5.2

Réglementation et lignes directrices

5.2 RÉGLEMENTATION ET LIGNES DIRECTRICES

5.2.1 Consultation

Ligne directrice sur la gestion des risques liés à la criminalité financière
***(Loi sur les assurances*, L.R.Q., c. A-32, art. 325.0.1)**
***(Loi sur les coopératives de services financiers*, L.R.Q. c. C-67.3, art. 565)**
***(Loi sur sociétés de fiducie et les sociétés d'épargne*, L.R.Q. c. S-29.01, art. 314.1)**

Avis est donné par l'Autorité des marchés financiers (l'« Autorité ») que le projet de *Ligne directrice sur la gestion des risques liés à la criminalité financière* est publié pour consultation. Cette ligne directrice s'adresse 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 ainsi qu'aux sociétés de fiducie et aux sociétés d'épargne qui sont régis par les lois administrées par l'Autorité.

Les institutions financières et toutes personnes intéressées à communiquer leurs commentaires sont invitées à les fournir au plus tard le 20 janvier 2012. Il est à noter que les commentaires soumis seront rendus publics à défaut d'avis contraire à cet effet.

Le projet de la ligne directrice est publié ci-après en versions française et anglaise. Ces documents sont également accessibles via la page d'accueil du site Web de l'Autorité au www.lautorite.qc.ca, à la section « Consultations publiques ».

Soumission des commentaires

Les commentaires doivent être soumis à :

M^{e} Anne-Marie Beaudoin
Secrétaire générale
Autorité des marchés financiers
800, square Victoria, 22^{e} étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Télécopieur : (514) 864-6381
Courrier électronique : consultation-en-cours@lautorite.qc.ca

Renseignements additionnels

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

Denis Fortin
Direction des normes et de l'assurance-dépôts
Autorité des marchés financiers
Téléphone : (418) 525-0337, poste 4647
Numéro sans frais : 1 877 525-0337
Courrier électronique: denis.fortin@lautorite.qc.ca

Le 18 novembre 2011

AUTORITÉ DES MARCHÉS FINANCIERS

PROJET

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

Novembre 2011

PROJET

TABLE DES MATIÈRES

PROJET

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.

PROJET

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[1] 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[2]. 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.

1 *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.

2 *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.

PROJET

Enfin, les attentes de l'Autorité s'inspirent des principes fondamentaux et des orientations des organismes internationaux[3] 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 »).

[3] 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.

PROJET

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[4]. 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.

[4] 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.

PROJET

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.

PROJET

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[5], 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[6], 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.

[5] 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).

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

PROJET

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[7] 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[8], 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;

[7] 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.

[8] 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[9].

  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[10]. 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[11]. 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;

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

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

11 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[12].

[12] 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.

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[13] 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[14];
- 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.

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

14 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.

PROJET

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 fidéicommis. Elle devrait également s'assurer que le client ne figure pas sur les listes des personnes et organisations présumément associées à des activités terroristes[15].

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;

[15] 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 »[16];

- qui sont des mandataires d'un client ou des bénéficiaires d'un contrat d'assurance[17].

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[18], 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;

[16] *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (2000, ch.17), article 9,3.

[17] L'identification et la vérification du bénéficiaire devraient être effectuées, au plus tard, lors de la prestation de la police d'assurance.

[18] Autorité des marchés financiers, Ligne directrice sur les pratiques commerciales (projet), mars 2011.

- pour les virements électroniques[19] 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.

[19] 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.

PROJET

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[20]. 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*[21], 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[22], 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*[23].

[20] Article 2.1 b) de l'entente entre le CANAFE et l'Autorité signée en juin 2006.

[21] 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.

[22] 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.

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

PROJET

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.

AUTORITÉ DES MARCHÉS FINANCIERS

DRAFT

FINANCIAL CRIME RISK MANAGEMENT GUIDELINE

November 2011

DRAFT

TABLE OF CONTENTS

DRAFT

Preamble

The *Autorité des marchés financiers* ("AMF") establishes guidelines setting out its expectations with respect to financial institutions' legal requirement to follow sound and prudent management practices and sound commercial practices. These guidelines therefore cover the execution, interpretation and application of this requirement.

The AMF favours a principles-based approach rather than a specific rules-based approach. As such, the guidelines provide financial institutions with the necessary latitude to determine the requisite strategies, policies and procedures for implementation of such management principles and to apply sound practices based on the nature, size and complexity of their activities.

The AMF considers governance, integrated risk management and compliance (GRC) as the foundation stones for sound and prudent management practices and sound commercial practices and, consequently, as the basis for the prudential framework provided by the AMF.

This guideline is part of this approach and sets out the AMF's expectations regarding sound and prudent financial crime risk management practices, including sound commercial practices.

DRAFT

Introduction

In the ordinary course of their activities, financial institutions may unwittingly or not be used to facilitate or be the target of activities associated with financial crime.

In addition to any losses the institution might sustain, the lack of diligence in its financial crime risk management could damage its reputation. In certain cases, this could lead to the public losing confidence in the institution itself and in the entire financial sector.

Thus, the scope of financial crime, and the growing threat these risks pose for consumers of financial products and services and for financial institutions require that the AMF encourage the implementation by financial institutions of an effective financial crime risk management framework.

In this context and pursuant to the authority[1] conferred upon the AMF under the various sectorial statutes it administers, it is issuing this guideline to inform financial institutions of its expectations with respect to financial institutions' legal requirement to follow sound and prudent financial crime risk management practices, including sound commercial practices.[2] The guideline favours *a priori* the need for financial institutions to have effective governance and to implement risk management practices in order to prevent and detect activities associated with financial crime.

The principles set forth in this guideline favour a proactive approach aimed at reducing the risk that a financial institution will be involved in financial crime activities. The application of these principles and compliance therewith by financial institutions should therefore be combined with the sustained efforts of the AMF and other stakeholders, including the police forces and Financial Transactions and Reports Analysis Centre of Canada *(*"FINTRAC") to fight financial crime so as to better promote the integrity of the markets and provide better protection for the public.

1 *An Act respecting insurance*, R.S.Q., c. A-32, ss. 325.0.1 and 325.0.2;
An Act respecting financial services cooperatives, R.S.Q., c. C-67.3, s. 565;
An Act respecting trust companies and savings companies, R.S.Q., c. S-29.01, s. 314.1.

2 *An Act respecting insurance,* R.S.Q., c. A-32, s. 222.2;
An Act respecting financial services cooperatives, R.S.Q., c. C-67.3, s. 66.1;
An Act respecting trust companies and savings companies, R.S.Q., c. S-29.01, s. 177.3.

DRAFT

Lastly, the AMF's expectations are based on core principles and guidelines issued by international organizations,[3] including the Basel Committee on Banking Supervision ("BCBS"), the Financial Action Task Force ("FATF") and the International Association of Insurance Supervisors ("IAIS").

[3] Basel Committee on Banking Supervision, Customer due diligence for banks, October 2001;

Basel Committee on Banking Supervision, Core Principles Methodology, October 2006;

Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, February 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;

Financial Action Task Force, The FATF Forty Recommendations, October 2003. The IX Special Recommendations, October 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.

Scope

This financial crime risk management guideline is intended for insurers of persons (life and health), damage insurers, portfolio management companies controlled by an insurer, mutual insurance associations, financial services cooperatives as well as trust and savings companies, which are governed by the following Acts:

- *An Act respecting insurance*, R.S.Q., c. A-32
- *An Act respecting financial services cooperatives,* R.S.Q., c. C-67.3
- *An Act respecting trust companies and savings companies*, R.S.Q., c. S-29.01.

This guideline applies to financial institutions operating independently as well as to financial institutions operating as part of a financial group.[4] In the case of financial services cooperatives and mutual damage-insurance associations that are members of a federation, the standards or policies adopted by the federation should be consistent with—and even converge on—the principles of sound and prudent management practices, including sound commercial practices prescribed by law and detailed in this guideline.

The generic terms “financial institution” and “institution” refer to all financial entities covered by the scope of this guideline.

[4] For purposes of this guideline, “financial group” refers to any group of legal persons composed of a parent company (financial institution or holding company) and legal persons affiliated therewith.

Coming into effect and updating

This financial crime risk management guideline will come into effect on month xx, 201X.

With respect to the legal requirement of institutions to follow sound and prudent management practices, including sound commercial practices, the AMF expects each institution to develop strategies, policies and procedures based on its nature, size, complexity and risk profile, and to ensure the adoption of the principles underlying this guideline by month XX, 201X (two years after coming into effect). Where an institution has already implemented such a framework, the AMF may verify whether it enables the institution to satisfy the requirements prescribed by law.

This guideline will be updated based on developments in financial crime risk management and in light of the AMF's observations in the course of its supervision of financial institutions.

DRAFT

Financial crime risks

In the insurance and deposit sectors, a financial institution may be the target of activities of every type and scope associated with financial crimes and involving a variety of parties, including customers, employees, officers and those with whom it has business dealings, such as suppliers.

For purposes of this guideline, the principal activities associated with financial crime are internal fraud and external fraud,[5] money laundering, embezzlement, the illegal transfer of funds to financial or tax havens,[6] illegal tax avoidance (tax evasion) and terrorist financing. Certain activities are frequently reported in the media, such as fraudulent insurance claims, fraud involving mortgage loans, debit cards and credit cards, and the fraudulent use of confidential customer information.

Financial crime can expose a financial institution to various risks, including operational, legal, regulatory and reputational risks. The extent of these risks, alone or in combination, is particularly wide when the perpetrators take advantage of deficiencies in the institution's management or the complicity of its employees or officers.

A financial institution should have a global perspective on financial crime risks. It should establish measures to prevent financial crime and detect activities that may be associated with it. These measures should also facilitate examinations, inspections and investigations relating to financial crime.

[5] Generally speaking, internal fraud is fraud committed by a senior executive, a director or an employee, whether or not in collusion with an internal or external party (for example, embezzlement by an employee).

Generally speaking, external fraud is fraud committed by a customer or a third party (for example, a forged signature on a cheque, an insurance claim in which the value of an item claimed has intentionally been overestimated).

[6] The Organisation for Economic Co-operation and Development (OECD) defines a tax haven as a country or territory with no or nominal taxation. A financial haven is a country or territory where banking secrecy prevails. Reference: www.oecd.org.

DRAFT

Financial crime risk management governance

Principle 1: Roles and responsibilities of the board of directors and senior management

The AMF expects a financial crime risk management framework to be supported by effective governance.

The AMF considers the board of directors[7] and senior management to be ultimately responsible for establishing sound and prudent financial crime risk governance management practices and sound commercial practices.

In light of the roles and responsibilities incumbent upon them under the Governance Guideline,[8] the board of directors and senior management should, among other things:

- develop, approve and implement strategies, policies and procedures.

  In order for an institution to manage financial crime risks effectively and efficiently, these strategies, policies and procedures should focus primarily on preventing and detecting activities associated with financial crime and address the institution's vigilance with respect to customers, employees, officers and those with whom it has business dealings. To this end, the institution should take into account its vulnerability to these risks, particularly with respect to the following elements:

  - customers and the nature of their transactions;
  - employees, officers and service providers;
  - the financial products and services offered;
  - the institution's information systems and internal controls;
  - the methods of used by the authors of activities associated with financial crime and the possibility of operational events and their potential impact.

7 A reference to the board of directors can also include a board committee, such as a board committee established to examine specific issues.

8 *Autorité des marchés financiers*, Governance Guideline, April 2009.

Strategies, policies and procedures should be documented and reviewed on a regular basis, particularly in light of changes in the institution's customers, the marketing of new products and the growing complexity of activities associated with financial crime;

- promote a culture that encourages ethical conduct at every level of the institution;
- ensure that staff and officers have proper training and that the people assigned to manage financial crime risks are experienced.[9]

  Responsibility for developing and implementing the financial crime risk management strategy should be entrusted to the chief risk officer.[10] Depending on the size of the institution and the extent of the financial crime risks, a person could also be appointed to be in charge of financial crime risk management;

- adequately monitor financial crime activities that are suspected or have been identified. They should also ensure that these activities are reported to the appropriate authorities and that any relevant information and results of examinations and investigations are communicated;
- ensure that the institution complies with all statutes, regulations and guidelines.[11] As such, they should ensure, in particular, that reports, documents and declarations are completed and sent to the AMF and to the other appropriate authorities, in the prescribed form and within the stipulated time limits.

Framework for financial crime risk management

Principle 2: Financial crime risk management

The AMF expects financial crime risk management to form an integral part of a financial institution's integrated risk management.

The financial institution should manage financial crime risks within its integrated risk management framework. Accordingly, it should give consideration to the interrelationships and interdependencies between risks. This means that the institution should:

- identify, assess and quantify financial crime risks;
- implement risk mitigation measures in order to reduce the likelihood of events that could affect the institution.

9 *Autorité des marchés financiers*, Guideline Governing Integrity and Competency Criteria (draft), October 2011.

10 *Autorité des marchés financiers*, Integrated Risk Management Guideline, April 2009.

11 *Autorité des marchés financiers*, Compliance Guideline, April 2009.

The integrated risk management approach should allow the institution to identify operational risk events associated with financial crime and to implement measures to reduce the occurrence of such events and their potential impact on the institution.

Thus, the institution should take the following, in particular, into account:

- internal factors such as:
  - its organizational structure, the nature of its activities, its strategic orientations and its policies;
  - the quality of its internal controls, including the segregation of duties and the delegation of powers;
  - the nature and characteristics of its products;
  - the risk profile of its customers, their business activities and the volume of their local and cross-border transactions;
  - the information technology used;
  - its business dealings, including any possible outsourcing;
  - employee versatility and turnover, the degree of employee knowledge about financial crime, the quality of its labour relations;
- external factors such as:
  - legal, regulatory and normative requirements relating to the fight against financial crime, including the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (2000, c.17) ("Proceeds of Crime Act"), and changes to the designated persons list established by the United Nations;[12]

    Among other things, the institution should participate in an electronic funds transfer tracing system. The AMF expects the institution to fulfill its obligation to declare certain electronic funds transfers made by its customers to the FINTRAC;[13]

[12] Reference: *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*. Additional information is available on the AMF website: http://www.lautorite.qc.ca/en/suppress-terrorism.html.

[13] *Guideline 8B: Submitting SWIFT Electronic Funds Transfer Reports to FINTRAC*, published by FINTRAC in June 2011.

- the economic and social context, new threats and opportunities involving financial crime as well as changes in the techniques and methods used;[14]

- changes in international orientations for fighting financial crime.

Principle 3: Intra-group management

The AMF expects a financial institution to manage its financial crime risks in accordance with the management framework applicable to the group to which it belongs.

Activities associated with financial crime carried out through a financial institution that forms part of a group are likely to have significant repercussions on the other entities in the group and adversely affect their solvency and, ultimately, the reputation of the entire group.

Consequently, it is important to adopt a comprehensive approach to financial crime risk management at the group level, locally, nationally and internationally.

It is essential that coherent standards be adopted within the group and that the entities forming part of the group exchange information, particularly in order to identify and assess areas of vulnerability and reduce financial crime risks.

Principle 4: Customer vigilance

The AMF expects a financial institution to conduct continuous vigilance with respect to customers by having sufficient knowledge about them and applying appropriate procedures so as to detect transactions likely to be associated with financial crime.

In applying customer vigilance measures, the financial institution should consider the extent of financial crime risks, particularly with respect to monetary transactions, insurance products and investment products.

[14] Acting on information gathered by its investigators, including through cyber-surveillance, the AMF regularly issues warnings. The information may also be received from investors and from regulators in other jurisdictions. http://www.lautorite.qc.ca/en/alerts.html

Know your customer

The know your customer rule is an essential component of financial crime risk management. It contributes to reducing the likelihood that operational events will occur through a financial institution.

Knowing customers, including their dealings with the institution's other customers and, if applicable, with the other entities forming part of the institution's group, will also allow an institution to measure its concentration risk. Extra vigilance should be conducted especially in the context of related counterparties and related party lending.

An institution should establish appropriate identification procedures and a risk profile and acceptance criteria for its customers, particularly for categories of customers that are likely to present a greater risk. Accordingly, it should require all appropriate supporting documents based on the type of customer and the particular characteristics of certain accounts, such as corporate, institutional or trust accounts. It should also ensure that the customer is not on the lists of persons and organizations believed to be associated with terrorist activities.[15]

To the extent possible, an institution should conduct increased vigilance with respect to customers:

- whose structure or type of activity makes it difficult to identify the owner or controlling interests;
- who act as financial intermediaries, securities dealers, advisers or representatives, custodians, trustees or professionals;
- where something seems odd, for example, a customer who often changes addresses, who refuses to provide proof of identity or who is more interested in the surrender of an insurance policy than meeting insurance needs;
- who are large depositors or borrowers, groups of related borrowers, or "politically exposed foreign persons";[16]
- who are the mandataries of a customer or the beneficiaries of an insurance contract.[17]

[15] See note 12.

[16] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c.17), s. 9.3.

[17] The identity and verification of the beneficiary should take place no later than the payment of benefits provided for under the insurance policy.

The institution should keep an up-to-date register of its customers and their transactions. It must also protect its customers' personal information,[18] particularly so as to prevent the unauthorized use of that information.

Monitoring customer transactions

Based on the risk profile of its various customer categories, an institution should take appropriate vigilance measures, including:

- determining the criteria for controlling, monitoring and overseeing its customers' transactions, in particular as regards the source of funds, the nature of the transactions, transactions that appear to be linked, the type of currency and the country where the recipient is located;

- reviewing all transactions with no apparent economic or lawful purpose or in respect of which it has reasons to believe that the transaction is likely to be associated with financial crime;

- carrying out a more in-depth review of the context and purpose:

  - of any complex transaction or any transaction whose source of funds is questionable or inconsistent with the person's risk profile;

  - of any unusual transaction, particularly if the volume of transactions is unusual in light of the customer's history and the nature of its activities;

  - of frequent cash (or cash equivalent) transactions or transactions carried out in unusual circumstances in light of the customer's profile, and of important fund transfers carried out with no apparent purpose for a specific customer;

  - of electronic transfers[19] made by a customer through another financial institution for the purpose of making a significant amount of money available to a beneficiary (the customer or another person);

  - of any transaction with certain countries that represent a greater financial crime risk.

The institution should implement an appropriate process for minimizing fraud by its customers with respect to insurance claims. Additional measures, particularly relating to the validation of amounts claimed, should be implemented, as needed and depending on the size of the claims.

Lastly, the results of customer transaction monitoring should be recorded in management reports.

[18] *Autorité des marchés financiers*, Commercial Practices Guideline (draft), March 2011.

[19] Including fund transfers, cross-border transfers and domestic transfers.

Principle 5: Employees, officers and business relationships vigilance

The AMF expects a financial institution to conduct continuous vigilance with respect to employees, officers and those with whom it has business relationships through effective internal controls and appropriate procedures so as to detect situations likely to be associated with financial crime.

The institution should focus on preventing activities associated with financial crime involving its employees and officers. However, it should also exercise vigilance as regards individuals who might carry on criminal activities and closely monitor those with whom it has business relationships, particularly its suppliers.

Identifying vulnerabilities

An institution should identify its vulnerability to operational risk events or schemes that could involve employees in the performance of their work or officers in the fulfilment of their roles and responsibilities, such as:

- employee theft of money or property belonging to the institution;
- unauthorized use of customers' personal information;
- supplier corruption, bribes, kickbacks or commissions;
- payments to fictitious suppliers for services not rendered to the institution;
- falsification of documents, failure to record transactions and willful presentation of incorrect financial information.

Controls

The institution should implement internal controls to deal with these sources of vulnerability to financial crime risks. To this end, it should establish:

- controls focused on allocating responsibilities and segregating tasks related to customer transactions and protection of the institution's assets;
- security mechanisms for its information technology, including outsourced information technology activities, in order to prevent the unauthorized use by employees of customers' personal information;
- a rigorous and documented process for awarding contracts.

Lastly, the institution should pay close attention to clues or signals that could lead to the discovery of a scheme associated with financial crime activities, for example, deficiencies involving controls, a failure to follow established processes, an employee who often postpones his vacations or has unusual behaviour, customer complaints and missing assets following an inventory.

It should also consider possible collusion among several individuals for the purpose of sidestepping the internal controls implemented by the institution to protect itself against financial crime risks.

Principle 6: Examination of suspicious activities

The AMF expects a financial institution to carry out examination when it suspects or detects activities associated with financial crime.

The financial institution should react promptly to any situation where activities associated with financial crime are suspected or detected. The examinations may require skills in several fields of expertise, such as legal, tax or information technology skills. The institution should document the results of its examinations and ensure to achieve the various examinations within the legislative framework applicable to it.

When an institution has been the target of an activity associated with financial crime, it should use the event as a learning opportunity and, if applicable, adjust its policies and procedures to reduce the likelihood of recurrence.

An institution may also be required to co-operate with the AMF during inspections and investigations authorized under the sectorial statutes applicable to it, the scope of this collaboration shall be limited to the extent permitted by applicable law. To this end, the AMF may, during these inspections or investigations, have access to information relating to instructions and mechanisms implemented by the institution under Part 1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and could then provide them to FINTRAC[20]. If applicable, the institution may also be required to co-operate during examinations and investigations carried out by financial crime fighting authorities, including the *Sûreté du Québec*, the Royal Canadian Mounted Police and FINTRAC.

[20] Section 2.1 (b) of the memorandum of understanding signed between FINTRAC and the AMF in June 2006.

Principle 7: Communication of information

The AMF expects a financial institution to communicate information regarding activities associated with financial crime to every appropriate authority, subject to applicable laws.

In order to facilitate the application and enforcement of fiscal, penal and criminal statutes or foreign legislation involving the same matters, the AMF recalls the legal obligation for a financial institution to communicate all information concerning activities associated with financial crime to every other appropriate regulator, including the AMF, FINTRAC,[21] the *Sûreté du Québec* and the *Agence du revenu du Québec*.

An institution also has the obligation to verify and report to the AMF on[22] the existence of property in their possession or control and belonging by an entity found on the list established by the Regulations Establishing a List of Entities[23].

[21] On June 19, 2006, the AMF and FINTRAC signed a memorandum of understanding ("MOU") to share information. The MOU also seeks to prevent duplication of efforts by FINTRAC and the AMF while reducing the burden of such efforts on the institutions and representatives targeted thereby. FINTRAC website: www.canafe.ca.

[22] Under subsection 83.11(2) of the *Criminal Code* (R.S.C., 1985, c. C-46), financial institutions subject to the AMF's oversight must provide such a report.

[23] SOR/2002-284made under article 83.05 of the Criminal Code.

DRAFT

Supervision of sound and prudent management practices and sound commercial practices

To foster the establishment of sound and prudent management practices within financial institutions and sound commercial practices, the AMF, acting within the scope of its supervisory activities, intends to assess the degree of compliance with the principles set forth in this guideline in light of the specific attributes of each institution. Consequently, it will examine the effectiveness and relevance of the strategies, policies and procedures adopted by financial institutions as well as the quality of oversight and control exercised by their board of directors and senior management.

Financial crime risk management practices are constantly evolving. The AMF therefore expects decision makers at financial institutions to remain current with best practices and to adopt such practices, to the extent that they address their needs.