RECOMMANDATIONS

La Réforme BÂLE 2

Une présentation générale

Décembre 2004

Groupe de travail Bâle 2

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Semard
Téléphone : 01 53 25 08 80 Fax : 01 53 25 08 88
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.f

Remerciements

Le CLUSIF remercie les personnes qui ont rendu possible la réalisation de ce document :

Gérard	**CHAMORET**	**VALOR**
Frédéric	**CHAVOUTIER**	**LA POSTE**
Michèle	**COPITET**	**EGONA-CONSULTING**
Jean-Paul	**GODARD**	**SOCIÉTÉ GÉNÉRALE**
Paul	**GRASSART**	**ARSEO**
Jean	**MAUFERON**	**CAP GEMINI**
Lionel	**MOURER**	**BULL SERVICES FRANCE**
Thierry	**RAMARD**	**AGERIS**
Gérard	**REMY**	**XP CONSEIL**

Avec l'aimable participation de :

Pascal	**AUCLERT**	**ALGORIEL**
Philippe	**CAILLE**	**TELINDUS FRANCE**
M'Baireh	**LISETTE**	**SUNGARD**
Jean-Louis	**ROULE**	
Axel	**VERGELY**	**SUNGARD**

Table des matières

1. INTRODUCTION

La réforme Bâle II du ratio de solvabilité bancaire s'inscrit dans une démarche mondiale de réglementation de la profession bancaire remontant à la fin des années 80, dont l'objectif premier est de prévenir les faillites.

Cette réforme repose sur la quantification de la relation entre risques et fonds propres, ces derniers représentant le moyen ultime permettant de faire face à des pertes importantes. En pratique, il s'agit de respecter un ratio réglementaire entre fonds propres et actifs pondérés par leur niveau de risque.

Mais cette réforme va plus loin : elle s'attaque au processus métier d'évaluation et de gestion des risques, dans une perspective qualité. Au-delà de la dimension financière qui est le calcul des fonds propres à allouer, Bâle II prend en compte et place ses exigences sur les systèmes de notation et de surveillance. Bien plus, et c'est l'aspect le plus novateur, la réforme ne se limite plus aux seuls risques financiers « classiques », comme le risque de crédit ou les risques de marché (risque de change, risque de taux, etc.), mais couvre aussi le Risque « Opérationnel » :

> « Le Risque Opérationnel se définit comme le risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs. La définition inclut le risque juridique, mais exclut les risques stratégiques et d'atteinte à la réputation » (définition du Comité de Bâle). À ce titre, il ne suffit plus de se préoccuper de la capacité de paiement d'un tiers, mais il faut, entre autres, évaluer les éventuelles défaillances des processus internes ou des systèmes informatiques, ainsi que les risques d'erreur ou de fraude.

1.1. A qui s'adresse ce document ?

Ce document se situe dans la perspective des travaux menés par le CLUSIF. Il traite donc plus particulièrement de la prise en compte des risques liés à la sécurité des Systèmes d´Information, à savoir une partie du volet « Risques Opérationnels » dans le cadre de la régulation des multiples risques auxquels sont confrontés les établissements financiers. À ce titre, le présent document s'adresse plus particulièrement aux Risk Managers et RSSI du domaine financier souhaitant acquérir une connaissance générale simplifiée de la réglementation Bâle II et s´interrogeant, plus particulièrement, sur les impacts de la réforme dans leur périmètre de responsabilité.

D'autre part, ce document aborde les apports potentiels de Bâle II pour les domaines et entreprises non soumis à cette réglementation et offre des éléments de réflexion sur l'intérêt de la prise en compte du Risque Opérationnel dans leur domaine d'activité. Au-delà, il peut apporter des informations aux autres intervenants du secteur : chefs de projets, responsables d´exploitation, etc.

En revanche, ayant été rédigé dans un souci de vulgarisation, ce document ne s'adresse pas aux spécialistes de ce domaine réglementaire. Il n'est pas non plus un document général sur la nouvelle réforme, car il ne prend pas en compte tous ses aspects.

1.2. Périmètre du document

Ce document décrit essentiellement les approches du Risque Opérationnel sur les Systèmes d'Information dans les « Mesures Avancées[1] » de calcul des fonds propres.

- les parties « risques de crédit » et « risques de marché » ne sont pas abordées dans ce document,
- seule la problématique des Systèmes d'Information est traitée dans la suite,
- les approches « Indicateurs de Base » et « Standard », qui permettent un calcul forfaitaire des fonds propres liés au risque opérationnel ne sont pas présentées.

[1] Cf. présentation des « Risques Opérationnels » et de leur gestion au chapitre 2.2.

2. PRÉSENTATION

2.1. Les grands principes de la réforme Bâle 2

Dans le cadre des travaux menés par le Comité de Bâle et la Commission Européenne, le ratio de solvabilité des établissements bancaires fera l'objet d'une réforme importante à l'échéance de fin 2006.

Le nouvel accord de Bâle sur les fonds propres a été finalisé en juin 2004 et adopté par les gouverneurs des banques centrales et les superviseurs des pays du G10.

Le dispositif repose sur trois types d'obligations (les 3 piliers) :

- les établissements devront disposer d'un montant de fonds propres (Pilier I) au moins égal à la somme des montants calculés selon l'une des méthodes proposées pour chacune des catégories de risques :
    - Risques de Crédit,
    - Risques de Marché,
    - **Risques Opérationnels,**
- les autorités disposeront de pouvoirs renforcés (Pilier II) et pourront en particulier imposer, au cas par cas, des exigences de fonds propres supérieures à celles résultant de la méthode utilisée,
- les établissements étant soumis à la « discipline de marché » (Pilier III), seront tenus de publier des informations très complètes sur la nature, le volume et les méthodes de gestion de leurs risques ainsi que sur l'adéquation de leurs fonds propres.

Les nouvelles règles en matière de capital vont encourager la gestion professionnelle des risques et du capital par les banques. Bâle II est une réforme structurante et les établissements ne pourront faire l'économie d'un investissement significatif (Systèmes d'Information, gestion des risques, communication, formation, etc.). L'enjeu du nouveau dispositif est tout aussi essentiel pour les autorités de contrôle (ressources, application cohérente entre pays).

2.2. Les « Risques Opérationnels » et leur gestion

Définition : Risque Opérationnel = risque de pertes dues à une inadéquation ou à une défaillance des procédures, personnels, systèmes internes ou à des événements extérieurs.

Les Risques Opérationnels, dont la prise en compte constitue une des innovations de la réforme, incluent notamment :

- les risques relatifs à la sécurité des biens et des personnes (incendie, inondation, tremblement de terre, attaque physique, sabotage, vol et fraude),
- les risques informatiques, liés aux développements et à la maintenance des programmes, aux traitements et à l'utilisation des services de télécommunications. Cette catégorie inclut en particulier le risque lié aux défauts de conception ou de réalisation d'une application, les incidents d'exploitation dans les systèmes de production, les accès non autorisés et les erreurs de traitement, ainsi que les pertes ou altérations accidentelles des données transmises et les défaillances dans la conservation de ces données,

- les risques de gestion interne, liés au fonctionnement interne de la banque, incluant les erreurs dans les traitements administratifs et comptables des opérations, les erreurs de conception ou de mise en place de nouveaux produits ou projets, la malveillance interne, les risques légaux, réglementaires ou déontologiques, les risques en matière de ressources humaines, de sous-traitance et de communication externe.

Dans le cadre du risque opérationnel, Bâle II prévoit trois approches[2], chacune possédant son mode de calcul des exigences en fonds propres :

- une approche « Indicateur de Base »,
- une approche « Standard »,
- une approche « Mesures Avancées ».

Dans le cadre de l'approche « Mesures Avancées », l'organisme financier doit calculer lui-même sa charge de capital. La notion de risque prend ici toute son importance car il s'agira d'évaluer la perte potentielle que pourrait avoir l'organisme financier dans 99,9 % des cas. Cette approche, permettant moins d'exigences en fonds propres, doit respecter les critères suivants :

- un critère général : l'approbation préalable de l'autorité de supervision,
- des critères qualitatifs :
    - fonction « gestion du Risque Opérationnel » indépendante,
    - implication des dirigeants,
    - intégration dans la gestion des risques au quotidien,
    - reporting régulier des expositions et des pertes,
    - programme régulier d'analyse de scénarios,
    - documentation sur les procédures, contrôles, etc.,
    - audits internes et/ou externes[3],
- des critères quantitatifs :
    - prise en compte des pertes sévères mais rares et calibrage à partir des pertes attendues et inattendues,
    - processus de gestion et bases de données cohérents avec la définition du Risque Opérationnel,
    - Système d'Information approprié,
    - procédures en cas de changement de taille,
    - procédures pour l'usage des données d'origine externe,
    - revue périodique des méthodologies et paramètres,

[2] L'approche « Mesures avancées » est une approche plus complexe, réservée aux établissements bancaires les plus avancés et les plus exposés aux risques, permettant une optimisation des exigences en fonds propres.

[3] L'accord prévoit « et/ou » (réf. 666 alinéa e). Il est vraisemblable que le régulateur national précisera ce point.

- historique de données sur 5 ans,
- reconnaissance possible des corrélations, assurances et ajustements qualitatifs (tenant compte de la qualité des contrôles et/ou de l'environnement économique).

2.3. Les catégories de pertes liées aux risques opérationnels

Les modèles de Risques Opérationnels utilisés doivent inclure une modélisation liée à l'historique des évènements. Les types d'événements caractérisant le Risque Opérationnel, identifiés par le Comité de Bâle et pouvant induire des pertes substantielles, comprennent :

- la fraude interne. Par exemple, le défaut intentionnel d'information sur les positions, le vol par un employé et le virement interne sur le compte détenu par un employé,
- la fraude externe. Par exemple, le vol, la contrefaçon, le chèque de cavalerie et les dommages résultant d'un piratage informatique,
- les pratiques en matière d'emploi et de sûreté du lieu de travail. Par exemple, les compensations demandées par les travailleurs, la violation des règles sur la santé et sur la sûreté du personnel, sur l'organisation des activités de travail, les réclamations sur la discrimination et sur la responsabilité en général,
- les clients, les produits et les procédures de gestion. Par exemple, les infractions fiduciaires, les abus d'information confidentielle sur le client, les transactions interdites sur les comptes de la banque, le blanchiment d'argent et la vente de produits interdits,
- les dommages aux biens corporels. Par exemple, le terrorisme, le vandalisme, les tremblements de terre, les feux et les inondations,
- les perturbations des processus métiers et les pannes de système. Par exemple, les pannes de matériel et de logiciel, les problèmes de télécommunication et les pannes issues de services sous-traités,
- l'exécution, le résultat et le contrôle de processus. Par exemple, les erreurs de saisie de données, les effets collatéraux des erreurs de gestion, la documentation légale incomplète, l'accès non autorisé donné aux comptes de clients, le défaut de la contrepartie non-cliente et les conflits entre fournisseurs.

2.4. La gouvernance à mettre en place

Le document « Sound Practices[4] » définit les conditions du développement d'un environnement approprié de gestion des risques.

2.4.1 Développement d'un environnement approprié de gestion des risques.

Principe 1 : Le Conseil d'Administration devrait identifier les aspects principaux des Risques Opérationnels de la banque, en les considérant comme une catégorie distincte de risques à gérer ; de plus, il devrait approuver, et périodiquement passer en revue, le modèle de référence de la gestion du risque opérationnel de la banque. Ce modèle de référence devrait donner une définition du Risque Opérationnel valable pour toute la banque, et définir les principes d'identification, d'évaluation, de suivi et de contrôle/réduction de ces risques.

[4] La traduction du texte et les développements correspondants sont fournis en annexe 6.

Principe 2 : Le Conseil d'Administration devrait s'assurer que le modèle de référence de la gestion du risque opérationnel de la banque est soumis à un audit interne efficace et complet, et ceci par un personnel effectivement indépendant, convenablement formé 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 la responsabilité de mettre en œuvre le modèle de gestion du Risque Opérationnel approuvé par le Conseil d'Administration. Le modèle de référence devrait être mis en œuvre de manière cohérente partout dans toute l'organisation bancaire, et tous les niveaux de personnel devraient comprendre et assumer leurs responsabilités en ce qui concerne la gestion du Risque Opérationnel. La Direction devrait aussi avoir la responsabilité de développer les politiques, les processus et les procédures pour gérer le Risque Opérationnel pour tous les produits, activités, processus et systèmes de la banque.

2.4.2 Gestion du risque : Identification, Évaluation, Suivi et Réduction/Contrôle.

Principe 4 : Les banques devraient identifier et évaluer le Risque Opérationnel pour tous les produits, activités, processus et systèmes. Avant de présenter ou d'introduire de nouveaux produits, de nouvelles activités, de nouveaux processus ou de nouveaux systèmes, les banques devraient aussi s'assurer que le Risque Opérationnel qui leur est inhérent est bien soumis à des procédures d'évaluation adéquates.

Principe 5 : Les banques devraient mettre en œuvre un processus pour contrôler régulièrement les Risques Opérationnels et les principaux facteurs d'expositions à des pertes. Il devrait y avoir une présentation régulière des informations pertinentes à la Direction et au Conseil d'Administration afin de favoriser une gestion proactive du Risque Opérationnel.

Principe 6 : Les banques devraient avoir des politiques, des processus et des procédures pour contrôler et/ou réduire les principaux Risques Opérationnels. Les banques devraient périodiquement passer en revue leurs modalités de réduction du risque et les stratégies de contrôle et ajuster leur profil de Risque Opérationnel, en utilisant, en conséquence, des stratégies appropriées, à la lumière du profil de risque qu'elles souhaitent adopter.

Principe 7 : Les banques devraient mettre en place des plans de reprise et de continuité des activités métiers afin de s'assurer de leur capacité à fonctionner et à limiter les pertes en cas d'incidents affectant gravement leurs activités.

2.4.3 Rôle de Surveillance

Principe 8 : Les autorités de supervision devraient exiger que toutes les banques, indépendamment de leur taille, disposent d'un modèle de référence efficace, mis en place pour identifier, évaluer, suivre et contrôler/réduire les Risques Opérationnels importants et que celui-ci soit considéré comme un des éléments d'une approche plus complète de la gestion des risques.

Principe 9 : Les autorités de supervision devraient régulièrement conduire, directement ou indirectement, une évaluation indépendante des politiques, des procédures et des pratiques liées aux Risques Opérationnels d'une banque. Les autorités de supervision devraient s'assurer que les mécanismes appropriés sont mis en place pour leur permettrent de rester immédiatement informés des évolutions des situations des banques.

2.4.4 Rôle de publication

Principe 10 : Les banques devraient produire les déclarations publiques nécessaires pour permettre aux participants du marché d'évaluer leur approche de la gestion du Risque Opérationnel.

3. RISQUES OPÉRATIONNELS ET SYSTÈME D'INFORMATION

3.1. Présents dans toutes les catégories de pertes…

Une lecture rapide de la typologie d'événements [cf. § 2.3] pourrait laisser croire que les événements sont regroupés dans la catégorie « Perturbations des processus métiers et pannes systèmes ». En fait, il n'en est rien.

La classification proposée par le Comité de Bâle ne se substitue pas à une classification propre à une analyse de risques : elle n'est que le « plan de classement » d'un historique des évènements.

Sous réserve de la maîtrise des risques qui lui sont propres (indisponibilité, fraude, risque systémique lié à l'automatisation), l'informatique peut également apparaître comme un dispositif d'atténuation du risque. On peut citer : la réduction des risques d'erreur humaine par la mise en place de traitements automatisés (STP : Straight Through Processing), la mise en place de supports assurant la fiabilité des processus métiers (pistes d'audit, pilotage de processus par un workflow), etc.

3.2. Quels outils peut-on mettre en place ?

3.2.1 Perspective générale

La réglementation Bâle II correspond à une vision économique des risques liés aux Systèmes d'Information, car elle demande de contrôler l'adéquation entre les niveaux de fonds propres évalués par les modèles et les pertes potentielles qu'ils doivent couvrir. Même si elle ne procure pas de retour direct immédiat pour la gestion de la sécurité du Système d'Information, cette perspective contribue à l'analyse préalable des risques potentiels, sa dimension économique offrant par ailleurs, la possibilité d'une comparaison entre les risques du SI et les autres risques du périmètre.

Le nouvel accord de Bâle sur les fonds propres (juin 2004) prévoit, aux paragraphes 670 à 676, que l'estimation des risques doit être basée sur :

- les données internes de pertes (bases des incidents et des pertes),
- des données externes pertinentes, notamment pour l'analyse des pertes peu fréquentes mais potentiellement lourdes,
- des analyses de scénarios, pour les événements pouvant engendrer des pertes sévères,
- indicateurs clés de risques et évaluation du Contrôle Interne.

3.2.2 Base des incidents et base des pertes

L'intérêt de la base des incidents est de constituer un historique détaillé de la sinistralité, qui permet de connaître et d'analyser les types de sinistres constatés et leur fréquence. De cette démarche on pourra tirer une meilleure connaissance de la sensibilité des activités, un suivi des évolutions des différents risques et de leurs mesures correctrices.

L'exigence de disposer également d'un historique de pertes amène à effectuer une analyse fine de l'impact et du coût réel des sinistres.

Si le premier inventaire peut être constitué dans le seul périmètre « Systèmes d'Information », et donc dans le périmètre de responsabilité du RSSI, la mesure des pertes effectives amène à rechercher des informations opérationnelles auprès des métiers.

3.2.3 Outils d'analyse de scénarios

Les principes d'analyse de risque retenus par le Comité de Bâle reposent sur une approche fondamentalement quantitative. Il s'agit donc de construire des modèles statistiques de prévision des risques, à partir d'un historique de pertes avérées, internes ou externes à la banque.

Toutefois, et c'est pourquoi le Comité de Bâle impose une analyse complémentaire de scénarios, les modèles quantitatifs se montrent souvent limités pour des types de pertes particuliers :

- les pertes à très faible fréquence mais potentiellement lourdes, pour lesquelles l'insuffisance de données rend difficile la construction d'un modèle statistique précis,
- les pertes liées à de nouveaux types d'incidents (apparition de nouveaux enjeux, de nouvelles menaces ou de nouvelles vulnérabilités) : bien que ces incidents puissent être classés sans difficulté dans la typologie des incidents collectés, les modèles historiques peuvent se montrer incapables de les quantifier,
- les scénarios plausibles et non réalisés : du fait de l'évolution permanente des Systèmes d'Information, la seule analyse des expériences passées ne donne qu'une vue partielle des impacts financiers possibles d'un incident. Il devient donc nécessaire d'établir de façon régulière une revue de scénarios catastrophes que l'entreprise a jugés plausibles et insupportables.

Des outils[5] d'analyse de scénarios de risque (telle que la méthode MEHARI™ du CLUSIF), apportent un support pour le traitement de ces cas exceptionnels. Ils présentent les avantages suivants :

- ils ont été conçus pour quantifier des risques à partir de l'historique ainsi que sur la base d'une analyse des facteurs de risque présents au moment de l'étude. Ils restent donc pertinents dans les cas où d'autres modèles atteignent leurs limites,
- en tant qu'outils, ils facilitent la révision périodique de l'analyse, par une mise à jour de l'estimation des facteurs de risques.

3.2.4 Indicateurs clés de risques et évaluation du Contrôle Interne

Parmi les autres mécanismes permettant l'évaluation des risques, il est possible de se reposer sur les études permettant de visualiser les évolutions du risque. Elles peuvent également aider à la justification de l'analyse liée à l'environnement. Parmi ces études, citons :

- l'étude annuelle de sinistralité du CLUSIF,
- les études des « analystes » (Gartner, Meta Group, IDC, etc.),
- l'étude annuelle du FBI, etc.

[5] L'adaptation de ces outils à un domaine plus vaste que le périmètre spécifique des Systèmes d'Information n'est pas abordée dans ce document.

3.3. Rôles et relations entre RSSI, Risk Management Opérationnel et Contrôle Interne

3.3.1 Le Contrôle Interne

Le Contrôle Interne est un ensemble de dispositifs mis en œuvre sous l'impulsion des plus hautes autorités de la banque (Conseil d'Administration, Comité Exécutif, etc.), les responsables d'unités opérationnelles ou fonctionnelles et l'ensemble du personnel. Il vise à assurer la maîtrise globale des risques et de la gestion, l'efficacité de l'organisation, la qualité des informations et le respect de la réglementation.

Le Contrôle Interne doit respecter les principes généraux suivants :

- couvrir de manière exhaustive les activités et les risques,
- s'intégrer à l'exercice des activités,
- être adapté à la nature et à la dimension des activités,
- réaliser un juste équilibre entre les gains de sécurité escomptés et le coût des contrôles à mettre en place,
- être en ligne avec la stratégie de la banque.

À ce titre, le Contrôle Interne dispose de plusieurs dispositifs visant à la maîtrise des risques :

- identification des risques liés au fonctionnement des unités,
- évaluation des risques mesurables,
- élaboration de politiques de prises de risques adaptées aux enjeux,
- limite des risques, prévoyant la fixation de limites globales et opérationnelles, la revue, la mesure, le suivi des dépassements et des régularisations,
- suivi des performances d'ensemble.

3.3.2 Risk Management Opérationnel (RMO)

Le Risk Management Opérationnel est un acteur clé du processus de contrôle, chargé de veiller à l'existence et à l'efficacité des dispositifs permettant de maîtriser les Risques Opérationnels.

Plus concrètement, le gestionnaire des Risques Opérationnels a les missions suivantes :

- identification des risques,
- évaluation des risques,
- suivi et réduction/contrôle (surveillance et maîtrise des risques).

Il propose, met en place, maintient et fait évoluer en fonction des risques le dispositif de contrôle interne de l'entité, de la direction opérationnelle ou fonctionnelle ou de la ligne métier dont il est en charge. Pour ce faire, il est assisté des autres acteurs du Contrôle Interne (management opérationnel et fonctionnel, direction des risques, pilotage du Contrôle Interne, audit).

3.3.3 RMO et Sécurité des Systèmes d'information

Parmi les Risques Opérationnels se trouvent ceux liés aux Systèmes d'Information ; ceux-ci pouvant être la cible ou le vecteur de réalisation du risque.

La Sécurité des Systèmes d'Information est assurée par l'ensemble des moyens humains, organisationnels et techniques constituant une réponse adaptée aux risques et aux niveaux de risques identifiés, notamment par le RMO, mais aussi par les dispositifs permanents de surveillance des risques institués dans le cadre du Contrôle Interne.

On peut donc positionner le RMO comme un relais pour la maîtrise des risques, entre le contrôle interne, chargé de la maîtrise globale des risques et la Sécurité des Systèmes d'Information.

3.3.4 Contrôle Interne et Sécurité des Systèmes d'Information

Le Contrôle Interne et la Sécurité des Systèmes d'Information doivent collaborer, notamment dans les domaines suivants :

- management des entités : les mesures de sécurité organisationnelles et fonctionnelles doivent s'intégrer dans le dispositif de Contrôle Interne de chaque entité, c'est-à-dire *in fine* dans l'organisation de ces entités. C'est le management, fonctionnel ou opérationnel, qui est chargé de mettre en œuvre et de superviser le dispositif de Contrôle Interne dans l'entité placée sous sa responsabilité,
- prise en compte des Risques Opérationnels sur les nouveaux produits ou processus afin d'intégrer ces besoins de sécurité lors de développement ou d'évolution des Systèmes d'Information, et notamment ceux mettant en œuvre de nouvelles technologies,
- intégration des contrôles dans les applications,
- élaboration des cartographies des risques et des enjeux,
- élaboration, mise en place et contrôle du plan de continuité d'activité,
- mise en place d'un plan d'assurance permettant soit de financer l'activation des mesures de protection, soit de financer le risque résiduel,
- mise en place des différents relais (y compris correspondants sécurité),
- définition, mise en place et exploitation des tableaux de bord,
- coordination et suivi des plans d'actions (RMO, Contrôle Interne, SSI).

Mais ils doivent aussi collaborer pour d'autres actions de prévention des risques, telles que :

- sensibilisation du management des entités,
- formation des opérationnels,
- diffusion des normes,
- conseil / expertise,
- constitution et participation à la veille technologique.

Dans cette dynamique, le Responsable de la Sécurité du Système d'Information (RSSI) est appelé à jouer un rôle important pour le progrès de la démarche de réduction des risques opérationnels.

Cette collaboration sera, *a minima*, une contribution du RSSI – pour sa connaissance du risque informatique – à l'analyse et au traitement des risques opérationnels liés au traitement de l'information (nous avons ainsi déjà vu comment des méthodes de sécurité des systèmes d'information peuvent être utilisées pour enrichir l'analyse des risques opérationnels).

Toutefois, on peut s'attendre à une influence réciproque. L'un des éléments fondamentaux des accords de Bâle II est le traitement économique du risque. Or, les RSSI, peut être par manque d'outils et/ou de formation, n'ont généralement aujourd'hui qu'une vision technique et organisationnelle des risques et de leur traitement.

En particulier, très peu de RSSI sont responsables du financement du risque lié aux Systèmes d'Information (assurance, fonds propres ou financements alternatifs), activités dévolues au Risk Manager (RM). Cette collaboration facilitera la connaissance par le RSSI des moyens de justifier et défendre des actions légitimes de sécurité.

Par son approche économique du risque, Bâle II va faciliter les échanges entre les acteurs de l'organisation (contrôle interne, RMO et RSSI mais aussi les métiers et la DSI) pour répondre à ces besoins :

- en premier lieu, la meilleure connaissance du coût du non-risque va permettre de mieux calculer le retour sur investissement d'un projet de sécurité (qui doit permettre de réduire les fonds propres dédiés au financement du risque désormais traité),

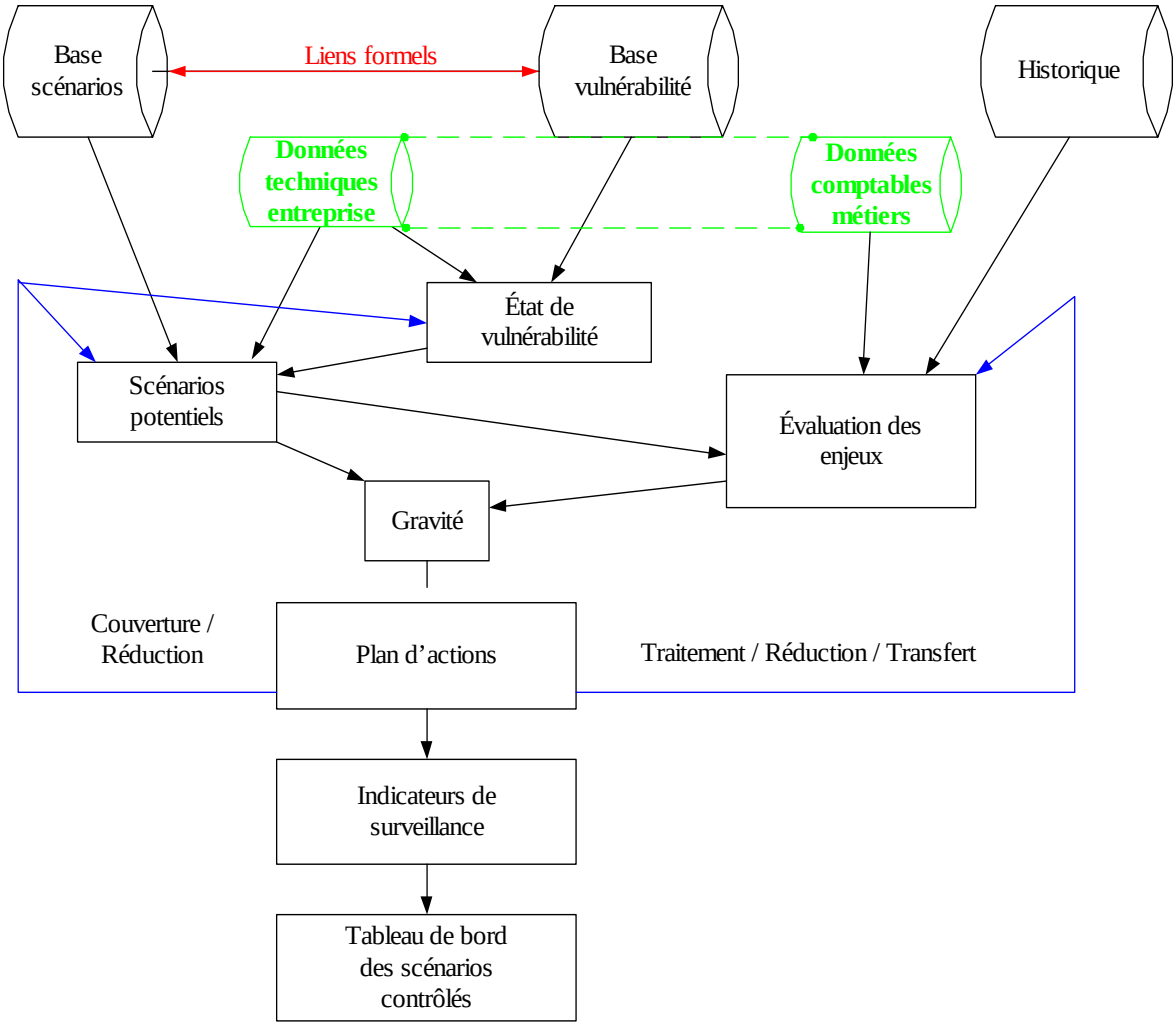
- en second lieu, en s'appuyant sur cette vision économique du risque, il devient envisageable de déterminer la création de valeur de la gestion de risque, en démontrant l'effet de la sécurité sur la préservation des résultats de l'entreprise.

La méthode MEHARI™

À partir de la base des vulnérabilités, la méthode MEHARI™ permet aisément à une entreprise d'en déduire les failles et vulnérabilités propres à son environnement.

Il est donc possible, après l'identification des failles de sécurité d'une part et la quantification et/ou qualification des pertes potentielles d'un sinistre d'autre part, d'en évaluer l'impact et donc d'apprécier la gravité du risque engendré. La mise en œuvre des mesures de sécurité nécessaires à la réduction du risque permettra d'obtenir le niveau de gravité cible défini comme acceptable ou tolérable.

L'historique des incidents et la base de données des pertes constatées permettront de construire une base personnalisée.



[Hors texte N°1]

4. CE QUE PEUT APPORTER BÂLE II AUX ENTREPRISES NON TENUES À LA RÉGLEMENTATION BANCAIRE

En tant que tels, les accords de Bâle II ne concernent que les banques et les établissements financiers (la Commission Européenne en étend le champ d'application aux fonds d'investissements et certains pays reprennent certains éléments dans la réglementation des compagnies d'assurance). Toutefois, les exigences contenues dans ces accords ne sont pas une réelle spécificité bancaire. Comme on va le voir au cours de ce chapitre, ils s'inscrivent dans une tendance générale qui concerne l'ensemble du tissu économique mondial.

La communauté financière, notamment aux États-Unis et en Europe, a été secouée par les scandales financiers mettant en cause la confiance dans la fiabilité des comptes des entreprises et dans la qualité de leur Contrôle Interne.

Cette crise a conduit les pouvoirs publics à légiférer afin de :

- réformer les instances de contrôles des marchés,
- inciter les entreprises à plus de transparence,
- mieux protéger les épargnants,
- réformer certains aspects de la mission de contrôle légal des comptes.

Cela s'est traduit par un renforcement des règles de gouvernement d'entreprise, ou « gouvernance », et par la recherche d'une meilleure maîtrise des risques par les entreprises.

La réforme de Bâle II s'inscrit, elle aussi, dans cette logique. On peut en effet constater que les trois piliers sur lesquels repose le nouvel accord peuvent servir de guide pour aider les entreprises non bancaires à se positionner vis-à-vis des évolutions en cours. Nous allons le montrer en examinant l'apport potentiel de chacun de ces piliers.

4.1. Apports du pilier III

Pilier III : obligation de publier des informations complètes sur la nature, le volume et les méthodes de gestion des risques ainsi que l'adéquation de leurs fonds propres.

Le troisième pilier des accords vise à renforcer la discipline de marché, ce qui nécessite une plus grande transparence des entreprises quant à leurs pratiques de gestion des risques.

On peut constater que la réglementation évolue dans ce sens et ce au niveau mondial. De nombreuses lois ont été promulguées pour rendre obligatoire la communication sur les risques : Loi sur la Sécurité Financière (France), Sarbanes-Oxley Act (USA), Combined Code (Royaume-Uni), etc. La présentation de l'information financière aux marchés est complétée pour mieux rendre compte des risques, et notamment du « hors bilan » (normes IAS/IFRS).

> *« À titre liminaire, il est rappelé que tout émetteur qui publie sur un marché étranger des informations autres que celles prévues ci-après est tenu de publier simultanément une information équivalente à destination du marché français. Tel sera notamment le cas des*

émetteurs faisant appel public à l'épargne en France qui appliqueront les dispositions du Sarbanes-Oxley Act américain ou du Combined Code britannique ».[6]

Rappelons que la Loi sur la Sécurité Financière (LSF) ne concerne pas que les grands groupes, mais s'applique à toutes les Sociétés Anonymes, cotées ou non cotées, et est applicable dès la présentation des comptes de 2003. La LSF fait notamment obligation au Président du Conseil d'Administration ou du Conseil de Surveillance de rendre compte, dans un rapport, des travaux du conseil et des procédures de Contrôle Interne mises en place par la société. Le Président détermine les modalités à appliquer pour produire ce rapport. Ces modalités doivent ensuite être transmises à la Direction Générale, afin d'être mises en œuvre par le Contrôle Interne.

Dans ce contexte de renforcement du Contrôle Interne, il est recommandé aux entreprises concernées de bien distinguer les risques liés à l'information comptable et financière et les Risques Opérationnels.

En ce qui concerne le Risque Opérationnel, notamment par l'ampleur de sa réflexion et des méthodes qu'elle met en œuvre, la réforme Bâle II offre une base de référence significative sur laquelle peuvent s'appuyer les entreprises non bancaires.

4.2. Apports du pilier II

Pilier II : Les autorités disposent de pouvoirs renforcés pour imposer des exigences de fonds propres supérieurs à ceux envisagés par l'entreprise.

Dans un contexte économique et culturel d'esprit libéral, les évolutions réglementaires en cours, tous pays et tous secteurs confondus, tendent à mettre l'accent sur la discipline de marché, qui implique la transparence en matière de gestion des risques.

Toutefois, le régulateur vise à prévenir les imperfections du marché (et notamment les asymétries d'informations) en renforçant le pouvoir des autorités de contrôle. Dans le contexte bancaire, ce renforcement fait l'objet du pilier II des accords. On peut toutefois vérifier qu'il s'agit là encore d'une tendance de fond, qui n'est pas spécifique aux banques. On peut ainsi la rapprocher en France du renforcement des pouvoirs de la CNIL[7] en matière de protection de la vie privée, mais aussi du pouvoir des DRIRE[8] (risque industriel), de l'Inspection du Travail (santé et conditions de travail), ou encore de la création de l'ADAÉ[9].

Ces quelques exemples mettent en exergue une spécificité des établissements bancaires, dont le métier est réglementé de manière globale par les autorités financières, alors que dans la majorité des cas, une entreprise est « multi-réglementée », la multiplicité des règlements en matière de risque compliquant l'exposé et l'analyse de ses risques.

Dans ce contexte, il apparaît que l'augmentation de la réglementation en matière de gestion des risques, loin de diminuer le rôle du commissaire aux comptes en le réduisant à sa principale vocation de certification des comptes sociaux, pourrait être amenée à le renforcer en tant que principal interlocuteur des entreprises, allant presque jusqu'à jouer le rôle de corps de contrôle en refusant de certifier les comptes tant que l'entreprise ne serait pas conforme aux exigences réglementaires de gestion des risques.

---

[6] AMF, « Conditions de publication des informations article 122 de la loi sur la sécurité financière », 23 janvier 2004.

[7] CNIL : Commission Nationale de l'Informatique et des Libertés (http://www.cnil.fr).

[8] DRIRE : Directions Régionales de l'Industrie, de la Recherche et de l'Environnement (http://www.drire.gouv.fr/).

[9] ADAÉ : Agence pour le Développement de l'Administration Électronique (http://www.adae.gouv.fr/).

4.3. Apports du pilier I

Pilier I : Disposer d'un montant de fonds propres pour couvrir les risques

De manière globale, mais particulièrement dans le pilier I, les accords de Bâle II incitent à mener une analyse économique globale du risque, et ce à chaque étape du processus de Risk Management : identification, analyse, traitement et financement.

Par ses exigences en termes de capitaux propres (et donc de structure des passifs), mais aussi par les indicateurs sur lesquels sont construits les ratios, le pilier I montre directement l'impact des risques et de leur gestion sur le bilan d'une entreprise. Outre l'objectif affiché de limiter les faillites par un financement suffisant des risques, on peut considérer que le but sous-jacent est d'inciter les dirigeants à appréhender globalement leurs risques et à les traiter de manière à en limiter l'impact sur le bilan.

Ainsi, bien que le pilier I concerne explicitement les méthodes de calcul de fonds propres, il doit sur le fond être interprété comme le renforcement des incitations à mieux gérer ses risques.

5. ANNEXE : ANALYSE DE SCÉNARIOS À L'AIDE DE LA MÉTHODE MEHARI™

Dans le cadre de la discipline de marché et de la communication sur la gestion des risques les scénarios de risque analysés doivent être des scénarios métier. Toutefois, pour de nombreuses entreprises, et en particulier pour les établissements financiers, la forte dépendance de l'entreprise vis-à-vis de ses Systèmes d'Information fait que la plupart des catégories de risques opérationnels peuvent avoir pour origine un scénario de risque lié au traitement de l'information.

Par exemple, il est possible d'identifier des scénarios de risque informatique pour chaque famille d'événements proposée par la documentation Bâle II :

- fraude interne. Par exemple, réalisation intentionnelle d'une transaction non notifiée (faiblesse des contrôles programmés),
- fraude externe. Par exemple, vol ou détournement financier, falsification de chèques, dommages dus au piratage informatique (perte ou altération de données, qu'elles soient intentionnelles ou non de la part du pirate), vol d'informations avec pertes financières, etc.
- pratiques en matière d'emploi et de sécurité sur le lieu de travail. Par exemple, divulgation dans l'entreprise des rémunérations de catégories de personnel sensibles, entraînant une grève, édition et divulgation de listings de membres du personnel triés ou filtrés selon des critères contraires à la loi (opinions politiques, appartenance religieuse, origine raciale, etc.),
- clients, produits et pratiques commerciales. Par exemple, divulgation des opérations réalisées sur le compte de clients, divulgation d'informations liées à la connaissance de la clientèle (marketing direct), entraînant une perte de compétitivité, faiblesse de contrôles programmés entraînant une erreur sur l'analyse de l'exposition d'un client, vol d'informations personnelles sur un client,
- dommages aux actifs corporels. Par exemple, destruction d'un centre informatique, tous risques liés à la sécurité physique des Systèmes d'Information, terrorisme, vandalisme,
- dysfonctionnement de l'activité et des systèmes. Par exemple, panne matérielle, plantage logiciel, rupture d'un câble de télécommunication, attaque en déni de service,
- exécution, livraison et gestion des processus. Par exemple, erreur dans la saisie de données, perte d'éléments constitutifs d'un contrat dématérialisé, accès non autorisés aux comptes des clients, conflits avec des fournisseurs ou sous-traitants.

La méthode MEHARI™ propose, quant à elle, la décomposition en plusieurs familles de scénarios, parmi lesquels :

- l'indisponibilité passagère de ressources, la destruction d'équipements,
- les performances dégradées, la destruction de logiciel,
- l'altération de logiciel, l'altération de données,

- la manipulation de données, etc.

De fait, il est possible d'utiliser MEHARI™ pour analyser ces scénarios métier d'au moins deux manières :

- moyennant une « traduction » d'un risque métier en un ou plusieurs scénarios tirés de la base MEHARITM,
- en construisant spécifiquement des scénarios de risque selon le modèle MEHARITM.

Illustration du premier cas (traduction) :

Le scénario métier « Réalisation intentionnelle d'une transaction non notifiée (faiblesse des contrôles programmés) » correspond dans la base MEHARI™, au scénario-type « Saisie faussée de données par un agent autorisé, mais déloyal ».

Le scénario métier « Divulgation des opérations réalisées sur le compte de clients » peut être traité par plusieurs scénarios-type standard de MEHARI™ concernant la divulgation ou le détournement de données. Ces scénarios-types doivent, bien entendu, être appliqués sur un contexte particulier (les données des opérations réalisées sur le compte des clients et les différents moyens de stocker et traiter ces données). Dans la démarche MEHARI™, cette interprétation de scénarios-type dans un contexte spécifique est appelée « découpage cellulaire ».

Illustration du deuxième cas (construction de scénarios sur mesure) :

Certains scénarios métier ne pourront pas être aisément interprétés en terme de scénarios-types fournis dans les bases de connaissance de la méthode. Dans ce cas, il est facile de compléter les bases standard en créant des scénarios sur-mesure.

Par exemple, le scénario métier « Falsification de chèques » pourra être construit en inventoriant les mesures de sécurité destinées à limiter les falsifications, que ce soit en exposition structurelle (par exemple, établissement financier n'ayant pas d'activité de traitement de chèque, donc structurellement non exposé à ce scénario), en dissuasion (campagnes d'affichage chez les commerçants informant de la vérification systématique des chèques), en prévention (utilisation de formules de chèques sécurisés et difficiles à falsifier), en protection (détection des chèques volés chez les commerçants), en palliation (pas de mesure identifiée) ou en récupération (assurances et recours juridiques).

6. ANNEXE : « SOUND PRACTICES » BONNES PRATIQUES POUR LA GESTION ET LA SURVEILLANCE DU RISQUE OPÉRATIONNEL

Cette annexe reprend des extraits du document « Sound Practices for the Management and Supervision of Operational Risk » publié (en anglais) par le Comité de Bâle, sous la référence n°96 en février 2003.

Ce document, à l'usage des banques et des autorités de tutelles, décrit un ensemble de principes qui fournissent un cadre à la gestion et à la surveillance efficace du risque opérationnel, afin de leur permettre d'évaluer les politiques et les pratiques de gestion des risques opérationnels. […]

Le comité de Bâle du contrôle bancaire reconnaît que l'approche concrètement retenue par un établissement bancaire pour la gestion des risques opérationnels dépendra d'une gamme de facteurs, comprenant sa taille, la sophistication, la nature et la complexité de ses activités. […]

Cependant, hormis ces différences, une stratégie claire et une maîtrise globale de gestion des risques par le conseil d'administration et la direction, une forte culture du risque opérationnel et une culture du contrôle interne (y compris la définition claire des responsabilités et la séparation des fonctions), un reporting interne efficace, ainsi que le plan de secours constituent les éléments cruciaux d'un modèle efficace de gestion des risques opérationnels pour toutes les banques quels que soient leur taille et leur domaine d'activité.

Le lecteur trouvera ici les commentaires extraits du document « Sound Practices » sur certains des principes [4 à 7] déjà présentés dans le chapitre 2.4.

Principe 4 : Les banques devraient identifier et évaluer le risque opérationnel pour tous les produits, activités, processus et systèmes. Avant de présenter ou d'introduire de nouveaux produits, de nouvelles activités, de nouveaux processus ou de nouveaux systèmes, les banques devraient aussi s'assurer que le risque opérationnel qui leur est inhérent, est bien soumis à des procédures d'évaluation adéquates.

> 23. L'identification du risque est primordiale pour que puissent être développés un contrôle et un suivi viable du risque opérationnel. L'identification efficace du risque prend en compte des facteurs internes (tels que la structure de la banque, la nature de ses activités, la qualité des ressources humaines, les changements d'organisation et le taux de rotation des employés) et des facteurs externes (tels que des changements dans le métier et des progrès technologiques) qui pourraient compromettre l'accomplissement des objectifs de la banque.
>
> 24. En plus d'identifier les risques les plus potentiellement défavorables, les banques devraient évaluer la vulnérabilité à ces risques. L'évaluation efficace des risques permet à la banque de mieux comprendre son profil de risque et de cibler plus efficacement ses ressources de gestion du risque.
>
> 25. Pour identifier et évaluer le risque opérationnel, les banques disposent notamment des outils suivants :
>
> - l'évaluation et l'auto évaluation des risques : une banque évalue ses opérations et ses activités vis-à-vis d'une liste de vulnérabilités potentielles au risque opérationnel. Ce processus est conduit en interne et incorpore souvent des listes de contrôle et/ou des ateliers pour identifier les forces et les faiblesses de

l'environnement de gestion du risque opérationnel. Les *scorecards*, par exemple, fournissent des moyens de traduire des évaluations qualitatives en métriques quantitatives qui donnent un rang relatif de différents types d'expositions au risque opérationnel. Certains de ces *scores*, peuvent être associés à des risques qui concernent uniquement une branche d'activité spécifique, tandis que d'autres peuvent adresser les risques qui sont transversaux à plusieurs branches de l'activité. Les *scores* peuvent être inhérents aux risques eux-mêmes ou encore aux contrôles pour les atténuer. En outre, les *scorecards* peuvent être employés par les banques pour assigner le capital économique aux branches d'activité en fonction des performances dans la gestion et le contrôle des divers aspects du risque opérationnel,

- la cartographie des risques : dans ce processus, différentes entités de gestion, différentes fonctions d'organisation ou différents flux entre processus sont cartographiés par type de risque. Cet exercice peut faire apparaître des zones de faiblesse et aider à fixer les priorités sur les actions de gestion induites,

- les indicateurs de risque : ce sont des éléments de statistiques et/ou des métriques, souvent financières, qui peuvent apporter un point de vue analytique sur une position de risque de la banque. Ces indicateurs sont périodiquement passés en revue (sur une base mensuelle ou trimestrielle) pour alerter les banques des changements qui peuvent impacter une évolution dans la gestion du risque. De tels indicateurs peuvent inclure le nombre d'affaires qui n'ont pas abouti, le taux de rotation du personnel et la fréquence et/ou l'importance des erreurs et des omissions,

- la quantification du risque : certaines sociétés ont commencé à mesurer leur exposition au risque opérationnel en utilisant différentes approches. Par exemple, les données sur l'historique des pertes de la banque ont pu fournir des informations significatives pour évaluer l'exposition de la banque au risque opérationnel et développer une politique de réduction/contrôle du risque. Une manière efficace de faire une bonne utilisation de cette information est d'établir un cadre de référence pour systématiquement dépister et enregistrer la fréquence, la gravité et toute autre information appropriée sur les différents événements de perte. Quelques sociétés ont également combiné ces données internes sur les pertes subies, avec des données externes de pertes, avec des analyses de scénario et avec des facteurs d'évaluation des risques.

Principe 5 : Les banques devraient mettre en œuvre un processus pour contrôler régulièrement les risques opérationnels et les principaux facteurs d'expositions à des pertes. Il devrait y avoir une présentation régulière des informations pertinentes à la direction et au conseil d'administration afin de favoriser une gestion proactive du risque opérationnel.

26. Un processus de surveillance efficace est essentiel pour gérer convenablement le risque opérationnel. Les activités régulières de surveillance peuvent permettre de détecter rapidement puis de corriger les insuffisances des politiques, des procédés et des procédures pour contrôler le risque opérationnel. Promptement détecter et adresser ces insuffisances peut notablement réduire la potentialité et/ou la gravité d'un événement de perte.

27. En plus de surveiller des événements de perte opérationnelle, les banques devraient identifier les indicateurs appropriés qui permettent une détection précoce d'un risque croissant de pertes futures. De tels indicateurs (souvent désignés sous le nom d'indicateurs principaux de risque ou indicateurs de détection précoce) devraient être prospectifs et pourraient refléter les sources potentielles de risque opérationnel telles que la croissance

rapide, l'introduction de nouveaux produits, le taux de rotation des employés, les interruptions de transaction, les temps d'arrêt de système, etc. Quand des seuils sont directement liés à ces indicateurs, un processus de surveillance efficace peut aider à identifier des risques matériels significatifs d'une façon transparente et ainsi permettre à la banque d'agir opportunément sur ces risques.

28. La fréquence de la surveillance devrait être fixée en fonction des risques encourus, de la potentialité et de la nature des changements du contexte de l'activité. La surveillance devrait être intégrée aux activités de la banque. Les résultats de ces activités de surveillance devraient être inclus dans des rapports réguliers de gestion et de direction, de même que devraient être exécutées les revues de conformité par le contrôle interne et/ou les fonctions gestion des risques. Les rapports produits par (et/ou pour) des autorités de supervision peuvent également servir d'information pour les fonctions de surveillance et devraient de même être, le cas échéant, communiqués en interne à la direction générale et au conseil d'administration.

29. La direction générale devrait recevoir des rapports réguliers de secteurs appropriés tels que les entités commerciales, les fonctions de niveau groupe, le bureau de gestion des risques opérationnels et le contrôle interne. Les rapports sur les risques opérationnels devraient contenir des données financières internes, des données opérationnelles et des données sur la conformité, aussi bien que des informations externes sur les marchés, sur les événements et les conditions qui sont significatives dans la prise de décision. Des rapports devraient être diffusés aux niveaux appropriés de direction et aux secteurs de la banque sur lesquels les sujets impliqués peuvent avoir un impact. Les rapports devraient complètement refléter tous les domaines de préoccupation identifiés et devraient déclencher, sur les questions en suspens, l'action de correction au moment opportun. Pour assurer l'utilité et la fiabilité de ces rapports sur la gestion des risques et sur le contrôle, les responsables de gestion devraient régulièrement vérifier l'opportunité, l'exactitude, et la pertinence de systèmes de reporting et du contrôle interne en général. Les responsables peuvent également utiliser des rapports préparés par des sources extérieures (auditeurs, autorités de surveillance) pour évaluer l'utilité et la fiabilité des rapports internes. Les rapports devraient être analysés en vue d'améliorer la performance de la gestion des risques existante, mais aussi de développer de nouvelles politiques, de nouvelles procédures et de nouvelles pratiques en matière de gestion des risques.

30. En général, les membres du conseil d'administration devraient recevoir une information de haut niveau qui leur soit suffisante pour leur permettre de comprendre le profil global de risque opérationnel de la banque et de se focaliser sur les implications matérielles et stratégiques pour l'activité.

Principe 6 : les banques devraient avoir des politiques, des processus et des procédures pour contrôler et/ou réduire les principaux risques opérationnels. Les banques devraient périodiquement passer en revue leurs modalités de réduction du risque et leurs stratégies de contrôle, ainsi qu'ajuster leur profil de risque opérationnel, en utilisant, en conséquence, les stratégies appropriées, conformément au niveau et profil de risque accordés.

31. Les activités de contrôle sont conçues pour adresser les risques opérationnels qu'une banque a identifiés. Pour tous les risques opérationnels qui ont été identifiés, la banque devrait pouvoir décider, si elle emploie les procédures appropriées pour contrôler et/ou atténuer les risques, ou si elle supporte les risques. Pour ces risques qui ne peuvent pas être contrôlés, la banque devrait décider si elle accepte ces risques (en les assurant par exemple), si elle réduit le niveau de l'activité économique impliquée, ou si elle se retire complètement de cette activité. Des processus et des procédures de contrôle devraient être établis et les banques devraient avoir mis en place un système pour assurer la conformité à un ensemble

documenté de politiques internes concernant le système de gestion des risques. Les éléments principaux de ce système pourraient inclure, par exemple :

- l'examen par des dirigeants de l'état d'avancement et de progression de la banque vers les objectifs fixés,
- la vérification de la conformité avec les contrôles de la direction,
- les politiques, les processus et les procédures concernant la revue, le traitement et la résolution des éléments de non-conformité,
- un système d'approbations et d'autorisations documentées afin d'assurer la responsabilité à un niveau approprié de direction.

32. Bien qu'un cadre formel des politiques et des procédures écrites soit essentiel, il doit être renforcé par une culture forte de contrôle qui favorise des pratiques saines en matière de gestion des risques. Le conseil d'administration et la direction générale sont responsables de l'établissement d'une culture interne forte de contrôle dans laquelle les activités de contrôle sont intégrées aux activités régulières d'une banque. Les contrôles qui sont intégrés aux activités régulières permettent de donner des réponses rapides aux situations en évolution et évitent des dépenses inutiles.

33. Un système de contrôle interne efficace exige également qu'il y ait séparation appropriée des fonctions et que le personnel ne soit pas assigné à des responsabilités qui pourraient créer un conflit d'intérêt. Assigner de telles fonctions contradictoires aux individus ou à une équipe, peuvent leur permettre de cacher des pertes, des erreurs ou des actions inadéquates. Par conséquent, des secteurs des conflits potentiels d'intérêt devraient être identifiés, réduits au minimum et faire l'objet d'une surveillance rigoureuse et indépendante.

34. En plus de la séparation des fonctions, les banques devraient s'assurer que d'autres pratiques internes appropriées sont en place pour contrôler le risque opérationnel. Voici quelques exemples :

- la surveillance étroite du respect des limites de risque ou des seuils assignés,
- la mise en place de protections dans l'accès et dans l'utilisation des actifs et des informations de la banque,
- s'assurer que le personnel a l'expertise et la formation adaptées,
- l'identification des branches ou des produits de l'activité où les retours semblent être en dehors des attentes raisonnables (par exemple, où une activité, censément à faible risque et à faible marge, produit de hauts rendements, ce qui devrait permettre de s'interroger pour savoir si de tels retours n'ont pas été réalisés en infraction aux règles de contrôle interne),
- la vérification et le rapprochement réguliers des transactions et des comptes. Ces dernières années, le défaut de la mise en application de telles pratiques a eu comme conséquence des pertes opérationnelles significatives pour certains établissements bancaires.

35. Le risque opérationnel peut être plus prononcé lorsque les banques s'engagent dans de nouvelles activités ou développent de nouveaux produits (en particulier lorsque ces activités ou ces produits ne sont pas alignés avec les stratégies qui sont au cœur des activités de la banque), lorsqu'elles accèdent à des marchés qui leur sont moins familiers, et/ou lorsqu'elles s'engagent dans des entreprises qui sont géographiquement éloignées du siège social.

D'ailleurs, dans beaucoup de tels exemples, les sociétés ne s'assurent pas que l'infrastructure de contrôle de la gestion des risques suit la croissance de l'activité économique. Un certain nombre des pertes les plus importantes en terme de taille et de profil à haut risque de ces dernières années ont eu lieu là où une ou plusieurs de ces conditions existaient. Par conséquent, il incombe aux banques de s'assurer qu'une particulière attention est accordée aux activités internes de contrôle, là où de telles conditions existent.

36. Quelques risques opérationnels significatifs ont de faibles probabilités mais un impact financier potentiellement très grand. D'ailleurs, tous les événements de risque ne peuvent pas être contrôlés (par exemple, les catastrophes naturelles). Des outils ou des programmes de réduction de risque peuvent être employés pour réduire l'exposition, ou la fréquence et/ou la sévérité, de tels événements. Par exemple, des polices d'assurances, en particulier celles avec des dispositifs de remboursement rapides et certains, peuvent être employées pour externaliser les risques de pertes "avec une fréquence faible et une sévérité élevée" qui peuvent se produire en raison des événements tels que des réclamations de tiers résultant des erreurs et des omissions, de la perte physique de valeurs, ou de la fraude d'employés ou de tiers et des catastrophes naturelles.

37. Cependant, les banques devraient considérer les outils de réduction de risque uniquement comme des outils complémentaires, plutôt que comme un complet remplacement du contrôle interne du risque opérationnel. Disposer de mécanismes en place pour pouvoir identifier rapidement et rectifier des erreurs légitimes du risque opérationnel peut considérablement réduire les degrés d'exposition. Une attention rigoureuse doit aussi être accordée afin de vérifier si des outils de réduction de risque, tels que l'assurance, permettent réellement de réduire le risque, ou s'ils transfèrent le risque à un autre secteur ou à une autre activité, ou même, s'ils font naître un nouveau risque (par exemple le risque juridique ou le risque de contrepartie).

38. Des investissements en technologie de traitement de l'information et en sécurité des technologies de l'information sont également importants pour la réduction de risque. Cependant, les banques devraient se rendre compte que l'automatisation accrue peut transformer des pertes à haute et de faible sévérité en des pertes de faible fréquence et de haute sévérité. Ce dernier point peut être associé à la perte ou à l'interruption prolongée des services provoqués par des facteurs internes ou par des facteurs indépendants de la volonté immédiate de la banque (par exemple, événements externes). De tels problèmes peuvent occasionner des difficultés graves pour les banques, et pourraient compromettre la capacité d'une institution à conduire les activités économiques essentielles. Comme discuté, ci-dessous, dans le principe 7, les banques devraient établir des plans de reprise et de continuité d'activité qui adressent ce type de risque.

39. Les banques devraient également établir des politiques pour contrôler les risques liés aux activités de sous-traitances externes (outsourcing). La sous-traitance des activités à l'extérieur peut réduire le profil de risque d'une institution en transférant des activités à d'autres disposant d'une plus grande expertise et d'un plus grand volume pour permettre de contrôler les risques liés aux activités économiques spécialisées. Cependant, le recours à des tiers par la banque ne diminue pas la responsabilité du conseil d'administration et de la direction qui doit s'assurer que l'activité tierce est conduite d'une manière sûre et saine, et en conformité avec les lois. Les accords de sous-traitance à l'extérieur devraient être basés sur de solides contrats et/ou conventions de niveau de service qui assurent une attribution claire des responsabilités entre les fournisseurs des services et la banque qui sous-traite. En outre, les banques doivent contrôler les risques résiduels liés aux accords de sous-traitance, y compris en ce qui concerne la rupture de services.

40. Selon le volume et la nature de l'activité, les banques devraient comprendre l'impact

potentiel sur leurs opérations et sur leurs clients, de toutes les insuffisances potentielles dans les services fournis, par des fournisseurs ou d'autres intermédiaires, ou par des fournisseurs de service en intra-groupe, y compris les cas de pannes opérationnelles et de faillite commerciale, ou de défaillance potentielle de tiers externes. Le conseil d'administration et la direction générale devraient s'assurer que les attentes et les engagements de chaque partie sont clairement définis, compris et exécutoires. L'ampleur de la responsabilité externe et de la capacité financière de la part des tierces parties à compenser pour la banque des erreurs, des négligences, et d'autres échecs opérationnels devrait être explicitement considérée en tant qu'élément de l'évaluation des risques. Les banques devraient effectuer un test initial de "due diligence" et surveiller les activités des tiers fournisseurs, particulièrement ceux qui manquent de l'expérience de l'environnement régulé du métier bancaire, et passer en revue les processus (réévaluations y compris du "due diligence") de façon régulière. Pour des activités critiques, la banque peut devoir considérer des plans d'urgence, y compris le recours à des parties alternatives externes, ainsi que les coûts et les ressources requises pour permuter les parties externes, et cela potentiellement sur un délai très court.

41. Parfois, les banques peuvent décider de maintenir un certain niveau de risque opérationnel ou de s'auto-assurer contre ce risque. Là où c'est effectivement le cas, et où le risque est avéré, la décision de maintenir le risque ou de s'auto-assurer devrait être transparente dans l'organisation, et devrait être conforme à la stratégie commerciale globale de la banque, et à l'objectif de risque.

Principe 7 : les banques devraient mettre en place des plans de secours et de continuité d'activités, afin de s'assurer de leur capacité à fonctionner de façon ininterrompue et à limiter les pertes en cas d'interruptions graves des activités.

42. Pour des raisons qui peuvent être au-delà du contrôle de la banque, un événement grave peut avoir comme conséquence l'incapacité de la banque à accomplir tout ou parties de ses engagements commerciaux, en particulier lorsque les infrastructures de télécommunications de la banque, ou les infrastructures de technologie de l'information ont été endommagées ou ont été rendues indisponibles. Ceci peut avoir comme conséquence des pertes financières significatives pour la banque, ainsi que de plus larges ruptures du système financier, notamment via les systèmes de paiements. Ce potentiel exige que les banques établissent des plans de continuité et de reprise d'activité sur incidents qui tiennent compte de différents types de scénarios plausibles auxquels la banque peut être vulnérable, et cela en proportion de la taille et de la complexité des opérations de la banque.

43. Les banques devraient identifier les processus critiques, y compris ceux où il y a de la dépendance à l'égard de fournisseurs externes ou d'autres tiers, et pour lesquels la reprise rapide du service serait la plus essentielle. Pour ces processus, les banques devraient identifier les mécanismes alternatifs pour reprendre le service en cas de panne. Une attention particulière devrait être accordée à la capacité de reconstituer les supports disques électroniques ou physiques des fichiers qui sont nécessaires pour la reprise des activités. Là où de tels fichiers sont sauvegardés sur un site distant, ou encore, lorsque des opérations de la banque doivent être relocalisées sur un nouveau site, une attention particulière devrait être accordée pour s'assurer que ces sites sont à une distance suffisante des opérations impactées pour permettre de réduire au minimum le risque sur les fichiers primaires et sur les fichiers de secours, ainsi que sur les équipements qui puissent être indisponibles simultanément.

44. Les banques devraient périodiquement passer en revue leurs plans de continuité des activités et de secours de sorte qu'ils soient conformes aux besoins des opérations courantes de la banque et aux stratégies commerciales. D'ailleurs, ces plans devraient être testés périodiquement pour s'assurer que la banque pourrait assurer la continuité des opérations, dans l'éventualité, peu probable, d'un sinistre majeur impactant les affaires.

7. GLOSSAIRE DE LA TERMINOLOGIE BÂLE 2

AMC (AMA)	Approches de Mesures Complexes. C'est une méthode de calcul des exigences de fonds propres en regard du Risque Opérationnel. Les deux autres approches sont l'approche indicateurs de base et l'approche standardisée.
Appréciation du risque (Risk Assessment)	Ensemble du processus d'analyse du risque et d'évaluation du risque (ISO guide 73[10]).
Attaque (Attack)	Exploitation d'une ou de plusieurs vulnérabilités à l'aide d'une méthode d'attaque avec une opportunité (probabilité de survenance de l'attaque) donnée.
Besoin de sécurité (Sensitivity)	Définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (DICP) qu'il convient d'assurer.
CAD	Capital Adequacy Directive. Directive Européenne transposant au niveau réglementaire les recommandations du comité de Bâle.
CP3	Troisième document soumis à consultation sur le Nouvel Accord (Bâle II).
Évaluation du risque (Risk Evaluation)	Processus de comparaison du risque avec des critères de risque donnés pour déterminer l'importance d'un risque (ISO guide 73).
GAA	Groupe pour l'Application de l'Accord. Créé par le Comité de Bâle afin de favoriser une application homogène de l'accord Bâle II dans les différents pays.
Gestion du risque (Risk Management)	Activités coordonnées visant à diriger un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque (ISO guide 73).
Menace (Threat)	Attaque possible d'un élément menaçant sur des biens. L'élément menaçant peut être caractérisé par son type (naturel, humain ou environnemental) et par sa cause (accidentelle, délibérée).
Piliers (Trois)	L'accord Bâle II se décompose en trois parties appelées aussi piliers : • Pilier 1 : Exigences minimales de fonds propres, • Pilier 2 : Surveillance prudentielle de l'adéquation des fonds propres, • Pilier 3 : Discipline de marché.
QIS3 Technical Guidance	The Quantitative Impact Study for Operational Risk n° 3 : étude lancée par le Comité de Bâle auprès des Banques pour calibrer l'impact de la méthode.
Ratio de Solvabilité	Voir Ratio Mc DONOUGH.
Ratio Mc DONOUGH	Ratio d'adéquation des fonds propres appelé aussi ratio de solvabilité (dettes/capitaux propres ou dettes/actif net car capitaux propres = actif net dans un bilan). Du nom de l'actuel directeur de la BIS.
Risque (risk)	Combinaison d'une menace et des pertes qu'elle peut engendrer.
Risque opérationnel (Operational risk)	Risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à des évènements extérieurs. La définition inclut le risque juridique, mais exclut les risques stratégiques et d'atteinte à la réputation.
Vulnérabilité (vulnerability)	Caractéristique qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.

[10] ISO/IEC Guide 73:2002 « risk management – Vocabulary – Guidelines for Use in Standards ».

8. BIBLIOGRAPHIE

Site Banque de France

http://www.banque-france.fr/fr/infobafi/cb/page2.htm

Sites généraux

http://www.bis.org (Site en anglais)

http://www.banque-france.fr

http://www.commission-bancaire.org

Documents particuliers :

International Convergence of Capital Measurement and Capital Standards: a Revised Framework
Basel Committee Publications No. 107 - June 2004
http://www.bis.org/publ/bcbs107.htm

Sound Practices for the Management and Supervision of Operational Risk
Basel Committee Publications No. 96 (Février 2003)
http://www.bis.org/publ/bcbs96.htm

An Overview of Sarbanes-Oxley for the Information Security Professional
http://www.sans.org/rr/papers/index.php?id=1426

IT Control Objectives for Sarbanes Oxley:
http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=14133&TEMPLATE=/ContentManagement/ContentDisplay.cfm

La méthode MEHARI™ V3
https://www.clusif.asso.fr/fr/production/mehari/