminel (L.R., 1985, ch. C-46), les institutions financières encadrées par l'Autorité doivent faire ce compte rendu à l'Autorité.

<sup>23</sup> *Règlement établissant une liste d'entités* (DORS/2002-284) pris en application de l'article 83.05 du Code criminel.

## **Surveillance des pratiques de gestion saine et prudente et des saines pratiques commerciales**

En lien avec sa volonté de favoriser l'instauration de pratiques de gestion saine et prudente et de saines pratiques commerciales au sein des institutions financières, l'Autorité entend procéder dans le cadre de ses travaux de surveillance à l'évaluation du degré d'observance des principes énoncés à la présente ligne directrice, en considérant les attributs propres à chaque institution. En conséquence, l'efficacité et la pertinence des stratégies, politiques et procédures mises en place ainsi que la qualité de la supervision et du contrôle exercé par le conseil d'administration et la haute direction seront évaluées.

Les pratiques en matière de gestion des risques liés à la criminalité financière évoluent constamment. L'Autorité s'attend à ce que les instances décisionnelles de l'institution financière connaissent les meilleures pratiques en la matière et se les approprient, dans la mesure où celles-ci répondent à leurs besoins.