BANK AL-MAGHRIB

LE GOUVERNEUR

DN 29/G/2007 **Rabat, le 13 avril 2007**

Directive relative au dispositif de gestion des risques opérationnels

Le gouverneur de Bank Al-Maghrib :

vu la loi n° 34-03 relative aux établissements de crédit et organismes assimilés promulguée par le dahir n° 1-05-178 du 15 moharrem 1427 (14 février 2006), notamment ses articles 19 et 51 ;

vu les dispositions de la circulaire de Bank Al-Maghrib relative au système de contrôle interne des établissements de crédit ;

après examen par le Comité des établissements de crédit en date du 14 mars 2007;

fixe par la présente directive les règles minimales devant être observées par les établissements pour la gestion des risques opérationnels.

Objet de la directive

La présente directive, issue des recommandations émises par le comité de Bâle en la matière, s'inscrit dans le cadre de la mise en œuvre du deuxième pilier de Bâle II. Elle constitue un référentiel de saines pratiques pour la mise en place par les établissements de crédit, désignés ci-après par « établissements », d'un dispositif de gestion des risques opérationnels à même de leur permettre d'identifier les sources potentielles de tels risques et d'en assurer la mesure, le suivi, le contrôle et l'atténuation en rapport avec leurs taille et profil de risque ainsi que la complexité de leur activité.

I- Champ d'application de la directive

Les établissements qui optent pour l'approche standard ou l'approche standard alternative (ASA) sont tenus, en vertu des dispositions des articles 59 à 62 de la circulaire 26/G/2006 relative aux exigences en fonds propres au titre des risques de crédit, de marché et opérationnels, de se conformer strictement à la présente directive.

Les autres établissements se réfèrent à cette directive afin de renforcer leur dispositif de gestion des risques opérationnels.

II - Définition des risques opérationnels

Aux termes de l'article 56 de la circulaire 26/G/2006, les risques opérationnels sont définis comme étant les risques de pertes résultant de carences ou de défaillances inhérentes aux procédures, au personnel et aux systèmes internes ou à des événements extérieurs.

Cette définition inclut le risque juridique, mais exclut les risques stratégique et de réputation.

III - Sources potentielles des risques opérationnels

Les dispositifs de gestion des risques opérationnels permettent d'identifier l'ensemble des sources majeures des risques opérationnels et de couvrir au moins celles mentionnées ci-après :

- **Fraude interne** : Tout acte impliquant au moins une partie interne à l'établissement et visant à détourner des biens, des règlements ou des paiements, ou à contourner des dispositions légales ou réglementaires (informations inexactes sur les positions, vol commis par un employé, opérations ou activités non autorisées, transactions sciemment non notifiées, détournement de fonds, falsification de documents, délit d'initié, commissions occultes,...).
- **Fraude externe** : Tout acte imputable à des tiers visant à détourner des biens, des règlements ou des paiements, ou à contourner des dispositions légales ou réglementaires (vol, fraude, dommages liés au piratage informatique, contrefaçon, falsification de chèques,...).
- **Pratiques inappropriées en matière d'emploi et de sécurité sur les lieux de travail** : Tout acte non conforme au code du travail ou aux conventions collectives. relatives à l'emploi, la santé ou la sécurité des employés, ou susceptible de donner lieu à des demandes d'indemnisation au titre d'un dommage personnel, d'atteinte à l'égalité des employés ou d'actes de discrimination, d'activités syndicales ou de responsabilité civile d'une manière générale.
- **Pratiques inappropriées concernant les clients, les produits et l'activité commerciale** : Tout manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients ou imputable à la nature ou la conception d'un produit donné (violation de la confidentialité des informations sur la clientèle, blanchiment de fonds, exercice illégal de certaines activités

soumises à agrément, vente agressive, dépassement des limites d'exposition autorisées pour un client, ..).

- **Dommage aux biens physiques** : Destructions ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres (vandalisme, terrorisme,...).
- **Interruption d'activité et pannes de systèmes** : dysfonctionnement de l'activité (interruption ou perturbation d'un service) ou des systèmes (matériel informatique, logiciel,télécommunication,...).
- **Inexécution des opérations, livraisons et processus** : problèmes dans le traitement d'une opération ou dans la gestion des processus ou des relations avec des fournisseurs et d'autres contreparties commerciales (données incorrectes ou erronées sur des clients, pertes ou endommagement d'actifs de la clientèle, documentation légale insatisfaisante, gestion des sûretés inadéquate, inexactitudes dans les rapports externes,...).

IV- Surveillance des risques opérationnels par les organes d'administration et de direction

A. Organe d'administration

L'organe d'administration (conseil d'administration, conseil de surveillance ou toute instance équivalente) approuve la mise en place du dispositif de gestion des risques opérationnels en tant que catégorie de risques distincte. A cet effet, il définit de manière claire et précise les orientations et principes sous-tendant le dispositif devant être mis en place par l'organe de direction et approuve les politiques y afférentes élaborées par ce dernier.

Le dispositif de gestion des risques opérationnels prend en compte le niveau acceptable, par l'établissement, de tels risques, en précisant les politiques de leur

gestion et la priorité donnée à leur mise en application, ainsi que les conditions dans lesquelles la gestion de ces risques peut être éventuellement confiée à une entité externe à l'établissement. Le dispositif comporte également des politiques définissant la méthodologie d'identification, d'évaluation, de suivi et de maîtrise et/ou d'atténuation des risques. Le niveau de formalisation et de complexité de ce dispositif doit correspondre au profil de risque de l'établissement. Il définit, en outre, . les processus essentiels à mettre en place pour la gestion de ces risques.

L'organe d'administration peut confier à un comité ad hoc la charge de la mise en œuvre du dispositif de gestion des risques opérationnels de l'établissement. Il veille également à la mise en place d'un contrôle interne solide. A cet effet, il est particulièrement important que soient définis de manière claire les niveaux de responsabilité et de reporting en distinguant les fonctions de contrôle des risques,

les unités opérationnelles et les fonctions support afin d'éviter tous conflits d'intérêts. L'organe d'administration procède, régulièrement, à l'évaluation du dispositif mis en place pour s'assurer de la bonne prise en charge des risques opérationnels résultant d'évolutions extérieures ainsi que de ceux liés aux produits, activités ou systèmes nouvellement mis en place. Ce réexamen a pour objet de déterminer les pratiques les mieux adaptées aux activités, systèmes et processus de l'établissement.

L'organe d'administration veille à ce que le dispositif de gestion des risques opérationnels soit révisé à la lumière de cette analyse, de façon à prendre en compte les risques opérationnels importants.

B. Organe de direction

L'organe de direction (direction générale, directoire ou 'ioute instance équivalente) assure la déclinaison du dispositif de gestion des risques opérationnels, tel qu'agréé et validé par l'organe d'administration, en politiques, processus et procédures précis pouvant être appliqués et contrôlés au sein des diverses entités de l'établissement. Il veille également à doter les fonctions ou services, en charge de cette mission, des ressources appropriées et à évaluer l'adéquation du processus de surveillance de cette gestion au regard des risques inhérents à l'activité de chaque unité de l'établissement.

L'organe de direction s'assure, en outre, que les agents dédiés aux activités bancaires disposent de l'expérience professionnelle et de l'expertise technique requises et que les préposés au contrôle du respect de la politique en matière de risques opérationnels soient investis d'une autorité indépendante à l'égard des unités qu'ils surveillent.

Il veille, de même, à la diffusion de la politique de gestion des risques opérationnels au profit de l'ensemble du personnel et à la mise en place de canaux garantissant une communication efficace entre le responsable de la gestion des risques opérationnels et les responsables chargés de la gestion des autres catégories de risques (risques de crédit, de marché,...), ainsi qu'avec ceux chargés des relations avec les entités fournissant des services externes (par exemple, sociétés d'assurance et sociétés de sous-traitance).

L'organe de direction porte une attention particulière à la qualité du contrôle de la documentation et aux pratiques d'exécution des transactions. En particulier, les politiques, processus et procédures liés aux technologies modernes, traitant d'importants volumes de transactions, devraient être bien documentés et diffusés à l'ensemble du personnel.

V- Système d'identification, de mesure, de suivi, de maîtrise et d'atténuation des risques opérationnels

A. Identification et mesure des risques opérationnels

Le système de gestion des risques opérationnels permet d'identifier les risques les plus significatifs et d'apprécier la vulnérabilité de l'établissement à ces risques. A cet effet, il prend en compte à la fois les facteurs internes (notamment la nature des activités, la qualité des ressources humaines, les modifications de l'organisation et le taux de rotation du personnel) et externes (notamment les évolutions du secteur bancaire et les progrès technologiques).

Pour identifier et évaluer leurs risques opérationnels, les établissements peuvent recourir aux techniques suivantes :

- **autoévaluation** : Les opérations et les activités de l'établissement sont évaluées sur la base de l'examen d'un ensemble de points potentiellement exposés aux risques opérationnels.

  Ce processus repose, en général, sur un ensemble de contrôles effectués en interne et destinés à identifier les forces et faiblesses de l'environnement opérationnel. Les différents types d'expositions aux risques opérationnels font l'objet d'un classement sur la base d'une matrice de scoring qui prend en considération les instruments d'atténuation de ces risques.

  La matrice en question permet de convertir les évaluations qualitatives en mesures quantitatives et de recenser les risques propres à une activité donnée, ainsi que ceux qui sont transversaux à plusieurs activités. Elle peut également être utilisée pour l'affectation, aux diverses activités, des fonds propres économiques destinés à couvrir les risques opérationnels.

- **cartographie des risques** : Dans le cadre de ce processus, ies diverses unités, fonctions organisationnelles et chaînes d'opérations sont déclinées en catégories de risques opérationnels, permettant ainsi à l'organe de direction d'identifier les zones de risques et d'établir des priorités pour les actions à entreprendre.

- **indicateurs de risque** : Etablis sur la base de statistiques et/ou de diverses mesures, souvent à caractère financier, les indicateurs de risque (nombre d'opérations non exécutées, mobilité des effectifs, fréquence et/ou gravité des erreurs et omissions,...) donnent une idée sur l'exposition de l'établissement aux risques opérationnels.

Ces indicateurs sont généralement revus de façon périodique de manière à tenir informés les organes d'administration et de direction sur les changements porteurs de risques.

B. Suivi des risques opérationnels

Outre le suivi des cas de pertes opérationnelles, les établissements mettent en place des indicateurs d'alerte avancés, qui leur permettent d'identifier les sources potentielles de risques opérationnels (taux de croissance anormalement élevé, lancement de nouveaux produits, rotation des employés, ruptures de transactions, pannes de système). Ces indicateurs comportent généralement des seuils, dont le dépassement déclenche la mise en œuvre d'actions préventives.

Le suivi des risques opérationnels doit faire partie intégrante de l'activité de l'établissement. La périodicité de ce suivi est adaptée aux risques ainsi qu'à la fréquence et à la nature des changements de l'environnement opérationnel.

La mise à la disposition de l'organe d'administration d'informations opportunes lui permettrait d'apprécier le profil global de l'établissement vis-à-vis des risques opérationnels et d'appréhender les retombées pratiques et stratégiques découlant de ces risques.

En outre, les services concernés de l'établissement (unités opérationnelles, fonctions de groupe, responsable chargé du suivi des risques opérationnels, audit interne,...) établissent régulièrement, à l'attention des niveaux appropriés de la direction et aux lignes d'activité générant les expositions aux risques, des rapports sur les risques opérationnels.

Ces rapports intègrent les données internes (aspects financiers, opérations et conformité), ainsi que les informations externes (de marché) relatives aux événements et conditions susceptibles d'influencer le processus de décision. Ils doivent porter sur l'ensemble des zones de risques identifiées et donner lieu à des actions correctives rapides. Leurs résultats peuvent servir de base pour la mise en place de politiques, procédures et pratiques de gestion des risques plus appropriées.

Pour s'assurer de l'exhaustivité et de la fiabilité de ces rapports, l'organe de direction vérifie régulièrement la rapidité, l'exactitude et la pertinence des systèmes de reporting et des contrôles internes.

Lorsque les risques opérationnels identifiés sont importants, les mesures appropriées doivent être prises rapidement en vue de ramener à un niveau maîtrisable l'exposition à ces risques. A défaut, le positionnement de l'établissement par rapport à l'activité générant ces risques devrait faire l'objet de révision.

Les établissements mettent en place des processus et procédures de contrôle, ainsi qu'un système assurant la conformité des opérations à un ensemble de politiques internes dûment documentées.

Les politiques et procédures, formalisées et documentées, doivent être appuyées par une solide culture de contrôle favorisant la mise en œuvre de saines pratiques de gestion des risques opérationnels. Dans ce sens, il incombe aux organes d'administration et de direction de mettre en place un solide processus de contrôle. interne encadrant toutes les activités de l'établissement, afin d'assurer la réactivité nécessaire vis-à-vis de tout événement imprévu.

C. Maîtrise et atténuation des risques opérationnels

Les établissements veillent à adopter des pratiques internes visant à assurer la maîtrise et l'atténuation des risques opérationnels, telles que :

- le suivi attentif du respect des limites et seuils de risque fixés ;
- la sécurisation de l'accès aux patrimoines et archives de l'établissement et de leur utilisation ; . la mise à niveau des compétences et de la formation des agents ;
- l'identification des activités et produits dont les rendements paraissent disproportionnés par rapport à des attentes raisonnables ;
- la vérification et le rapprochement réguliers des opérations et des comptes.

Les activités externalisées font l'objet de politiques appropriées de gestion des risques. Le recours à des prestataires de services externes ne diminue pas la responsabilité des organes d'administration et de direction, à qui il incombe de veiller à ce que l'activité de ses prestataires soit menée de façon sûre et saine, dans le respect du cadre réglementaire applicable. Les contrats d'externalisation doivent être solides et reposer sur des conventions de service assurant une répartition claire des responsabilités entre les prestataires de service externes et l'établissement. En outre, la gestion des risques résiduels liés à ces contrats d'externalisation, y compris toute perturbation dans l'offre de services, doit être prise en charge par l'établissement.

VI- Contrôle du système de gestion des risques opérationnels

Les établissements mettent en place un système d'audit interne qui vérifie périodiquement que le dispositif de gestion des risques opérationnels est mis en œuvre avec efficacité au niveau de l'ensemble de l'établissement.

L'organe d'administration s'assure de l'adéquation du système d'audit interne et de sa capacité à vérifier que les politiques et procédures opérationnelles sont

correctement mises en place. Il veille, en outre, directement ou par l'intermédiaire du comité d'audit, à ce que la portée et la fréquence du programme d'audit interne concordent avec le degré d'exposition aux risques opérationnels.

La fonction d'audit interne peut fournir des indications précieuses aux personnes responsables de la gestion des risques opérationnels, mais elle ne doit pas être, elle-même, chargée de responsabilités directes à cet égard. Aussi, il importe de veiller à son indépendance et à sa non implication dans le processus de gestion au jour le jour des risques opérationnels, notamment dans le cas où elle serait chargée du suivi du dispositif de gestion des risques opérationnels ou de l'élaboration du programme de leur gestion.

VII- Plan de continuité de l'activité

En vue d'assurer le fonctionnement continu de leurs activités et de limiter les pertes en cas de fortes perturbations des opérations dues aux événements majeurs, les établissements se dotent d'un plan de continuité de l'activité et désignent un responsable chargé d'assurer la mise en œuvre des mesures liées à ce plan.

Les établissements revoient périodiquement ces plans et les testent pour vérifier qu'ils sont en mesure de les mettre en œuvre, même dans les situations de crises dont l'occurrence est très peu probable.

VIII- Reporting destiné à Bank Al-Maghrib

Les établissements communiquent périodiquement à la Direction de la supervision bancaire de Bank Al-Maghrib un reporting spécifique sur les pertes générées par les risques opérationnels. Celle-ci peut demander d'autres informations portant sur ces risques.

IX- Entrée en vigueur

Les dispositions de la présente directive entrent en vigueur à partir de la date de sa signature.