Note de mise en œuvre

Objet : La gouvernance d'entreprise au sein des institutions appliquant l'approche standard ou une AMA

Catégorie : Fonds propres

N^{o} : A & A-1 Date : Mai 2006

I. Introduction

L'objectif de cette note de mise en œuvre est de présenter les lignes directrices et les pratiques qui doivent présider à la gouvernance d'entreprise au sein des institutions[1] qui appliquent l'approche standard ou une approche de mesure avancée (AMA) au risque opérationnel. La note étoffe les exigences minimales décrites au chapitre 6 de l'ébauche de la ligne directrice A, *Normes de fonds propres* (NFP), et au chapitre 7 de l'ébauche de la ligne directrice A-1, *Normes de fonds propres*.

Les institutions qui appliquent l'approche indicateur de base (AIB) et qui, par conséquent, n'ont pas à se plier au processus d'évaluation du risque opérationnel du BSIF[2], sont encouragées à adopter les pratiques clés décrites ici, selon les besoins.

La présente décrit les exigences et les attentes établies en fonction des principes, des considérations qui touchent le conseil d'administration, la direction générale, la fonction de gestion du risque, la préparation de rapports et la vérification interne dans le cadre de la gouvernance d'entreprise au sein des institutions qui appliquent l'approche standard ou une AMA.

[1] Les banques et les sociétés de portefeuille bancaires auxquelles la *Loi sur les banques* s'applique et les sociétés de fiducie et de prêt auxquelles la *Loi sur les sociétés de fiducie et de prêt* s'applique sont collectivement désignées « institutions ».

[2] Note de mise en œuvre du BSIF : *Évaluation du risque opérationnel par les institutions appliquant l'approche standard ou une approche de mesure avancée (AMA)*, septembre 2005.

Table des matières

II. Contexte

Dans le cadre du Processus d'évaluation du risque opérationnel du BSIF[3], on s'attend à ce que les institutions satisfassent aux exigences des NFP liées à l'approche qu'elles cherchent à mettre en œuvre en ce qui a trait au risque opérationnel, c.-à-d., l'approche standard ou une AMA. De plus, les institutions devront systématiquement démontrer au BSIF que la gouvernance d'entreprise[4] qu'elles exercent ainsi que la gestion du risque et les pratiques en matière de contrôle du risque opérationnel qu'elles appliquent reflètent leur nature, l'étendue de leurs activités, leur complexité et leur profil de risque.

L'orientation présentée dans le présent document est compatible avec l'évaluation faite par le BSIF de l'efficacité dont font preuve les institutions au chapitre de la gouvernance d'entreprise, de la gestion du risque et des pratiques de contrôle du risque opérationnel décrites par le *Cadre de surveillance* du BSIF (1999) et dans le document *Ligne directrice sur la gouvernance d'entreprise* (janvier 2003). Le BSIF utilisera son approche de surveillance basée sur le recours afin d'évaluer l'à-propos et l'efficacité de la gestion du risque opérationnel et des pratiques de contrôle des institutions appliquant l'approche standard ou une AMA, et pour évaluer leur respect soutenu des exigences minimales.

III. Lignes directrices et pratiques

Le dispositif de gestion du risque opérationnel d'une institution met à contribution les politiques et les pratiques qui président à l'identification du risque opérationnel, à sa mesure et à son évaluation, au contrôle et au suivi dont il fait l'objet, ainsi qu'à la préparation des rapports afférents. Ces politiques et pratiques comprennent les responsabilités de surveillance imputées à la direction générale et au conseil d'administration, et celles qui ont été attribuées à d'autres au chapitre du risque opérationnel.

L'institution doit appliquer des mesures de contrôle adéquates qui garantissent le respect systématique des exigences liées aux NFP visant l'approche standard ou l'AMA, le cas échéant.

[3] Note de mise en œuvre du BSIF : *Évaluation du risque opérationnel par les institutions appliquant l'approche standard ou une approche de mesure avancée (AMA)*, décembre 2005.

[4] Le document *Ligne directrice sur la gouvernance d'entreprise* du BSIF décrit la gouvernance d'entreprise comme un ensemble de « mécanismes de surveillance » qui comprend les processus, les structures et l'information utilisés pour assurer la direction et la supervision de la gestion de l'entreprise. Dans le document *Cadre de surveillance*, le BSIF décrit le rôle des six « fonctions de contrôle de gestion des risques » dont peut se doter une institution pour assurer une surveillance indépendante de ses opérations, au nombre desquelles on trouve le conseil d'administration, la direction générale et la vérification interne. Dans la présente note de mise en œuvre, les références à ces fonctions de surveillance tiendront compte de la description qui est faite de leur rôle dans le *Cadre de surveillance*.

1. Conseil d'administration

Le conseil d'administration doit, au besoin, participer activement à la surveillance du dispositif de gestion du risque opérationnel (NFP, paragraphe 660). Ainsi, le conseil d'administration devrait :

- comprendre à fond le profil de risque opérationnel de l'institution, dont les agents internes et externes qui pourraient constituer un risque opérationnel pour l'institution;
- établir un seuil de tolérance ou d'affinité convenable, ce qui peut inclure une gamme d'énoncés quantitatifs ou subjectifs, le cas échéant, compte tenu des types et du degré de risque opérationnel qu'une institution pourrait se permettre;
- bien saisir les conséquences de l'application de telle ou telle approche de risque opérationnel au sein de l'institution (l'approche standard ou une AMA);
- passer en revue les politiques de gestion des expositions d'envergure au risque opérationnel et les pratiques de gestion[5];
- examiner au besoin les rapports sur le risque opérationnel conformément à la section 4 ci-après;
- s'assurer que les processus et les systèmes[6] de gestion du risque opérationnel et de mesures soient solides et ne perdent pas leur vigueur avec le temps;
- être informé de tous les changements stratégiques importants qui pourraient être apportés au profil de risque opérationnel de l'institution et passer chacun d'eux en revue (p. ex., faire le suivi d'une fusion ou d'une acquisition, ou du recours à la sous-traitance étrangère pour la prestation de services administratifs).

2. Direction générale

La direction générale devrait prendre une part active à la surveillance et à la gestion du dispositif de gestion du risque opérationnel. C'est la direction générale qui, en regard du conseil d'administration, est responsable de l'efficacité de la mise en œuvre d'un dispositif de gestion du risque opérationnel qui convienne au profil de risque de l'institution.

---

[5] Le paragraphe h) de l'annexe 8 de la ligne directrice sur les NFP stipule que la politique qu'une institution utilise pour circonscrire son secteur d'activités devrait être soumise à l'approbation du conseil d'administration. Le BSIF reconnaît toutefois que la délimitation d'un secteur d'activités est, en soi, une activité opérationnelle et qu'elle n'est pas, *a priori*, le type d'information au sujet de laquelle le conseil d'administration a l'habitude de se prononcer. Dans cette optique, il serait peut-être indiqué de soumettre la politique utilisée pour circonscrire le secteur d'activités à l'approbation de la direction générale.

[6] Comme le mentionne le paragraphe 663 a) de la ligne directrice sur les NFP, le terme « système » ne fait pas nécessairement référence à un dispositif technologique de gestion des risques opérationnels; il faut plutôt y voir une référence à l'ensemble des politiques et des processus mis en place pour identifier, évaluer, surveiller et contrôler le risque opérationnel à l'échelle de l'institution.

En vertu des responsabilités qui lui incombent, la direction générale doit :

- comprendre à fond le profil de risque opérationnel de l'institution, dont les agents internes et externes qui pourraient constituer un risque opérationnel pour l'institution;
- établir un seuil de tolérance ou d'affinité convenable, ce qui peut inclure une gamme d'énoncés quantitatifs ou subjectifs, le cas échéant, conte tenu des types et du degré de risque opérationnel qu'une institution pourrait se permettre;
- bien saisir les conséquences de l'application de telle ou telle approche en matière de risque opérationnel au sein de l'institution (l'approche standard ou une AMA);
- définir de façon précise la hiérarchie, les ressources, les responsabilités et les exigences en matière de production de rapports afin que la responsabilité à l'égard de la mise en œuvre et de la gestion du dispositif de gestion du risque opérationnel soit sans équivoque;
- voir à ce que le cadre de gestion du risque opérationnel convienne aux besoins de l'institution, à ce qu'il soit bien appliqué de façon systématique à l'échelle de l'institution et à ce qu'il ne perde pas de sa vigueur avec le temps;
- donner son aval aux politiques, aux procédures, aux normes et aux documents d'appui ayant trait au dispositif de gestion du risque opérationnel;
- examiner les rapports sur l'exposition de l'institution au risque opérationnel et les activités de gestion, de même que sur l'évolution des situations comportant un important élément de risque opérationnel;
- voir à ce que le dispositif de gestion du risque opérationnel et son application fassent régulièrement l'objet d'un examen indépendant.

La direction générale des institutions qui appliquent une AMA est tenue de respecter certaines exigences supplémentaires; elle doit notamment :

- comprendre à fond les systèmes de mesures et les procédures qui peuvent affecter le dispositif de gestion du risque opérationnel et les répercussions que cela peut avoir sur les fonds propres liés au risque opérationnel;
- s'assurer que les systèmes et procédures de mesure tiennent compte d'éléments clés tels que l'usage de données internes, les données externes pertinentes, les analyses de scénarios et les facteurs reflétant l'environnement opérationnel et les systèmes de contrôle interne;
- s'assurer (et en donner l'assurance au conseil d'administration) que le cadre de gestion et les systèmes de mesure du risque opérationnel sont bien conçus et conformes au test d'application, afin que le système soit intégré de près aux processus appliqués quotidiennement dans le cadre de la gestion du risque;
- se tenir au courant des pratiques émergentes au sein de l'industrie en ce qui a trait à la mesure et à la gestion du risque opérationnel.

3. Fonction de gestion du risque opérationnel

Les institutions qui appliquent l'approche standard ou une AMA sont tenues d'avoir une « fonction de gestion du risque opérationnel » (FGRO) qui sera chargée de la conception et de la mise en œuvre, à l'échelle de l'entreprise, du dispositif de gestion du risque opérationnel de la banque. Dans ce contexte, une « fonction » désigne une instance organisationnelle spéciale composée d'une personne ou plus et vouée entièrement à la gestion du risque opérationnel.

Toutefois, selon le paragraphe 663 a) de la ligne directrice sur les NFP, il est admis qu'en raison de leur taille et de leur complexité, les institutions qui appliquent l'approche standard ne sont pas toujours en mesure de se doter d'une instance organisationnelle spécialement dédiée à la gestion du risque opérationnel[7]. Dans les institutions de plus grande taille et plus complexes, la FGRO peut s'appuyer sur d'autres unités organisationnelles indépendantes ayant une expertise liée à certaines expositions au risque opérationnel, comme l'impartition et la poursuite des activités.

Pour gérer le risque opérationnel, il faut notamment :

- mettre au point des stratégies afin d'identifier, d'évaluer/de mesurer, de surveiller et de contrôler/diminuer le risque opérationnel;
- élaborer et documenter des politiques et des procédures à l'échelle de l'entreprise ayant trait au cadre de gestion du risque opérationnel de la banque et à la gestion des expositions au risque opérationnel, le cas échéant;
- instaurer des moyens de retracer de façon rigoureuse les données pertinentes en matière de risque opérationnel, dont les pertes importantes;
- concevoir et mettre en œuvre un système de notification du risque opérationnel;
- s'assurer qu'il existe des procédures et des processus adéquats pour superviser adéquatement les pratiques de gestion du risque opérationnel de l'institution.

Afin de garantir la conformité, le cadre de gestion du risque opérationnel devrait comporter une série de politiques, de mesures de contrôle et de procédures internes qui auront été documentées afin de procéder au traitement des aspects non conformes et des cas d'exception. Les fonctions de gestion du risque opérationnel et les unités opérationnelles doivent se prêter aux tests de contrôle et aux vérifications, par les services de vérification ou une autre fonction tout aussi indépendante, afin de vérifier le degré de conformité de l'efficacité des contrôles internes au dispositif de gestion du risque opérationnel.

En vertu du paragraphe 666 a) de la ligne directrice sur les NFP, la FGRO d'une institution qui applique une AMA doit opérer de façon indépendante. Elle doit être capable de démontrer au Conseil et à la direction générale qu'elle est en mesure de livrer des évaluations neutres et objectives des expositions de l'institution au risque opérationnel et de l'efficacité des pratiques

[7] Les institutions qui aimeraient avoir des précisions concernant les attentes du BSIF à cet égard peuvent se reporter à la section 7.3.1 de la ligne directrice A-1 sur les NFP et à la section 6.3.1 de la ligne directrice A sur les NFP.

de gestion du risque opérationnel. Ainsi, outre les responsabilités énoncées précédemment, la FGRO d'une institution qui applique une AMA doit :

- concevoir et mettre en œuvre la méthode qui servira à mesurer le risque opérationnel de l'entreprise;
- s'assurer que les processus qui présideront à la mesure du risque opérationnel soient intégrés de près aux processus de gestion du risque de l'institution;
- définir les rôles qui seront attribués à la modélisation et à la validation, en veillant à ce que la ligne de démarcation entre les deux tâches soit bien définie.

4. Production de rapports

La production ponctuelle et périodique de rapports à l'intention du conseil d'administration, de la direction générale et de la direction de l'unité responsable des opérations fait partie de la gestion efficace du risque opérationnel. La nature et la portée du rapport devraient être adaptées aux besoins de son destinataire. La fréquence et la teneur des rapports internes ayant trait au risque opérationnel devraient refléter la nature, la portée et la complexité du profil de risque de l'institution. Par exemple, la direction générale et le conseil d'administration pourraient exiger que des renseignements leur soient fournis de façon périodique au sujet des tendances, des niveaux de vulnérabilité et d'autres enjeux clés. Les responsables de la gestion des opérations auront quant à eux plus fréquemment besoin d'une information détaillée afin de les aider à gérer convenablement le risque opérationnel sur une base quotidienne. Les institutions devraient établir des pratiques pour faire en sorte que les rapports sur le risque opérationnel donnent lieu à des actions appropriées et conséquentes.

Les rapports sur le risque opérationnel devraient comprendre les renseignements fondamentaux suivants :

- les exigences de fonds propres au titre du risque opérationnel, selon les besoins;
- les données relatives au risque opérationnel, notamment les pertes significatives par ligne de métier;
- les résultats des évaluations pertinentes des facteurs qui témoignent de l'environnement opérationnel, des autoévaluations en matière de risque et de contrôle ainsi que d'autres valeurs de contrôle internes.

5. Vérification interne[8]

La vérification interne (ou une autre fonction semblable tout aussi indépendante) est chargée d'évaluer l'efficacité des contrôles internes de l'institution à l'égard des processus et des systèmes de gestion du risque opérationnel conçus pour garantir le respect des exigences de l'approche standard ou d'une AMA. La portée et la fréquence des examens qui font partie d'une

[8] Comme le stipule la ligne directrice sur les NFP, le BSIF n'oblige pas les institutions à se prêter à des vérifications externes de leur système d'évaluation du risque opérationnel.

vérification interne devraient être proportionnelles au risque opérationnel que présente l'activité observée.

Les activités de vérification interne doivent inclure, sans s'y limiter :

- une évaluation de l'efficacité des contrôles internes de l'institution, ainsi que des éléments de conception de ces derniers, sous l'angle du respect des exigences de l'approche standard ou de l'AMA;
- la définition de la portée et de la fréquence des activités de vérification interne en accord avec les méthodes et les principes de vérification de cette fonction;
- une évaluation de la pertinence des ressources et des compétences requises pour la conduite des travaux de vérification;
- une évaluation périodique de l'efficacité des contrôles internes de l'institution à l'égard des processus de gestion du risque opérationnel à l'échelle de l'institution; ces évaluations doivent englober les activités des unités opérationnelles et de la fonction de gestion du risque opérationnel.

En plus des activités précitées, les vérifications internes au sein des institutions qui appliquent une AMA devraient :

- évaluer l'efficacité des contrôles internes de l'institution à l'égard des modèles de risque opérationnel et des systèmes de mesure des risques du cadre de gestion du risque opérationnel, de même que l'intégrité des données et les processus de validation.