Ligne directrice

Objet : Gestion du risque opérationnel

Catégorie : Saines pratiques commerciales et financières

Nº : E-21 **Date : Juin 2016**

1. Objet et champ d'application

La ligne directrice sur la gestion du risque opérationnel (gestion du risque opérationnel) rend compte des attentes du BSIF en matière de gestion du risque opérationnel et vise toutes les institutions financières fédérales (IFF).

Le BSIF est conscient que les pratiques de gestion du risque opérationnel peuvent varier en fonction de la taille, de la structure du capital social, de la nature, de l'étendue et de la complexité des activités, de la stratégie d'entreprise et du profil de risque de l'IFF.

Aux fins des présentes, le risque opérationnel se définit comme étant le risque d'encourir des pertes découlant de lacunes ou de défauts attribuables aux ressources humaines et matérielles, telles que des procédures et des systèmes internes, ou résultant d'événements déclencheurs externes, ce qui inclut le risque juridique, mais non le risque stratégique et le risque d'atteinte à la réputation. Le risque de pertes qui sont le fait d'employés inclut, par exemple, les incidents opérationnels se rapportant spécifiquement à la fraude interne ou externe ou à la dérogation aux procédures, aux valeurs ou aux objectifs internes, et, de manière plus générale, les incidents qui sont le fait d'un comportement contraire à l'éthique. L'exposition au risque en lien avec des événements externes et qui découle d'une protection vendue par un assureur à des tiers est exclue, alors que le risque pour les activités de l'assureur lui-même est considéré comme étant couvert.

Le BSIF reconnaît que, selon la pratique dans le secteur, une fraude externe peut constituer un risque d'entreprise (plutôt qu'un risque opérationnel distinct). Il encourage les institutions à songer à inclure les événements de fraude externe dans la définition du risque opérationnel à des fins de gestion du risque.

Table des matières

2. Cadre de gestion du risque opérationnel

Principe 1 :

La gestion du risque opérationnel devrait être bien consignée et entièrement intégrée au programme global de gestion des risques d'une IFF.

Le risque opérationnel est inhérent à tous les produits, toutes les activités, tous les processus et tous les systèmes. À ce titre, la gestion efficace de ce risque doit toujours constituer un élément fondamental du programme de gestion des risques des IFF. Le BSIF s'attend à ce que les IFF mettent en place un cadre de gestion du risque opérationnel qui comporte des mécanismes permettant d'identifier et de gérer ce risque[1].

Une bonne compréhension du risque opérationnel permet d'améliorer la prise de décision au moyen de l'observation et de l'analyse des incidents opérationnels passés et des tendances observées dans les comportements au sein de l'IFF. De plus, la mise en place d'un cadre de gestion du risque opérationnel fiable crée un mécanisme de discussion et de signalement des problèmes aux échelons supérieurs, ce qui conduit, à terme, à une meilleure gestion du risque ainsi qu'à une plus grande résilience institutionnelle. La collecte exhaustive de données qu'appuie le présent cadre permet d'analyser des questions panorganisationnelles complexes et facilite la prise de mesures adaptées d'atténuation des risques. D'autres outils, comme l'analyse d'événements externes ou de scénarios, peuvent accroître la valeur de la gestion prospective des risques et décourager la complaisance à l'égard de la gestion des risques opérationnels.

3. Déclaration de la propension à prendre des risques

Principe 2 :

La gestion du risque opérationnel devrait soutenir la structure globale de gouvernance de l'IFF. À ce titre, l'IFF devrait produire une déclaration de sa propension à prendre des risques et la mettre en œuvre; de leur côté, les IFF de petite taille et moins complexes dont le profil de risque opérationnel est moindre devraient avoir recours aux seuils de déclaration/signalement aux échelons supérieurs des événements importants liés au risque opérationnel.

Les IFF de plus grande taille et plus complexes dont le niveau de risque opérationnel découlant de leurs activités est élevé devraient élaborer et tenir à jour une déclaration complète de la propension à prendre des risques à l'égard du risque opérationnel, lequel se rattacherait directement au cadre global de la propension à prendre des risques de l'IFF (voir la ligne directrice *Gouvernance d'entreprise* du BSIF, y compris l'annexe B). Cette déclaration doit exposer clairement la nature et les types des expositions au risque opérationnel que l'IFF est

[1] Le point 1 de l'annexe 1 mentionne des éléments de cadres de risque opérationnel pouvant être considérés comme des pratiques exemplaires pour les IFF de plus grande taille et plus complexes, dépendamment de leur profil de risque individuel. Les attentes de surveillance à cet égard pourraient être accrues à mesure que la taille ou d'autres caractéristiques des IFF évolueront.

prête à accepter ou qu'elle prévoit assumer. Elle doit être brève et claire, et comporter un élément mesurable (limites ou seuils). L'élément mesurable a pour but d'indiquer le niveau de risque opérationnel considéré comme acceptable au sein de l'IFF. Les limites ou les seuils peuvent aussi servir à indiquer le niveau à partir duquel les incidents opérationnels, les quasi-préjudices ou les tendances cumulées entraînent un signalement à la haute direction (des seuils de signalement distincts peuvent être établis dans certains cas).

Au moment de formuler sa déclaration de la propension à prendre des risques à l'égard des risques opérationnels, l'IFF peut prendre en considération des éléments tels que l'évolution de l'environnement externe, les hausses et les chutes importantes du chiffre d'affaires ou du volume d'activités, la qualité de l'environnement de contrôle, l'efficacité des stratégies de gestion ou d'atténuation des risques, l'historique des incidents opérationnels enregistrés par l'IFF, et la fréquence, le nombre ou la nature des cas de violation de la limite ou du seuil prévus dans la déclaration.

La déclaration de la propension à prendre des risques opérationnels, le seuil de signalement des importants événements de risque opérationnel ou les deux doivent être réexaminés périodiquement pour veiller à ce qu'ils demeurent appropriés. Des processus de signalement aux échelons supérieurs et de communication des cas de violation réelle ou éventuelle doivent être en place.

4. Trois lignes de défense

Principe 3 :

L'IFF devrait veiller à la responsabilisation efficace des acteurs de la gestion du risque opérationnel . Une structure fiable, telle que le modèle « à trois lignes de défense », devrait permettre d'établir une démarcation entre les diverses pratiques clés de la gestion du risque opérationnel et d'en faire un examen indépendant et une analyse critique adéquate. L'instauration de cette mesure en termes de structure opérationnelle dépend du modèle d'affaires et du profil de risque de l'IFF.

Il est essentiel de responsabiliser les acteurs de la gestion du risque opérationnel , et c'est ce que permet une structure fiable telle que le modèle à trois lignes de défense. Sont décrites ci-après, à titre d'exemple, les attributions de chacune de ces trois lignes de défense. Pour déterminer ce qui constitue une structure adéquatement fiable, les IFF et le BSIF tiendront compte de la taille, de la structure du capital social, de la nature, de la portée et de la complexité des activités, de la stratégie organisationnelle et du profil de risque.

Première ligne de défense

Le secteur d'activité, qui forme la première ligne de défense, est propriétaire du risque, ce qui lui permet de détecter et de gérer le risque opérationnel dans le courant de ses activités. La première ligne de défense est chargée de planifier, de diriger et de contrôler les opérations courantes d'une activité d'envergure / d'un processus panorganisationnel et de relever et de gérer les risques

opérationnels inhérents aux produits, aux activités et aux processus et systèmes dont elle est responsable[2].

Deuxième ligne de défense

La deuxième ligne de défense correspond aux activités de supervision chargées de cerner, de quantifier, de surveiller et de communiquer objectivement le risque opérationnel à l'échelle de l'entreprise. Elles traduisent un ensemble d'activités et de processus de gestion du risque opérationnel, ayant notamment pour fonction la conception et la mise en place du cadre de gestion du risque opérationnel de l'IFF. La deuxième ligne de défense[3] est celle qui est le mieux placée pour effectuer un examen spécialisé de la gestion du risque opérationnel. À noter que d'autres employés et secteurs de l'IFF (p. ex. la division de la conformité) peuvent aussi faire partie de la deuxième ligne de défense.

L'une des principales fonctions de la deuxième ligne de défense consiste à fournir une évaluation objective[4] des données d'entrée que les secteurs d'activités introduisent dans les outils de gestion (ce qui comprend la mesure/l'estimation du risque) et à établir des outils de production de rapports, de même que les données de sortie qu'elles en tirent, afin de fournir l'assurance raisonnable qu'ils sont adéquatement complets et étayés.

Troisième ligne de défense

C'est la fonction d'audit interne qui constitue la troisième ligne de défense, laquelle doit être distincte des deux premières lignes de défense et doit procéder à la vérification et à l'examen objectifs des mesures de contrôle, des processus et des systèmes de gestion du risque opérationnel et de l'efficacité des deux premières lignes. La troisième ligne de défense est celle qui est le mieux en mesure d'observer et d'examiner la fonction de gestion du risque opérationnel de façon générale dans le contexte des fonctions globales de gouvernance et de gestion du risque de l'IFF. Le champ d'application des vérifications et examens objectifs[5] doit être assez large pour permettre de vérifier si le cadre de gestion du risque opérationnel a été mis en place comme prévu et fonctionne bien.

---

2 On trouvera au point 2 de l'annexe 1 les responsabilités de la première ligne de défense qui peuvent être considérées comme des pratiques exemplaires pour les IFF de plus grande taille et plus complexes dépendamment de leur profil de risque individuel.

3 On trouvera au point 3 de l'annexe 1 les responsabilités de la deuxième ligne de défense qui peuvent être considérées comme des pratiques exemplaires pour les IFF de plus grande taille et plus complexes dépendamment de leur profil de risque individuel.

4 On trouvera au point 4 de l'annexe 1 des précisions sur la production d'une évaluation objective efficace.

5 On trouvera au point 5 de l'annexe 1 les responsabilités de la troisième ligne de défense qui peuvent être considérées comme des pratiques exemplaires pour les IFF de plus grande taille et plus complexes dépendamment de leur profil de risque individuel.

5. Identification et évaluation du risque opérationnel

Principe 4 :

L'IFF devrait veiller à la détermination et à l'évaluation complète du risque opérationnel à l'aide d'outils de gestion adéquats. Le fait d'avoir à sa disposition une série d'outils de gestion du risque opérationnel permet à l'institution de réunir des informations pertinentes sur le risque opérationnel et de les communiquer à l'interne et aux instances de surveillance.

Le BSIF est conscient du fait que ce sont les IFF qui sont le mieux à même de déterminer leur structure organisationnelle, leurs processus et la mesure dans laquelle elles doivent se servir d'outils[6] pour assurer une gestion fiable du risque opérationnel. Les IFF sont donc encouragées à concevoir et à parfaire sans cesse les outils qu'elles emploient pour gérer le risque opérationnel et pour adopter et surveiller la mise en application des pratiques exemplaires en ce domaine (en plus de prioriser la couverture panorganisationnelle[7]). Les outils spécifiques pour recenser ou analyser et évaluer le risque opérationnel sont fonction de divers facteurs, et particulièrement de la nature (notamment le modèle d'affaires), de la taille, de la complexité et du profil de risque de l'IFF.

L'utilisation des outils de gestion du risque opérationnel vise à produire une valeur ajoutée en proportion des autres risques auxquels l'institution est exposée. Le BSIF convient que l'emploi d'outils bien établis engendre une plus grande valeur ajoutée, et que les IFF disposent peut-être déjà d'outils pour la collecte et l'analyse de renseignements qui sont pertinents aux fins de la gestion du risque opérationnel. On trouvera au point 6 de l'annexe 1 d'autres pratiques exemplaires liées aux outils de gestion du risque opérationnel. Tous les outils peuvent s'appliquer, mais les descriptions fournies ne doivent pas être considérées comme une fiche de contrôle à utiliser aux fins de conformité ou d'audit.

[6] On trouvera au point 6 de l'annexe 1 la description des outils de gestion du risque opérationnel qui peuvent être considérés comme des pratiques exemplaires pour les IFF de plus grande taille et plus complexes dépendamment de leur profil de risque individuel.

[7] S'entend de manière à englober toutes les activités commerciales de l'IFF et de ses filiales à l'échelle mondiale.

Annexe 1 – Nouvelles pratiques

Les saines pratiques qui suivent s'adressent principalement aux IFF de plus grande taille et plus complexes. Or, certaines de ces pratiques peuvent être appliquées à plus grande échelle et peuvent servir à illustrer concrètement des pratiques courantes.

Les exemples de nouvelles pratiques présentées ci-après ne sont pas exhaustifs et ne constituent ni une fiche de contrôle ni un objectif à des fins d'examen de surveillance ou d'audit interne. Les discussions à ce sujet devraient porter sur l'amélioration de la gestion du risque opérationnel plutôt que sur les mesures à prendre pour se conformer à la ligne directrice.

Un cadre de gestion du risque opérationnel peut constituer un mécanisme d'exception pour obtenir les données que requiert la haute direction, d'où la collecte de données plus exhaustives sur des questions organisationnelles complexes. Par exemple, si les cadres dirigeants d'une IFF constatent un type précis d'événement qui constitue un risque opérationnel pour une partie de l'organisation, il pourrait s'avérer utile de réunir de l'information à savoir si des événements ou des tendances similaires se produisent ailleurs dans l'organisation (c'est-à-dire s'il y a des indices portant à croire que la problématique pourrait être panorganisationnelle).

La prise de décisions aux plus hauts échelons d'une organisation bénéficie d'une information plus complète. Les cadres de gestion du risque opérationnel sont conçus pour permettre de recueillir de l'information dans certains domaines auprès de l'ensemble des secteurs d'activités et à l'échelle panorganisationnelle. Cela peut être particulièrement utile dans des domaines comme la fraude externe entre les gammes de produits, les pertes juridiques à l'échelle de l'organisation et les intrusions/inadéquations systèmes (qu'elles soient le signe de gestes malhonnêtes isolés ou de problèmes systémiques de plus grande envergure). Dans les organisations de plus grande taille où la deuxième ligne de défense est bien établie, les capacités de collecte et d'agrégation de l'information de ces groupes professionnels peuvent aider à mieux cerner les problèmes, et donc les solutions à plus long terme à des problèmes panorganisationnels.

1. La documentation du cadre de gestion du risque opérationnel de l'IFF peut prendre en compte les éléments suivants :
   a) une description de la méthode suivie par l'IFF pour gérer le risque opérationnel, notamment une référence aux politiques et procédures pertinentes;
   b) un départage clair, entre les trois lignes de défense, des obligations redditionnelles et des responsabilités à l'égard de la gestion du risque opérationnel ;
   c) les outils de quantification et de communication du risque dont se sert l'IFF et la façon dont ils sont utilisés dans les faits;
   d) la méthode suivie par l'IFF pour établir et contrôler la propension à prendre des risques et les seuils de tolérance à l'égard du risque opérationnel;

e) les structures de gouvernance utilisées pour gérer le risque opérationnel, y compris les voies hiérarchiques et les obligations redditionnelles; il faut aussi veiller à ce que cette gestion ait assez d'importance au sein de l'institution pour en assurer l'efficacité;

f) l'application à l'ensemble de l'IFF;

g) l'obligation d'examiner et, selon le cas, de réviser périodiquement les politiques pertinentes;

h) une bonne documentation en matière de gestion du risque qui convienne à la cible et aux utilisateurs visés et leur procure une utilité proportionnée.

2. La première ligne de défense d'une IFF peut être chargée d'élaborer des moyens permettant de réaliser les objectifs suivants :

a) mettre en application le cadre de gestion du risque opérationnel et les politiques s'y rapportant;

b) identifier et quantifier le risque opérationnel inhérent au sein de sa propre unité opérationnelle et évaluer l'importance des risques qui la menacent;

c) mettre en place des mesures de contrôle visant l'atténuation et en évaluer la conception et l'efficacité;

d) superviser les profils de risque opérationnel des secteurs d'activité, en rendre compte et appuyer les activités conformément à la déclaration établie de la propension à prendre des risques à l'égard du risque opérationnel[8];

e) analyser et faire connaître le risque opérationnel résiduel que les mesures de contrôle n'ont pu atténuer, y compris les incidents opérationnels et les lacunes de mesures de contrôle, des ressources humaines, des processus et des systèmes[9];

f) faire valoir l'importance d'une bonne culture de gestion du risque opérationnel auprès de l'ensemble des acteurs de la première ligne de défense;

g) confirmer le signalement opportun et exact aux échelons supérieurs des problèmes importants qu'éprouve l'IFF;

h) former au besoin les employés quant à leur rôle en lien avec la gestion du risque opérationnel .

Dépendamment de la taille et de la complexité des institutions, la première ligne de défense pourrait être scindée davantage entre les rôles 1a et 1b[10].

[8] La deuxième ligne de défense peut aussi y contribuer, surtout pour agréger l'information à l'échelle panorganisationnelle.

[9] La deuxième ligne de défense peut aussi y contribuer, surtout pour agréger l'information à l'échelle panorganisationnelle.

[10] 1b – un secteur peut choisir de mettre sur pied des groupes de contrôle qui auront des responsabilités précises à l'égard d'activités spécifiques au risque opérationnel, par exemple :

3. Le BSIF est conscient que la nature, la taille, la complexité et le profil de risque des diverses IFF sont tels que les attributions des acteurs de la deuxième ligne de défense peuvent empiéter sur celles de la première ligne de défense. De plus, il sait que la taille et le degré d'indépendance de la deuxième ligne varient d'une IFF à l'autre. Par exemple, dans le cas des IFF de petite taille faiblement exposées au risque opérationnel, l'objectivité de l'examen peut être assurée par la séparation des tâches. Toutefois, pour ce qui est des IFF de grande taille, la deuxième ligne de défense est généralement constituée d'une fonction distincte qui, souvent, relève de la fonction de gestion du risque. La deuxième ligne de défense doit avoir les compétences et le niveau hiérarchique voulus pour pouvoir bien s'acquitter de ses devoirs.

Parmi les principales attributions de la deuxième ligne de défense d'une IFF se trouvent notamment les suivantes :

a) effectuer une évaluation critique efficace et objective, avec preuves à l'appui et résultats consignés, lorsque l'évaluation revêt une importance significative (par exemple, en donnant des exemples de contestations et de leur issue), à consulter ultérieurement par la première ligne de défense;

b) confirmer l'élaboration continue de stratégies adéquates permettant de cerner, de quantifier, d'observer et de contrôler ou atténuer le risque opérationnel;

c) confirmer l'établissement, la documentation de politiques et procédures adéquates dans l'ensemble de l'IFF dans l'esprit du cadre de gestion du risque opérationnel;

d) confirmer l'élaboration, la mise en œuvre et l'utilisation continues d'outils intégrés de gestion du risque opérationnel ;

e) confirmer l'existence de procédures et processus adéquats permettant de superviser l'application des pratiques de gestion du risque opérationnel de l'IFF;

f) confirmer que les processus de mesure du risque opérationnel sont bien intégrés à la gestion globale du risque de l'IFF;

g) revoir le contrôle du profil du risque opérationnel de l'IFF et l'information connexe, et y participer (peut comprendre l'agrégation et la présentation de l'information);

h) faire valoir l'importance d'une bonne culture de gestion du risque opérationnel dans l'ensemble de l'IFF;

i) confirmer le signalement opportun et exact aux échelons supérieurs des problèmes importants qu'éprouve l'IFF.

- Cerner, mesurer, gérer, surveiller et signaler les risques opérationnels découlant d'activités et de mesures d'exploitation qui cadrent avec les normes organisationnelles.
- Créer une structure de contrôle interne adéquate pour gérer les risques opérationnels dans leur secteur.
- Signaler, en temps utile, les risques opérationnels à la haute direction ou à la gestion des risques.
- Concevoir et mettre en place, en temps utile, des mesures visant à remédier aux problèmes de risque opérationnel qui ont été identifiés.

Comme dans le cas de la première ligne de défense, la deuxième peut être scindée davantage entre les rôles 2a et 2b[11].

4. L'évaluation objective consiste à adopter un point de vue objectif quant à la qualité et à l'adéquation des activités de gestion du risque opérationnel de l'unité opérationnelle, ce qui comprend la détermination et la quantification des risques opérationnels et des mesures de contrôle, la formulation d'hypothèses, et les décisions prises à l'égard des risques (p. ex., acceptation, transfert, refus, plan d'action). Cela comprend l'analyse critique lorsque cela convient.

Une évaluation objective doit :

- reposer sur un processus structuré et reproductible permettant l'amélioration continue (tout en étant flexible, au besoin);
- s'appliquer aux divers outils de gestion et de communication du risque opérationnel et aux autres processus de gouvernance;
- être effectuée par du personnel informé et compétent;
- être communiquée à l'unité opérationnelle de manière constructive;
- avoir lieu en temps opportun;
- être mesurée en fonction des résultats (p. ex., elle a influé sur une décision/action de la direction);
- s'appuyer sur des éléments de preuve et être documentée.

L'analyse critique peut reposer soit sur des preuves obtenues dans le cadre d'un certain processus, soit sur des preuves documentées aux divers stades, selon le cas. Comme c'est le cas des autres champs de la gestion du risque opérationnel et de la gestion des risques en général, le niveau de documentation requis est celui qui permet de créer de la valeur ajoutée sans pour autant compromettre la réalisation des objectifs généraux de la fonction de gestion du risque.

L'évaluation objective ne se limite pas à faciliter, à guider ou à documenter les décisions.

5. Troisième ligne de défense de l'IFF pour le risque opérationnel - En règle générale, les activités objectives d'examen et de vérification consistent à vérifier le respect des politiques et procédures établies de l'IFF ainsi qu'à déterminer si la gestion du risque opérationnel est adéquate compte tenu de la taille, de la complexité et du profil de risque de l'IFF. Ces activités portent généralement sur la structure et l'utilisation des outils de gestion du risque opérationnel à l'échelle des deux premières lignes de défense, sur la pertinence de l'évaluation objective effectuée par la deuxième ligne de défense, et sur les processus de contrôle, de production de rapports et de gouvernance.

[11] 2b – la deuxième ligne de défense peut choisir d'établir un programme d'assurance de la qualité remet en question la qualité et la nature des remises en question articulées par la deuxième ligne de défense (2a).

6. Voici des exemples d'outils de gestion du risque opérationnel qu'emploient certains IFF et qui pourraient être utiles :
   a) taxonomie du risque opérationnel;
   b) évaluation des risques et des mesures de contrôle ;
   c) évaluation des risques et des mesures de contrôle liés à la gestion du changement;
   d) collecte et analyse d'informations sur les incidents opérationnels internes;
   e) collecte et analyse d'informations sur les incidents opérationnels externes;
   f) indicateurs de risque et de rendement;
   g) cartographie des processus opérationnels importants;
   h) analyse de scénario;
   i) quantification et estimation de l'exposition au risque opérationnel;
   j) analyse comparative.

Chacun de ces outils est explicité ci-après.

(a) Taxonomie du risque opérationnel

Le cadre de gestion du risque opérationnel doit comporter une taxonomie des sources courantes des divers types de risque opérationnel qui assure l'uniformité des activités de recensement et de quantification des risques, et il doit indiquer clairement la nature et le type de risque opérationnel auquel l'IFF est exposée. Une taxonomie incohérente du risque opérationnel peut accroître le risque de problèmes d'identification, de classification et d'attribution des responsabilités en ce qui touche l'évaluation, le suivi et l'atténuation des risques.

(b) Évaluation des risques et des mesures de contrôle

L'évaluation des risques et des mesures de contrôle compte parmi les principaux outils servant à quantifier les risques opérationnels inhérents ainsi que la structure et l'efficacité des mesures de contrôle d'une IFF. Sa valeur découle de ce qu'elle :

- comporte une évaluation de l'environnement de l'entreprise, des risques inhérents, des mesures de contrôle, et des risques résiduels, en faisant référence à la taxonomie du risque opérationnel de l'IFF;
- favorise une correspondance adéquate entre le risque et les mesures de contrôle visant à atténuer les risques;
- est réalisée de façon périodique (pour assurer l'exactitude de l'information et sa production en temps opportun);
- repose sur des activités de soutien et une fréquence de mise à jour appropriées pour demeurer pertinente et utile aux fins de la gestion du risque opérationnel .

En règle générale, l'évaluation des risques et des mesures de contrôle est effectuée par la première ligne de défense, y compris les divers groupes chargés du contrôle, et elles doivent tenir compte de l'environnement actuel et prospectif. Les plans d'action découlant de la réalisation de ces quantifications doivent faire l'objet d'un suivi et d'un contrôle afin de contribuer à ce que les améliorations voulues soient bien mises en place. En outre, la deuxième ligne de défense examine et analyse d'un œil critique les résultats de l'évaluation ainsi que les plans d'action de la première ligne de défense qui en découlent.

(c) Évaluation des risques et des mesures de contrôle liés à la gestion du changement

L'évaluation des risques et des mesures de contrôle liés à la gestion du changement permettent d'établir un processus en bonne et due forme pour évaluer le risque opérationnel inhérent et le caractère approprié des mesures de contrôle visant l'atténuation, lorsque l'IFF procède à des changements importants. L'évaluation du risque opérationnel qui s'inscrit dans le processus de gestion du changement doit être effectuée par la première ligne de défense. Cette évaluation du risque peut prendre en considération :

- les risques inhérents au nouveau produit, au nouveau service ou à la nouvelle activité;
- les changements dans le profil de risque opérationnel de l'IFF et dans sa propension à prendre des risques;
- l'ensemble requis des mesures de contrôle, de processus de gestion du risque et de stratégies d'atténuation du risque à mettre en œuvre;
- le risque résiduel (non atténué);
- les changements dans la limite ou dans le seuil de risque considéré.

(d) Collecte et analyse d'informations sur les incidents opérationnels internes

Pour être efficaces, les activités de collecte et d'analyse d'informations sur les incidents opérationnels internes doivent comprendre la mise en place de systèmes et de processus de collecte et d'analyse de données sur tous les incidents opérationnels internes importants (p. ex., ceux qui dépassent une certaine limite ou un certain seuil interne). L'incident opérationnel, qui est par définition un résultat imprévu résultant d'un risque opérationnel, englobe les gains et les pertes, réels ou potentiels, et le quasi-préjudice (lorsque l'IFF n'a pas enregistré, de façon explicite, une perte ou un gain à la suite d'un incident opérationnel).

La collecte et l'analyse d'informations sur les incidents opérationnels internes procurent des renseignements utiles pour évaluer 1) l'exposition de l'IFF au risque opérationnel au moyen du contrôle des incidents au fil du temps et l'accumulation de données à leur propos, ainsi que 2) l'efficacité générale de l'ensemble des mesures de contrôle opérationnel. La saisie des données internes sur le risque opérationnel doit être gérée principalement par la première ligne de défense, et il doit y avoir en place des mesures de contrôle adéquates (c'est-à-dire, séparation des tâches, vérification) permettant de maintenir l'intégrité des données à un niveau acceptable.

Dans le cas des incidents opérationnels considérés comme importants, on s'attend à ce que les IFF effectuent une analyse afin d'en découvrir la cause première et de prendre des mesures correctives en vue d'empêcher qu'ils se répètent ou d'en atténuer adéquatement les conséquences. De plus, les normes établies d'analyse et de production de rapports doivent répondre aux attentes minimales relatives à l'analyse d'incidents, c'est-à-dire qu'elles indiquent notamment :

- si le risque d'incident est réel, potentiel ou un quasi-préjudice;
- le type de risque opérationnel existant, selon la taxonomie établie;
- les lacunes et les défaillances de mesures de contrôle visant l'atténuation;
- les mesures à prendre pour corriger les lacunes et les défaillances des mesures de contrôle;
- les autorités d'approbation.

En ce qui concerne les incidents opérationnels considérés comme importants, l'analyse des causes premières doit généralement être effectuée par la première ligne de défense, et ses résultats doivent être communiqués comme il se doit aux échelons supérieurs selon les conséquences réelles ou éventuelles de l'incident. La deuxième ligne de défense examine et analyse d'un œil critique l'analyse par la première ligne.

(e) Collecte et analyse d'informations sur les incidents opérationnels externes

Les incidents opérationnels externes sont des événements qui occasionnent un risque opérationnel et qui surviennent ailleurs que dans l'IFF. Les activités de collecte et d'analyse d'informations sur les incidents opérationnels externes consistent notamment à s'abonner à une base de données externe sur les déclarations d'incidents, à contrôler périodiquement ses propres statistiques d'incidents en comparaison de celles de ses pairs, et à évaluer ses expositions globales et l'efficacité générale de l'ensemble de ses mesures de contrôle opérationnel.

(f) Indicateurs de risque et de rendement

Les indicateurs de risque et de rendement sont des mesures servant à contrôler les principaux facteurs d'exposition aux risques opérationnels importants et qui permettent, par ailleurs, de détecter les faiblesses du contrôle et de déterminer le risque résiduel. Ces indicateurs, conjugués aux déclencheurs de contrôle et de signalement aux échelons supérieurs, permettent de cerner les tendances des risques et d'avertir les responsables lorsque les niveaux de risque approchent ou dépassent les seuils ou les limites, en plus d'inciter les cadres à établir des plans d'action et d'atténuation. Ces mesures pourraient inclure des indicateurs internes, externes ou environnementaux utiles pour la prise de décisions.

(g) Cartographie des processus opérationnels importants

La cartographie des processus opérationnels est fréquemment utilisée pour cerner et gérer les risques opérationnels inhérents aux processus importants ou aux processus d'entreprise. Elle

consiste à recenser les diverses étapes des processus, à évaluer leurs risques opérationnels inhérents ainsi que les dépendances entre les risques et l'efficacité des mesures de contrôle, et ensuite à mettre en œuvre les plans d'action de la direction afin de corriger les faiblesses constatées.

(h) Analyse de scénario

L'analyse de scénario consiste à repérer les incidents opérationnels potentiels et à évaluer leurs effets et leurs répercussions éventuels sur l'IFF. Elle est parfois un moyen efficace d'étudier les sources potentielles de risque opérationnel et la nécessité d'améliorer les solutions de contrôle ou d'atténuation. Afin de bien utiliser les analyses de scénario dans le cadre d'un programme de gestion des risques, les scénarios doivent prendre en compte les comportements attendus et les réponses organisationnelles inattendues en réaction à un incident ou à un type d'incident opérationnel. Si les résultats de l'analyse de scénario servent de données d'entrée à la quantification et à l'estimation de l'exposition au risque opérationnel, la deuxième ligne de défense doit déterminer si les scénarios retenus sont appropriés et compatibles avec le programme d'analyse de scénario.

(i) Quantification et estimation de l'exposition au risque opérationnel

La quantification et l'estimation de l'exposition au risque opérationnel sont abordées dans le cadre du processus interne d'évaluation de l'adéquation des fonds propres (PIEAFP[12]) et du dispositif d'évaluation interne des risques et de la solvabilité (dispositif ORSA[13]). Mieux encore, les résultats de la quantification et de l'estimation peuvent être comparés aux fonds propres requis au titre du risque opérationnel selon la ligne directrice sur les normes de fonds propres ou celle portant sur les exigences minimales de fonds propres, selon le cas. Quelle que soit la méthode employée pour quantifier le risque opérationnel, les principales hypothèses doivent être bien décrites et faire l'objet de mesures de validation, de contrôle et de vérification adéquates.

(j) Analyse comparative

L'analyse comparative consiste, pour la première ligne de défense, à examiner les résultats de la quantification des risques des outils de gestion du risque opérationnel , afin de confirmer l'évaluation globale du risque opérationnel. Cette méthode d'analyse aide à assurer la cohérence des résultats de la quantification et de l'évaluation et la mise en commun des leçons apprises. L'analyse comparative peut aussi cerner les domaines où une plus grande cohérence des outils, à l'échelle organisationnelle, peut créer de la valeur ajoutée au plan de la gestion des risques en favorisant une plus grande cohérence de la collecte, de l'agrégation et de l'analyse de l'information. Elle peut aussi permettre de détecter les outils de gestion du risque opérationnel qui ne fonctionnent pas bien ou n'ont pas bien été mis en œuvre.

[12] Voir la ligne directrice E-19 sur le PIEAFP du BSIF

[13] Voir la ligne directrice E-19 sur le dispositif ORSA du BSIF

Annexe 2 – Documents connexes

Renvoi direct dans la présente ligne directrice

Ligne directrice — Gouvernance d'entreprise

Comprennent des normes de fonds propres au titre du risque opérationnel, ou y font renvoi

Ligne directrice A — Normes de fonds propres

Ligne directrice A — Test de suffisance du capital des sociétés d'assurance-vie

Ligne directrice A — Test du capital minimal

Ligne directrice A — Test de suffisance du capital des sociétés d'assurance hypothécaire

Ligne directrice E-19 — Évaluation interne des risques et de la solvabilité (dispositif ORSA)

Ligne directrice E-19 — Processus interne d'évaluation de l'adéquation des fonds propres (PIEAFP)

Utile pour l'analyse des scénarios de risque opérationnel

Ligne directrice E-18 — La simulation de crise

Comprennent des directives spécifiques se rattachant aux processus des IFF

Conseils sur l'autoévaluation en matière de cybersécurité

Ligne directrice B-7 — Saine gestion des instruments dérivés

Ligne directrice B-8 — Mécanismes de dissuasion et de détection du recyclage des produits de la criminalité et du financement des activités terroristes

Ligne directrice B-10 — Impartition d'activités, de fonctions et de méthodes commerciales

Ligne directrice B-20 — Pratiques et procédures de souscription de prêts hypothécaires résidentiels

Ligne directrice B-21 — Pratiques et procédures de souscription d'assurance hypothécaire résidentielle

Ligne directrice E-4 — Entités étrangères exploitant une succursale au Canada

Ligne directrice E-5 — Conservation et destruction des registres

Ligne directrice E-13 — Gestion de la conformité à la réglementation (GCR)

Ligne directrice E-20 — Réponses au sondage sur le taux de référence CDOR