Autorité des marchés financiers

Juillet 2024

Balises d’autorisation quant à l’utilisation d’une approche standard au titre de risque opérationnel

Coopératives de services financiers

TABLE DES MATIÈRES

1. Introduction

L'Autorité des marchés financiers (l'« Autorité ») publie ce document à l'intention des institutions financières qui ont obtenu les autorisations aux fins d'utilisation de l'Approche standard pour déterminer le montant des exigences de fonds propres réglementaires relatif au risque opérationnel (l' « Approche standard »).

Ce document étoffe les exigences minimales décrites au chapitre portant sur le risque opérationnel de la *Ligne directrice sur les normes relatives à la suffisance du capital* (la « Ligne directrice ») applicable aux coopératives de services financiers faisant partie d'un réseau, aux caisses non membres d'une fédération, aux sociétés de fiducie, aux sociétés d'épargne et autres institutions de dépôts autorisées.

Les institutions financières doivent appliquer les exigences décrites dans la Ligne directrice à moins d'avoir obtenu de l'Autorité l'autorisation d'appliquer de façon transitoire les exigences décrites dans la *Ligne directrice sur les normes relatives à la suffisance du capital de base*, mise à jour en novembre 2019.

Les éléments qui y sont traités ne doivent pas être considérés isolément, mais plutôt intégrés dans un cadre global de gestion du risque opérationnel à l'échelle de l'institution financière[1].

Dans le cadre du calcul des exigences de fonds propres au titre du risque opérationnel, l'Autorité s'attend à ce que les institutions financières satisfassent aux dispositions de la Ligne directrice ainsi qu'aux principes énoncés dans le document *Principles for the sound management of operational risk*[2], publié en 2011 et mis à jour en 2021 par le Comité de Bâle sur le contrôle bancaire.

De plus, les institutions financières doivent démontrer en continu à l'Autorité que la gouvernance entourant leur gestion des risques et leurs pratiques en matière de contrôle du risque opérationnel correspondent à leur profil de risque et reflètent leur nature, leur taille et la complexité de leurs activités.

Chacun des éléments traités au sein du présent document devrait être considéré au cours de l'autoévaluation prescrite par le cadre d'agrément pour l'approche standard du risque opérationnel.

[1] Le périmètre de l'« institution financière » est défini aux paragraphes 3 à 5 du chapitre 1 de la Ligne directrice.

[2] Document CBCB intitulé *Revisions to the Principles for the Sound Management of Operational Risk* de mars 2021.

2. Gouvernance

Cette section présente les orientations et les pratiques qui doivent guider la gouvernance des institutions financières qui appliquent l'Approche standard.

Les éléments couverts par la présente section doivent être considérés comme des éléments supplémentaires et/ou des précisions aux éléments couverts par les autres lignes directrices de l'Autorité notamment la *Ligne directrice sur la gouvernance*[3], la *Ligne directrice sur la gestion intégrée des risques*[4], *la Ligne directrice sur la gestion du risque opérationnel*[5], *la Ligne directrice sur la gestion de la continuité des activités*[6], *ainsi que la Ligne directrice sur l'agrégation des données sur les risques et la divulgation des risques*[7].

2.1 Principes et pratiques

En sus des attentes[8] concernant la gouvernance déjà émises par l'Autorité, le cadre de gestion du risque opérationnel doit faire l'objet d'une documentation étayée et complète. Celle-ci doit être incluse aux politiques approuvées par le conseil d'administration de l'institution financière et intégrer une définition des concepts de risque et de perte opérationnels.

La documentation du cadre doit :

a) identifier les structures de gouvernance impliquées dans la gestion du risque opérationnel, y compris la définition des rôles et responsabilités des différents intervenants;

b) décrire les outils de mesure des risques et leur utilisation;

c) décrire l'appétit et la tolérance pour le risque opérationnel de l'institution financière, ses limites pour le risque inhérent et résiduel, ainsi que les stratégies et instruments d'atténuation des risques approuvés par le conseil d'administration;

d) décrire l'approche de l'institution financière pour l'établissement et le suivi des seuils ou des limites d'exposition au risque inhérent et résiduel;

e) établir l'approche de reddition de comptes et le système de gestion de l'information;

f) fournir une taxinomie commune des termes liés au risque opérationnel afin d'assurer la cohérence dans l'identification et les objectifs de gestion des risques;

[3] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance*.
[4] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gestion intégrée des risques.*
[5] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gestion du risque. opérationnel.*
[6] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gestion de la continuité des activités.*
[7] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur l'agrégation des données sur les risques et la divulgation des risques*.
[8] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance.*

g) favoriser la production d'une évaluation indépendante de la gestion du risque opérationnel et de l'arrimage de celle-ci avec l'appétit pour le risque de l'institution financière; et

h) être révisée lorsque approprié et être mise à jour lors de changements significatifs au profil de risque de l'institution financière.

A. Conseil d'administration

En sus des attentes[9] déjà émises par l'Autorité, le conseil d'administration doit :

- veiller à l'établissement, à l'approbation et à la révision périodique du cadre de gestion du risque opérationnel;

- veiller à ce que ses membres soient en mesure de comprendre la nature et la complexité des risques opérationnels inhérents au portefeuille de produits, services et activités de l'institution financière;

- s'assurer de bien saisir les conséquences liées à l'application de l'approche de calcul des exigences de fonds propres au titre du risque opérationnel qu'elle cherche à mettre en œuvre;

- approuver les politiques de gestion des expositions d'envergure au risque opérationnel et les pratiques de gestion[10] qui y sont reliées; et

- examiner au besoin les rapports sur le risque opérationnel.

B. Haute direction

En sus des rôles et responsabilités qui lui sont généralement dévolus[11], la haute direction doit :

- posséder une compréhension approfondie du profil de risque opérationnel de l'institution financière. La haute direction doit assurer l'identification[12] et l'évaluation du risque opérationnel inhérent à tous les produits, activités, processus et systèmes afin que tous les risques soient bien compris;

[9] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance.*

[10] La Ligne directrice prévoit que la politique qu'une institution financière utilise pour circonscrire ses secteurs d'affaires doit être soumise à l'approbation du conseil d'administration. L'Autorité reconnaît toutefois que la délimitation d'un secteur d'affaires est, en soi, une activité opérationnelle et qu'elle n'est pas, a priori, le type d'information sur lequel le conseil d'administration a l'habitude de se prononcer.

[11] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur la gouvernance.*

[12] Plusieurs exemples sont fournis au document « *Principles for the Sound Management of Operational Risk* », *Bank for international Settlements*.

- s’assurer de la bonne opérationnalisation, au sein des secteurs d’affaires, des cibles d’appétit pour le risque opérationnel et à l’arrimage avec l’appétit défini au niveau de l’entreprise;

- s’assurer que le cadre de gestion du risque opérationnel convienne aux besoins de l’institution financière, à ce qu’il soit bien appliqué à l’échelle de l’institution financière et à ce qu’il demeure efficace au fil du temps;

- définir de façon précise la hiérarchie, les ressources, les responsabilités et les exigences en matière de production de rapports afin que les responsabilités relatives à la gestion du risque opérationnel soient sans équivoque;

- valider les politiques, procédures et normes ayant trait au cadre de gestion du risque opérationnel;

- examiner les rapports sur l’exposition de l’institution financière au risque opérationnel ainsi que l’évolution de ces expositions;

- s’assurer que le cadre de gestion du risque opérationnel et son application fassent régulièrement l’objet d’un examen indépendant; et

- s’assurer qu’un processus[13] d'autorisation évaluant pleinement les risques opérationnels soit en place pour tous les nouveaux produits, activités, processus et systèmes.

Finalement, les institutions financières qui appliquent l’Approche standard doivent établir des procédures de gestion de la technologie de l’information et des données qui correspondent à la nature, la portée et la complexité de leurs besoins de tenue de données.

La haute direction doit évaluer, en temps opportun, l’efficacité du processus global de tenue des données, de même que les plans et les risques qui s’y rattachent et prendre des mesures efficaces pour atténuer ces risques.

La haute direction doit notamment :

- examiner et approuver la structure et les fonctions organisationnelles facilitant la mise en place d’une architecture de données appropriée, dans le but d’appuyer la mise en œuvre de la Ligne directrice;

- établir à l’échelle de l’institution financière un cadre de gestion des données définissant des politiques, une gouvernance, une technologie, des normes et des

[13] Des détails concernant ce processus sont fournis au document « *Principles for the Sound Management of Operational Risk* ».

processus qui supportent la collecte, la tenue et le contrôle des données, ainsi que la diffusion des données traitées;

- s'assurer que des politiques, procédures et processus adéquats soient en place et que les responsabilités soient bien définies;

- s'assurer du suivi de la conformité au cadre de gestion des données et de la mise à jour continue des procédures et de la documentation;

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

- instaurer des programmes d'audit interne qui permettront d'examiner de façon indépendante l'efficacité des contrôles par rapport aux processus et fonctions de tenue des données.

C. Fonction de gestion du risque opérationnel

Les institutions financières qui appliquent l'Approche standard sont tenues d'avoir une fonction de gestion du risque opérationnel (la « FGRO ») qui sera chargée de la conception et de la mise en œuvre, à l'échelle de l'institution financière, du cadre de gestion du risque opérationnel.

Dans ce contexte, une « fonction » désigne une instance organisationnelle composée d'une personne ou plus et vouée entièrement à la gestion du risque opérationnel. Cette instance doit relever du chef de la gestion des risques[14] (Chief Risk Officer, « CRO »).

Les responsabilités de la FGRO incluent :

- le développement des stratégies afin d'identifier, d'évaluer, de quantifier, de contrôler, d'atténuer et faire le suivi des risques opérationnels;

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

- l'identification rigoureuse des données critiques en matière de risque opérationnel;

- la conception et la mise en œuvre d'un système de rapports et de reddition des comptes efficace et efficient; et

- l'assurance que les procédures et processus existants sont suffisants pour surveiller adéquatement les pratiques de gestion du risque opérationnel.

[14] Voir la *Ligne directrice sur la gestion intégrée des risques* et *la Ligne directrice sur la gouvernance*.

Afin de garantir la conformité aux exigences de la ligne directrice et aux attentes des présentes balises, le cadre de gestion du risque opérationnel doit comporter des politiques, des procédures internes et de mesures de contrôle rigoureusement documentées. De plus, ce cadre de gestion doit inclure des politiques pour le traitement des cas de non-conformité et d'exceptions.

D. Production de rapports

Une gestion efficace du risque opérationnel comprend une production périodique et ponctuelle de rapports à l'intention du conseil d'administration, de la haute direction, du chef de la gestion des risques, de la FGRO et des responsables des secteurs d'affaires.

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

- les dérogations aux politiques d'appétit et de tolérance pour le risque ainsi qu'aux limites qui en découlent;
- les événements extérieurs d'intérêt et leur impact potentiel sur l'institution financière ainsi que les fonds propres liés au risque opérationnel;
- les données relatives au risque opérationnel, notamment les pertes significatives récentes par secteur d'affaires;
- les évaluations de l'environnement d'affaires, des autoévaluations des risques et contrôles ainsi que de tout autre contrôle interne d'intérêt; et
- les exigences de fonds propres au titre du risque opérationnel, selon les besoins, et l'évolution de la consommation de fonds propres pour le risque opérationnel.

Finalement, les institutions financières doivent se doter de pratiques pour faire en sorte que les rapports sur le risque opérationnel donnent lieu à des actions appropriées et conséquentes.

L'institution financière doit améliorer de façon continue la qualité de ses rapports, au niveau de leur complétude, précision et pertinence.

E. Unité[15] chargée de la revue indépendante et validation

Comme stipulé à la Ligne directrice, l'Autorité n'exige pas des institutions financières qu'elles se prêtent à des examens d'audit externe du système d'évaluation du risque opérationnel.

[15] Une unité correspond, selon la Ligne directrice sur la gestion du risque opérationnel, à la plus petite composante de l'institution à laquelle lui est attribuée une responsabilité opérationnelle ou administrative

Toutefois, l'unité chargée de la revue indépendante doit évaluer l'efficacité des mécanismes de contrôle interne de l'institution financière, dont font partie les processus et systèmes de gestion du risque opérationnel. La portée et la fréquence des examens effectués par cette unité doivent être proportionnelles au risque opérationnel encouru.

En ce sens, la fonction de gestion du risque opérationnel ainsi que les unités opérationnelles doivent se prêter aux tests de contrôle et aux audits[16], réalisés par les services d'Audit ou une autre fonction tout aussi indépendante, afin de vérifier le degré de conformité de l'efficacité des contrôles internes au cadre de gestion du risque opérationnel.

Les travaux de cette unité doivent inclure, sans s'y limiter :

- la définition de la portée, de l'exhaustivité et de la fréquence des activités d'audit interne en accord avec les méthodes et les principes d'audit de cette fonction;

- une évaluation des qualifications des ressources et des compétences requises pour la conduite des travaux d'audit; et

- une évaluation périodique de l'efficacité et de l'indépendance des contrôles internes de l'institution financière à l'égard des processus de gestion du risque opérationnel. Ces évaluations doivent englober les activités des unités opérationnelles et de la FGRO.

L'audit du cadre de gestion du risque opérationnel inclut l'examen de tous les aspects matériels du cadre, l'efficacité de leurs mises en œuvre, leur pertinence et leur fonctionnement. L'unité chargée de la revue indépendante et validation doit s'assurer que :

a) les politiques, procédures, processus, et systèmes qui constituent le cadre de gestion du risque opérationnel, y compris le système de mesure des risques opérationnels, soient conceptuellement solides, transparents et documentés ;

b) les activités des unités d'affaires, la fonction de gestion du risque opérationnel, les comités de gouvernance du risque opérationnel et les structures afférentes soient appropriées et efficaces;

c) les entrées et sorties du cadre de gestion du risque opérationnel soient exactes, complètes, cohérentes, pertinentes, autorisées et accessibles;

d) le suivi ainsi que la gestion de l'exactitude et de la solidité de tous les processus et systèmes importants soient efficaces;

e) des mesures correctives appropriées soient entreprises si des lacunes sont identifiées;

[16] Le document « *Principles for the Sound Management of Operational Risk »* fournit plusieurs exemples d'éléments de contrôle et de vérification.

f) l'analyse des résultats[17] soit incorporée dans les processus de l'institution financière d'une manière appropriée, et soit efficace;

g) les processus de validation soient satisfaisants;

h) des tests des contrôles de gestion des risques soient effectués afin d'apprécier leur capacité à prévenir, détecter et corriger les déviations matérielles ou la non-conformité avec les politiques, procédures et processus, ainsi qu'à fonctionner efficacement pendant toute la période de révision; et

i) chaque activité, filiale ou autre composante importante de l'institution financière soit incluse.

L'audit interne doit également s'attarder à l'examen de l'infrastructure technologique de l'institution financière et s'assurer que celle-ci permette l'atteinte des objectifs de court et long terme dans la tenue de ses activités.

L'utilisation de technologies liées à des produits, activités, processus et canaux de distribution expose les institutions financières à des risques stratégiques, opérationnels et de réputation, ainsi qu'à la possibilité de pertes financières importantes. Par conséquent, l'institution financière doit avoir une approche intégrée d'identification, d'évaluation, de quantification, de contrôle, d'atténuation et de suivi du risque technologique. Une saine gestion du risque technologique est basée sur les mêmes principes que la gestion du risque opérationnel et comprend :

- les contrôles de gouvernance et de surveillance qui assurent que la technologie, y compris les ententes d'impartition[18], est adaptée et soutient les objectifs d'affaires de l'institution financière;

- des politiques et des procédures permettant la mise en place d'un processus d'identification et d'évaluation des risques suffisamment granulaire;

- la mise en place d'un appétit pour le risque et d'un énoncé de tolérance pour le risque technologique;

- la mise en œuvre d'un environnement de contrôle efficace et l'utilisation de stratégies de transfert et d'atténuation des risques; et

- des processus de suivi qui valident la conformité avec les seuils ou les limites dictés par la politique.

[17] L'analyse des résultats inclus des comparaisons avec des éléments de données telles que la comparaison des résultats des scénarios avec des données de pertes internes et externes.

[18] La *Ligne directrice sur la gestion des risques liés à l'impartition* fournit les attentes globales de l'Autorité en la matière. Le document « *Principles for the Sound Management of Operational Risk* » précise également des éléments de base à ce sujet.

Le rapport de l’audit interne doit :

- résumer l’audit effectué, indiquer les limites de l'étendue des travaux effectués et détailler les déviations du plan d’audit, le cas échéant;
- contenir l'évaluation des auditeurs sur les éléments essentiels du champ d’activité ou modèle en cours de révision;
- identifier les faiblesses ainsi que leurs conséquences potentielles, y compris l'écart ou le non-respect de critères, de politiques, de procédures telles qu’énoncées dans les lignes directrices de l’Autorité;
- mettre en place un plan de mesures correctives et un calendrier spécifique pour la correction, le cas échéant, des lacunes et des faiblesses; et
- être distribué, en temps opportun, à la FGRO, à la haute direction, au conseil d'administration et aux personnes responsables des unités administratives impliquées.

Les activités de validation doivent :

a) avoir une vaste portée et évaluer tous les éléments pertinents du système de gestion des données, tels que :

   i. les hypothèses de répartition;

   ii. les hypothèses de corrélation;

   iii. la documentation;

   iv. les aspects qualitatifs (y compris les contrôles internes, le test d'utilisation, les rapports, le rôle de la haute direction et les aspects organisationnels);

   v. l’environnement technologique relatif aux processus de calcul;

   vi. les procédures pour l'autorisation et l'utilisation des nouveaux modèles de risque opérationnel ou méthodologies d'estimation ainsi que ceux qui ont été modifiés (de telles procédures doivent l’objet d’un avis explicite de la fonction de validation lors du processus d'autorisation).

b) évaluer les processus de l’institution financière lors de la validation afin d'assurer que :

   i. les processus de reddition de comptes sont suffisamment complets;

   ii. toutes les préoccupations importantes liées au système de mesure des risques opérationnels sont dûment prises en considération par la haute direction;

iii. toutes les préoccupations importantes liées au système de mesure des risques opérationnels sont acheminées aux comités de gouvernance appropriés;

c) évaluer la logique conceptuelle - y compris l'analyse comparative et l'analyse des résultats – du système de mesure des risques opérationnels et des résultats des modèles de risque opérationnel;

d) refléter les politiques et procédures visant à assurer que les efforts de validation des modèles de risque opérationnel sont compatibles avec les attentes du conseil d'administration et de la haute direction;

e) déterminer si les politiques et procédures sont suffisamment complètes pour traiter les éléments critiques du processus de validation. Plus précisément, l'indépendance de l'évaluation, la clarté de la définition des responsabilités dans l'élaboration et la validation des modèles de risque opérationnel, la documentation des modèles, les procédures et la fréquence de la validation;

f) confirmer que la relation entre les entrées et les sorties du modèle est stable et que les hypothèses et techniques qui sous-tendent les modèles de risque opérationnel sont transparentes et intuitives.

L'audit interne doit établir une procédure afin de résoudre les désaccords entre l'audit et les unités faisant l'objet de l'audit.

F. Continuité des activités[19]

En plus des pertes financières et de l'atteinte à la réputation énumérées dans la *Ligne directrice sur la gestion de la continuité des activités* de l'Autorité, les institutions financières sont exposées à des événements qui peuvent empêcher l'accès, la saisie ou la conservation de données.

Afin de se prémunir contre une telle éventualité, de s'assurer d'être en mesure d'opérer sur une base continue et de limiter les pertes advenant la matérialisation d'un tel événement, les institutions financières doivent mettre en place des analyses d'impacts, des stratégies de rétablissement, des programmes de formation et de vigilance ainsi que des programmes de gestion des crises.

Des plans de continuité des activités doivent être mis en place, incluant des procédures de recouvrement et de reprise des activités, des plans de communication auprès des gestionnaires, des employés, de l'Autorité, des clients et des fournisseurs de services.

Les plans de continuité doivent être évalués et révisés de façon périodique afin d'assurer que les stratégies de contingence demeurent cohérentes avec les opérations courantes, les risques, les menaces et les priorités de recouvrement.

[19] AUTORITE DES MARCHES FINANCIERS, *Ligne directrice sur la gestion de la continuité des activités.*

Lorsque possible, l'institution financière doit participer à des examens périodiques de ces plans avec ses fournisseurs de services clés. Les résultats de ces exercices doivent être communiqués à la haute direction.

G. Divulgation

La divulgation faite par l'institution financière doit permettre aux parties intéressées d'apprécier la gestion qui est faite du risque opérationnel. L'institution financière pourra assurer ainsi un niveau de transparence approprié et le développement de meilleures pratiques d'affaires. L'exhaustivité et la quantité des documents de divulgation produits doivent être représentatives de la taille, du profil de risque, et de la complexité de l'institution financière.

L'institution financière doit divulguer son cadre de gestion du risque opérationnel d'une façon telle que les parties intéressées soient en mesure de déterminer si l'institution financière identifie, évalue, quantifie, contrôle, atténue et assure un suivi des risques opérationnels efficacement.

La divulgation doit être cohérente avec la gestion qui est effectivement faite du risque opérationnel par la haute direction.

L'institution financière doit finalement être dotée d'une politique formelle de divulgation, approuvée par le conseil d'administration, qui spécifie l'approche de l'institution financière en matière de détermination des éléments à divulguer ainsi que les contrôles adéquats encadrant le processus de divulgation. L'institution financière doit également implanter un processus pour valider la justesse de leur divulgation, y compris la fréquence de celle-ci.

3. Tenue des données

Afin de mener à bien la mise en œuvre des différentes approches, l'institution financière doit relever les défis majeurs que posent la gestion des données et l'exécution en temps opportun des initiatives de technologie de l'information.

3.1 Principes et pratiques

En sus des attentes formulées dans la *Ligne directrice sur l'agrégation des données sur les risques et la divulgation des risques*[20] («Ligne directrice ADRDR ») et la *Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications*[21] (« Ligne directrice GRTIC », l'expression « Tenue des données RO» 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.

Relativement à la gestion de leurs initiatives de technologie de l'information et de leur processus de gestion des données, l'institution financière qui souhaite obtenir une autorisation pour l'utilisation de l'Approche standard du risque opérationnel doit adopter une démarche adaptée à la nature, à la portée et à la complexité des exigences de tenue des données.

Afin de garantir la réussite de leurs programmes de tenue des données, l'autorisation de l'Approche standard du risque opérationnel et la conformité continue à celles-ci, l'institution financière doit disposer de processus et de procédures appropriées qui font l'objet d'une supervision efficace par la haute direction.

Les requis des présentes balises sur le risque opérationnel qui sont couverts par la Ligne directrice ADRDR peuvent ne pas être repris. L'institution financière doit faire la correspondance entre les deux corpus de données et exigences (Ligne directrice ADRDR ou Ligne directrice GRTIC et Tenue des données RO). Pour les données identiques, elles pourront être traitées via la ligne directrice applicable, tout en mettant en place un système de correspondance entre les exigences de Tenue des données RO et celles des lignes directrices pour que les surveillants puissent valider la conformité aux exigences des présentes balises.

A. Collecte des données

Dans le cadre de la Ligne directrice, la composante « collecte des données » (également désignée sous le nom « d'acquisition » ou « de saisie des données ») consiste à déterminer les données requises par les divers systèmes internes et externes, à les valider et à les extraire pour ensuite les acheminer vers les banques ou dépôts de données appropriés.

Les processus de collecte de données des institutions financières doivent :

[20] AUTORITÉ DES MARCHÉS FINANCIERS, *Ligne directrice sur l'agrégation des données sur les risques et la divulgation des risques*, février 2016

[21] AUTORITÉ DES MARCHÉS FINANCIERS*, Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications, février 2020*

- documenter de façon claire et détaillée la définition, la collecte et le regroupement des données, en indiquant notamment la ventilation des données par secteurs d'affaires ainsi que des flux de données et/ou d'autres identificateurs, au besoin;

- mettre en place des normes de sécurité, d'intégrité, d'intégralité, d'exactitude, de fiabilité, de vérifiabilité, de qualité et de disponibilité des données;

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

- instaurer, au besoin, des normes, politiques et procédures d'épuration des données, de concordance, de validation des champs, de reformatage ainsi que de décomposition des données, le cas échéant; et

- mettre en place des procédures de détection et de signalement d'erreurs de données et de ruptures de liens entre les données et les systèmes, qu'ils soient source, en aval et/ou externes.

B. Traitement des données

Le traitement des données couvre un large éventail d'activités de gestion, tels la conversion des données au moyen de processus automatisés ou manuels, les transmissions, l'authentification de la source ou du réseau, la validation, la réconciliation, etc.

Les processus de traitement des données de l'institution financière doivent :

- assurer des niveaux appropriés de validation initiale et d'épuration des données pour chaque processus ainsi que lors d'une conciliation avec des processus connexes, le cas échéant;

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

- instaurer des procédures adéquates de contrôle des modifications apportées aux données, notamment, l'origine de la modification, l'autorisation, les modifications de programme, les tests, le traitement en parallèle, les approbations, la mise en production et les contrôles de la bibliothèque; et

- assurer un degré approprié de sauvegarde en cas de désastre et de reprise des activités afin d'atténuer la perte des données ou de leur intégrité.

C. Accès aux données et extraction

L'Autorité considère qu'une composante clé de la tenue des données consiste en une disponibilité continue des données nécessaires à la gestion des activités.

Les institutions financières doivent s'assurer, entre autres, que :

- les banques de données et les sous-programmes d'extraction, de requête et de récupération soient conçus de manière à répondre aux exigences de données, de même qu'aux besoins continus d'évaluation et de surveillance de l'évolution de certaines données précises;

- les contrôles d'accès et la diffusion des données reposent sur les rôles et les attributions des utilisateurs, les saines pratiques de l'industrie en termes de ségrégation des fonctions et le principe de l'accès sélectif. Le tout doit être certifié par les fonctions internes de conformité et d'audit interne de l'institution financière; et

- l'accès aux données ou à l'information ne soit limité par aucune entente d'impartition de services de tenue des données avec un ou plusieurs fournisseurs externes. En dépit de ces ententes, les institutions financières doivent être en mesure de fournir toute donnée ou information, sans coût supplémentaire et dans les délais prescrits, à l'Autorité.

D. Stockage et conservation des données

Le stockage des données doit répondre à la fois aux attentes de conservation et d'archivage des données électroniques établies dans la Ligne directrice, ainsi qu'aux exigences en termes de conformité continue permettant aux institutions financières de répondre aux demandes ponctuelles de l'Autorité en termes de données ou d'information relatives à leur gestion des risques.

En ce sens, les institutions financières doivent notamment :

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

- s'assurer que les versions électroniques de l'ensemble des données et de l'information pertinente soient en tout temps sous une forme lisible par machine et puissent être rendues accessibles; et

- 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.

La période minimale de conservation des données internes sur les pertes est établie à trois ans.

E. Catégories de données

Sous le régime de l'Approche standard, la mesure des fonds propres pour le risque opérationnel dépend largement de la capacité d'une institution financière à tenir des fichiers de données fiables à propos du risque opérationnel. Ces catégories comprennent le produit brut, les pertes opérationnelles, et d'autres données quantitatives et qualitatives couvrant le cadre opérationnel ainsi que le contrôle interne.

Selon la Ligne directrice, une institution financière 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 financière doit suivre et déclarer ses pertes importantes.

Aux principes clés de tenue des données abordés précédemment, s'ajoutent les principes spécifiques qui suivent, qui concernent les catégories de données sur le risque opérationnel propres à l'Approche standard.

Données sur le produit brut

La Ligne directrice stipule qu'une institution financière appliquant l'Approche standard doit fonder le calcul de ses exigences de fonds propres sur son produit brut.

Conformément aux exigences relatives au produit brut, l'institution financière doit :

- documenter le processus de distribution pour assurer la ventilation uniforme des données sur le produit brut par secteurs d'activités;

- 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 financière; et

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

Données sur les pertes opérationnelles

Données internes sur les pertes

Toutes les institutions financières appliquant l'Approche standard doivent être aptes à faire un suivi serré de leurs pertes internes importantes et des données connexes par secteur d'affaires.

Comme l'indique la Ligne directrice, la complexité du système de suivi de l'institution financière doit refléter adéquatement la taille et la structure de l'institution financière, de même que son exposition au risque opérationnel. Par conséquent, les systèmes de suivi d'une institution financière seront évalués d'après leur capacité à saisir adéquatement les pertes significatives liées au risque opérationnel.

Les responsables de la tenue des données internes de pertes (et ses éléments de données connexes) doivent notamment :

- garantir la conformité de la tenue des données internes sur les pertes au cadre de gestion des données établi par l'institution financière[22];

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

[22] Conformément aux responsabilités attribuées à la haute direction.

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

- établir et documenter le processus de distribution des données internes sur les pertes entre les secteurs d’affaires;

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

- s’assurer que les processus liés à la collecte des données sur les pertes fassent l'objet d'examens périodiques indépendants; et

- s’assurer que les données utilisées aux fins de la gestion du risque opérationnel soient fiables et fournissent un point de départ solide et représentatif pour gérer l’exposition de l’institution financière au risque opérationnel.