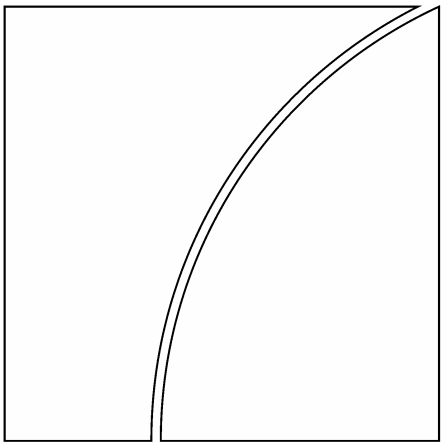
Comité de Bâle sur le contrôle bancaire



Saines pratiques pour la gestion et la surveillance du risque opérationnel

Février 2003

BANQUE DES RÈGLEMENTS INTERNATIONAUX

Pour obtenir un exemplaire des publications BRI, veuillez vous adresser à :

Secrétariat du
Comité de Bâle sur le contrôle bancaire
c/o Banque des Règlements Internationaux
CH–4002 Bâle, Suisse

Mél : publications@bis.org

Télécopie : +41 61 280 9100

La présente publication est disponible sur le site Internet BRI (www.bis.org).

Également publié en allemand, anglais, espagnol et italien.

Groupe gestion du risque du Comité de Bâle sur le contrôle bancaire

Président :
Roger Cole, Federal Reserve Board, Washington, D.C.

Banque nationale de Belgique, Bruxelles	Dominique Gressens
Commission bancaire et financière, Bruxelles	Jos Meuleman
Bureau du surintendant des institutions financières, Ottawa	Jeff Miller
Commission bancaire, Paris	Laurent Le Mouël
Deutsche Bundesbank, Francfort-sur-le-Main	Magdalene Heid Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Kirsten Straus
Banca d'Italia, Rome	Claudio D'Auria Fabrizio Leandri Sergio Sorrentino
Banque du Japon, Tokyo	Satoshi Yamaguchi
Financial Services Agency, Tokyo	Hirokazu Matsushima
Commission de surveillance du secteur financier, Luxembourg	Davy Reinard
De Nederlandsche Bank, Amsterdam	Klaas Knot
Banco de España, Madrid	Guillermo Rodriguez-Garcia Juan Serrano
Finansinspektionen, Stockholm	Jan Hedquist
Sveriges Riksbank, Stockholm	Thomas Flodén
Commission fédérale des banques, Berne	Martin Sprenger
Financial Services Authority, Londres	Helmut Bauer Victor Dowd
Federal Deposit Insurance Corporation, Washington, D.C.	Mark Schmidt
Federal Reserve Bank of New York	Beverly Hirtle Stefan Walter
Federal Reserve Board, Washington, D.C.	Kirk Odegard
Office of the Comptroller of the Currency, Washington, D.C.	Kevin Bailey Tanya Smith
Banque centrale européenne, Francfort-sur-le-Main	Panagiotis Strouzas
Commission européenne, Bruxelles	Michel Martino Melania Savino
Secrétariat du Comité de Bâle sur le contrôle bancaire, Banque des Règlements Internationaux	Stephen Senior

Table des matières

Saines pratiques pour la gestion et la surveillance du risque opérationnel

Introduction

1. Le présent document expose un ensemble de principes devant régir un dispositif pour la gestion et la surveillance efficaces du risque opérationnel, à utiliser par les banques et leurs superviseurs afin d'évaluer les politiques et pratiques de gestion de ce risque.

2. Le Comité de Bâle sur le contrôle bancaire (le « Comité ») reconnaît que la méthode de gestion du risque opérationnel choisie par chaque banque dépend d'une série de facteurs – sa taille, le perfectionnement de ses techniques, ainsi que la nature et la complexité de ses activités. Toutefois, au-delà de ces différences, un dispositif efficace de gestion du risque opérationnel se caractérise par des éléments essentiels, quels que soient la taille et le champ d'action des banques, à savoir : formulation claire des stratégies et surveillance active par le conseil d'administration et la direction générale ; solide culture du risque opérationnel[1] ; culture de contrôle interne (notamment, définition claire de la hiérarchie des responsabilités et de la répartition des tâches) ; information interne efficace ; mise en place de plans de secours. Le Comité estime donc que les principes décrits dans le présent document définissent de saines pratiques valables pour toutes les banques. Les travaux actuels du Comité dans le domaine du risque opérationnel se situent dans le prolongement de son document de septembre 1998, *Cadre pour les systèmes de contrôle interne dans les organisations bancaires*.

Généralités

3. La déréglementation et la mondialisation des services financiers, ainsi que la sophistication grandissante des techniques financières, rendent plus complexes les activités des banques, donc leur profil de risque (sur l'ensemble de leurs activités et/ou catégories de risque de l'établissement). Le développement des pratiques bancaires suggère que des risques autres que ceux de crédit, de taux d'intérêt et de marché peuvent prendre une grande importance. Parmi ces risques nouveaux et croissants qui menacent les banques, on peut citer les exemples suivants.

- L'automatisation accrue de techniques, si elle n'est pas bien maîtrisée, peut transformer les risques d'erreurs humaines (traitement manuel) en risques de pannes des systèmes, à mesure que l'on recourt davantage à des systèmes automatisés et intégrés.
- Le développement du commerce électronique entraîne des risques potentiels (par exemple, problèmes de fraude interne et externe et de sécurité des systèmes) qui ne sont pas encore parfaitement compris.
- Les acquisitions, fusions, regroupements et annulations de fusions mettent à rude épreuve la viabilité des systèmes nouveaux ou nouvellement intégrés.
- L'apparition de banques offrant des services nombreux pour des montants importants oblige à entretenir en permanence des contrôles internes et des systèmes de secours de haut niveau.
- Les techniques d'atténuation du risque (par exemple, sûretés, dérivés de crédit, accords de compensation et titrisation) utilisées par les banques afin d'optimiser leur exposition aux risques de marché et de crédit peuvent engendrer d'autres formes de risque (par exemple, juridique).

[1] Par « culture interne du risque opérationnel », on entend l'ensemble des valeurs, attitudes, compétences et comportements individuels et collectifs qui déterminent l'engagement de l'entreprise envers la gestion du risque opérationnel et la façon dont elle gère ce risque.

- Le recours croissant à l'externalisation et à la participation aux systèmes de compensation et de règlement peut atténuer certains risques, mais aussi présenter de nouveaux risques majeurs pour les banques.

4. On peut regrouper les divers risques énumérés ci-dessus sous le terme « risque opérationnel », que le Comité a défini comme « risque de pertes dues à des personnes, processus ou systèmes inadéquats ou défaillants, ou résultant d'événements extérieurs »[2]. Cette définition comprend le risque juridique mais exclut le risque stratégique et le risque de réputation.

5. Le Comité reconnaît que le concept de risque opérationnel prend des significations très diverses dans la profession bancaire et, par conséquent, aux fins du contrôle interne (y compris dans l'application du présent document sur les saines pratiques) ; les banques peuvent donc décider d'adopter leur propre définition de ce risque. Quelle que soit la définition retenue, il est crucial pour une gestion et un contrôle efficaces du risque opérationnel que les banques en aient une compréhension parfaite. Il est important aussi que la définition englobe toute la gamme des risques opérationnels importants qui menacent les banques et prenne en compte les principaux facteurs à l'origine de lourdes pertes opérationnelles. Parmi les types d'incidents de nature opérationnelle susceptibles d'occasionner de lourdes pertes, le Comité – en coopération avec la profession – a identifié les suivants.

- ***Fraude interne*** *:* par exemple, informations inexactes sur les positions, vol commis par un employé et délit d'initié d'un employé opérant pour son propre compte.
- ***Fraude externe*** *:* par exemple, hold-up, faux en écriture, chèques de cavalerie et dommages dus au piratage informatique.
- ***Pratiques en matière d'emploi et sécurité sur le lieu de travail*** *:* par exemple, demandes d'indemnisation de travailleurs, violation des règles de santé et de sécurité des employés, activités syndicales, plaintes pour discrimination et responsabilité civile en général.
- ***Pratiques concernant les clients, les produits et l'activité commerciale*** *:* par exemple, violation de l'obligation fiduciaire, utilisation frauduleuse d'informations confidentielles sur la clientèle, opérations boursières malhonnêtes pour le compte de la banque, blanchiment d'argent et vente de produits non autorisés.
- ***Dommages aux biens physiques*** *:* par exemple, actes de terrorisme, vandalisme, séismes, incendies et inondations.
- ***Interruption d'activité et pannes de systèmes*** *:* par exemple, pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité.
- ***Exécution des opérations, livraisons et processus*** *:* par exemple, erreur d'enregistrement des données, défaillances dans la gestion des sûretés, lacunes dans la documentation juridique, erreur d'accès aux comptes de la clientèle et défaillances des fournisseurs ou conflits avec eux.

Tendances et pratiques de la profession

6. Dans ses travaux sur la surveillance des risques opérationnels, le Comité a cherché à mieux connaître les tendances et pratiques actuelles du secteur bancaire pour la gestion de ce risque. Cela a nécessité de nombreuses réunions avec les associations professionnelles, des enquêtes sur les pratiques du secteur et l'analyse des résultats. Le Comité estime qu'il a ainsi acquis une bonne compréhension de l'éventail des pratiques suivies et du travail mené par les établissements pour élaborer des méthodes de gestion du risque opérationnel.

---

[2] Cette définition, empruntée à la profession, a été fixée par le Comité à l'occasion des travaux qu'il a menés en vue d'élaborer une norme réglementaire minimale de fonds propres pour le risque opérationnel. Si le présent document ne fait pas partie à proprement parler du dispositif de fonds propres, le Comité compte néanmoins que les éléments essentiels d'un dispositif de saine gestion du risque opérationnel, définis ici, aideront les autorités de contrôle à évaluer l'adéquation des fonds propres, par exemple dans le cadre du processus de surveillance prudentielle.

7. Le Comité reconnaît que la gestion de certains risques opérationnels n'est pas récente ; les banques ont toujours veillé à empêcher la fraude, préserver l'intégrité des contrôles internes, réduire les erreurs de traitement des transactions, etc. Toutefois, ce qui est relativement neuf est le choix d'une approche globale (dans le principe, sinon toujours dans la forme), comme pour les risques de crédit et de marché. Les tendances énumérées dans l'introduction du présent document, de même qu'un nombre croissant de pertes opérationnelles retentissantes, partout dans le monde, ont amené les banques et les superviseurs à considérer de plus en plus, comme cela est déjà le cas dans beaucoup d'autres secteurs, que la gestion du risque opérationnel constitue une discipline d'ensemble.

8. Dans le passé, les banques géraient le risque opérationnel en s'appuyant presque exclusivement sur les mécanismes de contrôle interne, appliqués par branche d'activité et complétés par la fonction d'audit. Si ces mécanismes restent importants, ils sont depuis peu associés à des structures et processus spécifiques. À cet égard, un nombre croissant d'établissements ont compris qu'un programme de gestion du risque opérationnel assure leur sécurité et leur solidité, et ils s'efforcent donc de traiter le risque opérationnel comme une catégorie distincte, à l'instar des risques de crédit et de marché. Le Comité estime que l'élaboration de lignes directrices pour la gestion des diverses formes de risque opérationnel passe par un large échange d'idées entre superviseurs et professionnels.

9. Le document s'articule autour des points suivants : élaboration d'un environnement adéquat pour la gestion du risque ; gestion du risque : identification, évaluation, suivi et maîtrise/atténuation du risque ; rôle des superviseurs ; rôle de la communication financière.

Saines pratiques

10. En élaborant ces saines pratiques, le Comité s'est inspiré de ses travaux antérieurs sur la gestion d'autres risques bancaires importants, tels que les risques de crédit, de taux d'intérêt et de liquidité, et il estime qu'il faut appliquer la même rigueur à la gestion du risque opérationnel. Il est clair, néanmoins, que ce dernier diffère des autres risques bancaires, dans la mesure où il ne constitue généralement pas la contrepartie d'un avantage attendu, mais est inhérent au déroulement naturel de l'activité de l'entreprise, et que cette différence affecte le processus de gestion du risque[3]. En même temps, l'incapacité de gérer le risque opérationnel peut aboutir à une présentation déformée du profil de risque de l'établissement et exposer celui-ci à de lourdes pertes. Pour tenir compte de cette différence, la « gestion » du risque opérationnel désigne, aux fins du présent document, « l'identification, l'évaluation, le suivi et la maîtrise/l'atténuation » du risque. Cette définition s'écarte légèrement de celle que le Comité a utilisée dans ses documents précédents, à savoir « identification, mesure, suivi et maîtrise » du risque. Comme il l'a fait dans ses travaux sur d'autres risques bancaires, le Comité a structuré ses saines pratiques autour de plusieurs principes.

Élaboration d'un environnement adéquat pour la gestion du risque

Principe 1 – Le conseil d'administration[4] devrait considérer les principaux aspects du risque opérationnel de la banque comme une catégorie distincte de risque à gérer, et il devrait approuver et réexaminer périodiquement le dispositif de gestion de ce risque. Ce dispositif devrait fournir une définition du risque opérationnel valable pour la banque tout entière et poser les principes servant à identifier, évaluer, suivre et maîtriser/atténuer ce risque.

---

[3] Toutefois, le Comité reconnaît que, dans certaines activités comportant un risque minimal de crédit ou de marché (par exemple, gestion d'actifs, paiement et règlement), la décision de prendre un risque opérationnel, ou l'avantage concurrentiel pouvant résulter de la capacité à gérer ce risque et à le tarifer précisément, fait partie intégrante du calcul risque/rémunération de la banque.

[4] Le présent document se réfère à une structure de gestion composée d'un conseil d'administration et d'une direction générale. Le Comité sait que, d'un pays à l'autre, les cadres législatif et réglementaire diffèrent notablement en ce qui concerne les fonctions du conseil d'administration et de la direction. Dans certains pays, le conseil a pour fonction essentielle, sinon exclusive, de surveiller l'organe exécutif (haute direction, direction générale) afin de s'assurer que ce dernier accomplit sa tâche ; pour cette raison, il est appelé conseil de surveillance, ce qui signifie qu'il n'a aucune fonction

Principe 2 – Le conseil d'administration devrait garantir que le dispositif de gestion du risque opérationnel de la banque est soumis à un audit interne efficace et complet, effectué par un personnel fonctionnellement indépendant, doté d'une formation appropriée et compétent. La fonction d'audit interne ne devrait pas être directement responsable de la gestion du risque opérationnel.

Principe 3 – La direction générale devrait avoir pour mission de mettre en œuvre le dispositif de gestion du risque opérationnel approuvé par le conseil d'administration. Ce dispositif devrait être appliqué de façon cohérente dans l'ensemble de l'organisation bancaire, et les membres du personnel, à tous les niveaux, devraient bien comprendre leurs responsabilités dans la gestion du risque opérationnel. La direction générale devrait aussi être chargée d'élaborer des politiques, processus et procédures de gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants.

Gestion du risque : identification, évaluation, suivi et maîtrise/atténuation du risque

Principe 4 – Les banques devraient identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles devraient aussi, avant de lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent.

Principe 5 – Les banques devraient mettre en œuvre un processus de suivi régulier des profils de risque opérationnel et des expositions importantes à des pertes. Les informations utiles à une gestion dynamique du risque opérationnel devraient être régulièrement communiquées à la direction générale et au conseil d'administration.

Principe 6 – Les banques devraient adopter des politiques, processus et procédures pour maîtriser et/ou atténuer les sources importantes de risque opérationnel. Elles devraient réexaminer périodiquement leurs stratégies de limitation et de maîtrise du risque et ajuster leur profil de risque opérationnel en conséquence par l'utilisation de stratégies appropriées, compte tenu de leur appétit pour le risque et de leur profil de risque globaux.

Principe 7 – Les banques devraient mettre en place des plans de secours et de continuité d'exploitation pour garantir un fonctionnement sans interruption et limiter les pertes en cas de perturbation grave de l'activité.

Rôle des superviseurs

Principe 8 – Les autorités de contrôle bancaire devraient exiger que toutes les banques, quelle que soit leur taille, aient mis en place un dispositif efficace pour identifier, évaluer, suivre et maîtriser/atténuer les risques opérationnels importants, dans le cadre d'une approche globale de la gestion du risque.

Principe 9 – Les superviseurs devraient procéder régulièrement, de manière directe ou indirecte, à une évaluation indépendante des politiques, procédures et pratiques des banques en matière de risque opérationnel. Les superviseurs devraient veiller à ce qu'il existe des mécanismes appropriés leur permettant de se tenir informés de l'évolution dans les banques.

Rôle de la communication financière

Principe 10 – La communication financière des banques devrait être suffisamment étoffée pour permettre aux intervenants du marché d'évaluer leur méthodologie de gestion du risque opérationnel.

---

exécutive. Dans d'autres pays, le conseil a des compétences plus larges et définit les grandes orientations de la gestion de la banque. En raison de ces différences, les expressions « conseil d'administration » et « direction générale » ne sont pas utilisées ici pour renvoyer à des concepts juridiques, mais plutôt pour désigner deux fonctions de décision au sein d'une banque.

Élaboration d'un environnement adéquat pour la gestion du risque

11. L'absence de compréhension et de gestion du risque opérationnel, présent dans pratiquement toutes les transactions et activités bancaires, peut beaucoup augmenter la probabilité que certains risques ne soient ni décelés ni maîtrisés. Le conseil d'administration et la direction générale ont pour responsabilité de créer une culture d'entreprise qui donne une haute priorité à la gestion effective du risque opérationnel et à l'observation de contrôles solides. La gestion du risque opérationnel atteint son efficacité maximum quand la culture de la banque met l'accent sur des critères élevés de comportement éthique à tous les niveaux de l'établissement. Le conseil d'administration et la direction générale devraient favoriser une culture qui, en actes et en paroles, impose un comportement d'intégrité à tous les employés de la banque dans le cadre de leur travail.

Principe 1 – Le conseil d'administration devrait considérer les principaux aspects du risque opérationnel de la banque comme une catégorie distincte de risque à gérer, et il devrait approuver et réexaminer périodiquement le dispositif de gestion de ce risque. Ce dispositif devrait fournir une définition du risque opérationnel valable pour la banque tout entière et poser les principes servant à identifier, évaluer, suivre et maîtriser/atténuer ce risque.

12. Le conseil d'administration devrait approuver la mise en œuvre d'un dispositif, valable pour l'établissement tout entier, visant à gérer expressément le risque opérationnel en tant que risque distinct pour la sécurité et la solidité de la banque. Le conseil d'administration devrait fournir à la direction générale des orientations claires sur les principes sous-tendant le dispositif et approuver les politiques correspondantes élaborées par la direction.

13. Le dispositif de risque opérationnel devrait se fonder sur une définition adéquate de ce qui constitue le risque opérationnel dans la banque. Le dispositif devrait prendre en compte l'appétit de l'établissement pour le risque opérationnel et son degré de tolérance à son égard, en spécifiant les politiques de gestion de ce risque et la priorité donnée par la banque à leur mise en application, en précisant les conditions dans lesquelles ce risque peut être transféré à l'extérieur de la banque. Le dispositif devrait aussi comporter des politiques définissant la méthodologie de la banque pour l'identification, l'évaluation, le suivi et la maîtrise/l'atténuation du risque. Le degré de formalisation et d'élaboration de ce dispositif devrait correspondre au profil de risque de la banque.

14. Le conseil d'administration a pour responsabilité de créer une structure capable de mettre en œuvre le dispositif de gestion du risque opérationnel de la banque. Comme la mise en place de contrôles internes solides constitue un élément essentiel de cette gestion, il est particulièrement important que le conseil d'administration définisse clairement les niveaux de responsabilité et de notification. En outre, il devrait établir une séparation des responsabilités et des circuits de notification entre les fonctions contrôle des risques, unités opérationnelles et fonctions de soutien, afin d'éviter les conflits d'intérêts. Le dispositif devrait aussi définir les processus essentiels à mettre en place par l'établissement pour gérer le risque opérationnel.

15. Le conseil d'administration devrait revoir régulièrement le dispositif pour s'assurer que la banque gère les risques opérationnels résultant d'évolutions extérieures sur le marché et d'autres facteurs environnementaux, ainsi que les risques liés aux produits, activités ou systèmes nouveaux. Ce réexamen devrait aussi chercher à déterminer, parmi les pratiques optimales du secteur pour la gestion du risque opérationnel, celles qui sont les mieux adaptées aux activités, systèmes et processus de la banque. Si nécessaire, le conseil d'administration devrait veiller à ce que le dispositif de gestion du risque opérationnel soit révisé à la lumière de cette analyse, de façon à prendre en compte les risques opérationnels importants.

Principe 2 – Le conseil d'administration devrait garantir que le dispositif de gestion du risque opérationnel de la banque est soumis à un audit interne efficace et complet, effectué par un personnel fonctionnellement indépendant, doté d'une formation appropriée et compétent. La fonction d'audit interne ne devrait pas être directement responsable de la gestion du risque opérationnel.

16. Les banques devraient posséder un système d'audit interne adéquat, apte à vérifier que les politiques et procédures opérationnelles sont correctement mises en place[5]. Le conseil

[5] Le document du Comité, *Internal Audit in Banks and the Supervisor's Relationship with Auditors* (août 2001), décrit le rôle de l'audit interne et externe.

d'administration devrait (directement ou par l'intermédiaire de son comité d'audit) veiller à ce que la portée et la fréquence du programme d'audit concordent avec le degré d'exposition au risque. L'audit devrait vérifier périodiquement que le dispositif de gestion du risque opérationnel est mis en œuvre avec efficacité dans l'établissement tout entier.

17. Dans la mesure où la fonction d'audit est chargée de la surveillance du dispositif de gestion du risque opérationnel, le conseil d'administration devrait s'assurer de son indépendance. Cette indépendance peut être menacée si la fonction d'audit est directement impliquée dans le processus de gestion du risque opérationnel. La fonction d'audit peut fournir des indications précieuses aux personnes responsables de la gestion du risque opérationnel, mais elle ne devrait pas elle-même être chargée de responsabilités directes à cet égard. En pratique, le Comité reconnaît que dans certaines banques (particulièrement les établissements relativement petits) la fonction d'audit peut être appelée, dans un premier temps, à élaborer un programme de gestion du risque opérationnel. Dans ce cas, les banques devraient veiller à ce que la responsabilité de la gestion au jour le jour soit rapidement transférée à une autre fonction.

Principe 3 – La direction générale devrait avoir pour mission de mettre en œuvre le dispositif de gestion du risque opérationnel approuvé par le conseil d'administration. Ce dispositif devrait être appliqué de façon cohérente dans l'ensemble de l'organisation bancaire, et les membres du personnel, à tous les niveaux, devraient bien comprendre leurs responsabilités dans la gestion du risque opérationnel. La direction générale devrait aussi être chargée d'élaborer des politiques, processus et procédures de gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants.

18. La direction devrait traduire le dispositif de gestion du risque opérationnel élaboré par le conseil d'administration en politiques, processus et procédures précis pouvant être appliqués et contrôlés au sein des diverses unités de l'entreprise. Alors que chaque niveau de gestion est responsable de l'adéquation et de l'efficacité des politiques, processus, procédures et contrôles dans son domaine, la direction générale devrait définir clairement les rapports d'autorité, de compétence et de notification, afin de préserver et de fortifier cette responsabilité. Elle devrait également faire en sorte que les ressources nécessaires soient disponibles pour une gestion efficace du risque opérationnel. La direction générale devrait en outre évaluer l'adéquation du processus de surveillance de cette gestion au regard des risques inhérents à la politique de chaque unité.

19. La direction générale devrait veiller à ce que les activités bancaires soient menées par un personnel qualifié doté de l'expérience, des capacités techniques et de l'accès aux ressources nécessaires et que le personnel responsable du suivi et du respect de la politique en matière de risque soit investi d'une autorité indépendante des unités qu'il surveille. La direction générale devrait s'assurer que la politique de gestion du risque opérationnel appliquée par la banque a été communiquée clairement au personnel, à tous les niveaux, dans les unités qui encourent des risques importants de ce type.

20. La direction générale devrait veiller à ce que le personnel responsable de la gestion du risque opérationnel puisse communiquer efficacement avec le personnel responsable de la gestion des risques de crédit, de marché et des autres risques, ainsi qu'avec les membres de l'établissement responsables des services fournis en externe (par exemple, polices d'assurance et contrats d'externalisation). Faute de cela, le programme global de gestion des risques pourrait présenter des lacunes ou des duplications fâcheuses.

21. La direction générale devrait aussi veiller à ce que la politique de rémunération de la banque concorde avec son appétit pour le risque. Les politiques de rémunération qui récompensent les agents s'écartant des politiques (par exemple, en dépassant les limites établies) affaiblissent le processus de gestion du risque.

22. Une attention spéciale devrait être portée 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 de gros volumes de transactions devraient être bien documentés et être diffusés à tout le personnel concerné.

Gestion du risque : identification, évaluation, suivi et maîtrise/atténuation du risque

Principe 4 – Les banques devraient identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles devraient aussi, avant de lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent.

23. Un bonne identification du risque est essentielle pour l'élaboration d'un système viable de suivi et de maîtrise du risque. Elle devrait prendre en compte à la fois les facteurs internes (comme la structure de la banque, la nature de ses activités, la qualité de ses ressources humaines, les modifications de l'organisation et le taux de rotation du personnel) et externes (comme les évolutions du secteur bancaire et les progrès technologiques) qui pourraient empêcher la banque d'atteindre ses objectifs.

24. Les banques ne devraient pas seulement identifier les risques les plus dangereux, mais aussi évaluer leur vulnérabilité à ces risques. Une bonne évaluation des risques permet à la banque de mieux appréhender son profil de risque et de déterminer plus efficacement les ressources nécessaires à leur gestion.

25. Parmi les outils que les banques peuvent utiliser pour identifier et évaluer le risque opérationnel, on peut citer les suivants.

- ***Autoévaluation ou évaluation du risque***. La banque évalue ses opérations et ses activités en fonction d'une liste de points potentiellement exposés au risque opérationnel. Ce processus, mené en interne, repose souvent sur des listes de contrôle et/ou des ateliers destinés à identifier les forces et faiblesses de l'environnement opérationnel. Les évaluations qualitatives peuvent être converties, au moyen d'une matrice (« tableau de bord »), en mesures quantitatives fournissant un classement relatif des différents types d'exposition au risque opérationnel. La matrice peut recenser des risques propres à une activité donnée et d'autres recoupant plusieurs activités. Elle peut prendre en compte les risques, mais aussi les moyens de les atténuer. En outre, elle peut aider les banques à affecter leur capital économique entre les diverses activités selon les résultats obtenus dans la gestion et la maîtrise des divers aspects du risque opérationnel.

- ***Cartographie des risques***. Ce processus, qui cartographie par type de risque les diverses unités, fonctions organisationnelles ou chaînes d'opérations, peut repérer les zones de faiblesse et permettre d'établir des priorités pour l'action à entreprendre par la direction.

- ***Indicateurs de risque***. Les indicateurs de risque sont des statistiques et/ou diverses mesures, souvent d'ordre financier, qui peuvent donner une idée de l'exposition d'une banque au risque. Ils sont généralement revus de façon périodique (chaque mois ou chaque trimestre) pour alerter les banques sur les modifications porteuses de risques. Ces indicateurs comprennent, par exemple, le nombre d'opérations non exécutées, le taux de rotation du personnel, la fréquence et/ou la gravité des erreurs et omissions.

- ***Quantification du risque***. Certains établissements ont commencé, en suivant diverses approches, à quantifier leur exposition au risque opérationnel. Par exemple, les séries historiques sur les pertes peuvent fournir des informations utiles afin d'évaluer l'exposition au risque opérationnel et d'élaborer une politique pour maîtriser/atténuer ce risque. Un moyen efficace pour exploiter ces informations est de mettre en place un cadre permettant de suivre et d'enregistrer systématiquement les caractéristiques des cas de pertes (fréquence, gravité et toutes autres informations pertinentes). Certains établissements ont aussi croisé leurs données internes sur les pertes avec des données externes de pertes, des analyses de scénarios et des facteurs d'évaluation du risque.

Principe 5 – Les banques devraient mettre en œuvre un processus de suivi régulier des profils de risque opérationnel et des expositions importantes à des pertes. Les informations utiles à une gestion dynamique du risque opérationnel devraient être régulièrement communiquées à la direction générale et au conseil d'administration.

26. Un processus efficace de suivi est essentiel pour une gestion adéquate du risque opérationnel. Un suivi régulier permet de détecter et de corriger rapidement les insuffisances des politiques, processus et procédures pour la gestion de ce risque, ce qui peut réduire sensiblement la fréquence et/ou la gravité potentielles des cas de pertes.

27. Les banques devraient non seulement suivre les cas de pertes opérationnelles, mais aussi identifier les indicateurs avancés d'un risque accru de perte. Ces indicateurs (appelés souvent indicateurs clés ou indicateurs d'alerte avancée) devraient être prospectifs ; ils pourraient faire apparaître des sources éventuelles de risque opérationnel, telles que la rapidité de la croissance, le lancement de nouveaux produits, la rotation des employés, les ruptures de transactions, les pannes de système, etc. Quand ces indicateurs comportent un seuil, un processus efficace de suivi peut permettre à la banque d'identifier les risques clés de manière transparente et de réagir de manière adéquate.

28. La périodicité du suivi devrait être adaptée aux risques ainsi qu'à la fréquence et à la nature des modifications de l'environnement opérationnel. Le suivi devrait faire partie intégrante de l'activité de la banque. Ses résultats devraient figurer dans les rapports réguliers à la direction et au conseil, tout comme les examens accomplis par les fonctions d'audit interne et/ou de gestion des risques. Les rapports rédigés par et/ou pour les superviseurs peuvent aussi contribuer au suivi et devraient donc être communiqués en interne à la direction générale et au conseil d'administration dans tous les cas appropriés.

29. La direction générale devrait recevoir régulièrement des rapports émanant des services appropriés, comme les unités opérationnelles, les fonctions de groupe, le service de gestion du risque opérationnel et l'audit interne. Les rapports concernant le risque opérationnel devraient contenir des données internes (aspects financiers, opérations et conformité), ainsi que des informations externes (de marché) sur les événements et conditions qui peuvent influencer le processus de décision. Les rapports devraient être distribués aux niveaux appropriés de la direction et aux secteurs d'activité qui peuvent être exposés au risque. Ils devraient intégralement rendre compte de tous les domaines identifiés comme présentant un risque et déclencher une action corrective rapide sur les problèmes décelés. Pour assurer l'utilité et la fiabilité de ces rapports de risque et d'audit, la direction devrait vérifier régulièrement la rapidité, l'exactitude et la pertinence des systèmes de notification et des contrôles internes en général ; elle peut aussi, pour ce faire, utiliser des rapports préparés par des sources extérieures (auditeurs, superviseurs). Les rapports devraient être analysés dans le but d'améliorer les résultats de la gestion des risques et d'élaborer de nouvelles politiques, procédures et pratiques de gestion des risques.

30. En règle générale, le conseil d'administration devrait recevoir suffisamment d'informations de niveau élevé pour comprendre le profil global de risque opérationnel encouru par la banque et se concentrer sur les conséquences pratiques et stratégiques pour l'entreprise.

Principe 6 – Les banques devraient adopter des politiques, processus et procédures pour maîtriser et/ou atténuer les sources importantes de risque opérationnel. Elles devraient réexaminer périodiquement leurs stratégies de limitation et de maîtrise du risque et ajuster leur profil de risque opérationnel en conséquence par l'utilisation de stratégies appropriées, compte tenu de leur appétit pour le risque et de leur profil de risque globaux.

31. Les activités de contrôle interne sont conçues pour traiter les risques opérationnels qui ont été identifiés[6]. Lorsque ces derniers sont importants, la banque est amenée à décider si elle va soit utiliser les procédures appropriées pour maîtriser et/ou atténuer les risques, soit assumer ceux-ci. Pour les risques qui ne peuvent pas être maîtrisés, elle devrait choisir de les accepter, de réduire l'activité concernée ou de se retirer complètement. Les banques devraient disposer de processus et procédures de contrôle, ainsi que d'un système assurant la conformité des opérations à un ensemble de politiques internes dûment documentées concernant la gestion du risque. Les principaux éléments de cet ensemble pourraient, par exemple, être les suivants :

- examens au plus haut niveau des progrès accomplis par la banque vers les objectifs définis ;
- vérification de l'application des contrôles de gestion ;
- politiques, processus et procédures concernant l'examen, le traitement et la résolution des problèmes de non-conformité ;

[6] Pour plus de détails, Comité de Bâle sur le contrôle bancaire, *Cadre pour les systèmes de contrôle interne dans les organisations bancaires*, septembre 1998.

- système d'approbation et d'autorisation documentées régissant la responsabilité des agents auprès d'un niveau approprié de la direction.

32. S'il est indispensable qu'une banque dispose d'un ensemble de politiques et procédures formalisées et documentées, celui-ci doit être renforcé par une solide culture de contrôle favorisant la mise en œuvre de saines pratiques de gestion du risque. Le conseil d'administration et la direction générale ont pour mission d'établir une solide culture de contrôle interne dans laquelle celui-ci fait partie intégrante des activités régulières de la banque, ce qui permet de réagir rapidement aux changements de conditions et d'éviter les coûts inutiles.

33. Pour qu'un système de contrôle interne soit efficace, il faut aussi qu'il comporte une répartition des tâches adéquate, de telle sorte que des agents ne se voient pas assigner des responsabilités pouvant donner lieu à des conflits d'intérêts. À défaut, la personne ou l'équipe en question pourrait être en mesure de dissimuler des pertes, des erreurs ou des actes inappropriés. Il convient, par conséquent, d'identifier les sources éventuelles de conflits d'intérêts, de les réduire au minimum et de les soumettre à un travail de suivi et d'examen indépendant et attentif.

34. Au delà de cette répartition des tâches, les banques devraient veiller à appliquer toute autre pratique interne nécessaire à la maîtrise du risque opérationnel, par exemple :

- suivi attentif du respect des limites ou seuils de risque fixés ;
- sécurisation de l'accès aux avoirs et archives de la banque et de leur utilisation ;
- mise à jour des compétences et de la formation des agents ;
- identification des activités ou produits dont les rendements paraissent disproportionnés par rapport à des attentes raisonnables (par exemple, une activité de négoce censée présenter de faibles risques et être peu rémunérée, mais qui génère des rendements élevés, amène à se demander si ceux-ci ne résulteraient pas d'une violation des règles internes) ;
- vérification et rapprochement réguliers des transactions et des comptes.

Faute de pratiques de ce type, certaines banques ont subi de lourdes pertes ces dernières années.

35. Le risque opérationnel peut être plus élevé quand les banques s'engagent dans de nouvelles activités ou élaborent de nouveaux produits (surtout quand ces activités ou ces produits s'écartent de leurs métiers traditionnels), pénètrent dans des marchés qu'elles connaissent mal et/ou se lancent dans des activités géographiquement éloignées de leur siège. En outre, bien souvent dans ce cas, les banques ne veillent pas à développer leur infrastructure de contrôle du risque parallèlement à leur activité. Les pertes parmi les plus lourdes et les plus médiatisées des dernières années trouvent leur origine dans un ou plusieurs de ces facteurs. Dans de telles situations, il incombe donc aux banques d'accorder une attention particulière aux activités de contrôle interne.

36. Certains risques opérationnels importants présentent une probabilité faible, mais une incidence financière potentielle considérable. En outre, il n'est pas possible de maîtriser tous les risques (par exemple, les catastrophes naturelles). On peut en revanche utiliser des instruments ou programmes d'atténuation des risques pour réduire l'exposition à ces risques, leur fréquence et/ou leur gravité. Les polices d'assurance, notamment, surtout si elles garantissent un paiement rapide et certain, peuvent être utilisées pour externaliser le risque de pertes peu fréquentes mais aux conséquences graves, qui peuvent résulter de divers événements comme l'indemnisation de tiers au titre d'erreurs et omissions, la perte physique de titres, la fraude d'un employé ou d'un tiers et les catastrophes naturelles.

37. Toutefois, les banques devraient considérer que, si les instruments d'atténuation du risque viennent compléter le contrôle interne minutieux du risque opérationnel, ils ne peuvent s'y substituer. Disposer de mécanismes permettant de reconnaître et de corriger rapidement les erreurs légitimement associées au risque opérationnel peut grandement réduire les expositions. Il convient aussi d'examiner soigneusement dans quelle mesure les instruments d'atténuation comme l'assurance réduisent vraiment le risque, ou le transfèrent à un autre secteur ou domaine d'activité, voire s'ils ne créent pas un nouveau risque (par exemple, risque juridique ou risque de contrepartie).

38. Les investissements dans les techniques appropriées de traitement des données et de sécurité informatique jouent aussi un rôle important pour l'atténuation du risque. Toutefois, les banques devraient être conscientes que le développement de l'automatisation peut transformer des pertes à fréquence élevée et de faible impact en pertes peu fréquentes mais aux conséquences

graves, telles que les pertes associées à un arrêt prolongé de l'offre de services sous l'effet de facteurs internes ou d'éléments échappant au contrôle direct de la banque (par exemple, événements extérieurs). De tels problèmes peuvent causer de grandes difficultés aux banques et pourraient mettre en danger la capacité d'un établissement à mener ses principales activités. Comme le précise *infra* le principe 7, les banques devraient disposer de programmes de reprise et de continuité d'exploitation pour traiter ce risque.

39. Les banques devraient aussi mettre en place des politiques de gestion des risques liés aux activités externalisées. L'externalisation peut réduire le profil de risque d'un établissement en transférant certaines activités spécialisées à des entreprises qui ont plus d'expertise et d'envergure pour gérer les risques qui y sont associés. Toutefois, le recours à des tiers ne diminue pas la responsabilité du conseil d'administration et de la direction générale, à qui il incombe de veiller à ce que l'activité de ces tiers soit menée de façon sûre et saine, dans le respect de la législation applicable. Les accords d'externalisation devraient reposer sur des contrats solides et/ou des conventions de service assurant une répartition claire des responsabilités entre les prestataires de service extérieurs et l'établissement. En outre, les banques devraient gérer les risques résiduels liés à ces accords d'externalisation, y compris toute perturbation dans l'offre de services.

40. Selon l'ampleur et la nature de l'activité, les banques devraient comprendre l'impact potentiel sur leur activité et leur clientèle de toute carence éventuelle des services confiés aux fournisseurs et autres prestataires (tiers ou membres du même groupe) – y compris les défaillances opérationnelles et l'échec commercial ou le défaut d'une partie extérieure. Le conseil d'administration et la direction générale devraient s'assurer que les attentes et les obligations de chaque partie sont clairement définies, comprises et juridiquement valides. La portée de la responsabilité juridique de la partie extérieure et sa capacité financière à indemniser la banque en cas d'erreur, de négligence et d'autres défaillances opérationnelles devrait être explicitement considérée comme faisant partie de l'évaluation du risque. Les banques devraient procéder, au départ, à un examen du devoir de diligence, et suivre régulièrement les activités des tiers prestataires, surtout s'ils n'ont pas l'expérience du cadre réglementaire du secteur bancaire ; elles devraient effectuer des réexamens périodiques de ce processus (notamment pour l'obligation de diligence). Pour ses activités critiques, la banque peut être amenée à envisager des plans de secours, y compris la possibilité de recourir à d'autres parties extérieures, et prévoir les coûts et ressources nécessaires pour opérer un tel changement, éventuellement dans un très bref délai.

41. Dans certaines situations, les banques peuvent décider soit de conserver un niveau donné de risque opérationnel, soit d'être leur propre assureur contre ce risque. Dans ce cas, si le risque est important, cette décision devrait être annoncée de façon transparente dans toute l'organisation et concorder avec la stratégie globale de la banque et avec son appétit pour le risque.

Principe 7 – Les banques devraient mettre en place des plans de secours et de continuité d'exploitation pour garantir un fonctionnement sans interruption et limiter les pertes en cas de perturbation grave de l'activité.

42. Pour des raisons qui peuvent échapper au contrôle de la banque, un incident grave peut l'empêcher d'exécuter entièrement ou partiellement ses obligations, en particulier quand ses infrastructures physiques, de télécommunications ou d'informatique ont été endommagées ou rendues inaccessibles. Cette situation peut à son tour provoquer de lourdes pertes financières pour la banque, ainsi que des perturbations générales du système financier par l'intermédiaire de canaux comme le système de paiements. Cette éventualité nécessite que les banques mettent en place des programmes de reprise et de continuité d'exploitation, en rapport avec sa taille et avec la complexité de ses activités, prenant en compte divers types de scénarios plausibles auxquels la banque peut être exposée.

43. Les banques devraient identifier les processus cruciaux, notamment ceux qui dépendent de fournisseurs extérieurs ou d'autres tiers, dont la reprise rapide est prioritaire. Pour ces processus, les banques devraient identifier des solutions de secours permettant de rétablir le service en cas de panne. Il convient de prêter une attention particulière à la capacité de restaurer les archives électroniques ou physiques nécessaires à la reprise de l'activité. Quand les archives sont dupliquées sur un autre site, ou quand les activités de la banque devraient reprendre dans d'autres locaux, il faudrait veiller à ce que ces facilités de secours soient suffisamment éloignées du site principal pour réduire le risque d'une mise hors service simultanée.

44. Les banques devraient revoir périodiquement leurs programmes de reprise et de continuité d'exploitation pour s'assurer qu'ils restent adaptés au niveau de leurs activités et stratégies. En outre,

ces programmes devraient être testés périodiquement pour vérifier que la banque serait en mesure de les mettre en œuvre même dans le cas improbable d'une grave perturbation de l'activité.

Rôle des superviseurs

Principe 8 – Les autorités de contrôle bancaire devraient exiger que toutes les banques, quelle que soit leur taille, aient mis en place un dispositif efficace pour identifier, évaluer, suivre et maîtriser/atténuer les risques opérationnels importants, dans le cadre d'une approche globale de la gestion du risque.

45. Les autorités de contrôle devraient exiger que les banques élaborent un dispositif de gestion du risque opérationnel conforme aux lignes directrices exposées dans le présent document et en rapport avec leur taille, leur complexité et leur profil de risque. Dans la mesure où le risque opérationnel constitue une menace pour la sécurité et la solidité des banques, il incombe aux superviseurs de les encourager à élaborer et utiliser les meilleures techniques pour gérer ces risques.

Principe 9 – Les superviseurs devraient procéder régulièrement, de manière directe ou indirecte, à une évaluation indépendante des politiques, procédures et pratiques des banques en matière de risque opérationnel. Les superviseurs devraient veiller à ce qu'il existe des mécanismes appropriés leur permettant de se tenir informés de l'évolution dans les banques.

46. Une évaluation indépendante du risque opérationnel par les superviseurs devrait porter, notamment, sur les éléments suivants :

- efficacité du processus de gestion du risque par la banque et de son système global de contrôle en ce qui concerne le risque opérationnel ;
- méthodes adoptées par la banque pour suivre et présenter son profil de risque opérationnel, y compris données sur les pertes d'exploitation et autres indicateurs de risque opérationnel ;
- procédures choisies par la banque pour résoudre de manière rapide et efficace les incidents de nature opérationnelle et traiter ses sources de vulnérabilité ;
- processus internes de contrôle, de réexamen et d'audit de la banque destinés à assurer l'intégrité de la gestion globale du risque opérationnel ;
- efficacité des instruments d'atténuation du risque opérationnel (assurance, par exemple) utilisés par la banque ;
- qualité et exhaustivité des programmes de reprise et de continuité d'exploitation de la banque ;
- processus appliqué par la banque pour évaluer l'adéquation globale de ses fonds propres au titre du risque opérationnel en fonction de son profil de risque et, le cas échéant, de ses objectifs de fonds propres économiques.

47. Les superviseurs devraient aussi veiller à ce que les banques faisant partie d'un groupe financier disposent de procédures garantissant que le risque opérationnel est géré de façon adéquate et intégrée sur l'ensemble du groupe. Dans le cadre de cette évaluation, ils peuvent être amenés à coopérer et échanger des informations avec d'autres superviseurs, conformément aux procédures établies. Pour ce processus d'évaluation, certains superviseurs peuvent choisir d'utiliser des auditeurs externes.

48. Les lacunes notées par les superviseurs dans l'exercice de la surveillance prudentielle peuvent appeler diverses actions. Les superviseurs devraient recourir aux instruments les plus adaptés aux conditions spécifiques de la banque et à son environnement opérationnel. Pour être convenablement informés, les superviseurs peuvent souhaiter établir des procédures de déclaration du risque opérationnel directement avec les banques et avec les auditeurs externes (par exemple, les établissements pourraient systématiquement transmettre aux superviseurs leurs rapports internes à la direction sur ce sujet).

49. Comme il est notoire que les banques en sont encore souvent au stade de l'élaboration d'un processus global de gestion du risque opérationnel, les superviseurs devraient encourager activement leurs efforts de développement interne en effectuant un suivi et une évaluation des améliorations en cours et projetées. Ces efforts pourront alors être comparés à ceux d'autres banques et servir à informer l'établissement, en retour, sur sa situation par rapport à la profession. De plus, dans la

mesure où l'on connaîtrait les raisons pour lesquelles certaines formules s'avéreraient inefficaces, une telle information pourrait être partagée, en termes généraux, pour faciliter le processus de développement. Par ailleurs, les superviseurs devraient examiner plus particulièrement à quel degré un établissement est parvenu à intégrer sa gestion du risque opérationnel sur l'ensemble de l'organisation bancaire, pour garantir une gestion efficace dans toutes les catégories d'activité, établir des canaux de communication et de responsabilité clairement définis, tout en favorisant une autoévaluation active des pratiques existantes et la recherche des améliorations possibles dans le domaine de l'atténuation du risque.

Rôle de la communication financière

Principe 10 – La communication financière des banques devrait être suffisamment étoffée pour permettre aux intervenants du marché d'évaluer leur méthodologie de gestion du risque opérationnel.

50. Le Comité estime que la rapidité et la fréquence de la communication par les banques d'informations financières pertinentes peuvent aboutir à un renforcement de la discipline de marché et, par conséquent, à une gestion plus efficace du risque. Le volume des données publiées devrait concorder avec la taille de l'établissement, son profil de risque et la complexité de ses activités.

51. Le détail des informations à publier en liaison avec le risque opérationnel n'est pas encore bien défini, principalement parce que les banques en sont encore à élaborer leurs techniques d'évaluation de ce risque. Toutefois, le Comité estime que les banques devraient faire connaître leur dispositif de gestion du risque opérationnel de telle façon que les investisseurs et les contreparties puissent savoir si elles identifient, évaluent, suivent et maîtrisent/atténuent efficacement leur risque opérationnel.