AUTORITÉ DES MARCHÉS FINANCIERS

CADRE DE TRAVAIL

Caisses non membres d'une fédération, sociétés de fiducie et sociétés d'épargne désirant adopter une approche standard pour le calcul des exigences de fonds propres au titre du risque opérationnel

Juillet 2010

Table des matières

INTRODUCTION

L'Autorité des marchés financiers *(*l'« Autorité »*)* a publié le XX mois 2011 sa *Ligne directrice sur les normes relatives à la suffisance du capital* (la « ligne directrice ») à l'intention des caisses non membres d'une fédération, sociétés de fiducie et sociétés d'épargne. Cette dernière repose sur l'approche décrite dans Bâle II[1] et permet de moduler les exigences minimales de fonds propres au profil de risque des institutions[2]. La ligne directrice expose les exigences des approches plus simples prévues par le dispositif Bâle II, soit l'approche standard pour le risque de crédit et les approches indicateur de base et standard pour le risque opérationnel.

Dans cette perspective, l'institution qui désire appliquer l'approche standard au titre du risque opérationnel devra démontrer qu'elle satisfait aux exigences applicables à l'utilisation de cette méthode de calcul, telles que décrites principalement au chapitre 6, mais également aux chapitres 8 et 9 de la ligne directrice[3].

À cette fin, l'Autorité publie le présent cadre de travail[4] qui précise les principes en matière de gouvernance ainsi que ceux relatifs à la « tenue des données »[5] qui doivent présider au sein de l'institution qui applique cette approche. Ces principes serviront à évaluer, initialement et de façon continue, dans quelle mesure l'institution satisfait aux exigences de la ligne directrice. Le respect de ces principes constituera un facteur déterminant sur lequel s'appuiera l'Autorité pour autoriser l'institution à appliquer l'approche standard au titre du risque opérationnel.

Les institutions qui appliquent l'approche indicateur de base (AIB) et qui par conséquent, n'ont pas à se soumettre au processus d'évaluation du risque opérationnel par l'Autorité, sont tout de même encouragées à adopter les saines pratiques décrites dans le présent document.

---

1 La ligne directrice incorpore le dispositif de la Banque des règlements internationaux (BRI) publié initialement en juin 2004 puis, révisé en novembre 2005 et en juin 2006, intitulé « *Convergence internationale de la mesure et des normes de fonds propres* ».

2 Dans le présent cadre de travail, les expressions génériques « institution financière » ou « institution » sont utilisées pour faire référence à toutes les caisses et sociétés visées par le champ d'application (chapitre 1) de la ligne directrice.

3 En vertu de la ligne directrice, l'institution qui met en œuvre l'approche standard doit être en mesure d'en faire le suivi et de rendre compte des données pertinentes relatives au risque opérationnel, notamment les pertes significatives que subit une ligne de métier importante. L'Autorité convient que le degré de complexité de ce mécanisme de suivi et de reddition de comptes doit être adapté à la taille de l'institution, en prenant en compte la structure de rapports de celle-ci, ainsi que son exposition au risque opérationnel.

4 Afin d'assurer une harmonisation dans l'application de la nouvelle approche proposée par le Comité de Bâle, le cadre de travail s'inspire des notes de mise en œuvre intitulées « Tenue des données par les instituions appliquant l'approche standard ou une approche de mesure avancée (AMA) » et « La gouvernance d'entreprise au sein des institutions appliquant l'approche standard ou une AMA », publiées en mai 2006 par le Bureau du surintendant des institutions financières. En effet, les institutions financières visées par la ligne directrice doivent répondre à des normes et aux pratiques saines équivalentes à celles des autres institutions qui opèrent sur les mêmes marchés.

5 L'expression « tenue des données » s'entend des principales composantes du processus de gestion des données, notamment la collecte des données, leur traitement, l'accès aux données et leur extraction, de même que la conservation et le stockage.

1. GOUVERNANCE AU SEIN DES INSTITUTIONS APPLIQUANT L'APPROCHE STANDARD AU TITRE DU RISQUE OPÉRATIONNEL

1.1 Introduction

L'Autorité a donné en 2009 deux lignes directrices aux institutions financières signifiant explicitement ses attentes en matière de gouvernance[6] et de gestion intégrée des risques[7]. L'objectif de la présente section est d'apporter des précisions sur la notion de gouvernance en lien avec l'utilisation de l'approche standard pour le risque opérationnel, particulièrement en ce qui a trait aux attributions du conseil d'administration, de la haute direction, de la fonction de gestion du risque opérationnel, des rapports et de la vérification interne.

1.2 Principes de gouvernance

Le cadre 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'aux rapports afférents.

L'institution financière doit appliquer des mesures de contrôle adéquates qui garantissent le respect des exigences de la ligne directrice en regard de l'approche standard.

1.2.1 Conseil d'administration

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

- comprendre le profil de risque opérationnel de l'institution, incluant les facteurs internes et externes qui pourraient constituer un risque opérationnel pour l'institution;
- examiner et approuver un niveau de tolérance au risque opérationnel de l'institution adéquat, ce qui peut inclure une gamme d'énoncés qualitatifs ou subjectifs, le cas échéant, pour les types et/ou le niveau du risque opérationnel que l'institution peut se permettre;
- bien saisir les conséquences de l'application de l'approche standard au titre du risque opérationnel;
- passer en revue les politiques de gestion des expositions d'envergure au risque opérationnel et les pratiques de gestion;
- examiner, au besoin, les rapports sur le risque opérationnel;

[6] Autorité des marchés financiers, Ligne directrice sur la gouvernance, Avril 2009.

[7] Autorité des marchés financiers, Ligne directrice sur la gestion intégrée des risques, Avril 2009.

- s'assurer que les processus et les systèmes de gestion et de mesures du risque opérationnel soient robustes et demeurent efficaces au fil du temps;

- être informé et passer en revue tous les changements stratégiques importants qui pourraient affecter le profil de risque opérationnel de l'institution (p. ex. : fusion, acquisition, recours à l'impartition, etc.).

1.2.2 Haute direction

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

En vertu des responsabilités qui lui incombent, la haute direction devrait :

- comprendre le profil de risque opérationnel de l'institution, incluant les facteurs internes et externes qui pourraient constituer un risque opérationnel pour l'institution;

- établir un niveau de tolérance adéquat au risque opérationnel de l'institution, ce qui peut inclure une gamme d'énoncés qualitatifs ou subjectifs, le cas échéant, pour les types et/ou le niveau du risque opérationnel que l'institution peut se permettre;

- bien saisir les conséquences de l'application de l'approche standard au titre du risque opérationnel;

- définir de façon précise la hiérarchie, les ressources, les responsabilités et les exigences en matière de rapports afin que la responsabilité à l'égard de la mise en œuvre et du cadre 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, soit bien appliqué à l'échelle de l'institution et demeure efficace au fil du temps;

- approuver les politiques, les procédures, les normes et les documents d'appui ayant trait au cadre 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 élément important de risque opérationnel;

- voir à ce que le cadre de gestion du risque opérationnel et son application fassent régulièrement l'objet d'un examen indépendant.

1.2.3 Fonction de gestion du risque opérationnel

L'institution financière qui applique l'approche standard est tenue 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'institution, du cadre de gestion du risque opérationnel. Dans ce contexte, une « fonction » désigne une instance organisationnelle spéciale vouée entièrement à la gestion du risque opérationnel, composée d'une personne ou plusieurs personnes[8].

La gestion du risque opérationnel devrait comprendre les responsabilités suivantes :

- la mise au point des stratégies afin d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et de suivre le risque opérationnel;

- l'élaboration et la documentation de politiques et de procédures à l'échelle de l'institution ayant trait au cadre de gestion du risque opérationnel et à la gestion des expositions au risque opérationnel, le cas échéant;

- l'instauration de moyens permettant de retracer de façon rigoureuse les données pertinentes en matière de risque opérationnel, dont les pertes importantes;

- la conception et la mise en œuvre d'un système de notification du risque opérationnel;

- l'assurance qu'il existe des procédures et des processus pertinents 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 documentées concernant le cadre de gestion du risque opérationnel incluant des politiques pour le traitement des aspects non conformes et des cas d'exception. La fonction de gestion du risque opérationnel et les unités d'affaires doivent se prêter aux tests de contrôle et vérifications, par la vérification interne (ou une autre fonction indépendante), afin de vérifier l'efficacité des contrôles internes du cadre de gestion du risque opérationnel.

1.2.4 Rapports

La production périodique et en temps opportun de rapports à l'intention du conseil d'administration, de la haute direction et des responsables de la gestion opérationnelle des unités d'affaires fait partie d'une gestion efficace du risque opérationnel. La nature et la portée des rapports devraient être adaptées aux besoins des destinataires. 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 haute direction et le conseil d'administration pourraient exiger que des renseignements leur soient fournis de façon périodique au sujet des tendances, des niveaux d'exposition et d'autres enjeux clés. Les

[8] Le paragraphe 663 a) de la ligne directrice mentionne qu'en raison de sa taille et de sa complexité, l'institution qui applique l'approche standard n'est pas toujours en mesure de se doter d'une instance organisationnelle spécialement affectée à la gestion du risque opérationnel. Dans le cas des 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. La sous-section 6.3.1 de la ligne directrice présente de plus amples détails concernant les attentes de l'Autorité à l'égard de l'approche standard.

responsables de la gestion opérationnelle des unités d'affaires auraient 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 portant 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;
- les données relatives au risque opérationnel, notamment les pertes significatives par ligne de métier;
- les résultats des évaluations pertinentes portant sur des facteurs qui témoignent de l'environnement opérationnel, des autoévaluations en matière de risque et de contrôle ou d'autres éléments du contrôle interne.

1.2.5 Vérification interne[9]

La vérification interne (ou une autre fonction indépendante) est chargée d'évaluer l'efficacité des contrôles internes de l'institution à l'égard des processus de gestion et des systèmes de mesures du risque opérationnel conçus pour garantir le respect des exigences de l'approche standard. La portée et la fréquence des examens de la vérification interne devraient être proportionnelles au risque opérationnel que présente chaque activité observée.

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

- une évaluation de l'efficacité des contrôles internes de l'institution, incluant leur conception, sous l'angle du respect des exigences de l'approche standard;
- la détermination de la portée et de la fréquence des activités de vérification interne en accord avec les principes et les méthodes de vérification;
- une évaluation de la pertinence des ressources et des compétences qui sont 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 d'affaires et de la fonction de gestion du risque opérationnel.

[9] Conformément aux directives de la ligne directrice, l'Autorité n'oblige pas les institutions à soumettre leur système d'évaluation du risque opérationnel à des examens de vérification externe.

2. TENUE DES DONNÉES PAR L'INSTITUTION DÉSIRANT APPLIQUER L'APPROCHE STANDARD AU TITRE DU RISQUE OPÉRATIONNEL

2.1 Introduction

Il incombe aux institutions appliquant l'approche standard de veiller à ce que les données sur le risque opérationnel soient uniformes et fournissent un point de départ solide, fiable et représentatif pour gérer l'exposition de l'institution au risque opérationnel.

Cette section énonce les principes clés de la tenue des données pour l'institution qui souhaite appliquer l'approche standard au titre du risque opérationnel. Elle énonce également les principes régissant certaines catégories de données internes sur le risque opérationnel, soit le produit brut et les pertes opérationnelles[10].

2.2. Principes de tenue des données

2.2.1 Supervision exercée par la haute direction

L'institution qui souhaite appliquer l'approche standard au titre du risque opérationnel devrait adopter des processus, relativement à la gestion de tous les principaux aspects liés à la technologie de l'information et à la gestion des données, qui soient adaptés à sa nature ainsi qu'à la portée et à la complexité de ses besoins en matière de tenue des données. Le cas échéant, elle devrait évaluer la portée, les plans et les risques inhérents à l'exécution, en temps opportun, des projets de tenue des données.

Dans ce contexte, la haute direction devrait notamment :

- examiner et approuver la structure et les fonctions organisationnelles afin de faciliter la mise en place d'une architecture appropriée des données qui appuiera la mise en œuvre de l'approche standard;

- établir à l'échelle de l'institution un cadre de gestion des données qui définit, le cas échéant, les politiques, la gouvernance, la technologie, les normes et les processus de l'institution favorisant la collecte, la tenue et le contrôle des données, ainsi que la diffusion des données traitées, c'est-à-dire de l'information;

- veiller à ce que les processus de tenue des données garantissent la sécurité, l'intégrité et la vérifiabilité des données, et ce, depuis la collecte des données jusqu'à leur archivage ou leur suppression logique;

- instaurer, au besoin, des programmes de vérification interne qui permettront d'examiner de façon indépendante et périodique les processus et les fonctions de tenue des données;

- veiller à ce que les politiques, les procédures et le partage des responsabilités soient en place et qu'ils permettent une surveillance appropriée, à l'échelle de l'institution, de l'application du cadre de gestion des données, y compris, le cas échéant, la mise à jour continue des procédures et de la documentation.

[10] La présente section ne traite pas des principes d'utilisation des éléments de données en vue de quantifier les fonds propres pour le risque opérationnel.

2.2.2 Collecte des données

La collecte des données sur le risque opérationnel (également désignée sous le nom « d'acquisition » ou « de saisie des données ») passe habituellement par le recensement des éléments de données propres à la gestion du risque opérationnel.

Les processus de collecte de données de l'institution devraient :

- documenter de façon claire et détaillée la définition, la collecte et le regroupement des données, en indiquant notamment la ventilation des données en lignes de métier[11], ainsi que des schémas des données, au besoin, et d'autres identificateurs, le cas échéant;

- instituer des normes d'exactitude, d'intégralité, de disponibilité en temps opportun et de fiabilité des données;

- repérer et consigner les données manquantes, et le cas échéant, noter les solutions manuelles ou informatisées utilisées pour combler ces données manquantes et répondre aux exigences en matière de données;

- instaurer des normes, des politiques et des procédures d'épuration des données par conciliation, validation des champs, reformatage, décomposition ou l'utilisation de normes cohérentes, selon le cas;

- mettre en place des procédures pour détecter et signaler les erreurs de données et les ruptures des liens entre les données et les systèmes sources, en aval et/ou externes.

2.2.3 Traitement des données

La composante « traitement des données » couvre un large éventail de tâches de gestion des données comme leur conversion au moyen de plusieurs processus automatisés ou manuels, les transmissions, l'authentification de la source ou du réseau, la validation, la conciliation, etc.

Le traitement des données par l'institution devrait :

- limiter le recours aux solutions de rechange et à une manipulation manuelle des données afin d'atténuer le risque opérationnel lié à l'erreur humaine et à une diminution de l'intégrité des données;

- assurer des niveaux appropriés de validation, d'épuration des données et de conciliation pour chaque processus, le cas échéant;

[11] Les lignes de métiers sont décrites à l'annexe 6-1 de la ligne directrice.

- mettre en place des contrôles adéquats pour s'assurer que du personnel autorisé effectue le traitement, et ce, conformément au partage des rôles et des pouvoirs établis;

- instaurer des procédures adéquates de contrôle des changements apportés au cadre de traitement comprenant, le cas échéant, l'initiation des changements, l'autorisation, les modifications de programme, les tests, le traitement en parallèle, les approbations, la mise en production et les contrôles de la bibliothèque;

- assurer des niveaux appropriés de sauvegarde en cas de désastre et de reprise des activités afin d'atténuer la perte des données ou de leur intégrité[12].

2.2.4 Accès aux données et extraction

Sous l'angle de la surveillance exercée par l'Autorité, l'un des éléments clés de la tenue des données est la disponibilité continue des données et de l'information se rapportant à l'institution.

L'institution financière devrait s'assurer que :

- les banques de données et les sous-programmes d'extraction, de requête et de récupération soient conçus de manière à répondre à ses besoins en matière de données, de même qu'à ses besoins continus relativement aux évaluations de surveillance de données diverses, le cas échéant;

- les contrôles d'accès et la diffusion des données et de l'information reposent sur les rôles et les attributions des utilisateurs et sur les saines pratiques de l'industrie dans le contexte de la ségrégation efficace des fonctions et sont conformes au principe de l'accès sélectif, le tout vérifié par les fonctions internes de conformité et de vérification de l'institution;

- l'accès aux données ou à l'information ne soit limité par aucune entente d'impartition[13] des services de tenue des données avec un ou plusieurs fournisseurs externes. En dépit de ces ententes, l'institution devrait être en mesure de fournir les données ou l'information à l'Autorité sans coût supplémentaire.

2.2.5 Stockage et conservation des données

La composante « stockage et conservation » des données répond à la fois aux attentes de conservation et d'archivage des données électroniques visant à satisfaire les critères minimaux de conservation des données historiques établis selon la ligne directrice, et aux exigences de l'institution elle-même.

L'institution devrait :

- établir des politiques et procédures documentées concernant le stockage, la conservation et l'archivage, y compris, au besoin, les procédures relatives à la suppression logique et physique des données et à la destruction des supports et des périphériques de stockage des données;

[12] Autorité des marchés financiers, Ligne directrice sur la gestion de la continuité des activités, Avril 2010.

[13] Pour plus de renseignements sur l'impartition, voir la Ligne directrice sur les risques liés à l'impartition publiée par l'Autorité en avril 2009.

- conserver des copies de sauvegarde des banques de données, des bases de données et des fichiers de données pertinents, de sorte que l'information soit facilement accessible afin de répondre aux demandes d'information relativement aux évaluations continues de la surveillance du respect des exigences de l'approche standard;

- s'assurer que les versions électroniques de l'ensemble des données et de l'information pertinentes soient lisibles par machine et qu'elles peuvent être rendues accessibles.

2.3. Catégories de données sur le risque opérationnel

La mesure des fonds propres à l'égard du risque opérationnel dépend largement de la capacité d'une institution de tenir des fichiers de données fiables sur les catégories de données sur le risque opérationnel. Ces catégories comprennent le produit brut, les pertes opérationnelles, et d'autres données qualitatives représentant les facteurs du cadre opérationnel et de contrôle interne.

Selon le paragraphe 654 de la ligne directrice, une institution appliquant l'approche standard doit fonder le calcul de ses exigences de fonds propres sur trois années de produit brut. En outre, par souci de gestion efficace du risque opérationnel, l'institution doit suivre et déclarer ses pertes importantes.

Aux principes clés de tenue des données abordés précédemment s'ajoutent les principes spécifiques suivants au sujet des catégories de données sur le risque opérationnel pour l'approche standard.

2.3.1 Données sur le produit brut

Selon le paragraphe 653 de la ligne directrice, une institution appliquant l'approche standard doit fonder le calcul de ses exigences de fonds propres sur son produit brut. Afin de tenir des données fiables sur le produit brut pour le calcul des exigences de fonds propres, et conformément aux exigences de la ligne directrice portant sur le produit brut, l'institution devrait :

- documenter le processus de distribution pour assurer la ventilation uniforme des données sur le produit brut;

- établir un système ou un processus qui facilite la conciliation du produit brut indiqué dans le formulaire de divulgation avec les résultats financiers déclarés par l'institution;

- veiller à ce que la robustesse du système soit proportionnelle à la complexité du processus de ventilation des données sur le produit brut.

2.3.2 Données sur les pertes opérationnelles

Toutes les institutions appliquant l'approche standard doivent pouvoir effectuer le suivi de leurs pertes internes importantes et des données connexes par ligne de métier. L'Autorité reconnaît que les pratiques de l'industrie sur la collecte des données internes sur les pertes opérationnelles prennent forme. Il est prévu que les systèmes de suivi varieront entre les institutions appliquant l'approche standard. Comme l'indique la ligne directrice, la complexité du système de suivi de l'institution doit refléter adéquatement sa taille et sa structure de rapport, de même que son exposition au risque opérationnel.

Par conséquent, le système de suivi d'une institution sera évalué d'après sa capacité à saisir, à l'échelle de l'institution, les pertes significatives relatives au risque opérationnel.

Les responsables au niveau du traitement des données internes sur les pertes (et ses éléments de données connexes) devraient :

- veiller à ce que la tenue des données internes sur les pertes soit conforme au cadre de gestion des données établi pour l'ensemble de l'institution[14];

- déterminer et documenter la portée des données internes sur les pertes à recueillir en fonction de ses besoins de gestion du risque opérationnel;

- établir et documenter le processus de distribution des données internes sur les pertes entre les lignes de métier,

- développer et documenter des normes pour assurer l'uniformité du processus de collecte des données internes sur les pertes;

- intégrer les données internes sur les pertes aux rapports sur le risque opérationnel pour appuyer de manière efficace la gestion continue du risque opérationnel;

- veiller à ce que les processus liés à la collecte des données sur les pertes fassent l'objet d'examens périodiques indépendants.

[14] Conformément aux attributions de la haute direction.