



Centre Africain d'Etudes Supérieures en Gestion

**CESAG BF – CCA
BANQUE, FINANCE, COMPTABILITE,
CONTROLE & AUDIT**

**Master Professionnel en Audit et
Contrôle de Gestion
(MPACG)**

**Promotion 6
(2011-2013)**

Mémoire de fin d'études

THEME

**CONTRIBUTION DE L'AUDIT INTERNE A LA
GESTION DES RISQUES OPERATIONNELS :
CAS DE LA BANK OF AFRICA MALI (BOA MALI)**

Présenté par :

BA Hamsatou Mohamed Lamine

Dirigé par :

BLE Koffi Léon Charles

Auditeur Principal à la BCEAO

Avril 2014

Dédicace

Je dédie ce mémoire à mon père Sidi El Moctar Oumar BA.

CESAG - BIBLIOTHEQUE

Remerciements

Le présent mémoire a été réalisé grâce à la participation effective et soutenue de diverses personnes. Il est de bon ton que nous leur présentons ici nos sincères sentiments de gratitude. Nous remercions :

- M. Igor DIARRA, Directeur Général de la Banque Of Africa pour nous avoir accordé le stage ;
- M. Moussa YAZI, Directeur de l'Institut Supérieur de Comptabilité de Banque et de Finance ;
- M. CHABI Bertin, Chef Département master à l'Institut Supérieur de Comptabilité, de Banque et de Finance ;
- M. Blé Koffi Léon Charles, notre Directeur de mémoire, pour les contributions et les conseils qui ont œuvré à la réalisation de ce travail ;
- M. Cheick Fantamady KANE, le contrôleur général de la Banque Of Africa, pour les contributions multiformes ;
- M. BAYO Souleymane, notre maître de stage, pour ses conseils et le suivi du mémoire
- les collègues de la 6^{ème} promotion de master particulièrement le Master en Audit et Contrôle de Gestion pour les meilleurs moments passés ensemble et les nombreux encouragements ;
- toute personne qui de loin ou de près, aurait contribué à la réalisation de ce travail.

Sigles et abréviations

AMF:	Autorité des Marchés Financiers
BCEAO :	Banque Centrale des Etats de l'Afrique de L'Ouest
BOA:	Banque of Africa
COSO:	Committee of Sponsoring Organizations of the Treadway Commission
DAC :	Direction Administrative et Comptable
DCG :	Département Contrôle de Gestion
DECD :	Direction de l'Exploitation Commerciale et de Développement
DER :	Direction des Engagements et des Risques
DG :	Direction Générale
DGPR :	Département de la Gestion Préventive des Risques
DI :	Département des Institutionnels
DO :	Direction des Opérations
DSIM :	Département des Systèmes et Monétiques
FRAP :	Feuille de Révélation et d'Analyse des Problèmes
IFACI :	Institut Français des Auditeurs et Contrôleurs Internes
IIA :	Institute of Internal Auditors
L'UEMOA :	Union Economique et Monétaire Ouest Africain
PME :	Petites et Moyennes Entreprises
QCI :	Questionnaire de Contrôle Interne
TFfA :	Tableau des Forces et Faiblesses Apparentes

Liste des tableaux et figures

❖ Tableaux

Tableau 1 : Typologie des risques opérationnels.....	14
Tableau 2 : Les lignes métiers occasionnant les risques opérationnels.....	16
Tableau 3 : Echelle d'évaluation des risques.....	67
Tableau 4 : Probabilité d'occurrence.....	67

❖ Figures

Figure 1 : Rôle de l'audit interne dans le management des risques	37
Figure 2 : Modèle d'analyse	40

Liste des annexes

Annexe 1 : Organigramme de la BOA-Mali 2012	81
Annexe 2 : Test d'existence du contrôle interne	82
Annexe 3 : Test d'application du contrôle interne	84

CESAG - BIBLIOTHEQUE

Table des matières

Dédicace	i
Remerciements	ii
Sigles et abréviations	iii
Liste des tableaux et figures	iv
Liste des annexes	v
Table des matières	vi
INTRODUCTION GENERALE	1
PREMIERE PARTIE : CADRE THEORIQUE DE L'ETUDE.....	7
Chapitre 1 : GESTION DES RISQUES OPERATIONNELS BANCAIRES.....	9
1.1. Les risques bancaires	9
1.1.1. Concept de risque	9
1.1.2. Caractéristiques des risques.....	10
1.1.3. Typologie des risques majeurs bancaires	10
1.1.3.1. Les risques de crédits	11
1.1.3.2. Les risques de marché	11
1.1.3.3. Les risques opérationnels	11
1.1.3.4. Autres risques bancaires.....	12
1.2. Les spécificités du risque opérationnel bancaire	12
1.2.1. Le risque opérationnel et Bâle II	13
1.2.2. Composantes du risque opérationnel	13
1.2.2.1. Les dimensions du risque opérationnel bancaire.....	15
1.3. La gestion des risques opérationnels	15
1.3.1. Les métiers de la banque générant les risques opérationnels	15
1.3.2. Le processus de gestion des risques opérationnels.....	17
1.3.3. Différentes étapes de la gestion des risques opérationnels.....	18
1.3.3.1. Identification des risques opérationnels	18
1.3.3.1.1. La définition du périmètre à analyser	18
1.3.3.1.2. Les évènements à risque	18
1.3.3.1.3. Les outils d'identification du risque opérationnel	19
1.3.3.2. Analyse et évaluation des risques opérationnels	22
1.3.3.3. Le suivi des risques opérationnels.....	22
1.3.3.4. Dispositif de maîtrise des risques opérationnels	22

Chapitre 2 : L'AUDIT INTERNE ET LA GESTION DES RISQUES OPERATIONNELS	24
2.1. Définition du management des risques.....	24
2.1.1. Avantages du management des risques	25
2.1.2. Les activités du management des risques	25
2.1.3. Responsabilité du management des risques.....	26
2.2. Rôle de l'audit interne dans le management des risques	27
2.2.1. Principaux rôles de l'audit interne dans le processus de management des risques	28
2.2.2. Le rôle de l'audit interne dans le management des risques selon les normes	28
2.2.2.1. Les modalités pratiques relatives à la norme 2120	29
2.2.3. Rôle que l'audit interne ne doit pas jouer dans le processus de management des risques	34
2.2.4. L'audit interne et la gestion des risques opérationnels.....	35
Chapitre 3 : METHODOLOGIE DE L'ETUDE	38
3.1. Modèle d'analyse.....	38
3.2. Outils de collecte de données	41
3.2.1. La revue documentaire	41
3.2.2. Les entretiens	41
3.2.3. Observation.....	41
3.2.4. Le questionnaire de contrôle interne	41
3.2.5. Tableau d'identification des risques	42
3.2.5.1. Le Tableau des Forces et faiblesses Apparentes (TFfA).....	42
3.2.5.2. La grille de séparation des tâches.....	42
3.2.6. Les tests de conformité et de permanence	42
DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE.....	45
Chapitre 4 : PRESENTATION DE LA BOA-MALI.....	47
4.1. Historique de la BOA-Mali	47
4.2. Actionnariat de BOA-Mali	48
4.3. Missions et objectifs	48
4.4. Les produits de BOA-Mali	49
4.5. Organisation et fonctionnement.....	49
4.5.1. Le Conseil d'Administration	50
4.5.2. La Direction Générale	50

4.5.3.	Le contrôle Général	50
4.5.4.	Direction de l'Exploitation Commerciale et de Développement (DECD)	51
4.5.4.1.	Centre d'affaires	51
4.5.4.2.	Département du Réseau d'Agence des PME.....	51
4.5.4.3.	Département des Institutionnels (DI)	51
4.5.5.	Direction Administrative et Comptable (DAC)	51
4.5.5.1.	Département de la comptabilité.....	52
4.5.5.2.	Département Contrôle de Gestion (DCG).....	52
4.5.6.	Département des systèmes et monétiques (DSIM).....	52
4.5.6.1.	Département Informatique	52
4.5.6.2.	Département Monétique	53
4.5.7.	Direction des opérations (DO).....	53
4.5.8.	Direction des Engagements et des Risques (DER).....	53
4.5.8.1.	Secrétariat des engagements.....	53
4.5.9.	Le Département de la gestion préventive des risques (DGPR)	54
4.6.	Département juridique	55
Chapitre 5 : LA GESTION DES RISQUES OPERATIONNELS : cas de la BOA- MALI		
5.1.	Les acteurs du contrôle interne et leurs missions	56
5.1.1.	Le conseil d'administration	56
5.1.2.	La direction générale	57
5.1.3.	Le contrôle général	57
5.1.4.	Le département compliance (conformité).....	59
5.1.4.1.	Le contrôle de gestion	59
5.1.4.2.	La cellule de rapprochement des comptes nostri et de suivi du résultat de change	59
5.1.4.3.	La cellule de rapprochement des comptes de liaison siège /Agences	59
5.1.4.4.	La cellule de suivi de la trésorerie.....	59
5.1.5.	Le comité d'audit et des risques	59
5.1.6.	La direction de l'inspection du groupe	60
5.2.	Les niveaux de contrôles	61
5.2.1.	Les agents opérationnels.....	61
5.2.2.	Les responsables hiérarchiques	61
5.2.3.	Le contrôle général	61
5.2.4.	La direction générale	61

5.2.5.	Le conseil d'administration	61
5.2.6.	La direction des inspections	62
5.3.	La gestion des risques opérationnels et l'audit interne.....	62
5.3.1.	La fraude interne.....	62
5.3.2.	La fraude externe	62
5.3.3.	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	63
5.3.4.	Clients, produits et pratiques Commerciales (de pertes résultant d'une mauvaise prestation envers un client).....	64
5.3.5.	Dommmages aux actifs corporels.....	64
5.3.6.	Dysfonctionnement de l'activité et des systèmes	65
5.3.7.	Exécution, livraison et gestion des processus.....	65
5.4.	Les dispositions de Bâle II sur les risques opérationnels	65
5.5.	L'appréciation du dispositif de contrôle interne.....	65
Chapitre 6 : ANALYSE DE LA CONTRIBUTION DE L'AUDIT INTERNE A LA GESTION DES RISQUES OPERATIONNELS		70
6.1.	Le dispositif de gestion des risques opérationnels.....	71
6.1.1.	L'analyse du dispositif de gestion des risques opérationnels	71
6.2.	Le rôle de l'audit interne dans le dispositif de gestion des risques opérationnels.....	72
6.2.1.	Identification des risques opérationnels	73
6.2.2.	L'évaluation des risques	73
6.2.3.	Construction de la cartographie des risques	73
6.2.4.	Suivi de l'évolution des risques et des plans d'actions	74
6.2.5.	La démarche d'auto évaluation des risques et des contrôles	74
6.2.6.	Promotion d'une culture éthique au sein de l'organisation	74
6.3.	Recommandations	75
6.3.1.	A l'endroit du département d'audit interne	75
6.3.2.	A l'endroit de la direction générale	75
CONCLUSION GENERALE		77
ANNEXES		80
BIBLIOGRAPHIE		86

CESAG - BIBLIOTHEQUE

INTRODUCTION GENERALE

Les mutations économiques entraînent de nouvelles opportunités tout en accroissant les incertitudes auxquelles sont confrontées les entreprises. De ce fait, elles rendent impérieuse la nécessité de méthodologies efficaces afin de mieux appréhender l'univers risqué auquel doivent faire face les organisations. L'une des missions principales imparties à la direction générale et au conseil d'administration des organisations est de veiller à ce qu'elle se dote de dispositifs de contrôle interne et de gestion des risques solides que possible et adaptés à l'activité. L'importance de l'enjeu, souligné par les déficiences, parfois les défaillances graves à l'origine des récentes crises financières mondiales est illustrées par le fait que la gestion des risque est de tous les sujets de management, celui sur lequel on a le plus légiféré, élaboré des référentiels et des outils, formé des praticiens, enseigné des bonnes pratiques. Il suffit pour s'en convaincre de se référer aux accords de Bale, aux centaines d'articles de la loi Sarbanes-Oxley, aux référentiels professionnels relatifs au contrôle interne, aux directives européennes etc.

Le contexte économique actuel exige plus que jamais aux banques de disposer d'un système de gestion des risques efficace et élaborée afin de préserver leur solidité financière, de continuer de croître et d'apporter la confiance au marché. Selon SARDI (2002 : 39) « le métier de banquier est le métier du risque. Les risques sont inhérents à l'activité bancaire. L'absence ou l'insuffisance de leur maîtrise provoque inévitablement des pertes qui affectent la rentabilité et les fonds propres. La persistance et la profondeur de ces pertes peuvent conduire à la défaillance, c'est-à-dire l'incapacité de faire face à ses engagements ». Abordant dans le même sens, GREUNING & al (2004 : 3) affirment que : « les banques au cours de leurs activités, sont exposées à une série de risques, qui se classent en général en quatre catégories : risques financiers, risques d'exploitation, risques accidentels et risques opérationnels ».

La gestion des risques opérationnels dans les banques a fortement évolué au cours des dernières années. Elle couvre tous les points susceptibles de poser problème dans une banque. Elle permet de mettre en place des mesures destinées à limiter les risques aux différentes opérations bancaires et à prévoir les fonds propres nécessaires pour faire face aux pertes potentielles. Les acteurs ayant une responsabilité en la matière se sont multipliés. Au nombre de ceux-ci figurent la fonction d'audit interne. En effet la fonction d'audit interne a pour but d'évaluer le niveau de contrôle interne c'est-à-dire la capacité des organisations à atteindre efficacement les objectifs qui leur sont assignés et à maîtriser les

risques inhérents à leur activité. En témoigne la définition de l'audit interne par l'IIA (1999) : « l'audit interne est une activité indépendante et objective qui donne à une organisation une assurance raisonnable sur le degré de maîtrise des opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systémique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité ». La fonction d'audit interne a donc une part importante dans la gestion des risques. A cette fin, il fournit à tous les niveaux de responsabilité de la banque, des assurances, des analyses, des plans d'actions approuvés ou des recommandations, des conseils et des informations concernant les activités qu'il a vérifiées. C'est pourquoi DUMONT (2007: 34) affirme que : « la valeur ajoutée d'une entité d'audit consiste à réussir à réduire les risques auxquels est exposée l'entreprise et à améliorer l'efficacité de son fonctionnement d'une part et d'autre part à faire évoluer la culture des audités à favoriser leur appropriation de la dimension contrôle interne ».

La Bank Of Africa Mali, filiale du groupe BOA a été créée le 20 décembre 1982 et ouverte au public le 19 décembre 1983. Elle effectue toutes les opérations autorisées aux banques en république du Mali notamment les opérations financières, commerciales, mobilières et immobilières. Son objectif est d'être leader sur le marché tout en augmentant le taux de bancarisation au Mali. Ces objectifs ne peuvent être atteints efficacement que grâce à un certain nombre de mesures de sécurité qui y règnent. Il s'avère alors impérieux de mettre en place les moyens nécessaires pour un contrôle des activités. Pour y parvenir la banque dispose dans son organisation d'une direction de contrôle général qui joue le rôle d'audit interne. Le problème qui se pose concerne l'efficacité du dispositif mis en place par cette direction dans la maîtrise des risques opérationnels liés aux activités de la banque. En d'autres termes comment ladite direction fait face aux risques opérationnels notamment :

- de fraudes internes ;
- de fraudes externes ;
- de pratiques en matière d'emploi et sécurité sur le lieu de travail ;
- de pertes résultant d'une mauvaise prestation envers un client ;
- de dommages liés aux actifs corporels,

- de dysfonctionnements de l'activité et des systèmes,
- d'exécution des livraisons et la gestion des processus.

De l'analyse du problème ci-dessus posé, il ressort les causes ci-après :

- insuffisances des procédures internes ;
- erreur humaine ;
- défaillances du système informatique mis en place ;
- insuffisance de contrôle et/ou complicité interne.

Les causes énumérées peuvent avoir comme conséquences :

- la falsification des documents par un employé ;
- la perte financière et de piratage dus au piratage informatique ;
- la violation des règles de santé et de sécurité des employés ;
- l'utilisation frauduleuse d'informations confidentielles sur la clientèle

Face à cette analyse du problème, nous pouvons proposer les solutions suivantes:

- sensibiliser l'ensemble du personnel sur les risques opérationnels ;
- évaluer et mettre à jour la cartographie des risques opérationnels ;
- analyser la contribution de l'audit interne dans la gestion des risques opérationnels.

Parmi les solutions, nous allons retenir dans le cadre de notre étude, celle relative à l'analyse de la contribution de l'audit interne dans la gestion risques opérationnels. Cette solution nous semble la plus importante car elle intègre les deux premières. Elle nous permettra de comprendre le processus de gestion des risques opérationnels à la BOA Mali et d'évaluer l'implication de l'audit interne dans la gestion de ces risques.

La principale question qui se pose est alors la suivante : quelle est la contribution de l'audit interne dans la gestion des risques opérationnels à la BOA Mali ?

De cette question principale, découlent les questions spécifiques ci-après :

- quelle est la typologie des risques opérationnels ?
- comment gérer les risques opérationnels ?
- quelle est le rôle de l'audit interne dans la gestion des risques opérationnels ?

Nous essayerons de répondre à ces différentes questions à travers l'étude du thème libellé comme suit : « **Contribution de l'audit interne à la gestion des risques opérationnels : cas de la BOA Mali** ».

Dans le but de mener à bien cette étude, il urge de se fixer quelques objectifs. Ces objectifs se déclinent en objectif général et en objectifs spécifiques.

L'objectif général de ce travail consiste à analyser la contribution de l'audit interne dans la gestion des risques opérationnels à la BOA Mali et d'apporter des recommandations pour une meilleure implication. Pour y arriver il faudra :

- mieux comprendre les risques opérationnels tels que définis par Bale 2 ;
- identifier les lignes métiers générant les risques opérationnels définis par le comité Bale ;
- présenter les saines pratiques de gestion des risques opérationnels édictées par le comité de Bale ;
- décrire le processus de gestion des risques opérationnels à la BOA Mali ;
- Apprécier la contribution de l'audit interne dans la gestion de ces risques.

Le sujet de notre étude revêt deux intérêts :

- cette étude permettra à la banque de mieux cerner ses risques opérationnels, de disposer d'une revue des bonnes pratiques en termes de gestion des risques opérationnels. Aussi de connaître les dispositifs adéquats pour les réduire et d'autre part d'assurer l'efficacité de leur gestion. En outre, elle permettra d'éveiller la conscience des autorités de la banque sur la maîtrise des risques opérationnels liés à leur activité et sur la contribution de l'audit interne à ce sujet.
- Pour nous, cette étude sera l'occasion d'appliquer sur le terrain les enseignements théoriques reçus au cours de notre formation. Aussi, elle nous permettra d'approfondir nos connaissances de façon spécifique sur la gestion des risques opérationnels par l'audit interne.

Le mémoire s'articule autour de deux (2) parties à savoir :

- la première partie consacrée au cadre théorique se compose de trois (3) chapitres. Elle abordera successivement la gestion des risques opérationnels bancaires, le rôle

de l'audit interne dans la gestion des risques opérationnels. Nous clôturons cette partie par la méthodologie de recherche de l'étude.

La deuxième partie appelée partie pratique comprend également trois (3) chapitres. Il s'agira de faire dans un premier temps une brève description de la structure d'accueil du stage (BOA MALI). Par la suite nous présenterons la gestion des risques opérationnels à la BOA Mali. Enfin nous procéderons à l'analyse de la contribution de l'audit interne dans la gestion de ces risques.

CESAG - BIBLIOTHEQUE

PREMIERE PARTIE :
CADRE THEORIQUE DE L'ETUDE

Les risques opérationnels sont considérés comme nouveaux. Pourtant, bien qu'isolés récemment des autres risques par les réglementations des banques et assurances, ils ont souvent fait la une de la presse, la faillite de la Barings en témoigne. Ainsi, derrière chaque événement ayant ébranlé fortement des entreprises, se cachent des risques opérationnels. C'est d'ailleurs surtout lorsqu'ils sont associés à d'autres types de risques qu'ils sont susceptibles de prendre une ampleur significative.

C'est pour ces raisons que l'on cherche, depuis une dizaine d'années, à mieux les appréhender et à évaluer plus finement leurs impacts. En effet, l'environnement nouveau des entreprises accentue fortement leur exposition aux risques opérationnels. Nous avons notamment : une concentration des acteurs qui amène à des volumétries et montants en jeu plus importants, une internationalisation des activités avec une multiplication des interconnexions, une sophistication des techniques financières, une sensibilité plus grande aux systèmes d'informations, une inventivité des fraudes ou encore une judiciarisation progressive qui conduit de plus en plus les acteurs à être assignés en responsabilité.

L'audit interne apparaît donc comme l'un des moyens nécessaires dans la maîtrise de ces risques à travers son rôle crucial dans le management des risques.

Dans cette première partie nous ferons le point sur la revue de littérature du sujet traité. Nous aborderons successivement la gestion des risques opérationnels bancaires, la gestion des risques opérationnels par l'audit interne de la banque et enfin la méthodologie de l'étude viendra clore la partie.

Chapitre 1 : GESTION DES RISQUES OPERATIONNELS BANCAIRES

Le risque est inhérent à l'entreprise. Il constitue, selon les économistes, son essence. Créer une entreprise, c'est déjà prendre un risque. Sa survie n'est jamais assurée. Même les entreprises de grande taille n'ont aucune garantie de pérennité. Enron, Arthur-Andersen, Alstom et Parmalat sont des exemples de multinationales qui ont disparu ou qui ont dû lutter pour leur survie. Si l'activité entrepreneuriale est à la base une activité risquée, d'autres risques sont venus se greffer avec l'avènement des nouvelles technologies et de la diversification des produits bancaires.

1.1. Les risques bancaires

Les banques sont des établissements de crédit qui collectent des dépôts d'argent puis les utilisent sous forme d'investissement ou de crédits accordés aux entreprises et aux ménages. Elles jouent ainsi le rôle d'intermédiaires financiers. De façon formelle, l'article 2 de la nouvelle loi bancaire de l'UEMOA précise que : « sont considérées comme établissements de crédits, les personnes morales qui effectuent, à titre de profession habituelle, les opérations de banque. Constituent des opérations de banque, au sens de la présente loi, la réception de fonds du public, les opérations de crédits, ainsi que la mise à disposition de la clientèle et la gestion des moyens de paiements. Les établissements de crédit sont agréés en qualité de banque ou d'établissement financier à caractère bancaire ». Si l'on reconnaît que le risque est inhérent à l'activité de l'entreprise, il l'est en plus pour les activités bancaires. C'est pourquoi, MONNIER & al (2013 : 7), affirment que : « de par sa nature, l'activité bancaire est une activité où le risque est permanent. Les banques doivent en effet faire face aux risques de crédit (risque d'immobilisation, de non remboursement et de taux), aux risques de marché et aux risques opérationnels ». De ce fait, l'absence ou l'insuffisance de leur maîtrise provoque inévitablement des pertes qui affectent la rentabilité de la banque et les fonds propres. Il urge donc d'identifier ces risques afin de mettre en place un dispositif capable de les prévenir ou de limiter leurs conséquences en cas de survenance.

1.1.1. Concept de risque

IFACI (2007 : 12), définit le risque comme : « la possibilité que se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs. Il se mesure en termes de

conséquences et de probabilité ». Abordant dans le même sens BARTHELEMY & al (2004 : 11) affirment que « le risque est la prise en compte d'une exposition à un danger, un préjudice ou autre évènement dommageable, inhérent à une situation ou une activité. Il est défini par la probabilité ou la fréquence de survenance de cet évènement et par l'ampleur ou la gravité de ses conséquences ».

Sur la base de ces définitions, nous pouvons affirmer que le risque est un évènement dont l'arrivée aléatoire, est susceptible de causer un dommage sur les activités de l'entreprise. Pour y faire face les dirigeants doivent mettre en place et parfaire les dispositifs nécessaires pour les maîtriser.

1.1.2. Caractéristiques des risques

La définition du risque de SCHICK & al (2010 : 10-11) selon laquelle : « le risque est un concept signifiant la possibilité que la combinaison d'un évènement incertain et d'un mode de fonctionnement aléatoire ait pour conséquence la non atteinte d'un objectif » permet de caractériser le risque. Ainsi le risque est caractérisé par :

- l'évènement incertain : il s'agit de la circonstance, l'incident avéré ou potentiel que l'entreprise doit pouvoir détecter, voire anticiper, pour y faire face. Cette caractéristique du risque est liée à deux dimensions que sont le temps et l'environnement ;
- le facteur de risque : c'est la cause de l'évènement qui, combinée à la survenance de l'évènement (ou des évènements) va ou ne va pas entraîner des conséquences dommageables ;
- l'impact dommageable : encore appelé l'objectif compromis, c'est ce que l'on court si l'évènement se réalise autrement dit la conséquence.

Notons cependant que le risque pour être caractérisé, doit être mesurable à travers sa criticité qui n'est rien d'autre que le produit de deux grandeurs : la probabilité d'occurrence ou la fréquence et les effets, ou l'impact (BARTHELEMY & al, 2004 : 11).

1.1.3. Typologie des risques majeurs bancaires

L'activité bancaire est caractérisée par une multiplicité de risques. Ces risques sont généralement regroupés en trois grandes catégories à savoir :

- les risques de crédits ;
- les risques de marché ;
- les risques opérationnels.

1.1.3.1. Les risques de crédits

Le risque de crédit se définit comme étant la probabilité qu'un débiteur soit dans l'incapacité de faire face au remboursement du crédit octroyé par une institution financière. Le risque de crédit est bien évidemment fonction de la qualité de l'emprunteur. Encore appelé risque de contrepartie, le risque de crédit est lié à l'activité d'intermédiation traditionnelle des banques (COUSSERGUES, 2007 : 108). Il est composé du :

- risque de garantie : la banque peut devoir supporter une perte si elle ne peut exercer la garantie attachée à un prêt en défaut ou si un produit de cette action s'avère insuffisant pour couvrir les engagements du débiteur;
- risque de concentration : il s'agit des pertes importantes dues à une diversification insuffisante du portefeuille de concours en termes de secteurs économiques, de régions géographiques ou de taille de l'emprunteur;
- risque pays : il se manifeste lorsqu'un pays étranger ne dispose plus de réserves suffisantes pour faire face aux engagements en monnaies étrangères de ses ressortissants.

1.1.3.2. Les risques de marché

Selon COUSSERGUES (2007 :110), « les risques de marchés sont issus d'une évolution défavorable du prix d'un actif en général négocié sur un marché et qui n'a pas comme origine la détérioration de la solvabilité de l'émetteur de l'actif ».

SARDI (2002 :40) définit les risques de marché comme « des pertes potentielles résultant de la variation du prix des instruments financiers détenus dans le portefeuille de négociation ou dans le cadre d'une activité de marché dite aussi trading ou négoce ».

1.1.3.3. Les risques opérationnels

Il existe bon nombre de définitions du risque opérationnel aussi divergentes les unes des autres ; cependant nous ne retiendrons dans le cadre de notre étude que celle du comité de

Bâle selon lequel : « le risque opérationnel peut être défini comme un risque direct ou indirect de perte résultant du processus interne, de personnes et de systèmes défaillants ou inadéquats, ou d'évènement externe. Typiquement, il s'agit des risques informatiques (incidents d'exploitations, pertes ou altération de données) ; des risques relatifs à la sécurité des biens et des personnes (sabotage, vol, incendie, fraude interne ou externe), des pratiques sociales (discrimination) et des risques de gestion internes (par exemple un défaut de conception d'un produit entraînant son retrait du marché, une manœuvre frauduleuse) ».

1.1.3.4. Autres risques bancaires

Ces risques sont les conséquences des premiers présentés. Il s'agit de :

- risque de réputation : selon SARDI (2002 : 44), le risque de réputation est l'atteinte à la confiance qu'une banque doit inspirer à sa clientèle et au marché à la suite d'une publicité sur des faits vrais ou supposés. A degrés élevés, il peut conduire au risque systémique ;
- risque systémique : les établissements de crédit sont interdépendants les uns par rapport aux autres. C'est pourquoi SARDI (2002 : 44) affirme que le risque systémique est le risque de défaillance de tout le système bancaire ;
- risque de liquidité : il est défini comme le risque de ne pas pouvoir faire face à ses engagements, du fait de l'impossibilité de se procurer des fonds (SARDI, 2002 : 43).

1.2. Les spécificités du risque opérationnel bancaire

Les risques opérationnels sont considérés comme nouveaux. Pourtant, bien qu'isolé récemment des autres risques par les réglementations des banques, ils ont souvent la une des presse. La faillite de la Barings en témoigne. Ainsi, derrière chaque événement ayant ébranlé fortement des institutions financières se cachent des risques opérationnels. Cet essor des risques opérationnels est notamment lié à la banalisation de la gestion en temps réel des opérations dans un contexte de globalisation et d'internationalisation des activités. Il est par ailleurs, le résultat de la sophistication de ces activités tant dans la conception de nouveaux produits. On y associe également des risques juridiques dans la mise en place de systèmes d'information de plus en plus complexe. C'est pour ces raisons que

l'on cherche depuis une dizaine d'années, à mieux les appréhender et à évaluer plus finement leurs impacts.

1.2.1. Le risque opérationnel et Bâle II

Le comité de Bâle pour la supervision bancaire (2001) définit le risque opérationnel comme « le risque de pertes résultant d'une inadéquation ou d'une défaillance imputable à des procédures, personnels et systèmes internes, ou à des événements extérieurs y compris les événements de faible probabilité d'occurrence mais à risque de pertes élevées ». Cette définition prend en compte les risques juridiques mais exclut les risques de réputation (risques de pertes résultant d'une activité, d'une atteinte à la réputation de l'institution bancaire) et les risques stratégiques (risques de perte résultant d'une mauvaise décision stratégique). La perte constatée permet de remonter à l'événement qui lui-même permet de remonter à une ou plusieurs causes (inadéquation des procédures, événements extérieurs, défaillance humaine, problèmes liés à la gestion du personnel...). Abordant dans le même sens, CAMARA (2006 : 130) affirme que : « le risque opérationnel est la probabilité de pertes subséquentes à une défaillance des procédures administratives, machines et outils de travail ».

Nous pouvons donc dire que le risque opérationnel est le risque de perte provenant de processus internes inadéquats ou défaillants (système d'information déficient, erreurs humaines, fraudes et malveillances), ou événements externes (accidents, incendies, inondations) perturbant la réalisation des objectifs de l'établissement (création de valeur). Ils comprennent, de ce fait, tous les risques de nature à compromettre le bon fonctionnement de l'entreprise, à remettre en cause l'atteinte de ses objectifs ou à entraîner des dommages susceptibles de porter atteinte à sa rentabilité ou à son image.

1.2.2. Composantes du risque opérationnel

Le risque opérationnel est composé de sept (07) catégories d'événements selon le comité de Bale. Ces différents évènements sont présentés dans le tableau ci après :

Tableau 1 : Typologie des risques opérationnels

Catégories d'évènements	Définitions	Sous catégories
Fraude interne	Pertes dues à des actes visant à frauder, détourner des biens ou à tourner des règlements, la législation ou la politique de l'entreprise (à l'exception des atteintes à l'égalité et des actes de discrimination) impliquant au moins une partie interne à l'entreprise.	<ul style="list-style-type: none"> - Activité non autorisée - Vol et Fraude
Fraude externe	Pertes dues à des actes visant à frauder, détourner des biens ou contourner la législation de la part d'un tiers.	Sécurité des systèmes
Pratiques en matière d'emploi et sécurité sur le lieu de travail	Pertes résultant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, de demandes d'indemnisation au titre d'un dommage personnel ou d'atteintes à l'égalité/actes de discrimination.	Relations de travail ; <ul style="list-style-type: none"> - Sécurité du lieu de travail ; - Egalité et discrimination.
Clients, produits et pratiques commerciales	Pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients spécifiques (y compris exigences en matière de fiducie et de conformité) ou de la nature conception d'un produit.	<ul style="list-style-type: none"> - Conformité, diffusion d'informations et devoir fiduciaire ; - Pratiques commerciales/de place incorrectes ; - Défaut de production - Sélection, parrainage et exposition ; - Services conseil.
Dommages aux actifs corporels	Destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres.	Catastrophes et autres sinistres.
Dysfonctionnement de l'activité et des systèmes	Pertes résultant de dysfonctionnements ou de l'activité ou des Systèmes.	Systèmes.
Exécution, livraison et gestion des processus	Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs.	Saisie, exécution et suivi des transactions <ul style="list-style-type: none"> - Surveillance et notification financière ; - Admission et documentation clientèle ; - Gestion des comptes clients ; - Contreparties commerciales ; - Fournisseurs.

Source : JIMENEZ & al (2008 :69-72)

1.2.2.1. Les dimensions du risque opérationnel bancaire

A l'instar de toutes les différentes catégories de risque, le risque opérationnel bancaire est mesuré par sa criticité : probabilité x impact.

- la probabilité du risque désigne ses possibilités de réalisation du risque. Selon DE MARESCHAL (2003 : 9), l'échelle de mesure de la probabilité peut être quantitative (valeur de 0 à 1) ou qualitative (probabilité importante à probabilité faible).
- L'impact désigne la réalisation effective de l'éventualité.

1.3. La gestion des risques opérationnels

La gestion du risque opérationnel se situe à un tournant de son évolution. De nombreuses approches ont été développées à travers différentes branches d'activités, mais beaucoup d'institutions s'efforcent de les rendre pleinement efficaces en les intégrant réellement dans la gestion quotidienne de leur activité. Pour ce faire gérer un risque c'est l'identifier, l'analyser, l'évaluer et enfin l'hierarchiser et mettre en place des mesures adéquates afin de réduire son impact ou même l'accepter.

1.3.1. Les métiers de la banque générant les risques opérationnels

Les risques opérationnels se retrouvent dans les activités bancaires. Ces différentes activités connues sous le nom de « ligne métier ou business line » dans le domaine bancaire correspondent aux principales sources de valeur ajoutée. Il s'agit en général des offres de la banque. Le comité de Bale a défini les lignes métiers qui peuvent générer les risques opérationnels. Ainsi, huit (8) lignes métiers et sept (7) catégories d'évènement peuvent occasionner les risques opérationnels.

Tableau 2 : Les lignes métiers occasionnant les risques opérationnels

Niveau 1	Groupe d'activité
Financement des entreprises	<ul style="list-style-type: none"> • Prise ferme d'instruments financiers et/ou placement d'instruments financiers avec engagement ferme ; • Service liés à la prise ferme ; • Conseil et services financiers aux entreprises ; • Conseil aux entreprises en matière de structure du capital, de stratégie industrielle et toute autre activité de conseil ; • Recherche en investissement et analyse financière ou toute forme de recommandation générale concernant les transactions sur instruments financiers.
Négociation et vente institutionnelle	<ul style="list-style-type: none"> • Négociation pour compte propre ; • Intermédiation sur les marchés interbancaires ; • Réception et transmission d'ordres portant sur un ou plusieurs instruments financiers ; • Exécution d'ordre au nom de clients ; • Placement d'instruments financiers sans engagements ferme.
Banque de détail	<ul style="list-style-type: none"> • Réception de dépôts ou d'autres fonds remboursables ; • Prêts ; • Contrats de location-financement et contrats de location à caractère financiers ; • Octroi de garantie et souscription d'engagement.
Banque commerciale	<ul style="list-style-type: none"> • Réception de dépôts ou autres fonds remboursables ; • Prêts ; • Contrats de location-financement et contrats de location à caractère financiers ; • Octroi de garantie et souscription d'engagement
Paiement et règlements	<ul style="list-style-type: none"> • Opérations de paiement ; • Emission et gestion de moyen de paiement ; • Compensation et règlement-livraison d'instruments financiers.
Service d'agences	<p>Garde et administration d'instruments financiers pour le compte de clients y compris la conservation et des services connexes comme la gestion de trésorerie/de garanties.</p>
Gestion d'actifs	<ul style="list-style-type: none"> • Gestion de portefeuille ; • Gestion d'OPCVM ; • Autres formes de gestion d'actifs.
Courtage de détail	<ul style="list-style-type: none"> • Réception et transmission d'ordres portant sur un ou plusieurs instruments financiers ; • Exécution d'ordres au nom de clients ; • Placements d'instruments financiers sans engagement ferme.

Source : arrêté de la république française du 20 février 2007 relatif au calcul de l'exigence de fonds propres applicables aux établissements de crédit.

L'identification des risques opérationnels générés par leurs activités demeure une étape fondamentale pour que les établissements de crédits puissent assurer les moyens adéquats pour leur quantification et leur gestion. Cette démarche d'identification et de gestion autonome est apparue ces dernières années comme une discipline séparée vue l'importance et l'impact de ces risques sur les banques quand ils interviennent.

1.3.2. Le processus de gestion des risques opérationnels

Avant de décrire le processus proprement dit de gestion des risques opérationnels, nous allons présenter les saines pratiques de gestion des risques opérationnels édictées par le comité de Bâle. Au nombre de dix (10) ces principes peuvent être regroupés en quatre (4) grandes catégories. Selon CLUSIF (2004 :5-6), il s'agit de :

- **Elaboration d'un environnement adéquat pour la gestion du risque :** le conseil d'administration devrait considérer les principaux aspects du risque opérationnel de la banque comme une catégorie distincte de risque à gérer, et devrait approuver et réexaminer périodiquement le dispositif de gestion de ce risque. Quant à la direction générale, elle a pour mission de mettre en œuvre le dispositif de gestion du risque opérationnel approuvée par le conseil d'administration. Ce dispositif devrait être appliqué de façon cohérente dans l'ensemble de l'organisation et les membres du personnel à tous les niveaux devraient bien comprendre leurs responsabilités dans la gestion de ce risque.
- **Gestion du risque ; identification, évaluation, suivi et maîtrise/atténuation du risque :** les banques doivent identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles doivent mettre en œuvre un processus de suivi régulier des profits de risques opérationnels et des expositions importants de ces risques. Elles doivent également réexaminer périodiquement leurs stratégies et limitation et de maîtrise du risque et en ajuster le profil de ce dernier et mettre en place des plans de secours et de continuité d'exploitation. Ces dispositions garantiront un fonctionnement sans interruption, limitant ainsi les pertes en cas de perturbation grave de l'activité ;
- **Rôle des superviseurs :** 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, dans le cadre d'une approche globale de la gestion ;

- **Rôle de la communication financière** : la communication financière des banques doit être suffisamment étoffée pour permettre à la direction d'évaluer leur méthodologie de gestion du risque opérationnel. BALE II (2003 :5)

1.3.3. Différentes étapes de la gestion des risques opérationnels

Les différentes étapes de la gestion du risque opérationnel telles que présentées par le comité de Bâle sont les suivantes : identification, évaluation, suivi et maîtrise/atténuation des risques opérationnels.

1.3.3.1. Identification des risques opérationnels

L'identification des risques permet de recenser les événements aussi bien internes qu'externes capables d'empêcher la réalisation des objectifs fixés par la banque. Selon le comité de Bâle : « l'identification des risques est primordiale pour que puissent être développés un contrôle et un suivi des risques et permettre l'établissement d'une typologie de risque opérationnels ». C'est pourquoi, MASSELIN & al (2014 :46), affirment : « l'étape d'identification des risques est à la fois assez simple et à incidences multiples. Il convient donc d'y apporter une attention plus soutenue que celle que l'on peut penser y accorder à première vue ».

1.3.3.1.1. La définition du périmètre à analyser

D'après JIMENEZ & al (2008 : 55), le périmètre à analyser comprend l'ensemble des activités de l'établissement. Cela nécessite toutefois de comprendre et de modéliser les activités pour permettre une identification de l'ensemble des risques opérationnels associés. Celle-ci consiste à découper les activités de l'entreprise en métiers et processus auxquels seront rattachés les événements à risques. Les risques sont alors analysés à un niveau de détail moindre et rattaché à un processus générique qui sera complété par des informations spécifiques et pertinentes pour l'identification des risques.

1.3.3.1.2. Les événements à risque

Selon JIMENEZ & al (2008 : 62), les événements à risque vont être associés à chaque processus opérationnel identifié dans la nomenclature. On cherche dans cette étape à

identifier tous les événements à risque qui peuvent se produire lors d'un processus et qui pourraient avoir des conséquences sur son développement.

Bâle II (in JIMENEZ & al, 2008 : 61-63) a défini la démarche d'identification des événements à risque. Celle-ci se présente comme suit :

- l'établissement d'une liste type d'évènement à risques : elle consiste à énumérer les divers risques génériques (interruption des systèmes d'information, erreur humaine, fraude). Cette liste permet d'éviter de refaire un travail complet d'analyse des risques avec les opérationnels métiers pour se concentrer sur les risques spécifiques à leurs activités) ;
- l'établissement de la liste des risques spécifiques : elle consiste à effectuer un listing des risques spécifiques de l'activité et des métiers que l'on retrouve quelque soit l'activité. Cette étape est construite avec les représentants des métiers et se déroule par des entretiens ou réunions avec les opérationnels responsables de processus qui pourront définir à quels type de risque ils sont sensibles ;
- la validation interne de la nomenclature des risques : celle-ci doit être adaptée au fonctionnement de l'entreprise. Sa validation doit permettre de s'assurer qu'un même risque dans deux entités ou activités différentes aura la même définition et le même sens afin de conserver un dispositif cohérent.

1.3.3.1.3. Les outils d'identification du risque opérationnel

Le comité de Bâle II a proposé aux banques des outils leur permettant d'identifier et d'évaluer les risques opérationnels liés à leurs activités. Il s'agit :

❖ La cartographie des risques

La cartographie des risques est un document permettant de recenser les principaux risques d'une organisation et de les présenter synthétiquement sous une forme hiérarchisée pour assurer une démarche globale d'évaluation des risques. Selon l'AMRAE (2002 :3), la cartographie des risques est un moyen permettant de classer, de comparer et de hiérarchiser les risques entre eux, de mettre en place des plans d'action pour les traiter en fonction des ressources disponibles. Abordant dans le même sens, AHOANGANSI (2010 :40-41),

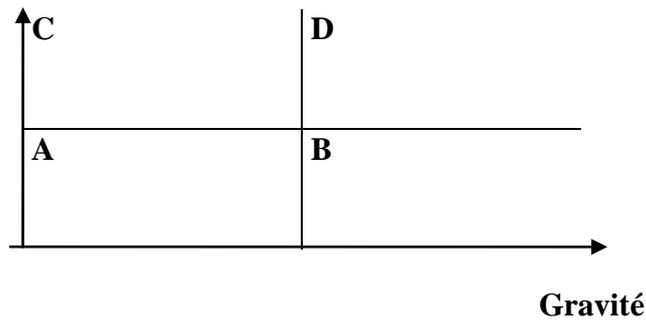
affirme que la cartographie des risques constitue un véritable inventaire des risques de l'organisation qui permet d'atteindre trois objectifs :

- Inventorier, évaluer et classer les risques de l'organisation ;
- Informer les responsables afin que chacun soit en mesure d'y apporter le management de ses activités ;
- Permettre à la direction et au risk manager, d'élaborer une politique de risque qui va s'imposer à tous.

Sa représentation conduit à la construction d'une matrice des risques qui permet de décliner les risques en quatre grandes catégories. Ainsi, on a :

- **Risques de fréquence et de gravité faible (A)** : Ce sont des risques qui se réalisent rarement et dont l'impact est limité même s'ils se réalisent. L'organisation peut vivre avec ces risques, nous parlerons de risques mineurs.
- **Risques de fréquence faible et de gravité élevée (B)** : ce sont des événements qui se produisent rarement mais dont les conséquences sont significatives lorsqu'ils se produisent. En raison de leur faible fréquence il est difficile de prévoir et d'anticiper leur survenance. La concrétisation du risque entraîne des conséquences pouvant affecter sérieusement l'activité de l'organisation, le redémarrage nécessite l'injection de capitaux extérieurs. Cette deuxième catégorie est dénommée risques catastrophiques
- **Risques de fréquence élevée et de gravité faible (C)** : ces événements se produisent assez régulièrement mais leurs conséquences sont relativement faibles. le risque est généralement prévisible, cette catégorie peut être dénommée risque opérationnel.
- **Risques de fréquence et de gravité élevée (D)** : les évènements se produisent régulièrement et leurs conséquences sont à chaque fois significatives. Dans la majorité des cas le décideur abandonne le projet à moins que le projet soit primordial pour le développement de l'organisation. On parle alors de situation d'évitement.

Fréquence



Source : Castelbajac & al (2003 :4)

❖ Les indicateurs de risques

La cartographie représente un support de base pour la mise en place des indicateurs de risque, de types statistiques et souvent financiers, ils fournissent un aperçu de la position de la banque, ils sont revus périodiquement. Les indicateurs de risque sont en effet de deux types :

- des indicateurs-clés de risque (key risks indicators) spécifiques à chaque activité et constituent des indices de perte ou des dangers à venir ;
- les indicateurs-clés de performances (key performance indicators) qui constituent des mesures d'évaluation de la qualité d'une activité.

Chaque activité disposera de son propre ensemble d'indicateur, spécifique à la nature des tâches effectuées, au mode d'organisation des fonctions, au niveau d'automatisation des opérations, au niveau des flux financiers impliqués ou de la législation en vigueur.

❖ Auto-évaluation des risques

La banque évalue ses opérations et activités à l'égard de vulnérabilités potentielle en termes de risque opérationnel. La cartographie des risque est une nécessité pour réussir le mécanisme de l'autoévaluation. Ce processus est mené en interne et comporte souvent des check listes et ou des work shops afin d'identifier les forces et les faiblesses de l'environnement du risque opérationnel. Le self-assesment utilise la technique de scorecard. A titre d'exemples les scorecards permettent de transformer des évaluations

qualitatives en mesures quantitatives qui donnent un classement relatif de différents types d'exploitation au risque opérationnel.

1.3.3.2. Analyse et évaluation des risques opérationnels

Une fois identifiés, les risques doivent faire l'objet d'une évaluation continue généralement mesurée en termes d'impact et de probabilité d'occurrence. Cette étape est bien sûr capitale dans la mesure où le niveau d'exposition aux risques bruts a un impact déterminant sur les stratégies mises en œuvre pour les traiter (CORDEL, 2013 : 139).

Selon MASSELIN & al (2014 : 48), l'évaluation du risque résulte généralement d'une combinaison de trois facteurs :

- sa probabilité d'apparition ;
- sa gravité en cas de survenance ;
- la durée pendant laquelle les conséquences de l'évènement ont un impact.

Quelques soient les risques identifiés, il est alors possible de tenter de coter sa gravité sur chacune de ces échelles.

1.3.3.3. Le suivi des risques opérationnels

Une fois les risques analysés et évalués, il convient d'en faire un suivi. Selon SARDI (2002 : 187), leur suivi est une composante essentielle du management des risques. Les politiques et les limites fixées doivent être surveillés sur une base constante pour s'assurer de leur respect. Cette surveillance est dévolue aux contrôles dits de « premier et deuxième niveaux » et le troisième niveau concerne l'audit interne qui doit éviter d'être impliqué dans la surveillance permanente. Son rôle est de s'assurer de l'efficacité du dispositif, le suivi passe généralement par le renforcement du contrôle interne, la mise en œuvre de nouvelles procédures.

1.3.3.4. Dispositif de maîtrise des risques opérationnels

La maîtrise des risques opérationnels constitue la phase la plus importante car c'est d'elle que dépendra la capacité de la banque à se doter de moyens de prévention. Elle se fait à travers l'identification des leviers d'actions à l'anticipation de certains évènements ou

réduire au maximum leur impact en cas de survenance. Elle s'appuie simultanément sur deux fonctions à savoir : la fixation d'un niveau maximum de risque opérationnel accepté par la banque (fixation des limites par typologie de risques opérationnels) et choix d'un mode de couverture tout en le traduisant par des plans d'actions précisant les mesures retenues, les responsabilités dans la mise en place et les délais de réalisation. Ainsi, selon JIMENEZ & al (2008 : 91), « le dispositif de base d'une bonne maîtrise des risques opérationnels doit comprendre plusieurs éléments qui peuvent se traduire par :

- une politique définie et documentée ;
- un réseau de responsables en charge de l'animation du dispositif et leur propre réseau de correspondants au sein de leur structure ;
- un dispositif d'identification et de gestion des risques opérationnels au quotidien ;
- la mise en place d'indicateurs avancés pertinents assurant les alertes sur toute perturbation d'un processus donné, des reportings adaptés au profil de risque de l'entité et des évaluations régulières du dispositif par des personnes en charge de son animation et par des interventions externes ».

Conclusion

Les risques opérationnels peuvent à la fois survenir au quotidien dans le cadre d'une activité commune mais également intervenir très ponctuellement et de façon dévastatrice dans des cas extrêmes. Face à cette diversité de manifestation du risque opérationnel, il est bon de savoir les gérer à travers la mise en place d'un bon dispositif de gestion des risques opérationnels comme évoqué dans le cadre de ce chapitre.

Chapitre 2 : L'AUDIT INTERNE ET LA GESTION DES RISQUES OPERATIONNELS

L'audit interne, depuis sa création, a connu un bon nombre de mutations quant à son utilité pour l'entreprise. Selon LEMANT (1995 : 39), on est passé d'une approche statique de la protection des actifs à une approche dynamique : efficacité de l'organisation, économie de moyens, célérité, fluidité. La nouvelle définition officielle de l'IIA (2004 : 1) approuvée le 21 mars 2000 par le conseil d'administration de l'IFACI, confirme bien cette nouvelle approche de l'audit interne : « L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise et en faisant des propositions pour renforcer son efficacité ».

Concernant le management des risques de l'entreprise le rôle essentiel de l'audit interne consiste à apporter au conseil une assurance objective quant à l'efficacité de cette activité, afin que les principaux risques de l'entreprise soient gérés correctement et que le système de contrôle interne fonctionne bien.

Dans ce chapitre, nous aborderons successivement le concept de management des risques, les avantages liés au management des risques pour une organisation, les activités intervenant dans le management des risques, la responsabilité du management des risques, le rôle de l'audit interne dans le management des risques, la démarche de conduite des missions d'audit interne et enfin les outils utilisés par l'audit interne pour accomplir les missions qui lui sont dévolues.

2.1. Définition du management des risques

Le management des risques traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Selon le COSO ERM, le management des risques est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer

les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.

2.1.1. Avantages du management des risques

Le dispositif de management des risques présente de nombreux avantages pour une organisation. En effet, ce dispositif contribue à la mise en place d'un reporting efficace et au respect de la conformité aux lois et réglementations. Ce faisant, il protège l'image de l'entité et lui épargne les conséquences néfastes d'une perte de réputation. En bref, grâce au déploiement d'un tel dispositif, une société est mieux armée pour atteindre ses objectifs et éviter les écueils et les impondérables. L'IIA dans sa prise de position sur le rôle de l'audit interne dans le management des risques à donner les avantages du management des risques de l'entreprise. En effet, selon l'IIA le management des risques peut aider de manière décisive l'organisation à gérer ses risques et atteindre ses objectifs. Aux nombres des nombreux avantages qu'elle présente, nous pouvons citer :

- une meilleure chance d'atteindre les objectifs ;
- une communication consolidée des risques au niveau du conseil ;
- une meilleure compréhension des principaux risques et de toutes leurs conséquences ;
- une identification et communication des risques transversaux au sein de l'entreprise et ;
- une meilleure chance de faire aboutir les changements.

2.1.2. Les activités du management des risques

Le management des risques étant défini comme un processus, est sous tendu par la réalisation de plusieurs activités. Selon le COSO ERM (2007 :4), le management des risques comprend les éléments suivants :

- **Aligner l'appétence pour le risque avec la stratégie de l'organisation**

L'appétence pour le risque est une donnée que la direction prend en considération lorsqu'elle évalue les différentes options stratégiques, détermine les objectifs associés et développe le dispositif pour gérer les risques correspondants

- **Développer les modalités de traitement des risques**

Le dispositif de management des risques apporte une méthode permettant de choisir de façon rigoureuse parmi les différentes options de traitement des risques que sont : l'évitement, la réduction, le partage ou l'acceptation du risque.

- **Diminuer les déconvenues et les pertes opérationnelles**

Les organisations améliorent leur capacité à identifier et traiter les événements potentiels, ce qui leur permet d'atténuer les impondérables et de diminuer les coûts ou pertes associées

- **Identifier et gérer les risques multiples et transverses**

Chaque entité est confrontée à une multitude de risque affectant différents niveaux de l'organisation. Le dispositif de management des risques renforce l'efficacité du traitement des impacts en cascade et apporte des solutions intégrées pour les risques à conséquences multiples.

- **Saisir les opportunités**

C'est en prenant en compte un large éventail d'événements potentiels que la direction est le mieux à même d'identifier et tirer parti des opportunités de façon proactive

- **Améliorer l'utilisation du capital**

C'est en ayant une vision claire des risques de l'organisation que la direction peut évaluer efficacement les besoins en capitaux et en améliorer l'allocation.

2.1.3. Responsabilité du management des risques

C'est le conseil qui est en général responsable de la gestion des risques. Dans la pratique, le conseil délègue le fonctionnement du cadre de la gestion du risque à l'équipe dirigeante, qui sera chargée de mener à bien les activités du management des risques.

Tous les collaborateurs ont leur rôle à jouer pour que la gestion des risques soit un succès à l'échelle de l'organisation, mais c'est à la direction que revient la responsabilité première

d'identifier les risques et de les gérer. Toutefois, l'une des principales missions de conseil dévolues à la fonction d'audit interne consiste à s'assurer que les processus de gestion des risques fonctionnent correctement et que les principaux risques sont maintenus à un niveau acceptable. Il est probable que cette assurance proviendra de différentes sources. Parmi ces sources, l'assurance provenant de la direction est fondamentale mais doit être complétée par une assurance objective émanant principalement de l'audit interne. L'IIA dans sa prise de position sur le rôle de l'audit interne dans le management des risques affirme que l'audit interne apporte normalement des assurances dans trois domaines :

- les processus de gestion de risque, à la fois concernant leur conception et leur fonctionnement ;
- la gestion des risques classées dans la catégorie « majeurs », y compris l'efficacité des contrôles et autres mesures de maîtrise des risques et ;
- la fiabilité des contrôles de l'évaluation et de la communication des risques et de l'état des contrôles.

2.2. Rôle de l'audit interne dans le management des risques

Selon l'IIA (2004 :5), L'audit interne est une activité indépendante qui apporte des conseils et une assurance objectifs. Concernant le management des risques, son principal rôle consiste à donner au Conseil l'assurance objective que la gestion des risques est efficace. D'après, Béatrice KI-ZERBO, des travaux de recherche ont montré que les membres du conseil et les auditeurs internes s'accordent à dire que les deux activités d'audit interne les plus porteuses de valeur ajoutée pour les organisations sont les suivantes : apporter l'assurance objective que les principaux risques sont bien gérés et apporter l'assurance que le cadre de la gestion des risques et du contrôle interne fonctionne correctement. Au regard de tout ce qui précède, il apparait donc claire que la fonction d'audit a une importance capitale dans le processus de management des risques et ceci en conformité avec la définition officielle attribué par l'IIA à la fonction. Dans sa prise position sur le rôle de l'audit interne dans le management des risques, l'IIA expose de façon détaillée le rôle qu'une fonction d'audit interne professionnelle doit et ne doit pas jouer dans le processus de management des risques. En outre, l'IIA précise les rôles légitimes de la fonction d'audit interne, sous réserve de prendre les précautions nécessaires.

2.2.1. Principaux rôles de l'audit interne dans le processus de management des risques

Selon l'IIA (2004 : 1), une fonction d'audit interne professionnelle doit jouer cinq (05) rôles dans le processus de management des risques. Ces différents rôles se présentent comme suit :

- donner une assurance sur les processus de gestion des risques ;
- donner l'assurance que les risques sont bien évalués ;
- évaluer les processus de gestion des risques ;
- évaluer la communication des risques majeurs ;
- examiner la gestion des principaux risques.

A ces principaux rôles, l'IIA à énumérer les rôles légitimes de l'audit interne sous réserve de prendre les précautions nécessaires. Il s'agit de :

- faciliter l'identification et l'évaluation des risques ;
- accompagner la direction dans sa réaction face aux risques ;
- coordonner les activités de management des risques ;
- consolider le reporting des risques ;
- actualiser et développer le cadre de gestion des risques ;
- promouvoir la mise en œuvre du management des risques ;
- élaborer une stratégie de gestion des risques à valider par le conseil.

Après avoir présenté les rôles de l'audit internes dans le processus de management des risques, il urge de faire un aperçu sur les rôles que l'audit interne ne doit pas jouer dans ledit processus.

2.2.2. Le rôle de l'audit interne dans le management des risques selon les normes

Selon l'IFACI(2013 :50), la norme 2120 sur le management des risques dispose que l'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration. Afin de déterminer si les processus de management des risques sont efficaces, les auditeurs internes doivent s'assurer que :

- les objectifs de l'organisation sont cohérents avec sa mission et y contribuent ;

- les risques significatifs sont identifiés et évalués ;
- les modalités de traitement des risques retenues sont appropriées et en adéquation avec l'appétence pour le risque de l'organisation ;
- les informations relatives aux risques sont recensées et communiquées en temps opportun au sein de l'organisation pour permettre aux collaborateurs, à leur hiérarchie et au Conseil d'exercer leurs responsabilités.

Pour étayer cette évaluation, l'audit interne peut s'appuyer sur des informations issues de différentes missions. Une vision consolidée des résultats de ces missions permet une compréhension du processus de management des risques de l'organisation et de son efficacité. Les processus de management des risques sont surveillés par des activités de gestion permanente, par des évaluations spécifiques ou par ces deux moyens.

Le risk manager établit le processus de management des risques à partir des informations que les opérationnels lui envoient. A partir de ces informations il établit la cartographie des risques et notamment la cartographie des risques opérationnels qui est une intégrante de la cartographie des risques. Une fois ce travail effectué l'audit interne vient évaluer la cartographie des risques en vue de faire des recommandations pour améliorer le dispositif.

2.2.2.1. Les modalités pratiques relatives à la norme 2120

Selon l'IFACI (2013 :51-56), les modalités pratiques d'application relatives à la norme 2120 sur «l'auto évaluation des contrôles pour évaluer la pertinence des processus de contrôle », étayent plusieurs points sur l'audit interne et la gestion des risques.

Il incombe à la direction générale de superviser la mise en place, la gestion et l'évaluation des processus de management des risques et les contrôles. Les directeurs opérationnels sont chargés notamment d'évaluer les risques et les contrôles en place dans leurs unités. Les auditeurs internes et les auditeurs externes apportent différents niveaux d'assurance quant à l'efficacité des processus de management des risques et de contrôle de l'organisation. Les managers et les auditeurs ont intérêt à utiliser des techniques et des outils centrés sur l'évaluation des processus de management des risques et de contrôle existants, ainsi que sur l'identification des moyens de renforcer leur efficacité.

La mise en œuvre d'une approche fondée notamment sur des enquêtes d'autoévaluation et sur l'animation d'ateliers (CSA ou Auto-évaluation des contrôles) constitue pour les managers et les auditeurs internes un moyen utile et efficace de collaborer à l'évaluation des procédures de contrôle. En principe, la prise en compte des objectifs et des risques fait partie intégrante de l'autoévaluation des contrôles (CSA), qui est parfois désignée par l'expression « autoévaluation des contrôles et des risques » (CRSA). Les professionnels ont recours à différentes techniques, mais la plupart des programmes mis en place présentent certaines caractéristiques et certains objectifs communs. Une organisation qui pratique l'auto-évaluation dispose d'un processus formalisé et documenté grâce auquel le management et les groupes de travail qui sont directement impliqués dans une unité opérationnelle, une fonction ou un processus, peuvent participer de façon structurée aux opérations suivantes :

- identification des risques encourus ;
- évaluation des processus de contrôle permettant d'atténuer ou de gérer ces risques ;
- élaboration de plans d'actions visant à ramener les risques à des niveaux acceptables ;
- estimation de la probabilité pour que les objectifs de l'organisation soient atteints.

Les processus d'auto-évaluation peuvent présenter les avantages suivants :

- les contrôles informels dits « soft » sont plus faciles à identifier et à évaluer ;
- les membres du personnel sont motivés pour « s'approprier » les processus de contrôle en place dans leurs unités, et les mesures correctives prises par les groupes de travail sont souvent plus efficaces et plus rapides ;
- l'ensemble de la chaîne objectifs risques contrôle de l'organisation fait l'objet d'un meilleur suivi et d'amélioration continues ;
- les auditeurs internes interviennent dans le processus d'auto-évaluation et en acquièrent une très bonne connaissance, soit en tant qu'animateurs, secrétaires ou rapporteurs des groupes de travail, soit pour dispenser une formation aux concepts de risque et de contrôle qui sous-tendent le programme d'auto-évaluation. Ils acquièrent ainsi une très bonne connaissance du processus ;
- l'audit interne est mieux informé sur les processus de contrôle de l'organisation. Il peut par conséquent exploiter ces informations et consacrer en priorité ses rares

ressources à l'examen des unités ou des fonctions dont les contrôles présentent des faiblesses significatives ou qui comportent des risques résiduels importants ;

- le management, dont la responsabilité au titre des processus de management des risques et de contrôle de l'organisation se trouve renforcée, sera moins tenté de déléguer ces tâches à des spécialistes, et notamment aux auditeurs ;
- le rôle premier de l'audit interne consistera, comme par le passé, à valider de processus d'évaluation au moyen de tests et à formuler un jugement professionnel sur la pertinence et l'efficacité de l'ensemble des systèmes de management des risques et de contrôle.

L'approche adoptée dans le cadre d'un programme d'auto-évaluation des contrôles varie fortement selon le secteur d'activité de l'organisation, sa localisation, sa structure, sa culture, le degré d'autonomie de son personnel, son style de management et sa façon de formuler les stratégies et les procédures, ce qui conduit à penser que le succès rencontré par un certain type de programme d'auto-évaluation dans une organisation donnée peut ne pas se reproduire ailleurs. Le processus d'auto-évaluation doit être personnalisé et adapté aux caractéristiques de chaque organisation. Il faut donc adopter une approche dynamique et la modifier en fonction de l'évolution de l'organisation.

Les programmes d'auto-évaluation revêtent principalement les trois formes suivantes : ateliers par équipe, enquêtes, et études réalisées par le management. Ces différentes approches sont souvent combinées dans les organisations.

Les ateliers rassemblent les informations collectées par des groupes de travail qui représentent, à différents niveaux, l'unité ou la collection concernée. L'atelier peut être centré sur les objectifs, les risques, les contrôles ou les processus.

- Les ateliers centrés sur les objectifs recherchent en priorité le meilleur moyen de réaliser un objectif de l'organisation. Le groupe commence par identifier les contrôles en place qui concernent à la réalisation de l'objectif, puis il détermine les risques résiduels. Le but de l'atelier est d'apprécier si les procédures de contrôle sont efficaces et si elles permettent de maintenir les risques résiduels à un niveau acceptable.
- Les ateliers centrés sur les risques s'efforcent en priorité d'identifier les risques liés à la réalisation d'un objectif. Le groupe commence par dresser la liste de tous les

obstacles, menaces et risques susceptible d'empêcher la réalisation d'un objectif, puis les principaux risques. Le but de l'atelier est de déterminer les risques résiduels significatifs. Ce type d'atelier porte sur l'intégralité de la chaîne objectifs-risques-contrôles.

- Les ateliers centrés sur les contrôles recherchent en priorité si les contrôles en place fonctionnent bien. Ce type d'atelier diffère des deux premiers car l'animateur identifie les principaux risques et contrôles avant le début de l'atelier. Durant l'atelier, le groupe de travail apprécie dans quelle mesure les contrôles contribuent à l'atténuation des risques et à la réalisation des objectifs. Le but de l'atelier est d'analyser l'écart entre l'efficacité réelle des contrôles et l'efficacité attendue par le management.
- Les ateliers centrés sur les processus portent en priorité sur certaines activités qui font partie d'un ensemble de processus. Les processus consistent généralement en une série d'activités qui sont liées et qui se déroulent du début jusqu'à la fin, telles que les diverses étapes d'un cycle achats, développement de produits ou génération de revenus. Ce type d'atelier couvre généralement l'identification des objectifs de l'ensemble du processus et de diverses étapes intermédiaires. Le but de cet atelier est d'évaluer, actualiser, valider, améliorer et même de rationaliser l'ensemble du processus et les activités qui le composent. Ce type d'atelier peut déboucher sur une analyse plus large que l'approche centrée sur les contrôles car il couvre plusieurs objectifs du processus et soutient les efforts effectués par ailleurs par le management dans le cadre d'opération engineering, amélioration qualité, et projets d'amélioration continue des processus.

Les enquêtes sont réalisées à l'aide d'un questionnaire auquel il faut généralement répondre par oui ou par non, les questions étant rédigées avec soin de façon à en faciliter la compréhension. Elles sont privilégiées lorsque l'atelier ou si le management souhaite minimiser les temps passés et les coûts engagés pour recueillir les informations.

L'Auto - évaluation désignée par la locution « études du management » regroupe la plupart des autres approches adoptées par les groupes de dirigeants pour rassembler des informations concernant certains processus, certaines activités de management des risques ou certaines procédures de contrôle. L'étude a souvent pour but de porter, dans des délais raisonnables, un jugement éclairé sur certaines caractéristiques des procédures de contrôle.

Elle est généralement réalisée par une équipe de poste ou jouant un rôle de support. L'auditeur interne peut faire la synthèse de cette étude et d'autres informations afin d'améliorer sa connaissance des contrôles et la partager avec les responsables d'unités opérationnelles ou fonctionnelles dans le cadre du programme d'auto-évaluation de l'organisation.

Tous les programmes d'auto-évaluation supposent que les membres du management et des groupes de travail possèdent une bonne connaissance des concepts de risque et de contrôle, et les utilisent pour communiquer. Dans le cadre des formations, les organisations utilisent souvent un cadre, tel que les modèles COSO et COCO, destiné à faciliter le bon déroulement des débats au sein des ateliers et à vérifier le caractère exhaustif de l'ensemble du processus. En règle générale, les ateliers donnent lieu à l'émission d'un rapport rédigé pour une large part durant les débats. Un consensus sera dégagé sur les divers sujets de discussion, le groupe examinera le projet de rapport avant la fin de dernière session. Certains programmes comportent sur un système de vote anonyme qui permet d'assurer la libre circulation des informations et des opinions durant les ateliers, et qui facilite la résolution des divergences de points de vue et d'intérêts.

L'audit interne s'investit de façon assez significative dans certains programmes d'auto-évaluation des contrôles. Il peut susciter, concevoir, mettre en place et en fait, s'approprier le processus, diriger la formation, fournir les animateurs, les secrétaires et les rapporteurs, et coordonner la participation du management et des groupes de travail. Dans d'autres programmes, l'audit interne réduit sa participation au minimum, et n'intervient qu'à titre de partie prenante et de consultant de l'ensemble du processus, ainsi que pour vérifier en dernier ressort les conclusions des équipes. Dans la plupart des cas, l'investissement de l'audit interne dans le programme d'auto-évaluation des contrôles se situe entre ces deux extrêmes. Plus la participation de l'audit interne au programme d'auto-évaluation et aux débats organisés dans les ateliers est importante, plus le responsable de l'audit interne doit s'assurer de l'objectivité de l'équipe d'audit interne, prendre des mesures à cet effet (si cela s'avère nécessaire), et intensifier les tests afin de vérifier que le jugement du personnel n'est pas faussé. Selon la Norme 1120 : « Les auditeurs internes doivent adopter une attitude impartiale et dépourvue de préjugés et éviter les conflits d'intérêts ».

L'existence d'un programme d'auto-évaluation des contrôles renforce le rôle traditionnel de l'audit interne car il lui permet d'assister le management dans l'exercice de ses

responsabilités, notamment en ce qui concerne la mise en place et le maintien des processus de management des risques et de contrôle, et l'évaluation du système. Dans le cadre d'un tel programme, l'audit interne, les unités opérationnelles et les fonctions coopèrent en vue d'améliorer des informations relatives au fonctionnement des processus de contrôle et à l'importance des risques résiduels.

Bien qu'il participe au programme d'auto-évaluation des contrôles en qualité d'animateur de d'expert, l'audit interne constate souvent que ce programme lui permet de réduire les efforts nécessaires pour recueillir des informations sur les procédures de contrôle et d'éliminer certains tests. Un programme d'auto-évaluation doit avoir pour effet d'élargir le champ de l'évaluation des processus de contrôle à travers l'organisation, d'améliorer la qualité des mesures correctives prises par les responsables des processus, et de centrer les travaux de l'audit interne sur l'examen des processus à haut risque et des situations inhabituelles. Il peut alors s'attacher à valider les conclusions qui remontent du programme d'auto-évaluation, à dresser la synthèse des informations provenant des diverses composantes de l'organisation et à formuler, à l'attention de la direction générale et du comité d'audit, une opinion d'ensemble sur l'efficacité des contrôles.

2.2.3. Rôle que l'audit interne ne doit pas jouer dans le processus de management des risques

Dans le but de ne pas porter atteinte à l'indépendance et à l'objectivité des auditeurs internes, l'IIA (2004 :2) ; dans sa prise de position sur le rôle de l'audit dans le management des risques a énuméré les différents rôles que l'audit interne ne doit pas jouer dans ledit processus. Il s'agit de :

- définir l'appétence pour le risque ;
- définir des processus de gestion du risque ;
- gérer l'assurance sur les risques ;
- décider de la manière de réagir face aux risques ;
- mettre en œuvre des mesures de risque au nom de la direction ;
- prendre la responsabilité de la gestion des risques.

2.2.4. L'audit interne et la gestion des risques opérationnels

La responsabilité de l'évaluation du dispositif de gestion des risques opérationnels incombe à l'audit interne ; ce, à travers le contrôle de second niveau. En matière d'attentes de Bâle II, selon LAURETOU & ZANOTA (2005 :67-68), « les responsabilités de l'audit interne sont :

- concernant le premier pilier : examen périodique des processus de gestion et des systèmes de mesure du risque opérationnel portant sur les activités des unités et sur la fonction indépendante de gestion des risques opérationnels ;
- pour le second pilier : il a pour rôle de donner l'assurance sur l'identification et la mesure des risques et les processus de contrôle de l'intégrité du processus de gestion ; l'assurance du caractère approprié du système de contrôle interne et le réexamen périodique du processus de gestion des risques (intégrité, fiabilité, pertinence) ;
- enfin l'audit interne pourrait assurer le conseil d'administration de l'efficacité des contrôles du processus de communication tels que décrits au troisième pilier ».

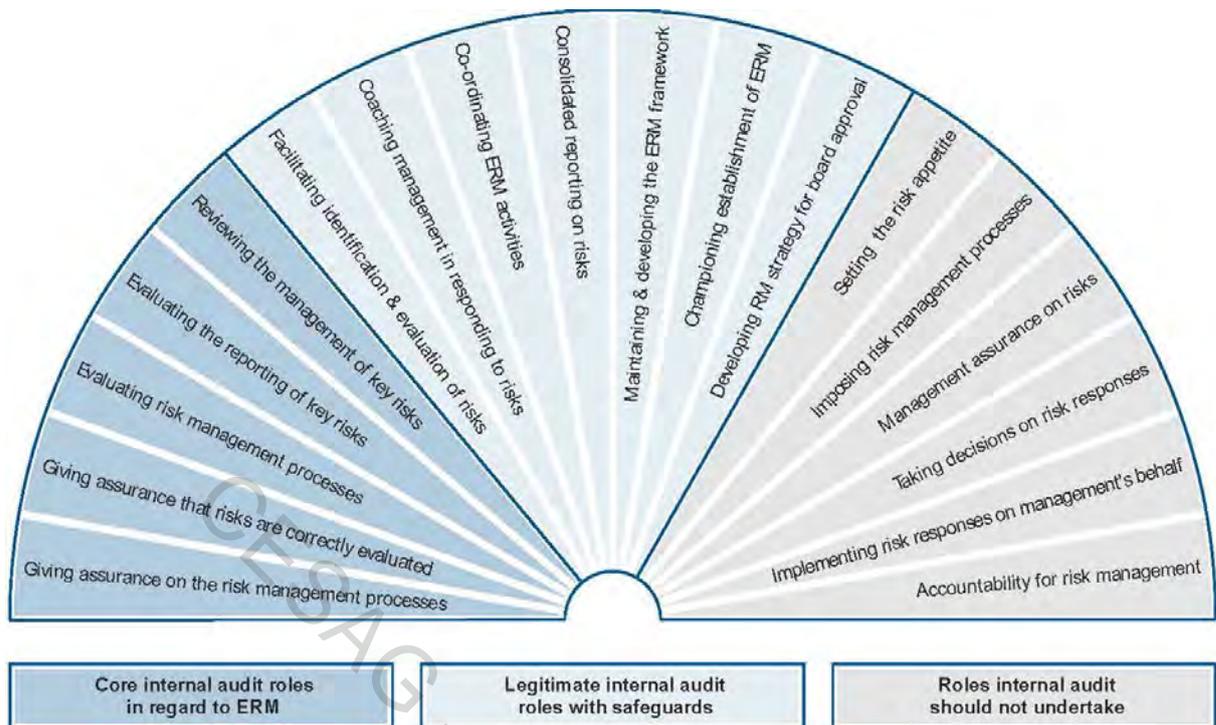
L'audit interne doit donc, périodiquement, évaluer, à travers des missions d'audit effectuées dans le cadre des plans annuels d'audit, ce dispositif afin de juger de la pertinence et de la qualité du système de maîtrise des risques et de proposer des mesures d'améliorations. En effet, selon RENARD (2010 :103), « l'objectif prioritaire de l'évaluation du processus de management des risques est donc l'évaluation du contrôle interne qui en est le produit fini ». Cette mission doit permettre d'assurer, tant à l'organe exécutif qu'au régulateur : l'appréciation et la maîtrise des risques de l'établissement ; la bonne application de la politique des risques définie ; la capacité de la banque à détecter, prévenir et gérer ses risques dans les limites qu'elle s'est fixées conforme à la réglementation en vigueur.

De nos jours plusieurs entreprises commencent à se doter d'une direction ou service qui s'occupent de la gestion des risques opérationnels, mais surtout dans les institutions financières. Mais la création de cette nouvelle fonction n'enlève pas les attributions de l'audit interne à la maîtrise des risques de l'organisation où il se trouve. La nécessité de mesurer le risque opérationnel provient des préconisations du comité de Bâle, qui requièrent des banques d'allouer une quantité de capital adéquate pour couvrir leur risque

opérationnel. Il propose aux institutions financières plusieurs méthodes plutôt quantitatives pour gérer les risques bancaires y compris les risques opérationnels. La gestion de ces risques ne peut se fonder sur les seules méthodes quantitatives. En effet, les démarches d'évaluation des risques pilotées par des directions de risques sont conduites par les opérationnels eux-mêmes, ce qui nécessitera comme l'a d'ailleurs prévu le Comité de Bâle, une validation indépendante.

L'audit interne aura un rôle majeur à jouer dans la validation des démarches de nature qualitative permettant de réaliser une cotation des risques et des contrôles. Il valide, par une méthode d'audit, la valeur des expositions résiduelles par la réalisation de tests de validation sur certains axes, ainsi que par l'analyse de la cohérence entre les résultats des missions d'audit, d'une part, et du *self-assessment*, d'autre part. L'évaluation des dispositifs de contrôle interne et de maîtrise des risques est une étape particulièrement importante dans la démarche d'évaluation des risques opérationnels. En effet, c'est par la définition des écarts entre le référentiel-cible et les dispositifs existants que seront cotés les systèmes de contrôle interne. Celle-ci permettra de mettre en place les plans d'actions destinés à sécuriser les processus et diminuer les risques. L'évaluation des dispositifs de contrôle est donc une étape essentielle des démarches de gestion des risques opérationnels, permettant à la fois de tracer la cotation des risques en justifiant le résultat obtenu, tout en assurant un pilotage des plans d'actions afin de sécuriser les processus.

Figure 1 : Rôle de l'audit interne dans le management des risques



Source : Prise de décision de l'IIA (2004 :5)

Conclusion du chapitre

La gestion du risque constitue un élément fondamental du gouvernement d'entreprise. C'est la direction qui doit instaurer un cadre de gestion des risques et le faire fonctionner à la demande du conseil. Le management des risques de l'entreprise peut se révéler très utile à de nombreux égards en raison de son approche structurée, cohérente et coordonnée. Dans le cadre du management des risques, le rôle essentiel de l'audit interne doit consister à apporter à la direction et au conseil l'assurance de l'efficacité de la gestion du risque. Lorsque l'audit interne étend ses activités au-delà de ce rôle central, il doit prendre des précautions et notamment traiter les missions comme des services de conseil et donc respecter toutes les normes y afférentes. L'audit interne protège ainsi l'indépendance et l'objectivité de ses services d'assurance. Dans ce cadre, le management des risques peut contribuer à rehausser le profil et accentuer l'efficacité de l'audit interne.

Chapitre 3 : METHODOLOGIE DE L'ETUDE

Dans une logique de fiabilité, l'analyse de tout problème doit s'inscrire dans une approche méthodologique. L'analyse de la contribution de la fonction d'audit interne dans la gestion des risques opérationnels que nous voulons effectuer n'est pas en reste. En effet la revue de littérature nous a permis de faire la synthèse des développements conceptuels sur la notion de risques opérationnels en milieu bancaire et leur techniques de gestion d'une part mais aussi sur le rôle de la fonction d'audit interne dans la gestion de ces risques. Il s'agira pour nous, dans ce chapitre de présenter la méthodologie de recherche à adopter pour l'analyse de la contribution de la fonction d'audit interne dans la gestion des risques opérationnels.

Notre approche s'articulera autour de trois (03) étapes principales à savoir :

- un modèle d'analyse ;
- les outils de collecte de données ;
- l'analyse des données.

3.1. Modèle d'analyse

Nous allons dans cette partie définir le modèle conceptuel de base de notre étude. Un tel dispositif permettra à notre analyse de se construire sur une base solide. Ce modèle d'analyse est composé de quatre (04) phases que sont :

1^{ère} phase : la prise de connaissance de la BOA-Mali : cette phase nous permettra de mieux connaître la structure à travers son historique, ses missions, ses produits et son organisation. Cette étude prendra aussi en compte les mécanismes internes de gestion des risques opérationnels mis en place. Pour ce faire nous allons procéder à une revue documentaire, des observations et des entretiens pour nous enquêter la situation de la BOA-Mali.

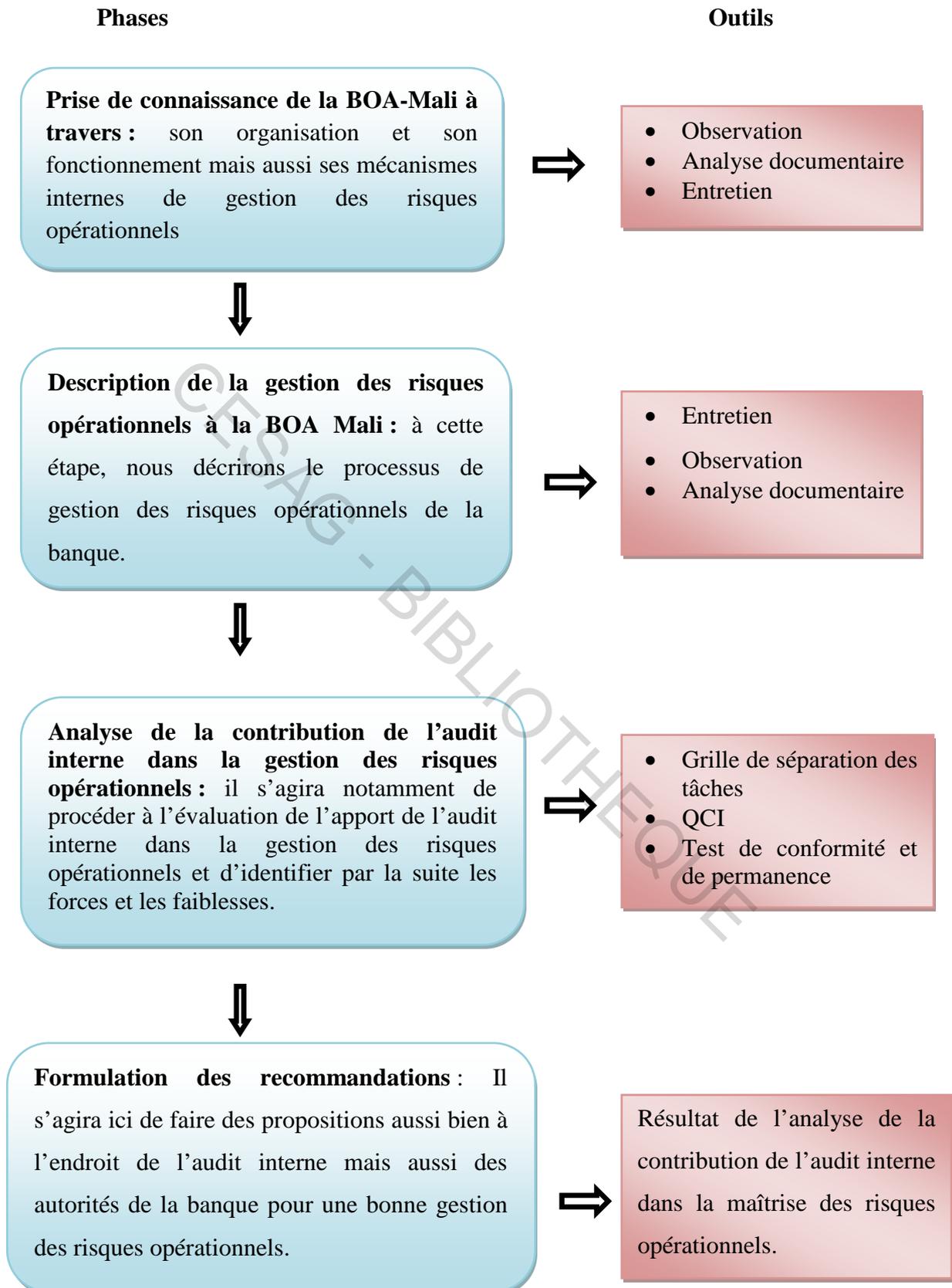
2^{ème} phase : la prise de connaissance de la fonction d'audit interne de la BOA-Mali. Suite à la prise de connaissance de la structure, nous nous sommes intéressés à l'étude de sa fonction d'audit interne. Cette étude a pris en compte le dispositif de contrôle interne existant pour la gestion des risques opérationnels et le rôle de l'audit interne dans ce dispositif. Les outils utilisés pour y arriver sont : des entretiens, des observations, l'établissement d'un tableau d'identification des risques opérationnels.

3^{ème} phase : Analyse de la contribution de l'audit interne dans la gestion des risques opérationnels. Cette analyse nous permettra d'évaluer la contribution de l'audit interne dans la gestion des risques opérationnels à la BOA Mali. Les outils que nous utiliserons à ce niveau se présentent comme suit : la grille de séparation des tâches, le questionnaire de contrôle interne (QCI), les tests de conformité et de permanence.

4^{ème} phase : Formulation des recommandations : une fois les forces et les faiblesses de la contribution de l'audit interne dans la gestion des risques opérationnels identifiés, nous allons formuler des recommandations à l'endroit des acteurs de l'audit interne mais aussi à l'endroit des différentes autorités de la banque pour une meilleure gestion de ces risques.

CESAG - BIBLIOTHEQUE

Figure 2 : Modèle d'analyse



Source : Nous-mêmes

3.2. Outils de collecte de données

Dans le cadre de notre travail de recherche, nous avons utilisé les techniques de collecte de données suivantes : la revue documentaire, les entretiens, l'observation, le questionnaire de contrôle interne, les tests de conformité et de permanence. Ces outils nous ont permis d'obtenir les informations nécessaires pour effectuer notre analyse.

3.2.1. La revue documentaire

La revue documentaire a consisté en la consultation des documents interne de la BOA-Mali. Ces documents sont les manuels de procédures, les rapports de mission, la cartographie des risques opérationnels de la banque, les notes de service et les rapports d'activité. Ils nous ont permis d'aiguiser notre compréhension et notre analyse.

3.2.2. Les entretiens

Nous avons eu des entretiens avec les différents responsables qui interviennent dans la gestion des risques opérationnels. Ces entretiens nous ont permis d'approfondir notre compréhension sur tous les aspects du dispositif de maîtrise des risques opérationnels qui est mis en place.

3.2.3. Observation

L'observation se fera de deux manières. Il y a celle directe qui nous permettra de comprendre et de valider les informations recueillies lors de l'interview sur le processus de gestion des risques opérationnels et les dispositifs mis en œuvre. La seconde forme d'observation est celle indirecte. Elle se focalisera sur le dispositif de maîtrise des risques opérationnels afin de voir la contribution de l'audit interne dans le processus de maîtrise de ceux-ci.

3.2.4. Le questionnaire de contrôle interne

Notre questionnaire sera administré à un échantillon d'agents de la banque qui intervient dans le processus de maîtrise des risques opérationnels. Il sera composé de questions fermées en vue d'analyser les risques, d'évaluer le dispositif de contrôle interne pour déceler les forces et les faiblesses de celui-ci. Une réponse « oui » à une question constitue

une force apparente du dispositif de contrôle interne. Une réponse « non » constitue une faiblesse réelle.

Nous établirons deux questionnaires :

- la première portera sur les risques opérationnels ainsi que le dispositif de maîtrise de ces derniers ;
- la seconde concernera l'évaluation des dispositifs de maîtrise et de contrôle interne.

3.2.5. Tableau d'identification des risques

Nous établirons à ce niveau le tableau des forces et faiblesses apparentes (TFfA) et la grille de séparation des tâches.

3.2.5.1. Le Tableau des Forces et faiblesses Apparentes (TFfA)

Le TFfA nous permettra d'identifier les différents risques opérationnels afin d'avoir une vue sur les dispositifs mis en place pour les réduire.

3.2.5.2. La grille de séparation des tâches

Ce document complète totalement les autres outils. La grille de séparation des tâches a pour objectif, pour une organisation adéquate ou un rattachement hiérarchique différent, d'éviter qu'une personne ou un groupe de personnes cumulent les fonctions d'engagement, de règlement, d'enregistrement et de contrôle dans un même processus opérationnel. Elle permet ainsi de prévoir une distinction nette entre celui qui décide et celui qui exécute, entre celui qui opère et celui qui valide tout en offrant une garantie d'un contrôle indépendant et permanent sur l'activité (OBERT, 2004 : 77). Elle nous permettra dans le cadre ce travail de vérifier le respect du principe de séparation des tâches et de déceler ainsi les tâches incompatibles et les cumuls de fonction.

3.2.6. Les tests de conformité et de permanence

Ces tests seront utiles pour s'assurer que les dispositifs de contrôle interne ont été appliqués, pour permettre la remontée à la source en passant par toutes les phases intermédiaires mais aussi de s'assurer que les opérations sont toujours traitées conformément à ce qui a été décrite lors des entretiens.

Conclusion

L'audit interne doit aider l'organisation à évaluer son processus de management des risques ceci à travers l'identification, l'analyse, l'évaluation des risques ainsi que le suivi régulier de la mise en œuvre des recommandations. Il doit donc aider à l'évaluation mais aussi à la mise en place en cas d'absence d'un département de gestion des risques.

CESAG - BIBLIOTHEQUE

Conclusion de la première partie

Ce chapitre nous permis de présenter la méthodologie retenue pour l'analyse de la contribution de l'audit interne dans la maîtrise des risques opérationnels à la BOA-Mali. Cette méthodologie s'articule autour de quatre phases que sont : la prise de connaissance de la banque, la prise de connaissance de la fonction de d'audit et de son rôle dans le dispositif de maîtrise des risques opérationnels, l'évaluation de la contribution de la fonction d'audit interne dans ledit dispositif et enfin la formulation des recommandations pour une meilleure maîtrise de ces risques. Aussi les outils qui nous permettrons d'effectuer notre analyse ont été présentés.

CESAG - BIBLIOTHEQUE

DEUXIEME PARTIE :
CADRE PRATIQUE DE L'ETUDE

La revue de littérature à laquelle nous avons procédé dans la première partie nous a permis de faire une synthèse des développements théoriques sur les exigences relatives à l'audit interne quant à la gestion des risques opérationnels. Celui-ci va nous permettre dans cette seconde partie d'assoir notre évaluation de la gestion des risques opérationnels au sein de la Banque Of Africa Mali sur la base du modèle conçu et de formuler des recommandations en vue d'une adéquation de la pratique de l'audit interne telle qu'effectuée à la Banque Of Africa Mali.

Ainsi cette seconde partie se déclinera en trois chapitres. Dans le premier chapitre nous allons présenter la Banque Of Africa Mali à travers son historique, ses missions et son organisation. Le deuxième chapitre nous permettra de faire état du contrôle interne et de la gestion des risques opérationnels à la Banque Of Africa Mali à travers la présentation de son département d'audit interne en abordant successivement son organisation, son fonctionnement et les moyens dont il dispose et sa méthodologie de conduite des missions d'audit interne. Enfin dans le troisième chapitre nous allons procéder à l'évaluation de la gestion des risques opérationnels par l'audit interne de la Banque Of Africa Mali.

Chapitre 4 : PRESENTATION DE LA BOA-MALI

Filiale du groupe Bank Of Africa, la BOA-Mali compte environ cinq cent (500) agents, quatorze (14) agences à Bamako, onze (11) agences régionales et dix-sept (17) points de vente en partenariat avec TOTAL MALI. Cela lui permet d'offrir une large gamme de service à sa clientèle répartie en clients particuliers et en clients entreprises.

Dans la présentation de cette entité nous aborderons successivement son historique, les missions qui lui sont assignées, ses produits ainsi que la structure organisationnelle qui lui permet de s'acquitter de ses missions.

4.1. Historique de la BOA-Mali

La BOA-Mali a été juridiquement créée le 20 décembre 1982 et ouverte au public le 19 décembre 1983.

Elle est née de la volonté et de l'effort conjugués de commerçants et d'industriels Maliens soucieux de créer une banque privée nationale, à la fois banque d'affaires et commerciale, plus en mesure de répondre à leurs intérêts et à leurs aspirations. Le système bancaire se caractérisait par l'existence d'une Banque Nationale de Développement et de deux banques commerciales dépendant de banques françaises peu incitées, par l'absence de concurrence, à un grand dynamisme ou à une politique active d'innovations.

En outre, l'Etat Malien appréciait favorablement le projet de création d'une nouvelle banque dans un contexte politique encourageant l'initiative privée à des fins productives, et où le rapatriement des capitaux maliens placés à l'extérieur était considéré comme primordial.

La BOA-Mali est la première banque privée malienne à capitaux africains. Près de 850 actionnaires, à majorité africains et appartenant au secteur privé ont souscrit au capital de la Banque, faisant de la BANK OF AFRICA une véritable banque populaire et une expérience unique dans le système bancaire africain.

A sa création, elle s'est fixée comme objectifs principaux :

- la vulgarisation de la politique de créativité en matière de collecte de l'épargne ;
- la relance de l'activité économique par le financement et les prêts aux entreprises et opérateurs économiques ;
- la recherche du profit c'est-à-dire la réalisation d'un bénéfice ;
- l'extension de la couverture géographique par la création des agences dont celle de Paris pour la satisfaction des Maliens de l'extérieur ;
- la lutte contre le chômage par le recrutement des jeunes diplômés maliens.

4.2. Actionnariat de BOA-Mali

Près de 850 actionnaires à majorité africains et appartenant au secteur privé ont souscrit au capital de la banque, faisant de la BOA-Mali une véritable banque populaire et une expérience dans le système bancaire malien.

De sa création à nos jours, le capital de la BOA-Mali a subi des modifications dans sa structure. Son capital au départ s'élevait à deux milliards (2.000.000.000) de francs CFA puis il est passé à quatre cent dix milliards (410.000.000.000) de Francs puis sept milliards deux cents millions (7.200.000.000) et se réparties comme suit :

- | | |
|---|--------|
| • BOA Groupe : | 50.22% |
| • Actionnaire privés nationaux : | 27.51% |
| • Société Financière Néerlandaise pour le Développement : | 16.38% |
| • ATTICA S.A : | 2.19% |
| • Autre actionnaire : | 3.70% |

4.3. Missions et objectifs

La BOA-Mali a pour mission la pratique de toutes opérations autorisées aux banques en république du Mali, de faire pour son compte, pour le compte de tiers ou en participation toutes les opérations financières ; commerciales, mobilières et immobilières pouvant être effectuées par les banques.

Au nombre des objectifs qu'elle s'est fixée nous pouvons citer :

- être leader sur le marché ;
- augmentée le taux de bancarisation au Mali ;

4.4. Les produits de BOA-Mali

La BOA-Mali offre plusieurs gammes de produits qui sont réparties en fonction de ses clients. La catégorisation des clients nous permet de distinguer les clients particuliers d'une part et les clients entreprises d'autre part. Les produits offerts à chacun de ses groupes de clients se présentent comme suit :

- **Les produits aux particuliers**

Il s'agit de :

- les comptes chèques ;
- les comptes épargnes ;
- les prêts personnels ;
- les prêts à l'habitat ;
- les prêts scolaires ;
- l'octroi de cartes visa internationale ;

- **les produits aux entreprises.**

Il s'agit de :

- l'ouverture de comptes courants ;
- l'appui aux PME ;
- le financement des PME.

4.5. Organisation et fonctionnement

Dans cette section nous décrivons les différents organes de la BOA-Mali.

4.5.1. Le Conseil d'Administration

Le Conseil d'Administration est l'organe exécutif de la BOA-Mali, il jouit de toutes les prérogatives et regroupe en son sein les gros actionnaires de la société (ceux qui détiennent une part importante des actions).

Il nomme et révoque le Directeur Général, valide les grandes orientations de la banque, fixe les objectifs fondamentaux, décide des réorganisations à opérer en vue de meilleures performances.

Les grandes décisions sont généralement issues des réunions tenues chaque année au plus tard au mois de mars.

En marge de ce conseil, se tient une assemblée des actionnaires au second trimestre de chaque année afin de présenter la situation de l'année écoulée aux différents actionnaires de la banque.

4.5.2. La Direction Générale

Dirigée par le Directeur Général (DG), elle coordonne toutes les autres directions de la banque à travers ses différentes cellules qui sont :

- le DECD ;
- le DAC et le service contentieux ;
- les ressources humaines.

Elle a pour rôle en matière de crédit, de donner son accord sur la base des propositions faites par les services compétents et de prendre des décisions de crédit qui lui sont déléguées. Elle s'occupe principalement de la gestion quotidienne des activités de l'établissement, et peut aussi convoquer un comité de crédit interne élargi.

4.5.3. Le contrôle Général

Rattaché à la Direction Général, il s'assure de la surveillance et du contrôle des risques opérationnels et veiller au bon fonctionnement du dispositif de contrôle interne. Ce dispositif doit permettre d'identifier l'ensemble des facteurs internes et externes susceptibles de compromettre la réalisation des objectifs fixés par la Direction Générale. Il

est composé de deux départements à savoir le département audit comptable et financier et le département audit des services et suivi des procédures.

4.5.4. Direction de l'Exploitation Commerciale et de Développement (DECD)

La DECD avec son volet commercial, a été le principal artisan du développement des ressources clientèle de la BOA-Mali avec un taux moyen annuel de 11,5%.

Elle a sous sa supervision : le réseau d'agences, le centre d'affaires, le département institutionnel chargés des grands comptes et les agences (agences de Bamako, des régions et de Paris).

4.5.4.1. Centre d'affaires

Le centre d'affaires est un espace entièrement dédié au grandes entreprises dont la prise en charge est assurée par les chargés d'affaires et les chargés de comptes.

Le Département des Grandes Entreprises s'occupe des entreprises dont le chiffre d'affaires est supérieur ou égal à un milliard (1.000.000.000) de francs CFA. Il a pour rôle de fidéliser les gros clients et d'en attirer d'autres.

4.5.4.2. Département du Réseau d'Agence des PME

Il s'occupe de l'animation des Petites et Moyennes entreprises (PME) et des agences de Bamako et des provinces.

4.5.4.3. Département des Institutionnels (DI)

Le Département des Institutionnels s'occupe des organisations non gouvernementales, professions libérales, etc. « ELITE » qui est réservée à la clientèle « haut de gamme » (personnel consulaire, organisations non gouvernementales, professions libérales, etc.).

4.5.5. Direction Administrative et Comptable (DAC)

La structure actuelle de la DAC lui permet, avec plus d'efficacité, d'assurer le suivi des comptes de gestion, les comptes internes et de correspondants, sécurisant ainsi la banque contre les effets néfastes des suspens sur la rentabilité. Elle a sous sa direction les départements suivants :

4.5.5.1. Département de la comptabilité

Sa mission s'articule autour de la comptabilité générale et comprend :

- la vérification de l'exactitude des imputations comptables ;
- la gestion quotidienne du compte suspens informatique ;
- la surveillance quotidienne des comptes sensibles comme les comptes de liaison débiteurs et créditeurs ; comptes Exodus ;
- la régularisation mensuelle des documents BCEAO et tous les annexes ;
- le suivi des ratios prudentiels ;
- l'établissement trimestriel d'un bilan provisoire et du compte de résultats ;
- l'arrêté du bilan annuel.

4.5.5.2. Département Contrôle de Gestion (DCG)

Il a pour principal mission de procéder à :

- la préparation et le suivi des budgets annuels de fonctionnement et d'investissement ;
- l'élaboration de tableau de bord mensuel ;
- le suivi de l'évolution des charges et des produits ;
- l'élaboration des indicateurs clés ;
- l'établissement d'un rapport trimestriel des réalisations budgétaires.

4.5.6. Département des systèmes et monétiques (DSIM)

Il est chargé de l'élaboration des procédures bancaires, du paramétrage de toutes les opérations de la banque, des modifications de cautions et des effets. Une cellule de digitalisation a été intégrée dont le rôle est de scanner les signatures pour les ouvertures des comptes. Elle compte deux départements à savoir : le département informatique et le département monétique et des produits technologiques.

4.5.6.1. Département Informatique

Il est chargé du traitement quotidien en temps réel et en différé des instructions financières. Il sert d'assistant aux utilisateurs et agences.

4.5.6.2. Département Monétique

Il tient à jour le tableau de bord des incidents de paiement et des solutions retenues du paramétrage et de la mise à jour des fichiers de base des développements spécifiques pour la banque.

4.5.7. Direction des opérations (DO)

Elle gère toutes les opérations du back-office et du service étranger à l'exception de celles du guichet.

4.5.8. Direction des Engagements et des Risques (DER)

Elle est chargée d'apprécier les opérations faites par les exploitants en fonction de la crédibilité du client et des grandes orientations de la banque avant d'émettre un avis. Afin de mieux exécuter sa mission, elle est constituée d'un secrétariat des engagements, d'un service gestion préventive des risques.

4.5.8.1. Secrétariat des engagements

Il s'occupe de l'administration et la mise en place du crédit. Il s'assure et inspecte de manière indépendante, que les concours ont bien été accordés selon les procédures d'autorisation en vigueur.

La mise en place du crédit consiste à la mise à disposition du crédit aux clients en créditant son compte par le débit d'un compte d'engagement en faveur du client.

Le remboursement des crédits se fait à partir des cash-flows générés par l'exploitation d'une entreprise et chez le particulier par prélèvement direct après virement sur son compte du salaire, de la pension ou autre revenu.

Les conditions de remboursement sont arrêtées avec les bénéficiaires et les bénéficiaires de crédits. La banque s'assure aussi que les concours devenus préoccupants font l'objet d'un déclassement, d'où la nécessité de certains contrôles. Il s'agit en effet des contrôles quotidiens et des contrôles périodiques.

Les contrôles quotidiens s'appliquent aux :

- débiteurs irréguliers de la veille ne disposant pas d'autorisation ;
- prêts sans autorisations correspondantes c'est-à-dire les dossiers de prêts pour lesquels un dossier d'autorisation n'a pas été trouvé (non saisi) avant la mise en place effective du concours.

Les contrôles périodiques quant à eux s'appliquent :

- au respect des dispositions prises en matière de crédit ;
- à la surveillance et le suivi des garanties.

4.5.9. Le Département de la gestion préventive des risques (DGPR)

Il s'occupe essentiellement du recouvrement des créances devenues préoccupantes du fait de la durée de l'impayé ou l'encours en situation irrégulière. En plus de sa mission principale qu'est le recouvrement, ce service s'occupe également de la régularisation des impayés en étudiant et en proposant des scénarios d'apurement. Pour se faire, il effectue certaines tâches qui sont :

- le suivi des impayés : il s'agit de faire une situation sur les prêts connaissant des difficultés au niveau du remboursement ;
- l'analyse des possibilités de recouvrement avec des propositions rééchelonnées (nouvelles échéances) de façon amiable.

Toutefois, il arrive que certains clients montrent de la mauvaise volonté ou un refus catégorique, alors les intimidations (convocations, menace de saisie etc.) deviennent obligatoires.

Les dossiers du Précontentieux connaissent généralement deux (02) issues après traitement :

- le client régularise sa situation ou s'engage sur un protocole d'accord qu'il respecte alors le dossier est reclassé sain ;
- le client n'arrive pas à honorer ses engagements, le dossier est alors déclassé en créances douteuses et litigieuses.

4.6. Département juridique

Il joue un rôle de conseiller juridique au sein de la banque. Ce département a pour attribution la prise de garanties, leur archivage, leur suivi, l'exécution des dossiers de succession (en cas de décès).

Conclusion

Le présent chapitre nous a permis de présenter la BOA-Mali à travers son historique, la répartition de son capital, ses différents produits mais aussi l'organisation qui a été mise en place pour lui permettre d'effectuer efficacement ses différentes activités et d'atteindre ses objectifs. Dans le chapitre suivant, nous allons présenter de façon synthétique le dispositif de maîtrise des risques opérationnels qui met l'accent sur le rôle joué par la fonction d'audit interne.

Chapitre 5 : LA GESTION DES RISQUES OPERATIONNELS : cas de la BOA-MALI

L'audit interne contribue à sensibiliser et former l'encadrement au contrôle interne mais n'est pas directement impliqué dans la mise en place et la mise en œuvre quotidienne du dispositif. Il a pour mission d'évaluer le fonctionnement des dispositifs de gestion des risques et de contrôle interne, d'en effectuer une surveillance régulière et de faire toute préconisation pour l'améliorer.

Le contrôle interne se manifeste par l'organisation, les méthodes et les procédures mise en place au niveau de chacune des activités de l'entreprise, pour maintenir la pérennité de celle-ci. Etant donc une composante essentielle de la gestion des risques et la finalité de l'audit interne, il joue un rôle prépondérant dans la sécurité de toute entreprise.

5.1. Les acteurs du contrôle interne et leurs missions

Nous donnerons sous cette section les rôles des acteurs du contrôle interne et leurs missions au sein de la BOA-Mali.

5.1.1. Le conseil d'administration

Le Conseil d'Administration est l'organe exécutif de la BOA-Mali, il jouit de toutes les prérogatives et regroupe en son sein les gros actionnaires de la société (ceux qui détiennent une part importante des actions).

Il nomme et révoque le Directeur Général, valide les grandes orientations de l'entreprise, fixe les objectifs fondamentaux, décide des réorganisations à opérer en vue de meilleures performances.

Les grandes décisions sont généralement issues des réunions tenues chaque année au plus tard au mois de mars.

En marge de ce conseil, se tient une assemblée des actionnaires au second trimestre de chaque année afin de présenter la situation de l'année écoulée aux différentes actionnaires de la banque.

5.1.2. La direction générale

Dirigée par le Directeur Général (DG), elle coordonne toutes les autres directions de la banque à travers ses différentes cellules. Ce sont :

- le conseiller DG ;
- le contrôle général ;
- le chargé de mission ;
- le secrétariat général ;
- les ressources humaines ;
- les moyens généraux ;
- le service contentieux.

Elle a pour rôle en matière de crédit, de donner son accord sur la base des propositions faites par les services compétents et de prendre des décisions de crédit qui lui sont déléguées. Elle s'occupe principalement de la gestion quotidienne des activités de l'établissement, et peut aussi convoquer un comité de crédit interne élargi.

5.1.3. Le contrôle général

Cette structure est répartie en trois départements à savoir :

- l'audit comptable et financier ;
- l'audit des services et suivi des procédures ;
- le contrôle des engagements.

Pour la bonne exécution des travaux assignés au titre du contrôle des comptes et des opérations le contrôle général dispose de trois (3) recueils de procédures élaborées par la direction de l'inspection du groupe. Ils sont intitulés comme le guide du contrôleur, de l'audit des services et des opérations bancaires et celui des contrôles de fonds.

Le contrôle général effectue des tâches au quotidien, mensuellement, annuellement et périodiquement.

Au quotidien il procède :

- au suivi des écarts d'encaisses en XOF et en devises étrangères au siège et dans les agences de provinces (excédents et manquants) ;
- à l'analyse des anomalies comptables à partir des états informatiques et suivi de leur régularisation ;
- au suivi de la position de change et de la formation du résultat de change ;
- au suivi des opérations remarquables dans le cadre de la lutte contre le blanchiment ;
- au traitement des demandes et réclamations de la clientèle, opérations bancaires et monétiques et enfin les interventions et recherches à la demande de la direction générale.

Mensuellement, il produit les tableaux de bord portant sur le contrôle des comptes selon le planning de la direction de l'inspection du groupe.

Annuellement, il contrôle les conditions, opérations et arrêtés de la clientèle, le rapport d'activité au conseil d'administration et à la commission bancaire.

Périodiquement, il effectue des :

- contrôles inopinés des caisses en XOF et en devises étrangères au siège et dans les agences ;
- contrôles inopinés des caisses DAB au siège et dans les agences ;
- contrôles de fonds et audit des services ;
- éditions des codes PIN ;
- contrôles des stocks des cartes monétiques non délivrées à la clientèle, contrôles des stocks des chéquiers domestiques et de correspondants bancaires ;
- des supervisions de la destruction des chéquiers et des cartes monétiques non retirés par la clientèle depuis plus de six mois ;
- enquêtes et le suivi des affaires frauduleuses ;
- contrôles des engagements ;
- contrôles des agios trimestriels ;
- contrôles des ratios prudentiels imposés par la banque centrale ;
- missions de contrôle dans les agences régionales, les rapports semestriels.

5.1.4. Le département compliance (conformité)

Le département de la conformité ou compliance s'occupe de :

- l'élaboration du compte rendu des travaux sur l'exploitation de l'état de surveillance des opérations remarquables,
- du contrôle de conformité des opérations d'ouverture de compte.

5.1.4.1. Le contrôle de gestion

Cette cellule est composée d'un agent qui produit quotidiennement à la direction générale une situation d'emplois /ressources et mensuellement une situation de charges et produits.

Il vérifie les imputations comptables afférentes aux frais généraux et effectue des calculs relatifs au budget et au plan triennal de développement. Il prépare sous l'autorité du Directeur Général l'analyse des comptes trimestriels présentée au conseil d'administration.

5.1.4.2. La cellule de rapprochement des comptes nostri et de suivi du résultat de change

Cette cellule est composée des agents qui exécutent les tâches de pointage des opérations, de suivi et de relances des suspens avec les correspondants bancaires à l'étranger ainsi que la vérification quotidienne de la formation du résultat de change.

5.1.4.3. La cellule de rapprochement des comptes de liaison siège /Agences

Cette cellule suit le dénouement des écritures comptables enregistrées dans les comptes de liaison réciproques Agences /siège.

Suite à la centralisation du système d'information (siège agences) des données saisies étant désormais en temps réel, l'essentiel des suspens est dénoué en 48h.

5.1.4.4. La cellule de suivi de la trésorerie

Cette cellule assure le suivi quotidien de la trésorerie de la banque et établit les reportings se rapportant à la gestion active- passif.

5.1.5. Le comité d'audit et des risques

Le Comité d'audit et des risques aide le Conseil d'administration à s'acquitter de ses responsabilités de surveillance de l'information financière, de la gestion des finances et des risques, du contrôle, des activités d'audit externe et des procédés appliqués par l'Ordre pour s'assurer de la conformité aux lois et règlements applicables. Ce comité examine les évolutions intervenues et émet des recommandations à cet effet. Le comité d'audit a un rôle critique dans l'amélioration de la qualité de l'audit. L'efficacité du comité d'audit et des auditeurs renforce la confiance du public dans l'intégrité de l'information financière.

Le comité d'audit joue un rôle essentiel dans la création d'un contexte propice à des audits de qualité. En effet, il est de la responsabilité du comité d'audit de créer un contexte favorisant la tenue d'un dialogue ouvert entre la direction et les auditeurs dans une culture d'intégrité, de respect et de transparence.

Le comité d'audit est aussi responsable de la surveillance des travaux des auditeurs. Entre autres, il doit comprendre la stratégie d'audit, voir à ce qu'elle prenne en compte les principaux risques d'audit et s'assurer que les auditeurs exercent suffisamment d'esprit critique. Ils doivent aussi vérifier que les auditeurs font preuve d'indépendance appropriée par rapport à la direction et qu'ils sont réellement objectifs. Ce faisant, le comité d'audit pourra tirer les conclusions quant à l'efficacité de l'audit.

5.1.6. La direction de l'inspection du groupe

La direction de l'inspection précise les différentes tâches du back office, les contrôles comptables à mener, les tableaux de bords à élaborer. Elle prévoit la confection d'un planning annuel de contrôles avec la transmission des comptes rendus mensuels à la direction de l'inspection et à la direction du groupe.

Elle élabore également les procédures opérationnelles du groupe BANK OF AFRICA.

Outre l'organisation du contrôle, la direction de l'inspection procède également sur place à des missions de vérification du contrôle, dispense des conseils, voir des formations aux contrôleurs

5.2. Les niveaux de contrôles

La collaboration avec les structures centrales notamment la Direction de l'Inspection, le contrôle général a permis de mettre en place des niveaux de contrôle permanents par différents niveaux de responsabilités hiérarchiques ainsi que des systèmes de validation des écritures.

5.2.1. Les agents opérationnels

Les agents opérationnels sont tenus de contrôler toutes opérations leurs incombant afin de s'assurer qu'elles ont été faites suivant les procédures et avec la plus grande prudence. Ce contrôle est appelé contrôle de premier niveau ou autocontrôle.

5.2.2. Les responsables hiérarchiques

Les responsables de département à leur niveau sont tenus de contrôler leurs collaborateurs quant à l'effectivité de l'autocontrôle devant être mené par les agents opérationnels, avant de valider les opérations effectuées dans le système d'information financière.

5.2.3. Le contrôle général

Le contrôle général s'assure que :

- les opérationnels exécutent les autocontrôles prévus ;
- les responsables hiérarchiques effectuent non seulement les autocontrôles à leur charge et vérifient ceux de leurs collaborateurs.

5.2.4. La direction générale

La direction générale prend des décisions correctives sur la base des travaux menés par le contrôle général.

5.2.5. Le conseil d'administration

Le conseil d'administration à son tour procède à l'évaluation des travaux effectués par la Direction Générale et les différentes directions de l'entreprise de concert avec le comité d'audit.

5.2.6. La direction des inspections

Faisant partie de BOA Groupe, elle effectue un contrôle sur les travaux menés par la direction générale et le contrôle général.

5.3. La gestion des risques opérationnels et l'audit interne

Comme toute institution bancaire, la BOA-Mali s'est dotée d'un dispositif de contrôle interne pour faire face aux risques et particulièrement aux (7) catégories de risques opérationnels édictées par le comité de Bâle II.

5.3.1. La fraude interne

Pertes dues à des actes visant à frauder, détourner des biens ou à contourner des règlements, la législation ou la politique de l'entreprise (à l'exception des atteintes à l'égalité et des actes de discrimination) impliquant au moins une partie interne à l'entreprise.

Afin de maîtriser la fraude interne, la BOA-Mali a mis en place les dispositifs de contrôle interne suivants :

- la mise en place d'un manuel de procédures décrivant chaque processus au sein de l'entreprise ;
- la séparation des tâches et des fonctions de la banque afin d'éviter des cumuls de tâches et de fonctions incompatibles ;
- l'autocontrôle et le système de validation par une personne différente de celle qui exécute ;
- le système de limitation d'accès à la base de données et à certains documents.

5.3.2. La fraude externe

Pertes dues à des actes visant à frauder, détourner des biens ou contourner la législation de la part d'un tiers.

La BOA-Mali situe la fraude externe à deux niveaux. Il s'agit donc de la fraude informatique et les fraudes sur les documents.

Exemple de fraude informatique : Une fraude sur des comptes clients a été commise par un tiers. Il se permet d'accéder dans les comptes de certains clients de la banque en faisant des transactions non autorisées ou proprement dit voler en infiltrant le réseau de la banque. De ce fait, les clients concernés se retrouvent victimes d'escroquerie et la banque risque un certain montant de perte occasionné par cet incident.

Les dispositifs pour palier la fraude informatique sont les suivants :

- opter pour un système de réseaux ;
- opter pour des pare feux afin d'empêcher les intrus d'accéder aux réseaux privés de la BOA ;
- impossibilité de connexion d'un appareil étranger à partir de l'intérieur de la banque ;
- impossibilité d'accès aux machines par ports USB.

Exemple de fraude sur les documents : faute de la négligence de contrôles des enregistrements journaliers des caissiers dans une agence du réseau de la banque. Une falsification des chèques a été détectée lors des visites des auditeurs internes dans cette agence. Grâce à la vérification de la cohérence entre des données informatiques et les pièces économiques c'est à dire la somme écrite sur le chèque est inférieure à celle enregistrée dans les outils informatiques. Ceci a généré des pertes financières pour la banque.

En ce qui concerne la fraude sur les documents la BOA a opté pour :

- la vérification locale ;
- les appels téléphoniques ;
- le système de sticker.

5.3.3. Pratiques en matière d'emploi et de sécurité sur le lieu de travail

Pertes résultant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, de demandes d'indemnisation au titre d'un dommage personnel ou d'atteintes à l'égalité/actes de discrimination.

Pour palier ce problème la banque s'est dotée de :

- d'une direction des ressources humaines (DRH) et d'une direction juridique, d'un comité d'hygiène et de sécurité ainsi que des comités syndicaux qui veillent au respect de la législation et des conditions de travail ;
- une infirmerie pour les premiers soins ;
- l'assurance maladie et retraite complémentaire.

5.3.4. Clients, produits et pratiques Commerciales (de pertes résultant d'une mauvaise prestation envers un client)

Pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients spécifiques (y compris les exigences en matière de confiance et de conformité) ou de la nature de conception d'un produit.

Pour éviter toute perte de cet ordre, la banque a pris les dispositions suivantes :

- mise en place d'une charte déterminant les engagements envers les clients ;
- fixation de critères de performances notamment de délai de traitements des dossiers ;
- fixation de bonnes pratiques de traitements des clients ;

5.3.5. Dommages aux actifs corporels

Destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres.

Pour palier un tel risque la banque s'est dotée :

- d'un site de secours ;
- d'un système de sécurité incendie ;
- d'une assurance sur le patrimoine de la banque ;
- d'un contrat d'entretien des actifs corporels de la banque.

5.3.6. Dysfonctionnement de l'activité et des systèmes

Les pertes résultant de dysfonctionnements ou de l'activité ou des systèmes.

Pour faire face à ces risques la banque s'est dotée :

- d'un plan de continuité d'activité ;
- et d'un site de secours.

5.3.7. Exécution, livraison et gestion des processus

Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs.

La banque s'est dotée de :

- un manuel de procédures concernant l'exécution de chaque tâche ;
- un service de moyens généraux qui suit les relations de la banque avec les prestataires externes ;
- une commission des marchés qui s'assurent que les acquisitions des biens et services se font dans les conditions optimales. (combien de personne le font, s'ils le font permanemment, les chaînes de validation, les exploitants qui doivent être formés).

5.4. Les dispositions de Bâle II sur les risques opérationnels

Conformément aux exigences du comité de Bale II, la BOA-Mali dispose d'un compte de provision pour risques et charges doté de 500 millions et de fonds pour risques bancaires généraux de 1300 millions.

5.5. L'appréciation du dispositif de contrôle interne

A l'instar d'autres institutions financières, la BOA-Mali a mis en place un dispositif de contrôle interne afin de s'assurer de la sauvegarde de son patrimoine. Il est donc important dans l'objectif de cette mission de s'assurer de l'existence effective de ce dispositif en question et de son application conforme par les agents de la banque.

Les tests que nous avons effectués ont révélé que la BOA Mali a mis en place un contrôle interne ainsi que des dispositifs dont les fonctionnements sont satisfaisants dans l'ensemble. Toutefois nous avons constaté qu'elle ne dispose pas encore de plan de continuité des activités.

Par ailleurs la cartographie des risques qu'elle a élaborée est partielle car ne porte que sur certain département de la banque.

5.6. L'apport de l'audit interne à la gestion des risques opérationnels

La gestion du risque opérationnel par l'audit interne se base sur les étapes suivantes :

5.6.1. L'identification du risque

Cela implique une définition claire et unique de la notion du risque opérationnel, tout en précisant avec détail le champ des risques qu'il couvre. A cet égard les départements d'Audit interne ne peuvent se lancer dans un tel travail, s'ils ne sont pas en mesure de connaître les activités, les objectifs et la stratégie de l'établissement de crédit, de réfléchir au-delà du cadre réglementaire et intégrer la réalité d'un environnement en très forte mutation, et enfin d'enrichir cette démarche en impliquant dans ce processus les responsables métiers et les opérationnels. L'identification des risques opérationnels liés à chaque activité se fait par l'intermédiaire des dispositifs de contrôle interne mis en place par la banque pour faire face aux risques. Il est donc important d'évaluer le contrôle relatif à chaque activité en vue de déceler les faiblesses afin d'améliorer ou de prendre les dispositions nécessaires pour y faire face.

Au regard des résultats, l'audit interne de la BOA-Mali recense les faiblesses du contrôle interne relatives à l'activité auditée à partir des risques identifiés. L'audit interne identifie donc les irrégularités et émet des recommandations qu'il soumet à la direction générale pour que ce dernier puisse prendre les dispositions nécessaires pour corriger les anomalies.

La gestion des risques ne doit pas se limiter uniquement à une simple identification, c'est-à-dire à un recensement plus ou moins exhaustif des risques potentiels et pertinents et à une analyse plus ou moins approfondie de leurs caractéristiques. Elle doit s'appuyer également sur une analyse pour mieux appréhender et estimer leurs probabilités de

survenance et la gravité de leurs impacts sur l'organisation comme nous l'indique les tableaux ci-dessous.

Tableau 3 : Echelle d'évaluation des risques

Gravité moyenne des conséquences	
5	Critique
4	Majeur
3	Important
2	Moyen
1	Mineur

Tableau 4 : Probabilité d'occurrence

Probabilité d'occurrence moyenne	
5	Très probable
4	Probable
3	Moyennement probable
2	Peu probable
1	Très peu probable

Source : Nous-mêmes

5.6.2. Une diffusion de la culture du contrôle interne vers les opérationnels :

Une fois que les risques identifiés sont cartographiés, hiérarchisés, et codifiés dans les procédures. L'étape suivante consiste à s'assurer que le dispositif de contrôle interne est efficace de façon continue et que le risque est correctement maîtrisé. Pour cela la mise en place des programmes d'auto-évaluation du dispositif apparait comme une nécessité, et les moyens de contrôle à mettre en œuvre seront de deux ordres :

- des check-lists (normatives) : des contrôles que doivent remplir périodiquement les opérationnels et qui leur rappellent les étapes essentielles à suivre. Ces check-lists peuvent être assimilées à des carnets de bord ;
- des indicateurs de contrôle clés de l'établissement : qui doivent être définis, en commun, entre l'audit interne et les responsables opérationnels, ces indicateurs peuvent être de deux natures (qualitative ou quantitative) ;

- Le suivi de ces indicateurs va permettre aux responsables opérationnels de détecter les erreurs, les anomalies et les dysfonctionnements qui peuvent causer d'énormes pertes et le cas échéant de prendre les mesures correctives nécessaires.

5.6.3. service d'Audit Interne

Dans ce contexte la fonction d'audit interne est assurée par un département expert qui pourra à tout moment disposer d'indicateurs (résultant des programmes d'auto évaluations) de mesure de la qualité des contrôles fondamentaux qui permettent de mesurer les risques clés.

5.6.4. L'auto évaluation du risque opérationnel

L'auto évaluation du risque est réalisée au niveau des contrôles de 1^{er} niveau. Elle consiste en l'examen et l'évaluation du contrôle interne et a pour objectif d'anticiper la dégradation d'un contrôle. La mise en œuvre de ce processus passe par les étapes suivantes :

- l'identification exhaustive préalable des dysfonctionnements potentiels (erreurs, irrégularités, fraudes) imputables au risques administratif et de leur source ;
- le recensement des faiblesses existantes de contrôle ;
- l'élaboration d'un programme d'auto évaluation du dispositif de contrôle.

Un programme d'auto évaluation du dispositif comprend :

- d'une part, l'élaboration et la mise en œuvre des check lists de contrôles que doivent remplir les opérationnels et qui leurs rappellent les étapes essentielles à suivre ;
- et d'autre part, la définition d'indicateurs de contrôles clés tant au plan qualitatif que quantitatif.

Finalement on peut dire, qu'une fois l'objectif du suivi régulier de la qualité des contrôles effectués et évalués par les opérationnels est atteint, on peut dire que la valeur ajoutée de l'audit interne réside dans sa capacité à :

- Présenter à la direction général et au comité d'audit une cartographie complète et actualisé des risques ;
- Piloter l'ensemble des dispositifs de contrôles définis à partir des risques clés ;

- Améliorer en continu ce dispositif sur la base des meilleures pratiques du secteur et des missions réalisées à partir d'un processus qualitatif de clignotants ;
- Promouvoir la culture du contrôle interne à tous les échelons de l'organisation ;

5.6.5. Suivi de l'évolution des risques et des plans d'actions

Tous les risques identifiés doivent faire l'objet d'un plan d'action réaliste visant à les réduire ou les supprimer. Il est toutefois utile, voire indispensable de dresser une synthèse des principales actions à mettre en œuvre en indiquant le délai maximum pour sa mise en œuvre. Le document unique permettra de rassembler l'ensemble des risques identifiés. Il doit être un outil dynamique qui s'enrichit lors de l'apparition de nouveaux risques liée à l'évolution des situations de travail (à défaut, il doit être actualisé au moins une fois par an).

Conclusion

L'audit interne joue un rôle capital dans la maîtrise des risques opérationnels à travers l'évaluation du contrôle interne.

L'audit interne est donc à la fois une intégrante de la gestion des risques mais aussi du contrôle interne. Ainsi nous pouvons dire que le management des risques englobe le contrôle interne qui à son tour englobe l'audit interne.

Chapitre 6 : ANALYSE DE LA CONTRIBUTION DE L'AUDIT INTERNE A LA GESTION DES RISQUES OPERATIONNELS

La gestion des risques est l'affaire de tous au sein de l'entreprise et se doit de couvrir l'ensemble des processus de l'entreprise de manière continue. C'est pourquoi son importance est capitale dans l'entreprise. L'entreprise pour gérer ses risques doit faire intervenir les différentes étapes de la gestion des risques permettant une maîtrise de ces derniers. Pour ce faire il est primordial pour la banque d'être en possession d'un dispositif de gestion couvrant tous les risques et notamment ceux opérationnels objet de cette étude.

Il est donc nécessaire de savoir si la banque possède un dispositif de gestion des risques opérationnels qui correspond à l'ensemble des moyens mis en place pour faire face aux risques.

L'audit interne est une source privilégiée d'informations, non seulement sur les nouvelles situations de risques, mais aussi sur la façon dont ils sont identifiés et ont été traités, de façon ponctuelle ou dans le cadre d'un programme global d'amélioration permanente. Ces contrôles permettent de suivre l'évolution des risques et d'éclairer les organes dirigeants sur la réalisation des objectifs du contrôle interne.

L'évaluation du contrôle interne est indispensable pour le traitement des risques existants ainsi que pour la détection des nouveaux ou incontrôlés. Ceci nous démontre la place et l'importance du système de contrôle interne efficace au sein de toutes organisations. Ce chapitre nous permettra de connaître l'état du dispositif de maîtrise des risques opérationnels de la banque ainsi que l'apport de la fonction d'audit interne quant à la maîtrise de ce dernier.

La BOA Mali a mis en place un dispositif de contrôle interne ; ces dernières années, elle a subi des malversations qui remettent en cause la pertinence des mesures prises. Nous avons procédé à une analyse du dispositif ; à faire ressortir le rôle de l'audit interne dans la gestion des risques opérationnels et enfin déterminer les faiblesses et faire des recommandations.

6.1. Le dispositif de gestion des risques opérationnels

Le chapitre précédemment étudié nous a permis de constater que la BOA-Mali a en place un dispositif de contrôle interne relatif à la gestion des risques opérationnels qui nous a permis de constater que la banque possède un manuel de procédure correctement mis en œuvre, des autocontrôles effectués plus ou moins par endroit, des mesures sécuritaires efficaces et appliquées. Toutefois on dénote une absence de politique formelle de gestion des risques à travers l'absence de plan de continuité d'activité et la présence d'une cartographie des risques qui sont l'essence même d'une bonne gestion des risques opérationnels.

Par ailleurs on ne peut pas affirmer qu'il n'existe pas de dispositif de gestion des risques dans la mesure où le département d'audit interne établit une cartographie des risques relative à chaque département dans le cadre de son audit de service.

6.1.1. L'analyse du dispositif de gestion des risques opérationnels

L'analyse du dispositif de gestion des risques opérationnels consiste à identifier les risques auxquels la banque est exposée, ainsi qu'à les mesurer en terme de probabilité et de fréquence afin d'apporter une réponse aux risques pour que l'entreprise puisse atteindre ses objectifs.

La BOA-Mali a donc mis en place des mesures de sécurité afin de s'assurer de la réduction de ces risques. Cette démarche traduit la volonté de la banque à réduire les risques à travers l'engagement continu des différents organes pour le suivi régulier de ces derniers. L'audit interne apparait donc comme l'un des facteurs importants dans la gestion des risques par le biais de la mise en place de la cartographie des risques par département lors de chaque mission d'audit. En effet l'audit interne identifie et évalue les risques auxquels l'entreprise est exposée et contribue à la mise en place de dispositifs adéquats afin de traiter le risque ou le réduire en fonction des objectifs de la banque. L'audit apparait donc comme l'outil incontournable dans la gestion des risques opérationnels dans la mesure où il évalue la pertinence du dispositif de contrôle interne relatif à chaque risque opérationnel.

6.2. Le rôle de l'audit interne dans le dispositif de gestion des risques opérationnels

Parmi toutes les entreprises existantes les banques sont celles connaissant des niveaux de risques les plus élevés eu égard à la manipulation des actifs financiers. Pour cette raison il est nécessaire de mettre en place un dispositif de management des risques permettant d'identifier ces risques et de prendre des mesures permettant de réduire leur impact. Le but de l'audit est donc de réduire le niveau de risque de façon à obtenir une assurance raisonnable du bon fonctionnement de la fonction ou du processus audité. Pour effectuer ce travail l'auditeur va baser sa démarche sur sa connaissance des objectifs de contrôle du domaine audité. Cependant ces derniers reposent sur la connaissance qu'il a des bonnes pratiques. Elles sont la base des règles de contrôle interne qu'il faut vérifier. L'audit est donc à la base de l'évaluation et de l'amélioration du contrôle interne. L'auditeur, va donc s'assurer que les règles de contrôle interne sont effectivement appliquées et donnent les résultats attendus.

A la BOA-Mali l'audit interne évalue le dispositif de contrôle interne relatif à la gestion des risques opérationnels afin de vérifier si réellement le dispositif mis en place correspond à une réponse aux risques, en d'autres termes si le dispositif est pertinent et efficace pour la gestion des risques. Cette évaluation passe par la vérification des opérations à travers les manuels de procédures, les réglementations et les normes en la matière pour apprécier le contrôle existant.

L'évaluation des risques est l'étape qui permet donc de se focaliser sur l'identification des différents risques de l'entreprise qui correspond à la première étape de la gestion des risques opérationnels qui à la fois permet de faire ressortir les faiblesses et les causes qui sont à l'origine des dits risques en vue d'y apporter une solution pour les réduire. L'audit interne évalue donc ces risques à travers leur probabilité de survenance ainsi que leur impact du risque en cas de survenance pour voir si le dispositif de contrôle permet de traiter le risque mais aussi savoir également si le dispositif en question est suffisant à lui seul pour traiter le risque et donc proposer des mesures pour conforter les autres risques.

6.2.1. Identification des risques opérationnels

L'audit interne à la BOA-Mali identifie les différents risques en découpant les activités en tâches élémentaires à travers une liste les énumérant. Ce travail préalable permettra de connaître les risques probables lorsqu'une tâche n'est exécutée dans le non-respect des procédures. En outre, cette identification est également basée sur une check-list qui énumère les risques relatifs aux différentes activités mais n'est pas mise à jour de façon permanente.

6.2.2. L'évaluation des risques

A la BOA-Mali, l'évaluation du dispositif de gestion des risques opérationnels consiste donc à voir si réellement le système de contrôle est pertinent et permet la réduction des risques opérationnels en d'autres termes de voir si le dispositif mis en place pour lutter contre la gestion des risques existe réellement et s'il est appliqué à tous les niveaux de la banque. La démarche de la banque ne donne aucune précision sur la quantification des risques. Nous constatons donc que la banque ne donne aucune analyse sur la sévérité du risque opérationnel pour l'appréciation de l'impact financier. Nous constatons donc qu'à la BOA-Mali, il existe un département compliance qui a en charge de vérifier si les procédures sont respectées à tous les niveaux de la banque et le département de prévention des risques qui n'est pas totalement opérationnel pour le moment qui se charge également de prévenir les risques potentiels auxquels la banque peut se trouver confrontée et prendre les dispositions nécessaires pour éviter que ces risques ne surviennent. L'audit interne à la BOA-Mali évalue les risques en termes de probabilité et d'impact pour mieux appréhender la criticité du risque, évaluer le dispositif mis en place pour maîtriser le risque.

6.2.3. Construction de la cartographie des risques

Pour mieux gérer un risque, il est important de l'identifier. En effet, la cartographie des risques s'avère importante dans la mesure où elle permet de cibler les risques à identifier en priorité. Dans la démarche de la BOA-Mali, nous remarquons que la banque s'est conformée à la typologie de risques opérationnels définie par le comité de Bâle et ce, dans le même ordre. Ceci est pertinent dans la mesure où, dans un premier temps, elle se conforme à la réglementation et dans un second temps, elle fait un découpage de ses activités de manière à les associer à la nomenclature de Bâle. Toutefois la BOA-Mali ne

dispose pas de cartographie des risques globale de l'entreprise. L'audit interne en fonction de ses missions d'audit ponctuelles établit la cartographie en fonction des départements.

6.2.4. Suivi de l'évolution des risques et des plans d'actions

Les plans offrent des références qui permettent d'évaluer la performance des résultats réels en tenant compte d'une évolution du contexte. L'audit interne à la BOA-Mali n'intervient pas dans la mise en œuvre des plans d'actions afin de gérer les risques opérationnels, car non prévus dans la charte. L'audit interne comme nous le rappelle les normes 2500 de l'IIA relatives à la surveillance des actions de progrès s'assure du degré de mise en œuvre des recommandations antérieures sur l'état du dispositif de contrôle interne et l'évolution des risques précédemment identifiés pour bien situer son champ d'intervention lors de la prochaine mission.

6.2.5. La démarche d'auto évaluation des risques et des contrôles

Il est pertinent de commencer toute démarche ou tout processus de gestion des risques opérationnels par une première évaluation des risques et contrôles. Cette technique est d'ailleurs utile à l'évaluation de l'efficacité du contrôle interne dans la mesure où un diagnostic du dispositif existant est indispensable pour déceler les forces et faiblesses du dispositif. Le fait pour la banque d'effectuer cette première évaluation de son dispositif est donc important dans le processus de gestion de ses risques opérationnels dans la mesure où elle donne aux opérationnels un rôle de premier plan dans la cartographie des risques. Nous constatons que :

- l'auto-évaluation permet à la banque de renforcer les procédures en cas de nécessité pour réduire le niveau de risque opérationnel ;
- la fréquence de l'auto-évaluation est faible et est faite annuellement ;
- l'audit interne intervient dans l'auto-évaluation des risques en tant que facilitateur ayant une large connaissance des processus de contrôle interne.

6.2.6. Promotion d'une culture éthique au sein de l'organisation

Il existe un code de conduite à la BOA-Mali applicable à tout le personnel. Ce document relate les attentes de l'entreprise en matière d'éthique au sein de la structure. L'audit

interne veille à la bonne application de ces règles à travers des missions à la demande de la direction générale.

6.3. Recommandations

6.3.1. A l'endroit du département d'audit interne

Recommandation 1 : mettre en place une cartographie des risques couvrant toutes les fonctions de l'entreprise afin d'avoir une vue sur tous les risques de la banque mais aussi permettre la performance du contrôle interne et veiller à sa mise à jour régulière.

Recommandation 2 : susciter l'élaboration d'un plan de continuité d'activité qui permettra à l'entreprise de faire face aux risques environnementaux comme la crise sociopolitique de 2012.

Recommandation 3 : planifier un audit de la sécurité du système d'information de la banque de façon régulière conformément aux recommandations de Bâle II.

Recommandation 4 : au regard de l'importance de l'audit interne il est primordial de se doter des ressources humaines suffisantes en la matière afin de couvrir tout le programme annuel.

Recommandation 5 : scinder le département d'audit et du contrôle permanent en deux afin de faire face aux exigences de la commission bancaire.

Accroître les contrôles inopinés afin de dissuader des fraudes et de détecter celle déjà réalisées.

6.3.2. A l'endroit de la direction générale

Recommandations 7 : rendre opérationnel le plutôt possible le département de prévention des risques qui permettra de conforter le département d'audit interne.

Recommandation 8 : en vue de faire face aux risques opérationnels, situations qui peuvent altérer la confiance des clients vis-à-vis d'elle, la banque gagnerait à mettre en œuvre des dispositifs de suivi des risques opérationnels.

Recommandation 9 : renforcer le dispositif de gestion afin de rendre la gestion des risques opérationnels plus rigoureuse. Aussi, le dispositif de gouvernement d'entreprise doit plus impliquer le comité d'audit qui doit également jouer un rôle important dans la surveillance des risques opérationnels

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

CONCLUSION GENERALE

La gestion du risque opérationnel constitue une des préoccupations majeures des dirigeants des institutions financières pendant ces dernières années. En effet, plusieurs champs de sa gestion sont encore à explorer et à découvrir alors que les autorités réglementaires mettent de la pression pour une quantification rigoureuse du capital risque opérationnel.

L'audit interne donne à toute organisation une assurance sur le degré de maîtrise des opérations, lui apporte des conseils pour améliorer ses activités. Il permet ainsi à l'entreprise d'atteindre ses objectifs dans la mesure où il évalue par une approche systématique et méthodique, ses processus de management des risques, de contrôle et de gouvernement d'entreprise en faisant des propositions pour renforcer leur efficacité. Cette définition nous pousse à affirmer alors que l'audit interne tient un rôle important dans la gestion de ces risques opérationnels.

Dans ce mémoire, nous avons démontré la maîtrise des risques opérationnels par l'audit interne. Nous avons pu expliquer que l'Audit interne a une responsabilité majeure dans la validation des démarches de nature qualitative permettant de réaliser une cotation des risques et des contrôles. Cette gestion requiert aussi les compétences des auditeurs internes ainsi que leur méthode d'intervention.

Nous avons essayé dans le cadre de notre mémoire d'évaluer le dispositif de gestion des risques opérationnels de la banque par l'intermédiaire de la fonction d'audit interne. Pour ce faire, nous avons effectué dans un premier temps, une revue de littérature qui nous a permis de nous imprégner du rôle de l'audit interne dans la gestion des risques opérationnels. Dans un second temps, nous avons présenté l'évaluation des risques opérationnels par l'audit interne.

Cette évaluation nous a permis de voir que la BOA présente un certain nombre de forces et de faiblesses liée au dispositif de gestion des risques opérationnels.

- Au plan des forces nous avons vu que, la banque possède un dispositif de contrôle interne présent à tous les niveaux de la structure permettant ainsi de réduire les risques opérationnels.
- Au plan des faiblesses, nous avons constatés que la banque présente un certains nombre d'insuffisance à savoir l'absence d'une cartographie des risques

opérationnels qui est l'essence même de la gestion des risques opérationnels, l'absence d'un plan de continuité des activités.

Au regard de ces insuffisances, pour contribuer efficacement à la gestion des risques opérationnels, l'audit interne doit :

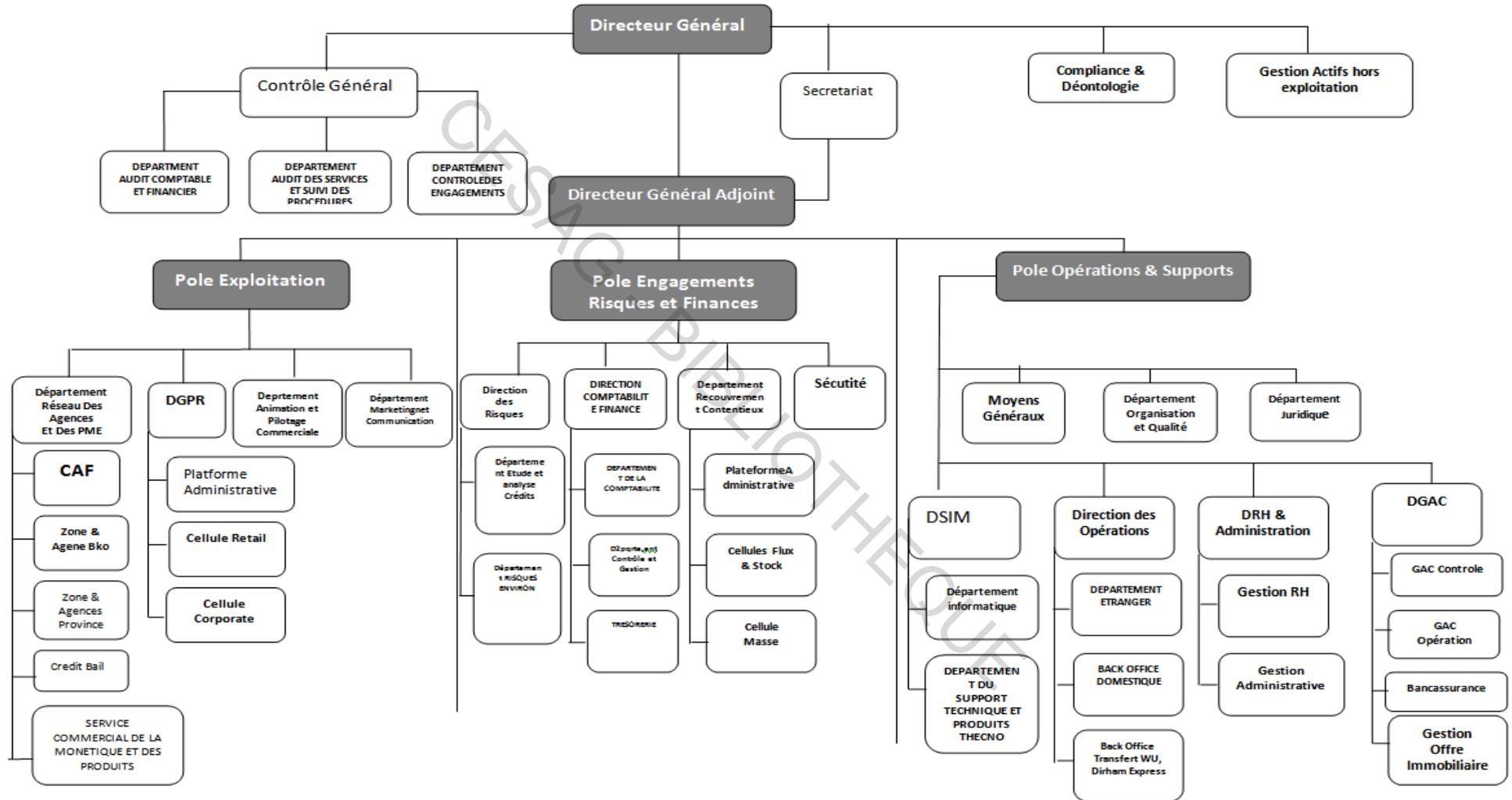
- solliciter la mise en place d'une cartographie des risques opérationnels ;
- solliciter l'élaboration d'un plan de continuité d'activité ;
- solliciter l'application des exigences de la commission bancaire ;
- planifier un audit de la sécurité du système d'information de la banque de façon régulière conformément aux recommandations de Bâle II ;
- accroître les contrôles inopinés afin de dissuader des fraudes et de détecter celle déjà réaliser ;
- accroître les contrôles inopinés afin de dissuader des fraudes et de détecter celle déjà réaliser ;
- se doter des ressources humaines suffisantes en la matière afin de couvrir tout le programme annuel.

La mise en place de ses recommandations permettra au département d'audit interne de la BOA de contribuer efficacement à la gestion des risques.

CESAG - BIBLIOTHEQUE

ANNEXES

Annexe 1 : Organigramme de la BOA-Mali 2012



Annexe 2 : Test d'existence du contrôle interne

N ^o	Eléments	Oui	Non	Observations
01	Existe-t-il un manuel de procédures au sein de la banque ?	X		
02	la séparation des tâches et des fonctions existe-t-elle dans la banque ?	X		
03	l'autocontrôle existe-t-il ?	X		
04	Existe-t-il un système de limitation d'accès à la base de données et à certains documents ?	X		
05	Existe-t-il un système de réseaux ?	X		
06	Existe-t-il des pare feu afin d'empêcher les intrus d'accéder au système d'exploitation ?	X		
07	Existe-t-il un moyen de connexion d'un appareil étranger à partir de l'intérieur de la banque ?	X		
08	Existe-il un système d'accès des ports USB ?	X		
09	Existe-t-il la vérification locale des documents ?	X		
10	Existe-t-il des appels téléphoniques pour s'assurer de la vraisemblance des documents ?	X		
11	Existe-t-il le système de sticker ?	X		
12	Existe-t-il une charte déterminant les engagements envers les clients ?	X		
13	Existe-t-il un délai de traitements des dossiers ?	X		
14	Existe-t-il les conditions de traitements des clients ?	X		
15	Existent-t-ils un service marketing, une direction de l'exploitation commerciale et de développement et le département de l'animation commerciale ?	X		
16	Existent-t-ils des sites de secours ?	X		
17	Existe-t-il un système de sécurité avec les	X		

	extincteurs ?			
18	Existe-t-il l'assurance globale des banques ?	X		
19	Existe-t-il un contrat d'entretien ?	X		
20	Existe-t-il un service de moyens généraux qui suit les relations de la banque avec les prestataires externes ?	X		
21	Existe-t-il un système d'approvisionnement dans les conditions optimales ?			
22	Existe-t-il une commission des marchés qui s'assure que les acquisitions des biens et services se font dans les conditions optimales ?	X		
23	Existent-ils une direction des ressources humaines, un comité d'hygiène et de sécurité ainsi que des comités syndicaux qui veillent au respect de la législation et des conditions de travail ?	X		
24	Existe-t-il une infirmerie pour les premiers soins	X		
25	Existent-ils une assurance maladie et retraite complémentaire ?	X		
26	Existe-t-il une cartographie des risques et un plan de continuité d'activité		X	

Annexe 3 : Test d'application du contrôle interne

N ^o	Eléments	Oui	Non	Observations
01	Les procédures au sein de la banque sont elles bien appliquées?	X		
02	la séparation des tâches et des fonctions est elle respectées dans la banque ?	X		
03	l'autocontrôle est il effectué?	X		Le contrôle interne est effectué par endroit au sein de la banque et ne concerne pas toutes opérations.
04	Le système de limitation d'accès à la base de données et à certains documents est il respecté ?	X		
05	Le système de réseaux est il mis en place et fonctionne t-il normalement ?	X		
06	les pare-feu afin d'empêcher les intrus d'accéder au système d'exploitation fonctionnent-ils ?	X		
07	Existe t-il un moyen de connexion d'un appareil étranger à partir de l'intérieur de la banque ?	X		
08	Le système de non accès des ports USB est il respecté ?	X		
09	la vérification locale des documents est elle effectuée ?			
10	les appels téléphoniques pour s'assurer de la vraisemblance des documents sont ils respectés ?	X		
11	le système de sticker est il respecté?	X		
12	la charte déterminant les engagements envers les clients est elle mise en application ?	X		
13	Le délai de traitements des dossiers est il respecté ?	X		
14	les conditions de traitements des clients sont elles respectées ?	X		
15	Le service marketing, la direction de l'exploitation	X		

	commerciale et de développement et le département de l'animation commerciale effectuent-ils leurs tâches convenablement ?			
16	Les sites de secours fonctionnent-ils convenablement?	X		
17	Le système de sécurité avec les extincteurs fonctionne-t-il ?	X		
18	l'assurance globale des banques est-elle respectée ?	X		
19	Existe-t-il un contrat d'entretien et le contrat est-il exécuté convenablement?	X		
20	Le service de moyens généraux suit-il les relations de la banque avec les prestataires externes ?	X		
21	le système d'approvisionnement est-il effectué dans les conditions optimales ?	X		
22	la commission des marchés s'assure-t-elle que les acquisitions des biens et services se font dans les conditions optimales ?	X		
23	La direction des ressources humaines, le comité d'hygiène et de sécurité ainsi que des comités syndicaux veillent-ils au respect de la législation et des conditions de travail ?	X		
24	L'infirmerie pour les premiers soins fonctionne-t-elle ?	X		
25	L'assurance maladie et retraite complémentaire sont-elles respectées ?	X		
26	la cartographie des risques opérationnels couvre-t-elle toutes les fonctions de l'entreprise		X	La cartographie des risques est parcellaire car elle ne couvre pas toutes les fonctions de l'entreprise.

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

❖ **Ouvrages**

1. AHOANGANSI Evariste (2010), *Audit et révision des comptes : aspects internationaux et espace OHADA*, Edition Mondexperts, 2^{ème} édition, 921 pages.
2. BARBIER Etienne (1996), *permanence et actualité*, Editions d'organisation, paris, 211 pages.
3. BARTHELEMY Bernard, COURREGES Philippe (2004), *Gestion des risques : méthodes d'optimisation globale*, 2^{ème} édition, Edition d'Organisation, Paris, 471 pages.
4. BERTIN Elisabeth (2007), *Audit interne : enjeux et pratiques à l'international*, Edition d'Organisation Eyrolles, 2007, 307 pages.
5. CAMARA Lucien (2006), *La gestion des risques en microfinance : comment gérer avec efficacité les risques d'une institution de microfinance*, Edition Plantation, Abidjan, 176 pages.
6. COLLINS Lionel & VALIN Gérard (1992), *audit et contrôle interne : aspect financiers, opérationnels et stratégique*, 4^e Edition édition Dalloz, 373 pages.
7. CORDEL Frédéric, LEBEEGUE Daniel (2013), *Gestion des risques et contrôle interne : de la conformité à l'analyse décisionnelle*, Edition Vuibert, Paris, 287 pages.
8. DE COUSSERGES Sylvie (2007), *Gestion de la banque : du diagnostic à la stratégie*, 5^e édition, Edition Dunod, Paris, 272 pages.
9. DE MARESCHAL Gilbert (2003), *la cartographie des risque*, Edition AFNOR, Paris 45 Pages.
10. DE MARESCHAL Gilbert (2003), *La cartographie des risques*, Edition AFNOR, Paris, 45 Pages.
11. GRAND Bernard (1998) *theoretical approaches to audit, internal Auditing*, 3^e Edition, CNCC édition, Londres, 231 pages.
12. GREEN WALD.R.N (1990), *an internal auditor's guide to self management, the internal auditor*, 2^e Edition, edition john Wiley & Sons Inc USA, 178 pages.
13. GREUNING Van Henri, BRAJOVIC-BRATANOVIC Sonia, ROZERBAUM Marc (2004), *Analyse et gestion du risque bancaire : un cadre de référence pour*

l'évaluation de la gouvernance d'entreprise et du risque, Edition ESKA, Paris, 386 pages.

14. IFACI (2007), *Référentiel Professionnel de l'audit interne*, Edition IFACI certification, 27 pages.
15. Institute Of Internal Auditor, (IIA), *Normes pour la pratique professionnelle de l'audit interne* (2004), The institute of internal auditors, Florida, 28 pages.
16. JIMENEZ Christian, MERLIER Patrick, CHELLY Dan (2008), *Risques opérationnels : de la mise en place du dispositif à son audit*, Revue Banque Edition, Paris, 271 pages.
17. KEREBEL Pascal (2009), *Management des risques : inclus secteurs Banque et Assurance*, Edition d'Organisations, Paris, 187 pages.
18. LEMANT olivier (1999), *Créer, organiser et développer l'audit interne*, Edition Maxima, Paris 177 Pages.
19. MASSELIN Jean-Luc, MADERS Henri-Pierre (2014), *Contrôle interne des risques : Cibler-Evaluer-Organiser-Piloter-Maîtriser*, Edition Eyrolles, Paris, 261 pages.
20. MONNIER Philippe, MAHIER-LEFRANCOIS Sandrine (2013), *Les techniques bancaires en 53 fiches : pratiques et applications corrigées*, Edition Dunod, Paris, 340 pages.
21. OUANICHE Mikael (2009), *La fraude dans l'entreprise : comment la prévenir, la détecter et la combattre*, Edition Maxima, Paris, 221 Pages.
22. RENARD Jacques (2004), *théorie et pratique de l'audit interne ; 5^e Edition*, Editions d'organisation, 422 pages.
23. RENARD Jacques (2010), *Théorie et pratique de l'audit interne*, 7^e édition, Edition d'organisation 469 Pages.
24. SARDI Antoine (2002), *Audit et contrôle interne bancaire*, Editions AFGES, Paris 1065 pages.
25. SARDI Antoine (2002), *Audit et contrôle interne bancaire*, Edition AFGES, Paris, 1065 pages.

26. SCHICK Pierre, VERA Jacques, BOURROUILH-PAREGE Olivier (2010), *Audit et référentiel de risques : gouvernance, management des risques, contrôle interne*, Edition Dunod, Paris, 339 pages.
27. IFACI(2013), cadre de référence international des pratiques professionnelles de l'audit interne, Edition IFACI certification, 237pages.

28.

❖ **Revue**

29. DUMONT Philippe (2007), Les perspectives de l'audit interne conduisent à la diversité du recrutement et des profils, *Revue Française de l'Audit Interne* (N°187) : 24-30.

❖ **Sources internet**

30. Banque de France (2014), le risque opérationnel : pratique et perspective réglementaire.
http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/documents/racb2003-le-risque-operationnel.pdf
31. Comité Bâle sur le contrôle bancaire (2014), Saines pratiques pour la gestion et la surveillance du risque opérationnel. <http://www.bis.org/publ/bcbs96fre.pdf>