



Centre Africain d'études Supérieures en Gestion

**Institut Supérieur de
Comptabilité, de Banque et de
Finance**

**Diplôme d'Etudes Supérieures
Spécialisées en Audit et Contrôle
de Gestion**

**Promotion 22
(2010-2011)**

Mémoire de fin d'étude

THEME

**AUDIT DU SYSTEME DE MANAGEMENT DES
RISQUES OPERATIONNELS LIES AUX DEPOTS
BANCAIRES: CAS DE LA BANQUE ATLANTIQUE
DU SENEGAL**

Bibliothèque du CESAG



Présenté par :

Dirigé par :

NGNEUTCHOUE KOUSOK Gaëlle

- **M. Abdoulaye FALL**
Directeur de l'audit interne à la Banque
d'Investissement et de Développement de la
CEDEAO (BIDC)
- **M. Alpha SY**
Directeur de l'audit interne à la Banque
Atlantique Sénégal

2011

DEDICACES

Ce mémoire est dédié à :

- DIEU en qui j'ai puisé la force d'avancer malgré toutes les difficultés rencontrées ;
- mes grandes sœurs Ariane et Jocelyne KOUSOK rappelées à DIEU le 02 Avril 2011 ;
- mes parents Marie Gisèle et Thomas KOUSOK, ainsi que mes frères et sœurs Elvire, Clovis, Cédrick, Donatien et Léna KOUSOK pour leur amour, leur soutien et surtout leurs prières.

CESAG - BIBLIOTHEQUE

REMERCIEMENTS

Ce mémoire est le fruit de ma formation au Centre Africain d'Etudes Supérieures en Gestion (CESAG) et d'un stage à la Banque Atlantique du Sénégal (BASN). Il n'a été possible que grâce à la compréhension, la disponibilité, et à la parfaite collaboration de plusieurs personnes. Qu'il me soit permis de leur exprimer ici, mes vifs remerciements et ma profonde gratitude. Il s'agit de :

- mes encadreurs Monsieur Abdoulaye FALL et Monsieur Alpha SY pour leur disponibilité et leurs orientations dans mes travaux de recherche ;
- messieurs El Hadj Malick NDOYE et N'GARY SOW auditeurs internes et enseignants au CESAG, pour leurs encouragements et précieux conseils ;
- tout le personnel de la Banque Atlantique Sénégal, en particulier les agents de la direction d'audit et de contrôle, à savoir Mesdames Rosine TCHANGAI et Mariama DIALLO, et Messieurs Mamadou SADIO, Hervé MAMA et El Hadj Mamadou SECK. ;
- tout le corps professoral du CESAG sans lequel je ne saurais prétendre à ce niveau de formation ;
- tous ceux dont les noms ne figurent pas et qui, de loin ou de près, m'ont aidé à mener à bien la rédaction de ce mémoire, qu'ils trouvent en ce travail l'expression de toute ma reconnaissance.

LISTE DES SIGLES ET ABREVIATIONS

AMA	: Advanced management Approach - approche des mesures dites avancées
BASN	: Banque Atlantique du Sénégal
BIA	: Basic Indicator Approach - Approche indicateur de base
BIP	: Bons à Intérêt Progressif
CEMAC	: Communauté Economique et Monétaire de l'Afrique Centrale
COSO	: Committee of Sponsoring Organizations of the Treadway Commission
CRBF	: comité de la réglementation bancaire et financière
FRAP	: Feuille de Révélation et d'Analyse de Problèmes
GI	: Gross Income - produit net bancaire
IFACI	: Institut Français de l'Audit et du Contrôle Interne
IIA	: Institute of Internal Auditors
LEP	: Livrets d'Epargne Populaire
OPCVM	: organismes de placement collectif en valeurs mobilières
PEL	: Plans d'Epargne Logement
PEP	: Plans d'Epargne Populaire
SA	: Standardised approach – approche standardisée
SWIFT	: Society for Worldwide Interbank Financial Telecommunication – réseau de télécommunication financières interbancaires mondiales.
TaRiR	: Tableau des Risques référentiel
TCN	: Titres de Créances Négociables
UEMOA	: Union Economique et Monétaire Ouest Africain

LISTE DES FIGURES ET TABLEAUX

Liste des figures

Figure 1 : Le champ du risque bancaire	11
Figure 2 : Classification des dépôts bancaires	19
Figure 3 : Le système de management des risques opérationnels bancaires.....	28
Figure 4 : Processus d'identification des risques opérationnels.....	30
Figure 5 : Cartographie des risques.....	32
Figure 6 : Approche quantitative de gestion des risques opérationnels	34
Figure 7 : Modèle d'analyse.....	42

Liste des tableaux

Tableau 1 : Classification des risques opérationnels bancaires.....	15
Tableau 2 : Classification des risques opérationnels bancaires (suite et fin).....	16
Tableau 3 : Tableau des Risques référentiel (TaRiR)	68
Tableau 4 : Les tests à effectuer	71

LISTE DES ANNEXES

Annexe 1 : Organigramme de la Banque Atlantique du Sénégal.....	84
Annexe 2 : Légende du flow-chart de description de processus de collecte de fonds	85
Annexe 3 : Questions posées au cours des entretiens	86
Annexe 4 : Questionnaire sur les stratégies de couverture des risques opérationnels liés aux dépôts bancaires	88
Annexe 5 : Questionnaire sur l'identification et l'analyse des risques	94

CESAG - BIBLIOTHEQUE

TABLE DES MATIERES

DEDICACES	i
REMERCIEMENTS	ii
LISTE DES SIGLES ET ABREVIATIONS	iii
LISTE DES FIGURES ET TABLEAUX	iv
LISTE DES ANNEXES.....	v
TABLE DES MATIERES	vi
INTRODUCTION GENERALE.....	1
PREMIERE PARTIE: CADRE THEORIQUE.....	7
CHAPITRE 1 : LES RISQUES OPERATIONNELS LIES AUX DEPOTS BANCAIRES	9
1.1. La notion de risque bancaire et de risque opérationnel en particulier	9
1.1.1. Quelques concepts	9
1.1.1.1. Le risque	9
1.1.1.2. Le risque bancaire.....	10
1.1.2. Les composantes du risque opérationnel.....	13
1.1.2.1. Les risques liés au système d'information :	14
1.1.2.2. Les risques liés aux processus	14
1.1.2.3. Les risques liés aux personnes.....	14
1.1.2.4. Les risques liés aux évènements extérieurs	14
1.1.3. Classification des risques opérationnels.....	14
1.2. Notion de dépôts bancaires.....	17
1.2.1. L'activité bancaire	17
1.2.1.1. La réception des fonds du public.....	17
1.2.1.2. Les opérations de crédit.....	17
1.2.1.3. La mise à la disposition du public des moyens de paiement.....	17
1.2.2. Les dépôts bancaires.....	18

1.2.2.1. Les dépôts ordinaires	19
1.2.2.2. Les dépôts à vue	19
1.2.2.3. Les dépôts sur comptes d'épargne.....	21
1.3. Les risques opérationnels pouvant survenir au cours des opérations de dépôts bancaires.....	22
1.3.1. La fraude interne.....	22
1.3.2. La fraude externe.....	22
1.3.3. L'insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail.....	23
1.3.4. Les clients, les produits et les pratiques commerciales	23
1.3.5. Les dommages aux actifs physiques.....	24
1.3.6. Le dysfonctionnement de l'activité et des systèmes.....	24
1.3.7. Les dysfonctionnements des processus de traitement	24
CHAPITRE 2 : LE SYSTEME DE MANAGEMENT DES RISQUES OPERATIONNELS LIES AUX DEPOTS BANCAIRES	25
2.1. Les bonnes pratiques en matière de management des risques opérationnels....	25
2.2. Le système de management des risques opérationnels	27
2.2.1. L'identification des risques	28
2.2.1.1. Les lignes métiers	29
2.2.1.2. Les processus.....	30
2.2.2. L'approche qualitative.....	31
2.2.3. L'approche quantitative.....	32
2.2.3.1. Observation des historiques d'incidents.....	33
2.2.3.2. Représentation du phénomène à partir d'une loi statistique.....	33
2.2.3.3. Définition de la probabilité pour l'ensemble des résultats possibles... 33	
2.2.4. Définition du niveau de risque acceptable.....	34
2.2.5. Mise en place de stratégie de couverture.....	35
2.2.5.1. Le contrôle interne.....	35

2.2.5.2. Le dispositif d'assurance	36
2.2.5.3. Le recours à l'emprunt.....	37
2.2.5.4. L'externalisation (outsourcing)	37
2.2.5.5. L'automatisation des transactions	37
2.2.5.6. La franchise	37
2.2.5.7. Les financements alternatifs	37
2.2.5.8. Les captives (filiales de réassurance)	38
2.2.6. Evaluation du risque net ou risque résiduel.....	38
2.2.6.1. Les risques attendus.....	38
2.2.6.2. Les risques exceptionnels	38
2.2.6.3. Les risques catastrophes	39
2.2.7. Le reporting	40
CHAPITRE 3: METHODOLOGIE DE L'ETUDE.....	41
3.1. Modèle d'analyse	41
3.1.1. La phase d'étude.....	43
3.1.1.1. La prise de connaissance générale de l'organisation et du processus de collecte des fonds	43
3.1.1.2. L'élaboration du tableau des risques référentiel (TaRiR)	43
3.1.2. La phase de vérification.....	44
3.1.3. La phase de conclusion.....	45
3.2. Outils de collecte et d'analyse des données.....	45
3.2.1. L'entretien	45
3.2.2. L'analyse documentaire.....	45
3.2.3. L'observation.....	45
3.2.4. Le questionnaire	46
DEUXIEME PARTIE : CADRE PRATIQUE.....	48
CHAPITRE 4 : PRESENTATION DE LA BANQUE ATLANTIQUE DU SENEGAL	50

4.1. Historique.....	50
4.2. Missions	50
4.3. Produits	51
4.3.1. Collecte de l'épargne	51
4.3.2. Opérations de crédit.....	51
4.3.3. Moyens de paiement.....	51
4.3.4. Monétique.....	52
4.3.5. Bancassurance	52
4.3.6. Les autres services	52
4.3.6.1. Inter médiation financière.....	52
4.3.6.2. ANET	53
4.3.6.3. SMS Banking.....	53
4.3.6.4. Transfert d'argent	53
4.3.6.5. Guichets automatiques de Banque.....	53
4.3.6.6. Terminaux de paiement électronique (TPE).....	53
4.4. Organisation.....	53
4.4.1. La Direction Générale	54
4.4.2. La Direction de l'Audit Interne	54
4.4.3. La Direction des risques	55
4.4.4. La Direction financière et comptable	55
4.4.5. La Direction des opérations.....	55
4.4.6. La Direction de la clientèle entreprise.....	55
4.4.7. La Direction de la Clientèle Particuliers et du Réseau	55
4.4.8. La Direction de la trésorerie	56
CHAPITRE 5 : L'AUDIT DU SYSTEME DE MANAGEMENT DES RISQUES OPERATIONNELS LIES AUX DEPOTS AU SEIN DE LA BANQUE ATLANTIQUE DU SENEGAL.....	57
5.1. Le processus de collecte des fonds	57

5.1.1.	Ouverture des caisses.....	57
5.1.2.	Versement des espèces et enregistrement de l'opération	58
5.1.3.	Enregistrement de l'opération	59
5.1.4.	Versement dans la caisse principale	59
5.1.5.	Versement à la BCEAO.....	60
5.1.6.	Fermeture provisoire de la caisse	61
5.1.7.	En cas de manquant ou d'excédent de caisse	61
5.2.	La gestion des risques opérationnels au sein de la Banque Atlantique du Sénégal	62
5.2.1.	Le contrôle interne.....	62
5.2.1.1.	Le personnel de la caisse	63
5.2.1.2.	Le gardiennage	63
5.2.1.3.	La sécurité des locaux.....	63
5.2.1.4.	La sécurité des fonds déposés.....	64
5.2.2.	Le dispositif d'assurance	66
CHAPITRE 6 : RESULTATS ET RECOMMANDATIONS		67
6.1.	Les résultats	67
6.1.1.	L'élaboration du tableau des risques référentiel (TaRiR)	67
6.1.2.	Les tests	71
	Source : nous-mêmes à partir de SCHICK (2007 : 84).....	71
6.1.3.	Présentation des forces et des faiblesses du système de management des risques opérationnels liés aux dépôts bancaires	72
	Source : nous-mêmes à partir de SCHICK (2007 :89).....	73
6.1.4.	Elaboration des Feuilles de Révélation et d'Analyse des Problèmes (FRAP)	74
6.2.	Recommandations.....	75
6.2.1.	Gestion des risques opérationnels formalisée.....	75
6.2.2.	Analyse des pertes survenues dans la banque	76

6.2.3. La sécurité des espèces et des chèques reçus par les caissiers	76
6.3. Sécurité lors des versements à la caisse principale.....	77
6.4. Sécurité des espèces dans la caisse principale (la réserve).....	77
CONCLUSION GENERALE.....	81
ANNEXES	83
BIBLIOGRAPHIE	95

CESAG - BIBLIOTHEQUE

CESAG - BIBLIOTHEQUE

INTRODUCTION GENERALE

Les scandales qui ont éclaboussé le monde économique ces dernières années, ont mis en évidence les failles du système financier mondial. En effet, des événements tels que la crise des subprimes de 2007, engendrée par une mauvaise gestion des prêts hypothécaires, ou les prises de position frauduleuses sur des contrats à terme par un opérateur de marché, en janvier 2008, à la société générale ont ainsi révélé la fragilité des dispositifs de maîtrise des risques en vigueur dans les marchés et établissements financiers.

D'après l'Institute of Internal Auditors (I.I.A.) et l'IFACI (in SCHICK; 2007: 12), le risque est la « possibilité qu'il se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs».

Dans le domaine bancaire, les risques peuvent résulter de l'évolution normale du système financier mondial (concurrence, sophistication croissante des produits financiers, innovations technologiques). Ils peuvent aussi provenir de défaillances des processus, des technologies utilisées, de fautes commises par le personnel employé (fraudes et mauvaise exécution des procédures de la banque), des actes de terrorisme, des guerres ou des catastrophes naturelles. Il s'agit alors des risques opérationnels.

Le risque opérationnel est défini par le comité de Bâle comme étant « le risque de pertes résultant d'une inadaptation 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 perte élevée.» (JIMENEZ & al, 2008 :19). Le risque opérationnel ainsi défini, inclut le risque juridique mais exclut les risques stratégiques et de réputation.

C'est à la publication des accords de Bâle II en 2001 que les risques opérationnels ont été introduits dans la liste des risques majeurs liés à l'activité bancaire. Ils sont désormais pris en compte avec les risques de crédit et de marché.

D'après DOV OGIEN (2006 :9), l'un des rôles traditionnels du banquier est la collecte des dépôts des détenteurs de capitaux qu'il utilise pour son propre compte en opérations de prêts aux emprunteurs. DUCLOS (2005 :158) quant-à-lui présente les dépôts comme étant l'une des principales ressources bancaires.

Malheureusement, plusieurs banques à l'instar de la Banque Atlantique du Sénégal, objet de notre étude, rencontrent des difficultés dans la mise en œuvre de dispositifs de maîtrise des risques opérationnels liés à leurs opérations de collecte de l'épargne ce qui impacte leurs résultats et l'atteinte de leurs objectifs.

Le problème de gestion des risques opérationnels auquel les banques sont confrontées pourrait tirer ses origines des aspects ci –après :

- les réticences des dirigeants à intégrer pleinement les risques opérationnels dans la liste des risques importants liés à l'activité bancaire ;
- la méconnaissance ou la mauvaise application des bonnes pratiques liées à la gestion des risques opérationnels (exigences réglementaires de Comité de Bâle II par exemple) ;
- la mauvaise maîtrise des paramètres et composantes des risques opérationnels en général et ceux liés aux dépôts des clients en particulier ;
- les difficultés dans l'élaboration d'un dispositif de maîtrise des risques adapté aux risques opérationnels liés aux dépôts des clients.

Les causes ci-dessus énumérées pourraient avoir pour conséquences :

- les vols et fraudes (détournements, usurpations de comptes, falsifications de chèques, blanchiments d'argent) ;
- les problèmes de communication dans le traitement de transaction de collecte de des capitaux (envoi de documents erronés par exemple) ;
- les dommages touchant les actifs physiques (exemple: des incendies ou des inondations entraînant la destruction du système informatique avec les informations sur les déposants) ;
- la rupture de contrat avec des clients due à la dégradation de l'image de la banque.

Au regard des causes et des conséquences évoquées ci-dessus, les solutions que nous envisageons sont les suivantes :

- détecter les risques opérationnels liés aux dépôts bancaires, les analyser et apprécier leurs impacts sur les résultats de la banque Atlantique ;

- concevoir une cartographie des risques opérationnels liés aux dépôts bancaires de la banque Atlantique;
- concevoir un référentiel de management des risques opérationnels concernant les opérations de collecte de l'épargne ;
- mettre en place un dispositif de maîtrise des risques opérationnels afin de limiter leur probabilité de survenance ;
- élaborer un système de transmission d'informations efficace entre les différents membres du personnel et les sensibiliser aux risques ;
- réaliser un audit du système de management des risques opérationnels liés aux dépôts bancaires conçu par les dirigeants de la banque Atlantique.

De toutes ces solutions la dernière nous paraît la plus adaptée car elle est plus complète et regroupe un ensemble d'activités à savoir :

- l'analyse du dispositif de couverture de ces risques mis en place par les dirigeants de l'organisation ;
- le recensement des points forts et des points faibles de ce dispositif ;
- la rédaction des recommandations en vue du renforcement des points forts et de la suppression des points faibles ;
- le suivi de la mise en œuvre de ces recommandations.

Ainsi, concernant les dépôts bancaires, les dirigeants pourront avoir un avis indépendant sur l'adéquation, l'application et l'efficacité du système de gestion des risques opérationnels qu'ils ont élaboré.

Au regard de la solution adoptée, la question de recherche que nous posons est la suivante : « Comment aider de manière objective et indépendante la banque Atlantique dans l'amélioration de son processus de management des risques opérationnels se rapportant à la collecte de l'épargne de ses clients ? »

En d'autres termes :

- quels sont les risques opérationnels qui peuvent survenir lors des opérations de dépôts dans la Banque Atlantique ?

- quel est le dispositif de couverture de ces risques mis en œuvre par la banque Atlantique ?
- quels sont les forces et les faiblesses de ce dispositif ?
- quels sont les conseils à apporter pour le renforcement de l'efficacité de ce dispositif ?
- comment aider les dirigeants de la banque à atteindre leurs objectifs et à créer de la valeur ajoutée à partir d'une gestion saine et efficace de ces risques ?

La recherche de réponses à toutes ces questions a motivé notre choix pour le thème suivant: « *Audit du système de management des risques opérationnels bancaires liés aux dépôts bancaires* ».

L'objectif principal de cette étude est de faire un audit du dispositif, de la politique, ainsi que des méthodes de management des risques opérationnels inhérent aux opérations dépôts des clients de la banque Atlantique du Sénégal.

De manière spécifique, il s'agira :

- d'identifier les risques opérationnels relatifs aux versements des clients et pouvant se manifester dans la banque;
- d'identifier les failles de ce processus;
- de donner des recommandations en vue de l'amélioration de ce processus.

Ce mémoire se limitera au management des risques opérationnels liés aux dépôts bancaires. Ainsi, nous ne parlerons que brièvement des autres opérations et risques liés à l'activité bancaire. Par ailleurs la méthodologie employée sera celle de l'audit interne.

L'intérêt de ce mémoire pourrait être perçu à trois niveaux :

Pour la banque Atlantique : Notre étude lui permettra dans un premier temps d'avoir une vue d'ensemble sur tous les risques opérationnels relatifs aux opérations de collecte de fonds pouvant survenir dans la banque et impacter ses résultats. Ensuite, elle pourra avoir une appréciation sur la gestion et le degré de maîtrise de ces risques afin d'appliquer des mesures correctives.

Pour nous-mêmes : Ce travail sera pour nous l'occasion de mettre en pratique les connaissances acquises lors de notre formation, de mieux cerner les risques opérationnels bancaires en général et ceux relatifs aux dépôts bancaires en particulier et de nous familiariser aux processus de management de ces derniers.

Pour le lecteur : Ce mémoire pourra être un support pour tous ceux qui mènent des études sur les risques liés à l'activité bancaire et voudraient avoir une meilleure compréhension de l'audit interne et du management des risques opérationnels.

Ce travail aura deux articulations ; nous aurons dans un premier temps un cadre théorique constitué de trois chapitres. Dans le premier chapitre, nous aborderons la notion de risques opérationnels bancaires en général et ceux liés aux dépôts bancaires en particulier. Le deuxième chapitre sera consacré à une présentation du système de management des risques opérationnels. Le troisième chapitre enfin sera réservé à la présentation de la méthodologie de notre étude.

Dans un deuxième temps, nous aurons un cadre pratique qui sera constitué d'une présentation de la banque Atlantique du Sénégal, suivie d'une description du système de management des risques opérationnels relatif aux dépôts des clients. Ensuite, nous donnerons les résultats de notre étude. Ces résultats seront analysés, et de cette analyse, découleront des recommandations.

PREMIERE PARTIE: CADRE THEORIQUE

CESAG - BIBLIOTHEQUE

L'Institut Français de l'Audit et du Contrôle Interne (2005: 5) définit le management des risques comme étant 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.

Dans le contexte économique actuel, le management des risques suscite un intérêt croissant auprès des dirigeants des organisations, et notamment les banques. En effet, l'environnement bancaire est de plus en plus incertain et complexe. Ceci est dû à plusieurs facteurs à savoir :

- la clientèle exigeante avec des attentes de plus en plus élevées ;
- la sophistication des produits financiers ;
- la concurrence nationale et internationale plus vive ;
- les exigences croissantes des régulateurs et des marchés ;
- la libéralisation et la volatilité des marchés financiers.

Les dirigeants ont donc le souci de s'assurer que, sur le fond aussi bien que sur la forme, la banque a tout mis en œuvre pour assurer une certaine maîtrise des risques et des pertes qui pourraient apparaître suite à la survenance d'un risque. De ce fait, il est important de faire un audit du dispositif de mesure et de suivi de ces risques.

Ainsi, la première partie de notre recherche sera donc une revue de littérature composée de trois chapitres à savoir:

- les risques opérationnels liés aux dépôts bancaires ;
- le système de management des risques opérationnels;
- la méthodologie de la recherche.

CHAPITRE 1 : LES RISQUES OPERATIONNELS LIES AUX DEPOTS BANCAIRES

La masse et la diversité des opérations traitées quotidiennement par une banque peuvent avoir pour conséquence la survenance de risques dits opérationnels. Ce sont par exemple des erreurs de saisie des transactions, des négligences, ou des fraudes. Selon SARDI (2002 :41), ces risques sont omniprésents c'est-à-dire qu'on les retrouve à tous les niveaux de l'activité bancaire notamment lors de la collecte de l'épargne des clients. Ainsi, dans l'optique d'une bonne compréhension des risques opérationnels liés aux dépôts bancaires, nous allons dans un premier temps, aborder la notion de risque opérationnel, puis de dépôt bancaire et enfin nous ferons le lien entre les deux en citant quelques risques opérationnels relatifs aux activités de collecte des fonds.

1.1. La notion de risque bancaire et de risque opérationnel en particulier

Cette section sera consacrée à la définition de quelques concepts, à la classification et à la présentation des composantes des risques opérationnels.

1.1.1. Quelques concepts

Il s'agit de la notion de risque en général et de risque bancaire en particulier

1.1.1.1. Le risque

HAMZAOUI (2005 :37) présente le risque comme étant un concept selon lequel la direction exprime ses inquiétudes concernant les effets probables qu'un événement ou une action ait un impact néfaste sur l'aptitude à réaliser ses objectifs avec succès dans un environnement incertain. Pour lui, le risque est l'expression de l'inquiétude des dirigeants de l'organisation. Or, le risque peut ne pas être exprimé, ou même ne pas être identifié.

RENARD (2010 :155) quant-à-lui, nous donne une définition du risque que propose l'IFACI en ces termes : « le risque est un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise ».

Il ressort de cette définition que le risque est la probabilité qu'un évènement ou une action puisse avoir des conséquences néfastes sur une activité ou sur l'atteinte d'objectifs freinant ainsi la création de valeur ou favorisant la destruction des valeurs existantes.

CLEARY & al (2006 :81), et tous les auteurs cités ci-haut s'accordent sur le fait que le poids du risque est la résultante de deux composantes à savoir la probabilité de survenance et le niveau d'impact.

A ces deux critères nous pouvons ajouter :

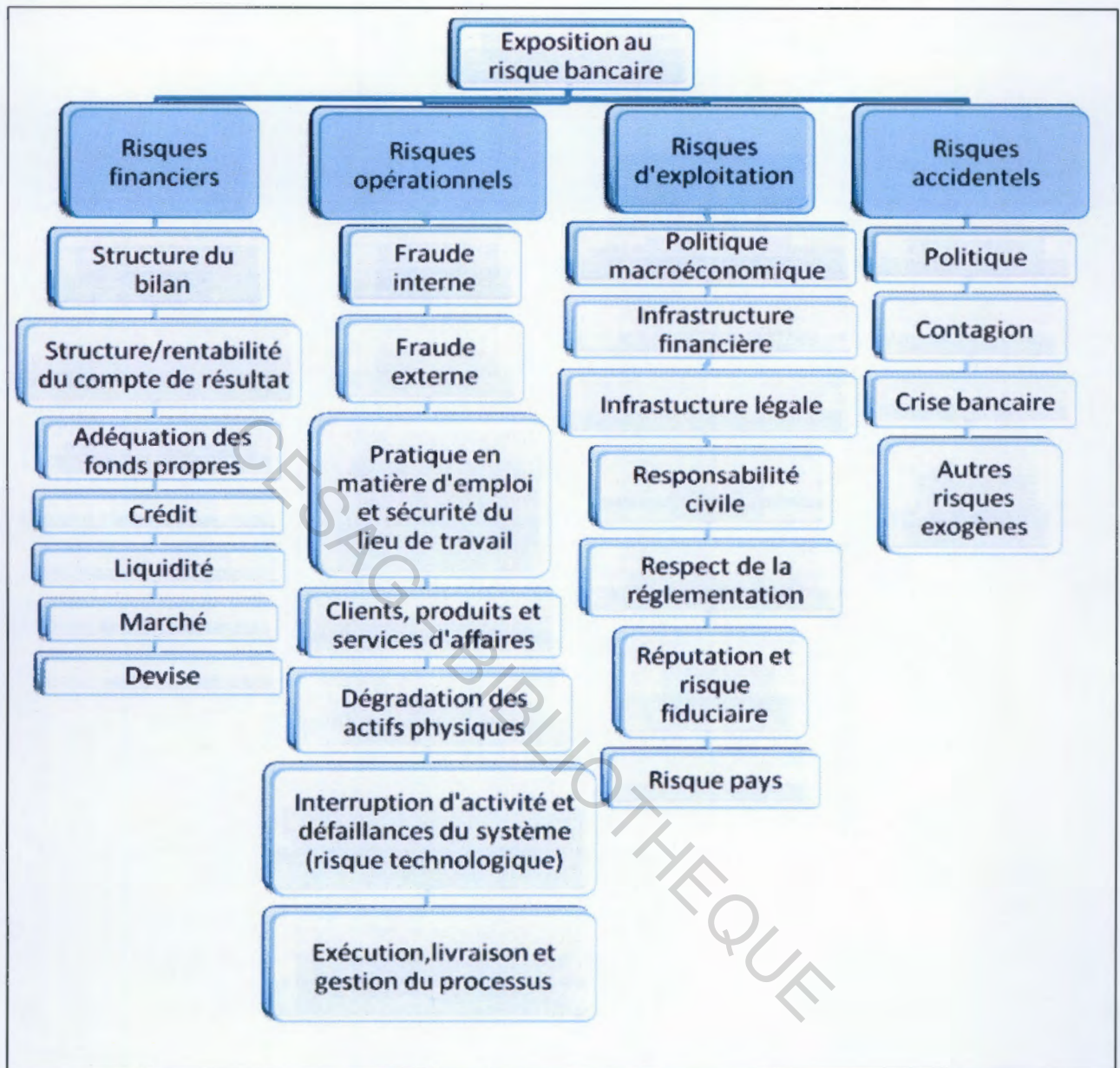
- la criticité qui est le produit des deux dimensions ci-dessus citées ;
- le « timing », c'est-à-dire la fréquence de son apparition ;
- la durée des conséquences, car les dommages causés par la manifestation d'un risque peuvent être réparables dans de brefs délais ou constituer un poids sur l'organisation pendant plusieurs années.

L'environnement bancaire est sans cesse en évolution du fait de la complexité croissante des produits financiers ou de la concurrence de plus en plus rude. Cela rend l'activité bancaire plus risquée.

1.1.1.2. Le risque bancaire

Au cours de leurs activités, les banques sont exposées à une série de risques, comme l'illustre la figure 1 de VAN GREUNING & al (2004 :04).

Figure 1 : Le champ du risque bancaire



Source : VAN GREUNING & al (2004 :04).

Le comité de Bâle considère les risques de crédit, de marché et opérationnels comme étant les risques majeurs inhérents à l'activité bancaire.

- Le risque de crédit

Pour SARDI (2002: 39), il s'agit de la perte potentielle consécutive à l'incapacité par un débiteur d'honorer ses engagements. Cet engagement peut être :

- de rembourser des fonds empruntés (risque enregistré dans le bilan)
- de verser des fonds ou d'attribuer des titres à l'occasion d'une opération à terme ou d'une caution ou garantie donnée (risque enregistré dans le hors bilan).

Il s'agit donc du risque qui découle de l'incertitude quant à la possibilité ou à la volonté des contreparties ou des clients de la banque de remplir leurs obligations.

- Le risque de marché

DESMICHT (2007 :269) définit le risque de marché comme étant le risque de réaliser des moins-values ou des pertes à la revente des titres détenus. Plusieurs raisons peuvent être à l'origine de cet effet :

- la baisse générale des cours des titres ;
- l'illiquidité du marché des titres à vendre (il n'ya pas suffisamment d'acheteurs) ;
- l'obligation de vendre rapidement les titres même à un cours inférieur

Cette définition se limite aux titres détenus par la banque. Or, le risque de marché s'étend à tous les instruments financiers détenus par la banque. Il s'agit donc de pertes potentielles résultant de la variation de prix de tous les instruments financiers détenus dans le portefeuille de négociation de la banque ou dans le cadre d'une activité de marché (trading).

- Le risque opérationnel

Selon SARDI (2002 :41), le CRBF 97-02 définit le risque opérationnel comme étant le risque résultant d'insuffisances de conception, d'organisation et de mise en œuvre des procédures d'enregistrement dans le système comptable et plus généralement dans le système d'information , de l'ensemble des événements relatifs aux opérations de l'établissement.

Cette définition du CRBF est incomplète car elle se limite au système d'information et au système comptable en particulier. Le Comité de Bâle propose une définition plus complète qui nous aide à mieux cerner les origines des risques opérationnels permettant ainsi de les catégoriser. Pour le Comité de Bâle, « le risque opérationnel est le risque de pertes

résultant d'une inadéquation ou d'une défaillance imputable à des procédures, au personnel et aux systèmes internes, ou à des événements extérieurs, y compris les événements de faible probabilité d'occurrence, mais à risque de perte élevée. Le risque opérationnel ainsi défini, inclut le risque juridique, mais exclut les risques stratégiques et de réputation » JIMENEZ & al (2008 :19).

Concernant les autres risques, la classification varie selon les auteurs. Nous avons par exemple le risque de liquidité et le risque de taux d'intérêt.

- Le risque de liquidité

Il s'agit du « risque pour une entreprise ou un établissement bancaire d'être dans l'impossibilité de se dessaisir d'un emploi ou de trouver une ressource sans supporter une perte importante. » (Duclos; 2005 :342).

- Le risque de taux d'intérêt

Pour Duclos (2005 :342), il s'agit du risque lié à des prêts ou des emprunts sur des périodes différentes. Compte tenu de la volatilité des taux, les banques pourraient emprunter plus cher qu'elles ne prêtent.

Après la définition de la notion de risque en général et de risque bancaire en particulier, nous allons maintenant nous attarder sur l'étude des risques opérationnels en commençant par ses composantes.

1.1.2. Les composantes du risque opérationnel

Le risque opérationnel est défini par le comité de Bâle comme étant « 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 perte élevée.» (JIMENEZ & al, 2008 :19).

Il ressort de cette définition que le risque opérationnel a quatre composantes essentielles à savoir :

- une défaillance due au système d'information ;
- une défaillance due aux processus ;

- une défaillance due aux personnes ;
- une défaillance due aux évènements extérieurs.

1.1.2.1. Les risques liés au système d'information :

Il s'agit des risques de pertes dues à un faible niveau de sécurité informatique ou à des procédures de secours informatique non disponibles ou inadéquates.

1.1.2.2. Les risques liés aux processus

Ce risque est dû au non respect des procédures et au mauvais traitement des transactions.

1.1.2.3. Les risques liés aux personnes

Ces risques naissent du fait que les exigences attendues des moyens humains (exigence de compétence et de disponibilité, exigence de déontologie...) ne sont pas satisfaites. Ils sont de deux ordres. Ces risques peuvent résulter d'intentions délibérées (exemple : maquillage des comptes, vols, blanchiment d'argent) ou d'actes involontaires (exemple : erreurs de saisie).

1.1.2.4. Les risques liés aux évènements extérieurs

La survenance de ce risque dépend d'évènements tels que les inondations, les séismes, les guerres.

Les travaux du Comité de Bâle ont défini une segmentation des risques opérationnels en sept grandes catégories d'évènements nous permettant ainsi de faire une classification des risques opérationnels.

1.1.3. Classification des risques opérationnels

Comme le présente le tableau 1, il existe sept catégories de risques opérationnels. Il s'agit de :

- la fraude interne ;
- la fraude externe ;
- les pratiques en matière d'emploi et de sécurité sur le lieu de travail ;
- les clients, produits et pratiques commerciales ;

- les dommages aux actifs corporels ;
- les dysfonctionnements de l'activité et des systèmes ;
- l'exécution, la livraison et la gestion des processus.

Pour chacune de ces catégories, le Comité de Bâle a proposé une définition et des exemples.

Tableau 1 : Classification des risques opérationnels bancaires

Catégories	Définition	Exemples
Fraude interne	Pertes liées à des actes commis à l'intérieur de l'entreprise visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou réglementaire, ou des règles de l'entreprise, à l'exclusion des cas pratiques discriminatoires ou contraires aux règles en matière d'égalité professionnelle, et impliquant au moins un membre de l'entreprise.	informations inexactes sur les positions, vol commis par un employé, délit d'initié d'un employé agissant pour son propre compte
Fraude externe	Pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou réglementaire.	hold-up, faux en écriture, dommages dus aux piratages informatiques
Pratiques en matière d'emploi et de sécurité du travail	Pertes liées à des actes contraires aux dispositions législatives ou réglementaires, ou aux conventions en matière d'emploi, de santé, ou de sécurité, à la réparation de préjudices personnels ou à des pratiques discriminatoires ou contraires aux règles en matière d'égalité professionnelle.	demandes d'indemnisation de travailleurs, violation des règles d'hygiène et de sécurité des employés, plaintes pour discrimination responsabilité civile

Tableau 2 : Classification des risques opérationnels bancaires (suite et fin)

Catégories	Définition	Exemples
Client, produits et pratiques commerciales	Pertes liées à un manquement, délibéré ou non, à une obligation professionnelle envers un client (y compris les exigences en matière de confiance et d'adéquation du service); à la nature ou aux caractéristiques d'un produit.	défaut de conseil, documentation fallacieuse, violation du secret bancaire, mauvaise sélection des clients et des apporteurs, blanchiment d'argent
Dommages occasionnés aux actifs physiques	Pertes liées à la perte ou à l'endommagement d'actifs physiques résultant d'une catastrophe naturelle ou d'autres événements	acte de terrorisme, vandalisme, séisme, incendie, inondation
Interruption de l'activité et dysfonctionnement des systèmes	Pertes liées à une interruption de l'activité ou au dysfonctionnement d'un système	pannes de matériel ou de logiciel informatique, défaillances des systèmes informatiques ou de télécommunication, pannes d'électricité
Exécution, livraison et gestion des processus	Pertes liées aux lacunes du traitement des transactions ou de la gestion des processus et aux relations avec les contreparties commerciales et les fournisseurs	Erreurs d'enregistrement des données, défaillances dans la gestion des sûretés, lacunes dans la documentation juridique, défaillances des fournisseurs...

Source : nous-mêmes à partir de JIMENEZ & al (2008 :52)

Toutes les activités de la banque comportent des risques qui rentrent dans au moins une de ces catégories. L'activité de collecte de l'épargne des clients n'est donc pas à l'abri de ces risques. Ainsi, pour mieux les appréhender, nous allons d'abord faire une présentation des différents types de dépôts que l'on retrouve au sein d'une banque.

1.2. Notion de dépôts bancaires

Nous présenterons dans un premier temps l'activité bancaire en générale, ensuite, nous aborderons la notion de dépôts bancaires.

1.2.1. L'activité bancaire

Selon TACONNE (2007 :75), les banques effectuent plusieurs types d'opérations. Nous pouvons ainsi distinguer les opérations principales des opérations secondaires.

Les principales opérations des banques sont :

- la réception des fonds du public ;
- les opérations de crédit ;
- la gestion et la mise à disposition des moyens de paiement.

1.2.1.1. La réception des fonds du public

Les banques sont essentiellement définies par leur activité d'intermédiation : la collecte de fonds qu'ils emploient sous forme de crédits. SARDI (2002 :873) considère comme fonds reçus du public « les fonds qu'une personne recueille d'un tiers, notamment sous forme de dépôt, avec le droit d'en disposer pour son propre compte, mais à charge pour lui de les restituer ».

1.2.1.2. Les opérations de crédit

Il s'agit de « tout acte par lequel une personne agissant à titre onéreux met ou promet de mettre des fonds à disposition d'une autre personne ou prend, dans l'intérêt de celle-ci un engagement par signature, tel qu'un aval, un cautionnement ou une garantie » (DOV OGIEN; 2006 :152).

1.2.1.3. La mise à la disposition du public des moyens de paiement

DOV OGIEN (2006 :146) nous apprend que la loi bancaire considère comme moyen de paiement « tous les instruments qui permettent à toute personne de transférer, quelque soit le support ou le procédé technique utilisé ». Pour cela, nous distinguons différents supports à savoir les chèques, les effets, les virements, les prélèvements.

Les opérations dites secondaires ou connexes effectuées par les banques sont :

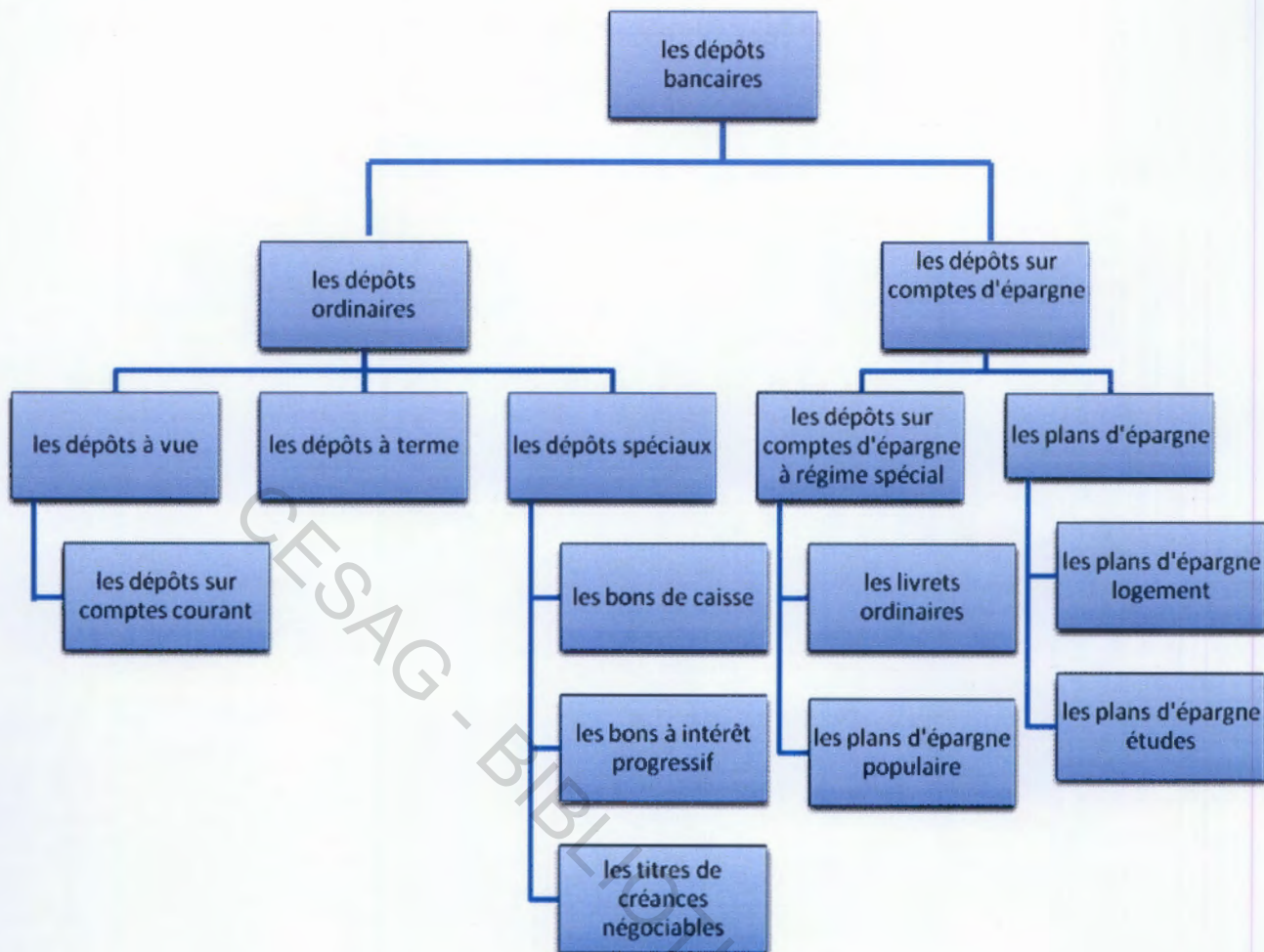
- les opérations de change ;
- les opérations sur or, métaux précieux et pièces ;
- le placement, la souscription, l'achat, la gestion, la garde et la vente des valeurs mobilières ;
- le conseil et l'assistance en matière de gestion du patrimoine ;
- le conseil et l'assistance en matière de gestion financière, l'ingénierie financière ;
- les opérations de location simple de biens mobiliers immobiliers pour les établissements habilités à effectuer des opérations de crédit-bail (TACONNE ; 2007 :75).

Notre étude portant sur les opérations de collecte de fonds, nous allons maintenant définir et présenter les différents types de dépôts que l'on retrouve au sein d'une banque.

1.2.2. Les dépôts bancaires

Ce sont des « sommes déposées par les clients sur leur compte en banque sous quelque forme que ce soit, rémunérées ou non » DUCLOS (2005: 158). Les clients des banques peuvent déposer leur argent et leurs valeurs sur divers comptes ou plans. Les comptes bancaires sont des conventions qui lient le titulaire de ce compte et la banque. Selon DOV OGIEN (2006: 138), ils peuvent revêtir deux formes. Les deux grandes familles de dépôts bancaires sont les dépôts ordinaires et les dépôts sur comptes d'épargne. Ainsi, nous avons pu recenser quelques types de dépôts que l'on retrouve dans les banques européennes et de la zone UEMOA. Il ressort de ce recensement le classement suivant (cf. figure 2, page 19).

Figure 2 : Classification des dépôts bancaires



Sources: nous-mêmes à partir de DOV OGIEN (2006: 138) ; TACONNE (2007: 133).

1.2.2.1. Les dépôts ordinaires

Il s'agit des dépôts à vue, des dépôts à terme et des dépôts spéciaux

1.2.2.2. Les dépôts à vue

Ce sont des « dépôts de fonds par un agent économique où la restitution peut avoir lieu à tout moment sur simple demande du déposant ou de son représentant » DUCLOS (2005 :159). Pour SARDI (2002 :883), les comptes à vue permettent aux clients d'effectuer leurs règlements courants et constituent aussi une réserve de trésorerie. Ils comprennent :

- les comptes courant : l'argent peut être retiré à tout moment. C'est souvent le compte utilisé afin de réaliser les mouvements de fonds avec les autres comptes bancaires.

Généralement, ce type de compte n'est pas rémunéré ou très faiblement. Une autorisation de découvert est parfois accordée afin de permettre que son solde soit négatif jusqu'à un certain plafond moyennant des frais bancaires ;

- les comptes d'épargne : l'argent est également disponible à vue mais son détenteur doit prêter attention à ce que son compte reste créditeur. En zone UEMOA, il y a un solde minimum à conserver en compte, par conséquent, ce dernier ne peut passer débiteur en principe. En effet, un bon dispositif de contrôle interne informatique est installé pour bloquer le montant minimum.

1.2.2.2.1. Les dépôts à terme

Pour DUCLOS (2005 :158), il s'agit de dépôts dont la restitution ne peut être demandée avant son terme. En contrepartie de cette immobilisation, le client bénéficie le plus souvent d'une rémunération plus importante de son épargne. Ainsi, le client versera une somme que l'institution bancaire va geler sur son compte pendant une durée déterminée dans le temps en contrepartie d'intérêts à taux variable selon l'entente de base avec la banque. L'entente est régie par une lettre approuvée par le détenteur du compte qui s'engage à ne pas utiliser l'argent du dépôt avant le terme du contrat, sans quoi il ne pourra toucher les intérêts promis.

1.2.2.2.2. Les dépôts spéciaux

Selon DOV OGIEN (2006: 139), ils peuvent prendre la forme de bon de caisse, de bons à intérêt progressif, de titres de créances négociables et de compte sur livret ordinaire.

- Les bons de caisse: Ce sont des produits de placement comparables aux dépôts à terme. « Les intérêts sont progressifs: plus le bon est conservé longtemps, plus le taux d'intérêt est élevé » DUCLOS (2005: 72) ;
- Les bons à intérêt progressif (BIP): Ce sont des bons d'épargne remboursables au gré du porteur à partir du premier mois après leur émission. Le taux d'intérêt augmente avec le temps ;
- Les titres de créances négociables (TCN) : Ce sont des formules de placements à échéance fixe. Ils sont rarement souscrits par des particuliers, mais plutôt par les grands investisseurs et les organismes de placement collectif en valeurs mobilières

(OPCVM). DUCLOS (2005 :384) précise qu'il existe les titres de créances négociables à :

- court terme (moins d'un an) : les certificats de dépôts négociables, les billets de trésorerie;
- moyen terme (d'un à sept ans): les bons à moyen terme négociables, les bons du trésor à taux annuel normalisé;
- long terme (plus de sept ans): les obligations.

1.2.2.3. Les dépôts sur comptes d'épargne

Il s'agit des comptes d'épargne à régime spécial et les plans d'épargne.

1.2.2.3.1. Les comptes d'épargne à régime spécial

Ils peuvent prendre plusieurs formes à savoir :

- Les comptes sur livret ordinaire : Ce sont des types de compte de dépôt rémunérés et bénéficiant d'avantages financiers et fiscaux.
- Les plans d'épargne populaire (PEP) : Il s'agit d'un « système de capitalisation qui permet la constitution d'une épargne totalement défiscalisée » DUCLOS (2005: 303).

1.2.2.3.2. Les plans d'épargne

Il s'agit des plans d'épargne logement (PEL) et des plans d'épargne études (PEE).

- Les plans d'épargne logement sont « les comptes rémunérés en partie par la banque et en partie par l'Etat » (DOV OGIEN; 2006: 140). DUCLOS (2005: 301) précise que l'épargne logement favorise l'épargne en vue de l'obtention d'un prêt immobilier à des conditions avantageuses.
- Les plans d'épargne études permettent de financer les études des enfants. Ils consistent tout d'abord à la constitution d'une épargne bien rémunérée en procédant à un versement initial, puis des versements périodiques (mensuels ou trimestriels) adaptables aux revenus du client et modifiables à tout moment.

1.3. Les risques opérationnels pouvant survenir au cours des opérations de dépôts bancaires

Le Comité de Bâle a retenu sept catégories de risques opérationnels. Nous allons donc donner quelques exemples se rapportant aux opérations de dépôts bancaires et rentrant dans ces catégories.

1.3.1. La fraude interne

Il s'agit des « pertes dues à des actes visant à frauder, détourner des biens ou à détourner 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 de l'entreprise » (JIMENEZ & al ; 2008: 69).

SIRUGUET & al (2006: 144), considère comme fraudes internes les détournements de capitaux, la contrefaçon, la falsification des chèques et les « dessous de table ».

VAN GREUNING (2004: 208) quant-à-lui cite parmi les fraudes internes les pertes et les erreurs d'affectation des fonds ou des fraudes pouvant se produire, par suite de modifications incorrectes et non autorisées des messages SWIFT (Society for Worldwide Interbank Financial Telecommunication – réseau de télécommunication financières interbancaires mondiales).

Il existe aussi des transactions non notifiées intentionnellement et des transactions non autorisées à l'instar de l'application « des taux non réglementaires ou non approuvés par la direction ; ou des dates rétroactives dans le but de générer des intérêts indus ». (SARDI ; 2002: 873).

1.3.2. La fraude externe

SIRUGUET & al (2006: 105) définit la fraude externe comme étant des pertes dues à des fraudes ayant eu pour objet de détourner des biens ou de contourner la loi, qui implique une personne extérieure à l'entreprise. Concernant la collecte des fonds, sont considérés comme risque de fraude externe le dépôt de faux billets, les hold-up et aussi des actes touchant la sécurité du système informatique tels que les dommages dus au piratage informatique et les vols d'informations.

A cet effet, VAN GREUNING (2004: 208), précise que si l'accès aux terminaux n'est pas strictement contrôlé, des instruments de transferts non autorisés peuvent passer.

1.3.3. L'insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail

Il s'agit de « 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 » (JIMENEZ al; 2008 :70). En effet, un personnel mal rémunéré pourrait poser des actes frauduleux en étant de connivence ou non avec les clients. Par ailleurs, un personnel démotivé du fait de la faible rémunération ou des mauvaises conditions de travail offrirai des services de moindre qualité entraînant ainsi la dégradation de l'image de la banque.

1.3.4. Les clients, les produits et les pratiques commerciales

Ce sont des « 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 résultant de la nature ou conception d'un produit » (JIMENEZ al ; 2008: 70).

VAN GREUNING (2004: 208) nous présente quelques situations relatives aux dépôts et pouvant engendrer des pertes dues à la négligence ou à l'incapacité d'un employé à remplir ses obligations professionnelles à l'encontre des clients

- des données mal introduites dans le système entraînant le retard ou le refus des transactions ;
- des chèques mal affectés, ou déposés sur un mauvais compte ou pas déposés du tout ;
- un versement par erreurs à quelqu'un d'autre que le bénéficiaire qui pourrait se traduire par une perte financière dans le cas où ce versement se révélerait ne pas être recouvrable.

JIMENEZ & al (2008 :70) quant-à-lui complète avec les exemples suivants :

- la violation de la confidentialité de la clientèle ;
- l'atteinte à la vie privée ;

- les opérations fictives ;
- le blanchiment d'argent ;
- les conflits sur l'efficacité des prestations de services et des conseils.

1.3.5. Les dommages aux actifs physiques

Ce sont « des pertes nées de dommages causés aux actifs corporels par des catastrophes naturelles ou d'autres événements » (SIRUGUET & al; 2006 :108).

En effet, des événements peuvent mettre en péril la sécurité des fonds des déposants. Il s'agit entre autres des inondations, des séismes, des incendies, des actes de terrorisme et des guerres.

1.3.6. Le dysfonctionnement de l'activité et des systèmes

Pour SIRUGUET & al (2006 :108), il s'agit de pertes nées d'interruption d'activité ou de pannes du système. Il peut s'agir de pertes liées aux matériels ou aux logiciels

1.3.7. Les dysfonctionnements des processus de traitement

Ce sont les « pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les partenaires commerciaux » JIMENEZ & al (2008 :72). Il s'agit par exemple des problèmes de communication ou des accès non autorisés aux comptes des clients.

Conclusion

Ce chapitre nous a permis d'appréhender tout d'abord les risques opérationnels en général, ensuite les types de dépôts que l'on retrouve au sein d'une banque et enfin les risques opérationnels liés à ces derniers. L'objet du deuxième chapitre sera la présentation du système de couverture de ces risques qui doit être mis en œuvre par les dirigeants des banques car les dépôts bancaires constituent l'une des principales ressources de leurs activités.

CHAPITRE 2 : LE SYSTEME DE MANAGEMENT DES RISQUES

OPERATIONNELS LIES AUX DEPOTS BANCAIRES

« Le management des risques est un processus qui contribue à la réalisation des objectifs de performance et de rentabilité de l'organisation et à la minimisation des pertes » (IFACI.2005 :4). La gestion des risques opérationnels en particulier revêt un caractère indispensable du fait de leur omniprésence dans l'organisation. Ainsi, la Direction Générale et l'ensemble des collaborateurs doivent établir un système de détection et de gestion des risques applicable à tous les niveaux de l'organisation. La première partie de ce chapitre sera donc réservée aux bonnes pratiques énoncées par plusieurs auteurs au sujet de la gestion des risques opérationnels et la deuxième partie sera celle de la présentation du système en question.

2.1. Les bonnes pratiques en matière de management des risques opérationnels

Dans le but de définir quelles sont les pratiques qui doivent s'appliquer aux établissements dans leur appréhension des risques opérationnels, le Comité de Bâle a rédigé en 2003 un document intitulé « *sounds practices for the management and supervision of operational risk* » (in JIMENEZ & al; 2008 :43). Dans ce document, il énonce sept grands principes de management des risques opérationnels :

- **Principe 1** : la Direction doit s'assurer que les risques opérationnels sont suivis de manière distincte et qu'elle dispose des éléments lui permettant de porter un jugement sur la gestion de ces risques.
- **Principe 2** : la Direction doit s'assurer que le dispositif de contrôle des risques opérationnels fait l'objet d'audits réguliers de la part de personnes indépendantes du fonctionnement opérationnel, formées de manière appropriée et compétente.
- **Principe 3** : le dispositif de gestion des risques opérationnels doit couvrir l'ensemble du périmètre d'un établissement et être diffusé à tous les niveaux de responsabilité.
- **Principe 4** : les banques doivent identifier et mesurer les risques opérationnels dans toutes leurs activités, produits ou systèmes. Les banques doivent s'assurer, avant de lancer un nouveau produit, une nouvelle activité ou un nouveau système, que les risques opérationnels ont bien été appréhendés et qu'ils font l'objet de procédures de maîtrise adéquates.

- **Principe 5** : les banques doivent mettre en place une organisation permettant de gérer les risques opérationnels et les expositions aux pertes. Des reportings réguliers et pertinents doivent être adressés à la Direction.
- **Principe 6** : les banques doivent disposer de politiques, processus et procédures permettant de contrôler et limiter les risques opérationnels. Les risques pris doivent être conformes à la stratégie de la banque et au degré de risque auquel elle accepte de s'exposer.
- **Principe 7** : les banques doivent disposer de plans de continuité d'activité permettant d'assurer le traitement des opérations et de minimiser les conséquences d'une interruption grave de l'activité.

Plusieurs auteurs ont aussi fait des propositions concernant les meilleures pratiques à adopter pour une gestion efficace des risques en général, et des risques opérationnels en particulier. MAURER (2006 :64) propose que les entreprises développent une culture du risque et améliorent le processus de prise de décision au sein de l'entreprise, plutôt que de se focaliser sur la maximisation des revenus.

L'IFACI (2001 :18) demande la mise en application des procédures et normes claires et cohérentes en matière de management des risques et des forums adaptés à la diffusion d'informations sur les risques et à leur analyse, une définition claire des responsabilités et des pouvoirs en matière d'acceptation et de management des risques, et leur attribution à des personnes clés, des procédures et programmes de management des risques adéquats accompagné d'un dispositif de suivi et de revue de ces procédures.

Pour HAMAZOUI (2005 :84), il existe plusieurs attitudes qui permettent de maintenir le risque à un niveau acceptable faible notamment :

- l'acceptation consciente et objective des risques en tenant compte de la tolérance au risque ;
- le transfert de ces risques à d'autres parties prenantes (par exemple, aux fournisseurs ou aux assureurs) ;
- la mise en place de procédures et de politiques appropriées de contrôle interne ;
- le refus de s'engager dans une activité à risque trop important.

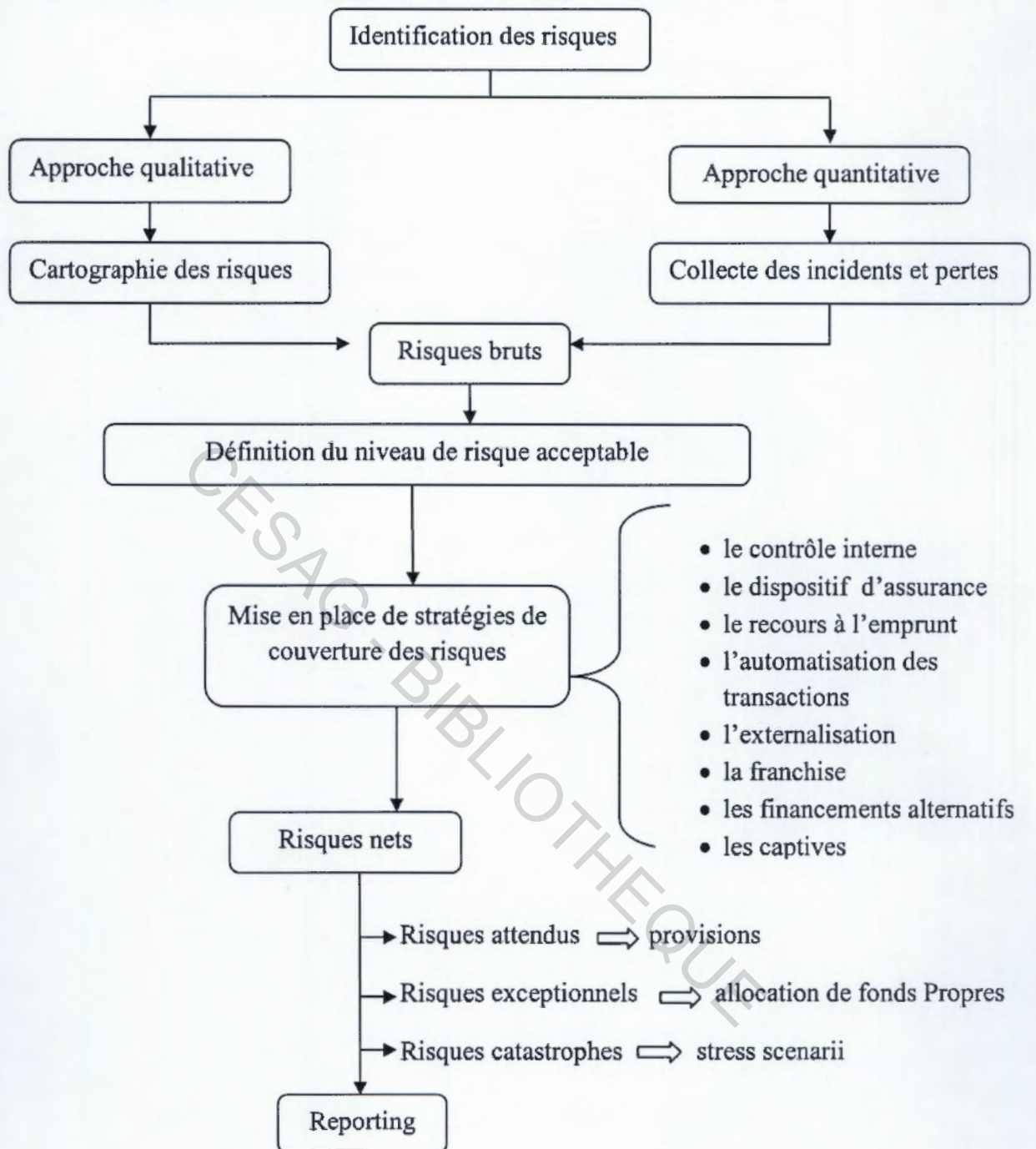
En plus des bonnes pratiques, plusieurs auteurs ont poussé la réflexion plus loin et ont présenté les éléments constitutifs de système de gestion des risques opérationnels.

2.2. Le système de management des risques opérationnels

Selon BARI & al (2011: 14), il existe deux approches de gestion des risques opérationnels: une approche qualitative matérialisée par la conception d'une cartographie des risques et une approche quantitative qui assure la mesure et la surveillance des incidents et des pertes sur risques opérationnels. JIMENEZ & al (2008: 164) est du même avis que lui et ajoute que l'approche quantitative repose sur des historiques d'incidents internes et externes. Ainsi, ce dispositif peut être synthétisé comme suit :

CESAG - BIBLIOTHEQUE

Figure 3 : Le système de management des risques opérationnels bancaires



Sources : nous-mêmes à partir de BARI & al (2011 :14) ; JIMENEZ (2008 :128) ; SIRUGUET (2006 :126)

2.2.1. L'identification des risques

L'identification des risques nécessite au préalable une définition du périmètre à analyser, c'est-à-dire une énumération de l'ensemble des activités de l'organisation. Pour cela, le Comité de Bâle a effectué une décomposition de la banque en lignes métiers.

2.2.1.1. Les lignes métiers

D'après JIMENEZ & al (2008 :55), ces lignes métiers constituent les principales sources de valeur ajoutée et correspondent généralement à un produit ou service, un segment de clientèle, un territoire géographique ou à la combinaison des trois.

A ces lignes métiers sont associées les différentes activités de la banque comme nous le présente le tableau 2 suivant.

Tableau 2 : Les lignes métiers

Lignes métiers	Activités
Financement des entreprises	<ul style="list-style-type: none"> ○ Prise ferme d'instruments financiers et/ou placement d'instruments financiers avec engagement ferme ○ Conseils et services financiers aux entreprises
Négociation et vente institutionnelles	<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
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 financier ○ Octroi de garanties et souscription d'engagements
Banque commerciale	<ul style="list-style-type: none"> ○ Réception de dépôts et autres fonds remboursables ○ Prêts ○ Contrats de location-financement et contrats de location à caractère financier ○ Octroi de garanties et souscription d'engagements
Paiements et règlements	<ul style="list-style-type: none"> ○ Opérations de paiement ○ Emission et gestion des moyens de paiement ○ Compensation et règlement-livraison d'instruments financiers
Service d'agence	<ul style="list-style-type: none"> ○ Garde et administration d'instruments financiers pour les comptes des clients, y compris la conservation et les services connexes, comme la gestion de trésorerie/ de garanties
Gestion des 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 des clients ○ Placement d'instruments financiers sans engagement ferme

Source : JIMENEZ & al (2008 :56)

2.2.1.2. Les processus

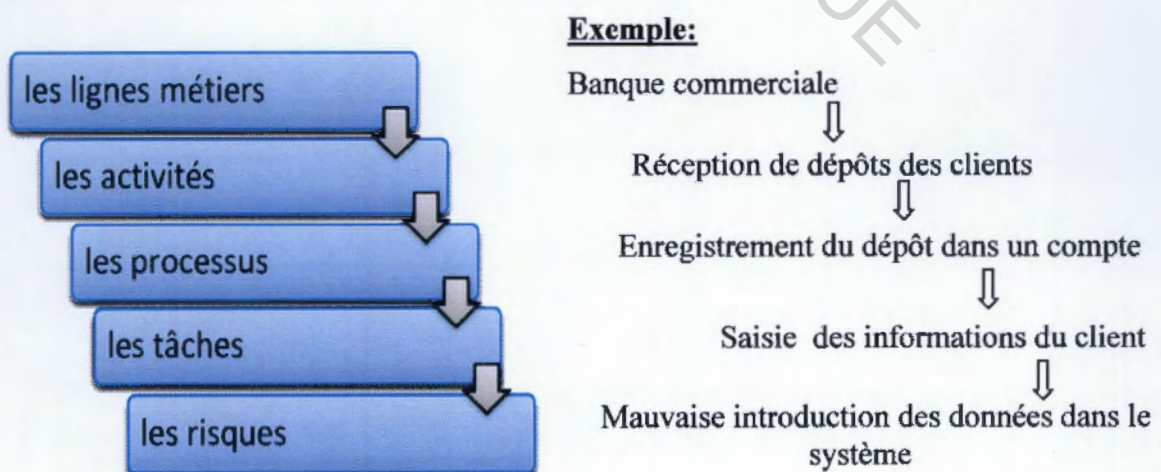
La décomposition en lignes métiers étant trop large pour pouvoir appréhender avec assez de précision les risques associés, il faudrait décrire plus en détail les activités de la banque sous forme d'une représentation des principaux processus qui participent à la création de valeur au sein de l'entreprise.

D'après JIMENEZ & al (2008 :57), on distingue trois types de processus

- Les processus opérationnels (processus métier), dont la finalité est de fournir des produits et services aux clients externes à l'établissement.
- Les processus de pilotage (processus de direction), dont la finalité est de fixer des orientations, d'évaluer la situation (présente, passée ou future) par rapport à celles-ci et de décider d'actions correctives nécessaires. Les clients de ces processus sont le management, les organismes de tutelles, les actionnaires.
- Les processus de support, dont la finalité est de gérer les ressources de l'établissement, de tenir à jour sa situation, ainsi que fournir ces éléments aux acteurs des processus opérationnels et de pilotage.

Ayant identifié les différents processus, il devient alors aisé de les décomposer en tâches. Ainsi de chaque tâche, nous pourrions ressortir les risques opérationnels.

Figure 4 : Processus d'identification des risques opérationnels



Source : Nous-mêmes à partir de JIMENEZ & al (2008 :60)

2.2.2. L'approche qualitative

Selon BARI (2011 :14), il s'agit d'une approche prospective basée sur la prévention des risques opérationnels. Elle consiste en une évaluation des risques prévisionnels matérialisée par une cartographie des risques.

La cartographie des risques est la représentation graphique synthétique et hiérarchisée des risques d'une organisation. D'après SIRUGUET & al. (2006 :107), l'importance d'un risque peut dépendre d'éléments mesurables (nature objective du risque) ou peut dépendre de la façon dont chaque personne perçoit ce risque (nature subjective du risque).

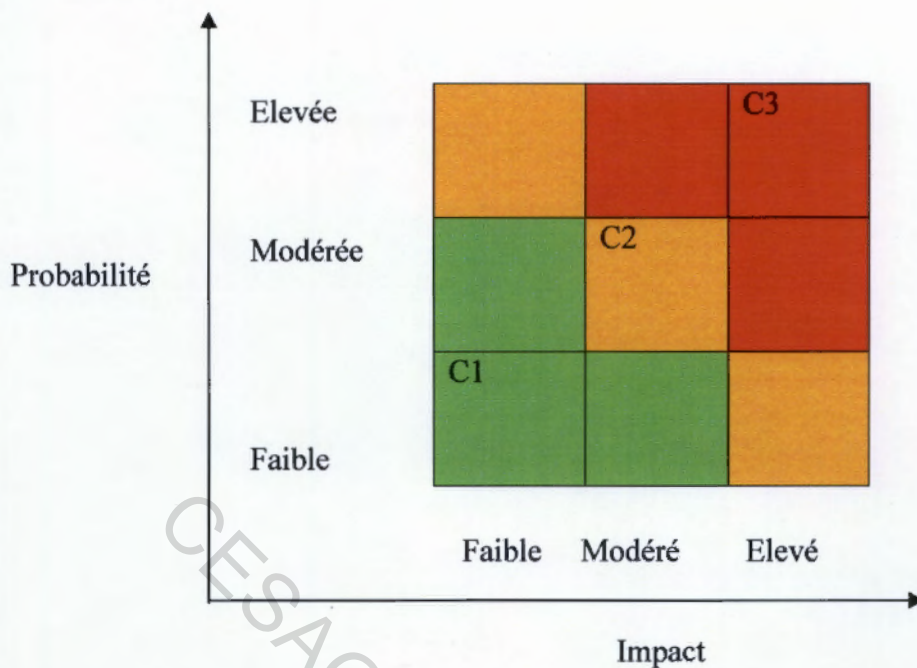
Le risque objectif tient compte de quatre éléments déterminants :

- le danger ou la menace potentielle ;
- la probabilité de survenance d'évènements ou de situations non voulues ;
- les effets et les impacts de la matérialisation de ces évènements ou situations ;
- l'exposition au risque, résultant de la pondération des impacts par la probabilité de réalisation du risque.

L'appréciation du risque subjectif dépend de chaque individu et tient compte de facteurs culturels, psychologiques et sociaux tels que la familiarité et la confiance existant au sein de l'entreprise ou l'importance pressentie de l'impact.

La figure 5 de la page 32 est une illustration de la cartographie des risques.

Figure 5 : Cartographie des risques



Classe de criticité	Niveau de risque	Commentaires
C1	Acceptable en l'état	Aucune action nécessaire
C2	Acceptable sous contrôle	Contrôle de l'évolution des marges et de gestion des actions associés.
C3	Inacceptable	Rejeter les événements et empêcher les scénarios y conduisant

Source : Desroches & al (2003 :5)

2.2.3. L'approche quantitative

« L'approche quantitative assure la mesure et la surveillance des incidents et des pertes sur risques opérationnels » BARI (2011 :14). Il s'agit de l'approche historique de la gestion des risques opérationnels car selon JIMENEZ & al (2008 :163), elle est basée sur des données d'incidents survenus au sein de l'organisation. Cette approche comprend les étapes suivantes :

- observation des historiques d'incidents ;
- représentation du phénomène à partir d'une loi statistique ;
- définition de la probabilité pour l'ensemble des résultats possibles.

2.2.3.1. Observation des historiques d'incidents

Des pertes réalisées suites à divers incidents survenus au sein de l'entreprise sont observées sur une certaine période. Ces observations sont effectuées à partir de deux critères à savoir :

- la sévérité : le montant des incidents, l'impact financier des événements de risques ;
- la fréquence : la date des incidents, la fréquence des événements de risques.

2.2.3.2. Représentation du phénomène à partir d'une loi statistique

Sur la base des observations effectuées, des outils statistiques permettent d'approcher la loi statistique la plus adaptée, et de calibrer celle-ci à partir de ses paramètres (espérance mathématique, variance..). En matière risques opérationnels, les lois les plus couramment utilisées sont :

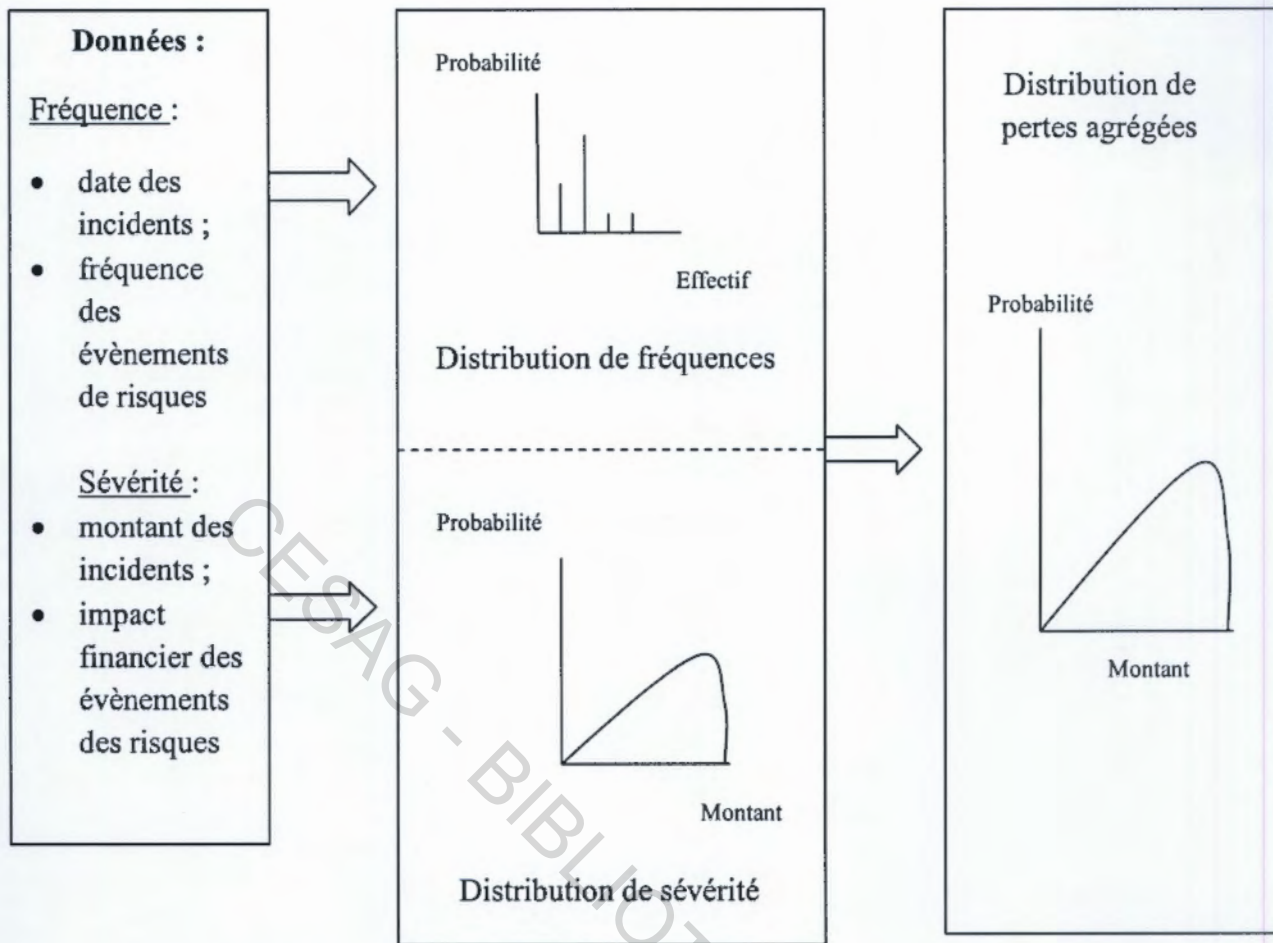
- pour la distribution de sévérité : Log normale, Weibull, Pareto, Gamma ;
- pour la distribution de fréquence : Poisson, Binomiale Négative (JIMENEZ & al ; 2008 :171).

2.2.3.3. Définition de la probabilité pour l'ensemble des résultats possibles

Lorsque l'on a réussi à représenter le phénomène observé par une loi statistique, il est possible ensuite d'utiliser cette représentation mathématique pour définir la probabilité de l'ensemble des résultats possibles. Dans le cadre des risques opérationnels, cela se fait en combinant la distribution de sévérité (montant) avec la distribution de fréquence. Nous obtenons ainsi la distribution de pertes brutes prévisionnelles qui représente pour chaque montant de perte la probabilité de survenance.

Cette approche est synthétisée dans la figure 6 de la page 34.

Figure 6 : Approche quantitative de gestion des risques opérationnels



Source : JIMENEZ & al (2008 : 172)

Cette approche permet de :

- définir une hiérarchie et des priorités des risques opérationnels au regard des enjeux financiers qu'ils représentent pour l'établissement ;
- de faire des comparaisons de ces risques au produit net de l'activité
- de « jauger » ces risques par rapport au coût des mesures de réduction ou au coût de financement du risque en cas d'investissement.

2.2.4. Définition du niveau de risque acceptable

Il s'agit de la détermination du niveau maximum de risque accepté. Pour cette étape du management, « il faut définir des seuils au-dessous desquels les risques sont acceptables, et que ceux qui courent le risque acceptent résolument d'en subir les conséquences

« négatives prévisibles » (IFACI, 2001 :45). Ce seuil de tolérance doit faire l'objet d'une remise en cause régulière afin de s'assurer de sa pertinence au regard de l'évolution des facteurs endogènes (politique commerciale, formation...) et exogènes (réglementation, concurrence...).

2.2.5. Mise en place de stratégie de couverture

Comme stratégie d'atténuation ou de réduction des risques opérationnels, JIMENEZ & al (2008 :129) nous propose l'amélioration du contrôle interne, le dispositif d'assurance et le compte de résultat (le recours à l'emprunt). SARDI (2002 :316) quant-à-lui considère les assurances, l'externalisation et l'automatisation des transactions comme principaux moyens pour limiter le risque opérationnel. SIRUGUET & al (2006 :125) abonde dans le même sens que les deux auteurs précédents et nous parle aussi de franchise, de financements alternatifs et de captives (filiales de réassurance).

2.2.5.1. Le contrôle interne

Pour BARRY, le contrôle interne est l'ensemble des sécurités qui contribuent à assurer d'une part, la protection, la sauvegarde du patrimoine et la qualité de l'information, d'autre part, l'amélioration des performances. Cette définition ne met pas en exergue l'objectif principal du contrôle interne qui est celui de donner une assurance raisonnable de la maîtrise des opérations de l'organisation.

HAMZAOUÏ (2005 :80), quant-à-lui nous donne la définition proposée par le Committee of Sponsoring Organizations of the Treadway Commission (COSO). Il s'agit d'un « processus mis en place par le Conseil d'Administration, les dirigeants et le personnel de l'entité, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité aux lois et aux règlements en vigueur » (HAMZAOUÏ 2005 :80).

Au sein d'une organisation, le contrôle interne se manifeste par « le suivi des décisions d'une part, et la qualité de leur exécution technique, d'autre part, effectué dans le cadre des

objectifs de l'organisation par ou pour le compte des fonctions dirigeantes à différents niveaux hiérarchiques. » (WILMOTS, 2002 :225).

Selon l'IFACI (2005 :33), le contrôle interne est composé de huit éléments à savoir :

- environnement interne : englobe la culture et l'esprit de l'organisation ;
- fixation des objectifs : les objectifs doivent avoir été préalablement définis pour que le management puisse identifier les événements potentiels susceptibles d'en affecter la réalisation ;
- identification des événements : distinction entre risques et opportunités ;
- évaluation des risques : analyse des risques, tant en fonction de leur probabilité d'occurrence que de leur impact.
- traitement des risques : évitement, acceptation, réduction, partage,
- activité de contrôle : des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques ;
- information et communication : les informations utiles sont identifiées, collectées et communiquées dans des délais raisonnables ;
- pilotage: le dispositif de management des risques est piloté et adapté aussi souvent que nécessaire.

L'efficacité d'un dispositif de management des risques peut s'apprécier en vérifiant que chacun des huit éléments est en place dans l'organisation et qu'ils fonctionnent efficacement.

2.2.5.2. Le dispositif d'assurance

Il s'agit d'une couverture externe des risques qui consiste à « transférer le risque à un tiers qui dispose de moyens ou de compétences mieux adaptés à sa gestion et qui accepte de les assumer (externalisation), ou de modifier l'impact qui sera partiellement ou totalement assumé par un tiers contre rémunération (assurance) » (JIMENEZ & al, 2008 :144).

Par exemple pour la gestion des pertes liées aux incendies (destruction des actifs physiques), la banque peut signer des conventions avec une compagnie d'assurance afin de lui transférer les charges de réparation.

2.2.5.3. Le recours à l'emprunt

Selon JIMENEZ & al (2008 :143), lorsque les risques sont considérés comme relevant de la gestion courante de l'entreprise (en général des risques à faible impact) et que l'on cherche à réduire leurs impacts en améliorant les outils et procédures en place, il est souhaitable de prévoir leur financement. Le recours à l'emprunt pour financer les besoins suite à un sinistre est aussi une option possible pour des sinistres significatifs que l'entreprise n'aura pas pu ou voulu transférer au secteur de l'assurance.

2.2.5.4. L'externalisation (outsourcing)

C'est moyen de transfert du risque opérationnel sur un tiers (sous-traitant). « Cette externalisation peut comporter de nombreux avantages : meilleure qualité des services, gain de productivité, rapidité de lancement d'un nouveau produit ou nouvelle activité etc... » (SARDI ; 2002 :316).

2.2.5.5. L'automatisation des transactions

Les investissements technologiques permettant d'automatiser et d'améliorer le traitement des opérations de masse sont non seulement des facteurs importants de réduction des coûts mais aussi des facteurs de réduction des risques. Selon SARDI (2002 :317), ils réduisent l'erreur humaine, et interdisent le traitement d'opérations non autorisées ou de procédures dérogatoires.

2.2.5.6. La franchise

« Le mécanisme de franchise consiste à garder à charge une partie du risque : les pertes inférieures au moment de la franchise sont supportées par la banque, les pertes excédant ce montant étant prises en compte par l'assurance. Le mécanisme de franchise permet à la banque de réaliser une économie de gestion : la prime d'assurance est réduite. » (SIRUGUET & al 2006 :126).

2.2.5.7. Les financements alternatifs

D'après SIRUGUET & al (2006 :126), il s'agit de techniques financières destinées à préfinancer une perte probable dans le temps ; utilisation de produits dérivés et de produits de transfert de risques par exemple.

2.2.5.8. Les captives (filiales de réassurance)

Ces sociétés sont appelées « captives » pour signaler leur lien avec la société mère. Pour SIRUGUET & al (2006 :127), cette solution est réservée aux banques de taille importante. La création d'une filiale agissant en tant que compagnie d'assurance ou de réassurance est un moyen de participer à la couverture des risques

2.2.6. Evaluation du risque net ou risque résiduel

Il s'agit du risque estimé après la prise en compte de toutes les couvertures existantes. Pour JIMENEZ & al (2008 :128), il doit être comparé à la limite de risque souhaitée et, si la limite est dépassée, des mesures complémentaires de contrôle ou de transfert doivent être envisagées afin de revenir à la limite souhaitée.

BARI & al (2011 :15) décompose les risques nets en trois catégories :

- les risques attendus ;
- les risques exceptionnels ;
- les risques catastrophes.

2.2.6.1. Les risques attendus

Il s'agit des pertes récurrentes observées au sein de la banque. Ils sont couverts par des provisions déductibles ou non fiscalement en fonction du caractère probable ou non des pertes.

2.2.6.2. Les risques exceptionnels

Ces risques sont couverts par des allocations de fonds propres. A cet effet, MAURER (2007 :46) présente trois approches élaborées par le comité de Bâle pour le calcul de ces fonds propres :

➤ L'approche indicateur de base (*Basic indicator approach –BIA*)

C'est une approche forfaitaire dans laquelle le capital requis (ou exigence de fonds propres) est de 15% du produit net bancaire (Gross Income ou GI).

$$K_{BIA} = \alpha \times GI$$

Avec K_{BIA} = capital requis
 α = taux forfaitaire = 15%

➤ L'approche standardisée (*standardised approach – SA*)

Pour cette approche, on applique un taux (β) au produit net bancaire de chaque ligne métier (i) de la banque. Le montant des fonds propre sera une somme des montants obtenus à chaque ligne métier.

$$K_{SA} = \sum \beta_i \times GI_i$$

Avec K_{SA} = capital requis

β = taux affecté à produit net bancaire de chaque ligne métier

➤ L'approche AMA ou approche des mesures dites avancées (*advanced management Approach*).

Pour MAURER (2007 :46), cette approche est la plus complète et la plus sophistiquée. Sachant qu'il existe sept catégories de risques opérationnels et huit lignes d'activités. A chaque ligne, on associe les sept catégories de risques opérationnels. Nous obtenons ainsi cinquante six couples activité/risque. Pour chaque couple, il faut calculer la mesure de la perte attendue (*Expected Loss : EL*).

$EL = PE \times LGE \times E$ Avec PE = probabilité de l'évènement (*probability of event*)

LGE = perte en cas d'évènement (*loss given by event*)

E = exposition au risque opérationnel

PE et LGE sont déterminés par la banque d'après ses modèles internes, le facteur E est donné par le régulateur. Les fonds propres alloués sont la somme des pertes attendues pour chaque couple pondérés d'un facteur y spécifique (les cinquante-six facteurs sont fixés par le régulateur).

$$K_{AMA} = \sum (y_{ij} \times EL_{ij})$$

Avec i = ligne d'activité et j = type de risque

2.2.6.3. Les risques catastrophes

« Les risques catastrophes sont pris en compte par le biais de la simulation de scénarii catastrophe et de la mise en place d'un plan de continuité des activités » BARI (2011 :15). En effet, pour ce qui concerne son exposition aux risques élevés, une banque doit utiliser des scénarii plausibles de pertes conçus par des experts.

2.2.7. Le reporting

Il fait partie intégrante du dispositif de gestion des risques opérationnels. Selon JIMENEZ & al (2008 :191, sa nature est fonction du destinataire :

- pour un opérationnel responsable d'un processus, il s'agit d'un outil d'alerte ou de prévention pour éviter les situations « à risque » ;
- pour un responsable des risques opérationnels, c'est un indicateur du degré de maîtrise obtenu à un instant « t » et de son évolution ;
- pour un dirigeant, il s'agit d'une vision synthétique des risques de l'entreprise et de ses zones de fragilité ;
- pour tous, il s'agit d'un outil de dialogue permettant la prise de décision sur une base consensuelle de mesure des risques portés et de leur évolution.

Nous avons appréhendé les risques opérationnels dans le chapitre précédent, qui nous a permis d'étudier les étapes du système de management des risques opérationnels mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation. Nous savons aussi que ce système est important pour la réalisation des objectifs de performance et de rentabilité de l'organisation et pour la minimisation des pertes d'où la nécessité d'un audit régulier. Ainsi le troisième chapitre de notre cadre théorique sera la présentation du modèle d'analyse et des outils employés pour l'audit de ce système au sein de la Banque Atlantique du Sénégal.

CHAPITRE 3: METHODOLOGIE DE L'ETUDE

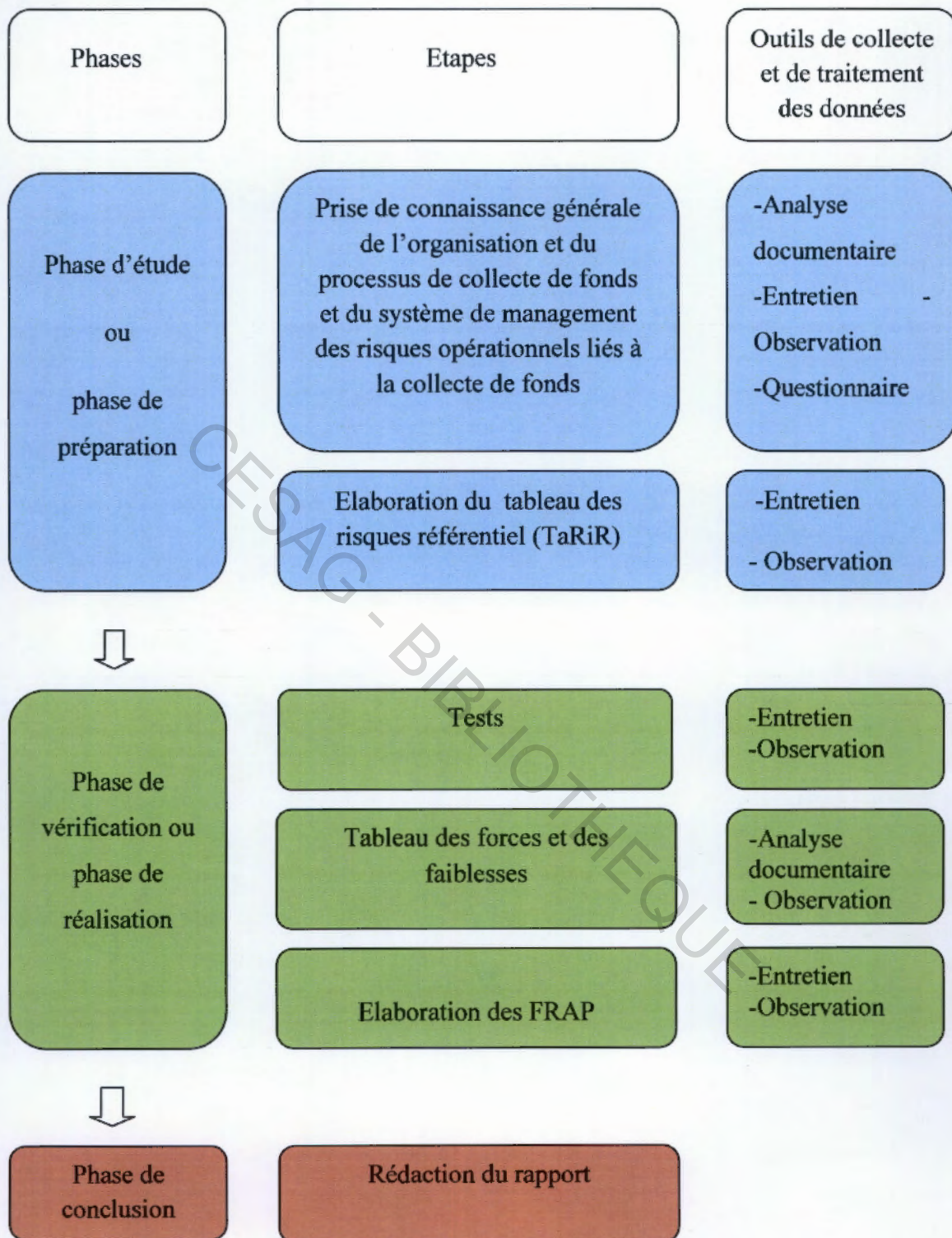
La revue de littérature nous a permis de comprendre le système de management des risques opérationnels liés aux dépôts bancaires. Ce chapitre est l'occasion pour nous de présenter la méthodologie que nous avons employée au cours de notre mission d'audit de ce système au sein de la Banque Atlantique du Sénégal. Cette méthodologie est basée sur un modèle d'analyse qui est une représentation schématique du rapprochement entre la théorie (revue de littérature) et la pratique. Nous présenterons aussi les outils de collecte et d'analyse des données.

3.1. Modèle d'analyse

Le modèle d'analyse adopté repose sur les étapes de la conduite d'une mission d'audit interne à savoir :

- la phase d'étude ;
- la phase de vérification ;
- la phase de conclusion.

Figure 7 : Modèle d'analyse



Source : nous-mêmes adaptée de SCHICK (2007: 64) et RENARD (2010: 214)

3.1.1. La phase d'étude

A cette étape, nous avons tout d'abord fait une analyse documentaire. Les documents qui ont été consultés sont le manuel de procédures, l'organigramme et le manuel de contrôle. Par la suite, nous avons effectué des entretiens avec les caissiers, le chef du service caisse et le contrôleur des opérations. Après, nous avons pu observer à la caisse les opérations de dépôts et tout le dispositif mis en œuvre pour la sécurisation des fonds.

3.1.1.1. La prise de connaissance générale de l'organisation et du processus de collecte des fonds

C'est l'étape de « familiarisation » avec l'organisation et du processus de collecte des fonds des clients. Cette étape nous a permis de faire un découpage de ce processus en objets auditables de la réception des fonds à la caisse à la sécurisation dans les coffres forts de la banque, et ensuite de la caisse principale vers la Banque Centrale. Les outils utilisés ont été l'analyse documentaire, les interviews et l'observation. A la fin de cette étape, nous avons fait une description schématisée (flow chart) du processus.

3.1.1.2. L'élaboration du tableau des risques référentiel (TaRiR)

Chaque étape du processus (sous- processus) de gestion des risques opérationnels se rapportant à la collecte des fonds a été analysée, et le tableau suivant a été élaboré.

Tableau 3 : Tableau des risques référentiel (TaRiR)

Etapes	Finalités (objectifs de contrôle interne)	Empêchements	Points de contrôle	Impact	Bonnes pratiques

Source : SCHICK (2007 : 79)

- les finalités de chaque sous- processus ont été définies ;
- pour chaque finalité, nous avons imaginé des scénarii qui empêcheraient de les atteindre ;
- pour chaque empêchement, nous avons eu des points de contrôle;

- pour chaque point de contrôle, nous avons donné les impacts qui sont les conséquences de la défaillance/déficience de ces points de contrôle ;
- enfin, nous avons donné les bonnes pratiques qui sont la description de ce qui devrait être, ce que les audités devraient faire, les moyens, les méthodes pour éviter les empêchements.

3.1.2. La phase de vérification

Cette phase commence par des tests, se poursuit par le tableau des forces et faiblesses pour déboucher sur l'élaboration des FRAP (Feuille de Révélation et d'analyse de problème).

3.1.2.1. Les tests

Il s'agit des tests de l'effectivité des points de contrôle énoncés dans le TaRiR. Ce sont les vérifications qui permettant de nous assurer que les objectifs de chaque étape du processus de réception des fonds des clients sont être atteints.

3.1.2.2. Le tableau des forces et faiblesses

Les forces et faiblesses du système mis en œuvre par la BASN pour la gestion de ses risques opérationnels liés aux dépôts bancaires découlent des résultats des tests effectués. Ainsi, des faiblesses, nous avons pu émettre des recommandations.

3.1.2.3. Les Feuilles de Révélation et d'Analyse des Problème (FRAP)

Ce sont des papiers de travail synthétiques par lesquels nous avons présenté et documenté chaque dysfonctionnement. Chaque FRAP comporte plusieurs éléments à savoir :

- le problème : c'est une formulation synthétique de l'objectif qui est compromis ;
- les constats : ce sont les preuves des problèmes observés ;
- les causes : ce sont les explications des constats. Elles ont été constatées ou déduites ;
- les conséquences : elles permettent de percevoir la gravité du problème ;
- les recommandations : ce sont les solutions.

3.1.3. La phase de conclusion

C'est la phase de rédaction du projet de rapport. Le projet de rapport résulte de l'ensemble des FRAP. Il constitue un relevé des lacunes, des faiblesses de dysfonctionnements constatés au cours de la mission ainsi que des recommandations. Nous n'avons pas pu rédiger de rapport définitif car cela nécessite la tenue d'une réunion de validation avec les audités, ce qui n'a pas pu être possible dans le cadre de la rédaction de notre stage.

3.2. Outils de collecte et d'analyse des données

Les différents outils que nous avons utilisés sont l'entretien, l'analyse documentaire, l'observation et le questionnaire.

3.2.1. L'entretien

Lors de notre mission d'audit au sein de la Banque Atlantique du Sénégal, nous avons eu des entretiens avec les risk-managers, les auditeurs internes, le chef de caisse, le gestionnaire de caisse, le gestionnaire des opérations, les caissiers, les assistants de la Directrice des Ressources Humaines, et le personnel de gardiennage. Les questions posées au cours de ces entretiens sont mentionnées en annexe à la page 88.

3.2.2. L'analyse documentaire

Les documents suivants ont été consultés :

- Les organigrammes de chaque Direction ;
- le manuel de procédures ;
- le manuel de contrôle

3.2.3. L'observation

Nous avons observé le processus de collecte des fonds des clients de la caisse jusqu'à la sécurisation dans la caisse principale (la réserve), puis le transfert de la caisse principale vers la BCEAO. Par la suite, nous avons pu observer tout le dispositif mis en œuvre pour la sécurisation de ces fonds.

3.2.4. Le questionnaire

Les questionnaires administrés sont :

- le questionnaire sur l'identification et l'analyse des risques ;
- le questionnaire sur les stratégies de couverture des risques opérationnels liés aux dépôts bancaires.

Ces questionnaires figurent en annexe à la page 89.

Ce chapitre nous a permis de présenter la méthodologie que nous avons employée pour mener à bien notre mission d'audit portant sur le système de management des risques opérationnels liés aux dépôts bancaires. Il s'agit des étapes qui constituent toute mission d'audit à savoir la préparation, la vérification et les conclusions. La phase de préparation est la phase de prise de connaissance du processus de collecte des fonds et du système mis en œuvre permettant de couvrir les risques opérationnels liés à ce processus. La phase de vérification est la phase d'identification et d'analyse des risques. Cette étape se termine par l'élaboration des Feuilles de Révélation et d'analyse de problème (FRAP). La phase de conclusion qui permet de présenter les lacunes, les faiblesses de dysfonctionnements constatés au cours de la mission ainsi que des recommandations. Nous avons par ailleurs présenté les outils que nous avons utilisés (entretien, questionnaire, observation et analyse documentaire).

Cette première partie a été pour nous l'occasion de recenser les avis de différents auteurs sur le système de management des risques opérationnels liés aux dépôts bancaires. Nous nous sommes rendu compte que la gestion des risques opérationnels revêt un caractère indispensable du fait de leur omniprésence dans l'organisation. Étant donné que les dépôts constituent l'une des principales ressources bancaires, la Direction doit s'assurer que le dispositif de contrôle des risques opérationnels fait l'objet d'audits réguliers de la part de personnes indépendantes du fonctionnement opérationnel, formées de manière appropriée et compétente.

Ceci nous a amené à présenter la méthodologie que nous avons employée pour mener à bien notre mission d'audit au sein de la Banque Atlantique du Sénégal. Cette mission est décrite dans la deuxième partie de notre mémoire.

CESAG - BIBLIOTHEQUE

DEUXIEME PARTIE : CADRE PRATIQUE

CESAG - BIBLIOTHEQUE

La première partie de notre étude a été pour nous l'occasion de décrire, à partir des points de vue de plusieurs auteurs, le système de management des risques opérationnels se rapportant à la collecte des fonds des clients au sein d'une banque.

Il nous est désormais possible de mener une mission d'audit au sein d'une organisation bancaire. Pour cela, il nous faudra à identifier les risques opérationnels relatifs aux versements des clients pouvant se manifester au sein de cette banque, décrire le système mis en œuvre pour leur suivi, identifier les failles de ce processus et de formuler des recommandations en vue de son amélioration. La structure qui a accepté de nous accueillir pour cela est la Banque Atlantique du Sénégal.

Ainsi, cette deuxième partie portera sur les chapitres suivants :

- la présentation de la Banque Atlantique du Sénégal ;
- l'audit du système de management des risques opérationnels liés aux dépôts au sein de la banque atlantique ;
- la présentation des résultats et les recommandations en vue de l'amélioration de ce système.

CHAPITRE 4 : PRESENTATION DE LA BANQUE ATLANTIQUE DU SENEGAL

La Banque Atlantique Sénégal (BASN) est l'une des banques du Groupe Atlantique, groupe privé africain dont le siège opérationnel est à Abidjan, en Côte d'Ivoire. Il est présent dans sept (7) pays de la zone UEMOA (la Côte d'Ivoire, le Bénin, le Burkina Faso, le Mali, le Niger, le Sénégal et le Togo) et un pays de la zone CEMAC (le Cameroun). Ainsi, afin de mener à bien notre étude, nous allons présenter de la BASN à travers son historique, ses missions, ses produits et services, et enfin son organisation.

4.1. Historique

La Banque Atlantique du Sénégal (BASN) a été créée le 26 Avril 2005 avec un capital de 2 milliards FCFA. Ayant son siège social à Dakar, elle compte à ce jour 19 agences (12 à Dakar et sa banlieue et 7 en région). Elle intervient dans la pratique d'opérations de banque au Sénégal ou dans tout autre pays, soit pour son propre compte, soit pour le compte d'un tiers et opère sur tous les segments de marché à savoir les entreprises, les professionnels, les associations et institutions, et les particuliers.

Les principaux faits marquants de l'histoire de la BASN sont les suivants :

- 26 avril 2005: création de la société anonyme Banque Atlantique du Sénégal ;
- 28 décembre 2005: arrêté n°005988/MEF/DMC portant agrément de la banque ;
- 28 janvier 2006: entrée du groupe d'assurances SONAM dans le capital à hauteur de 25% ;
- 20 septembre 2007: démarrage des activités de transfert d'argent MoneyGram ;
- 30 juin 2010: nomination d'un nouveau Directeur Général.

4.2. Missions

Les missions de la BASN rejoignent celle du Groupe Atlantique. Il s'agit de :

- relever le niveau de bancarisation de l'économie sénégalaise et améliorer l'accès des populations aux services financiers ;
- œuvrer pour un meilleur développement au travers des solutions durables et représentatives ;

- former une communauté humaine fière et solidaire, travaillant efficacement au bonheur de tous (clients, actionnaires et salariés) ;
- mobiliser jour après jour une expertise permettant aux clients de réaliser leurs projets en Afrique.

4.3. Produits

La Banque Atlantique du Sénégal offre différents produits selon la spécificité des agents économiques c'est-à-dire les particuliers, les professionnels, les entreprises, les associations et institutions. Il s'agit de la collecte de l'épargne, des opérations de crédit, de la mise à la disposition du public des moyens de paiement, de la monétique, et de la bancassurance.

4.3.1. Collecte de l'épargne

Au sein de la BASN, les clients ont le choix entre:

- les épargnes ordinaires (dépôts à vue, et dépôts à terme) ;
- des épargnes atlantiques : l'ouverture de ces comptes est réservé aux particuliers disposant d'une épargne supérieure à FCFA 5 000 000 ;
- les épargnes diaspora permettant d'investir dans son pays d'origine depuis l'étranger ;
- les bons de caisse.

4.3.2. Opérations de crédit

Il s'agit des découverts sur compte, des découverts sur carte privilège, des escomptes, des avances sur marché, des avances sur bon de commande, des crédits à court terme, des crédits équipement, des cautions en douane, des cautions de marché, des crédits documentaires import, des crédits SPOT, du financement du commerce extérieur, des engagements par signature (cautions/garanties/aval).

4.3.3. Moyens de paiement

Il s'agit des chèques, des virements, des virements permanents, des ordres de prélèvement, et des cash management.

4.3.4. Monétique

La banque Atlantique du Sénégal offre à ses clients professionnels plusieurs cartes pour leurs opérations. Il s'agit :

- des cartes épargne : carte de retrait sur un compte d'épargne ;
- des cartes privilège : carte de retrait et de paiement à débit immédiat associé à un compte courant ;
- des cartes cash : ce sont des cartes rechargeables qui ne nécessitent pas de compte bancaire ;
- des cartes traveller : cartes prépayées internationales
- des cartes premium : cartes adossées à un compte chèque avec une ligne de crédit renouvelable ;
- des cartes hajj : elles permettent d'effectuer des paiements et retraits d'argent en Rial Saoudien, sans frais de changes de devises.

4.3.5. Bancassurance

Il s'agit de l'assurance vie, qui, adossée à un compte garanti à son titulaire, ainsi qu'à ses proches, un capital en cas de décès ou d'invalidité temporaire ou définitive.

4.3.6. Les autres services

Il s'agit des services :

- d'intermédiation financière ;
- d'ANET ;
- de SMS Banking ;
- de transfert d'argent ;
- de guichets automatiques de banque
- des terminaux de paiement électronique (TPE)

4.3.6.1. Intermédiation financière

Les clients bénéficient d'une assistance en intermédiation financière, conseil financier, gestion de portefeuille, négociation à la Bourse Régionale des Valeurs Mobilières (BRVM) de l'UEMOA.

4.3.6.2. ANET

L'ANET permet aux clients d'avoir accès à leurs comptes par micro-ordinateur, ou par téléphone mobile grâce à internet.

4.3.6.3. SMS Banking

Il permet aux clients d'être informés en temps réel sur leurs téléphones mobiles des opérations remarquables effectués sur leurs comptes bancaires. Les clients reçoivent des informations automatiquement ou à leur demande.

4.3.6.4. Transfert d'argent

Toutes les agences de la Banque ont des guichets Money Gram, Money Cash ou Western-union pour les transferts d'argents à travers le monde.

4.3.6.5. Guichets automatiques de Banque

Ils permettent de retirer de l'argent, d'avoir le solde de son compte, d'éditer des mini relevés.

4.3.6.6. Terminaux de paiement électronique (TPE)

Les TPE permettent de régler les achats par carte bancaire auprès des commerçants affiliés au réseau Banque Atlantique (Carte Atlantique Privilège, Atlantique Flash) et au réseau Mastercard (Carte Atlantique Premium, Atlantique Traveler).

4.4. Organisation

Depuis le 1^{er} mars 2009, la Banque Atlantique du Sénégal est constituée des directions suivantes :

- La Direction Générale ;
- La Direction de l'Audit Interne ;
- La Direction des risques ;
- La Direction Financière et Comptable ;
- La Direction des Opérations ;

- La Direction de la Clientèle Entreprise ;
- La Direction de la Clientèle Particuliers et Réseau ;
- La Direction de la Trésorerie.

4.4.1. La Direction Générale

Elle est chargée de suivre, de coordonner et d'orienter des actions de toutes les directions de la banque en prenant en compte les recommandations de la Direction de l'Audit Interne. Ses missions sont les suivantes :

- coordonner les actions des Directions et des Services qui lui sont directement rattachés ;
- définir la politique générale de la banque en liaison avec le Conseil d'Administration,
- animer le Comité de Direction ;
- appliquer les directives de Conseil d'Administration ;
- représenter la banque vis-à-vis des tiers et des Autorités de tutelle.

4.4.2. La Direction de l'Audit Interne

L'objectif de l'audit interne est d'assister les dirigeants dans leur responsabilité en leur fournissant des recommandations établies sur la base d'évaluation et d'analyses objectives et indépendantes. Elle a pour attribution les activités ci-dessous :

- vérifier et apprécier la fiabilité, la conformité et l'application des principes comptables, financiers, et autres contrôles opérationnels et promouvoir un contrôle efficace à moindre coût ;
- s'assurer du respect de la réglementation qui établit les procédures institutionnelles, plans et procédures ;
- déterminer si les avoirs de la BASN sont correctement comptabilisés et protégés des pertes et risques en tout genre ;
- s'assurer de la fiabilité des données de direction développées au sein de l'organisation ;
- apprécier la qualité des performances en assumant des responsabilités définies ;
- recommander des améliorations opérationnelles.

4.4.3. La Direction des risques

Elle est constituée du service analyse des crédits et du service contrôle et administration de crédits.

- Le Service analyse des crédits est chargé de l'instruction de toutes des demandes de crédit émanant de la clientèle, la cotation de l'ensemble des clients de la Banque, de la réalisation des études sectorielles pour orienter la politique de crédit de la Banque.
- Le service contrôle et administration de crédits assure le contrôle et le suivi des dossiers de crédit.

4.4.4. La Direction financière et comptable

Elle a quatre services à savoir : le service de contrôle de gestion, le service de comptabilité, le service de rapprochement et le service contrôle, évaluation et conseil. Elle est chargée du contrôle, de la saisie et de la comptabilisation des opérations, ainsi que de l'enregistrement des ordres de dépenses après validation par les chefs de service.

4.4.5. La Direction des opérations

Trois services composent cette direction : le service du portefeuille local, de service du portefeuille étranger et le service gestion des caisses des agences. Cette Direction joue un rôle important dans la comptabilisation des opérations bancaires.

4.4.6. La Direction de la clientèle entreprise

Elle s'occupe de la gestion des clients Grandes Entreprises, PME/PMI.

4.4.7. La Direction de la Clientèle Particuliers et du Réseau

Elle a pour rôle la gestion de la clientèle « particuliers » et l'extension du réseau de la BASN pour se rapprocher d'avantage de la population. Dans cette direction, nous retrouvons le service monétique pour la vente et l'utilisation des cartes monétiques, le service de transfert d'argent et le service de communication.

4.4.8. La Direction de la trésorerie

Elle est chargée de gérer la liquidité à travers la gestion des comptes de la banque, et la participation aux opérations d'emprunts et de prêts interbancaires. Elle doit également générer des revenus de change, gérer les risques de change et les risques pris sur les contreparties bancaires.

Dans l'optique de l'atteinte de ses objectifs la Banque Atlantique du Sénégal a mis en œuvre un système de gestion des risques pouvant survenir en son sein, et en particulier des risques opérationnels portant sur la sécurisation des fonds déposés par leurs clients en particulier. Le prochain chapitre sera donc pour nous l'occasion d'effectuer un audit de ce système.

CESAG - BIBLIOTHEQUE

CHAPITRE 5 : L'AUDIT DU SYSTEME DE MANAGEMENT DES RISQUES OPERATIONNELS LIES AUX DEPOTS AU SEIN DE LA BANQUE ATLANTIQUE DU SENEGAL

D'après la norme 2100 de l'I.I.A, l'audit interne doit aider l'organisation en identifiant et en évaluant les risques significatifs et contribuer à l'amélioration des systèmes de management des risques et de contrôle. Cela suppose l'utilisation d'une approche systématique et méthodique nécessitant une bonne connaissance de ces systèmes et des processus de l'organisation. Ainsi, la première étape de notre mission qui fera l'objet de ce chapitre consistera à la prise de connaissance du processus de collecte de fonds et du système de couverture des risques opérationnels mis en œuvre pour sécuriser ce processus.

5.1. Le processus de collecte des fonds

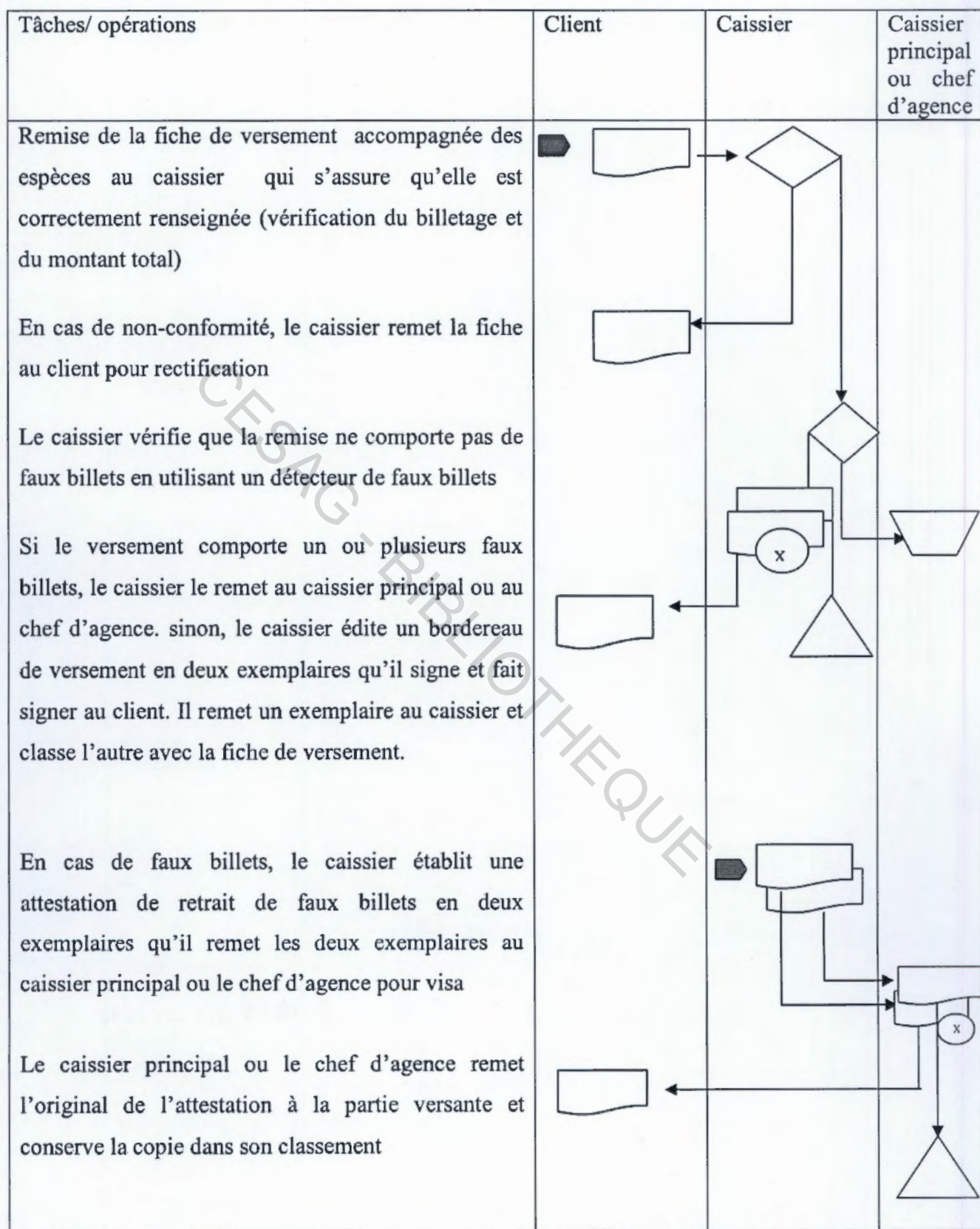
Ce processus commence par l'ouverture de la caisse chaque matin, ensuite la réception des fonds déposés par les clients, la sécurisation dans la caisse principale et le transfert vers la banque centrale. Il sera présenté sous forme de diagrammes (flow-chart) et la légende sera en annexe à la page 82.

5.1.1. Ouverture des caisses

L'ouverture des caisses est une procédure lancée le matin par chaque caissier

Tâches /opérations	Caissier
Saisie des informations d'ouverture de caisse dans le système	<pre> graph TD Start(()) --> B1[] B1 --> B2[] B2 --> B3[] B3 --> End(()) </pre>
Edition d'un relevé d'encaisses d'ouverture	
Vérification de la conformité entre le relevé d'encaisses d'ouverture et celui de clôture de la veille	
Classement du relevé d'encaisses d'ouverture	

5.1.2. Versement des espèces et enregistrement de l'opération



5.1.3. Enregistrement de l'opération

Tâches/ opérations	Caissier	Client
<p>Le caissier saisit l'opération dans le système et édite un bordereau de versement en deux exemplaires</p> <p>Le caissier appose le cachet de la caisse et son visa sur les deux exemplaires du bordereau et demande au client d'y apposer sa signature</p> <p>Le caissier remet l'un des bordereaux au client et agrafe l'autre à la fiche de versement d'espèces</p> <p>Le caissier range les deux justificatifs dans la boîte de la journée comptable des caisses</p>		

5.1.4. Versement dans la caisse principale

Ce versement peut être effectué sur l'initiative du caissier s'il a trop d'argent dans sa caisse ou si le caissier principal le lui demande (le plafond est de dix millions de FCFA).

Tâches/opérations	Caissier	Chef de caisse
<p>A la réception des fonds, le chef de caisse procède au recomptage des espèces et saisit l'opération dans le système</p> <p>Le système édite le bordereau de versement en deux exemplaires. le chef de caisse y appose le cachet « payé »</p> <p>Le chef de caisse signe les deux exemplaires et les remet au caissier qui les signe à son tour</p> <p>Il remet la copie du bordereau au caissier et conserve l'original qu'il classe dans la journée comptable</p> <p>Le caissier saisit également l'opération</p>		

5.1.5. Versement à la BCEAO

Les versements à la BCEAO interviennent lorsque la banque dispose d'encaisses jugées excessives notamment par rapport à sa couverture d'assurance (le plafond est de cinq milliards de FCFA).

Tâches /opérations	Caissier principal	Agent de la société de convoi de fonds (SAGAM)	Agent BCEAO
<p>Après le tri et la mise en sac des fonds, le caissier principal remplit un formulaire de versement d'espèces (imprimé BCEAO), le signe et le remet à l'agent de SAGAM (agence de transport de fonds) pour signature.</p> <p>L'agent de la SAGAM remet les fonds à l'agent de la BCEAO, puis le formulaire de versement pour signature</p> <p>L'agent de la BCEAO fait une copie du bordereau la remet à l'agent de SAGAM qui revient à la banque la remettre au caissier principal qui la classe</p>			

5.1.6. Fermeture provisoire de la caisse

Cette opération s'effectue en fin de journée par le caissier.

Tâches/opérations	Caissier	Chef de caisse
<p>Le caissier procède au comptage des espèces en caisse</p> <p>Il reporte ensuite le détail journalier de son encaisse sur le cahier de décomposition (billets-pièces), arrête le montant total de l'encaisse et le remet au caissier principal ou au chef d'agence pour visa</p>		
<p>Le caissier saisit le montant de l'encaisse physique déterminé lors du comptage</p> <p>Il vérifie qu'il n'y a pas d'erreur et valide la saisie de l'opération</p>		
<p>Le caissier remet au chef de caisse toutes les pièces comptables de la caisse de la journée</p> <p>Le caissier range les espèces dans sa malle et la ferme à clé. Il dépose la malle dans la salle des coffres</p>		

5.1.7. En cas de manquant ou d'excédent de caisse

Tâches/ opérations	Caissier principal ou chef d'agence	Audit interne	Caissier
<p>Le caissier principal ou le chef de caisse édite le ticket de différence de caisse et le transmet à l'audit interne</p> <p>Selon le montant et la récurrence des différences, une demande d'explication est adressée au caissier concerné</p>			

5.2. La gestion des risques opérationnels au sein de la Banque Atlantique du Sénégal

Après la phase de prise de connaissance du processus de collecte des fonds, notre mission d'audit s'est poursuivie par la prise de connaissance du dispositif mis en œuvre pour la gestion des risques opérationnels. A cet effet, nous avons, dans un premier temps administré un questionnaire puis, nous avons eu des entretiens avec les personnes suivantes :

- un risk-manager ;
- le chef service caisse ;
- la caissière principale ;
- le contrôleur des opérations ;
- les cinq auditeurs ;
- deux assistants des ressources humaines ;
- trois gardiens.

Après ces entretiens, nous avons procédé à une analyse du manuel de procédure et du manuel de contrôle. Enfin, nous étions aux services de la caisse pour vérifier par nous même l'effectivité des mesures prises par la Banque Atlantique Sénégal pour sécuriser les fonds reçus des clients. Ainsi, nous avons pu observer les opérations de caisse et tout le dispositif mis en œuvre pour la sécurisation des espèces déposées.

Nous avons pu constater qu'au sein de la Banque Atlantique du Sénégal, il n'existe pas de procédure formalisée d'identification des risques opérationnels. La BASN n'utilise non plus des outils statistiques dans l'analyse des incidents liés aux risques opérationnels. La gestion risques opérationnels se rapportant aux dépôts des clients se résume au contrôle interne et au dispositif d'assurance.

5.2.1. Le contrôle interne

Notre mission d'audit comportait une évaluation du contrôle interne. A cet effet, nous avons fait des constats sur les points suivants :

- le personnel de caisse ;
- le gardiennage ;

- la sécurité des locaux ;
- la sécurité des fonds déposés.

5.2.1.1. Le personnel de la caisse

Nous savons qu'il est nécessaire de mettre l'accent sur la qualité des personnes devant servir à ce point stratégique qu'est la caisse car elle représente le point de contact par lequel le client porte ses premières appréciations de la banque.

Ainsi, au cours de notre mission d'audit, nous avons eu des entretiens avec deux assistants du Directeur des ressources humaines. Ces derniers nous ont appris qu'il existe une procédure de présélection du personnel de la caisse qui débouche sur une période d'essai au cours de laquelle le nouvel employé suit une formation dispensée par les collaborateurs de la banque ou des intervenants extérieurs. Pendant et après cette période d'essai, le candidat est évalué. Il ne sera intégré que si le résultat de cette évaluation est satisfaisant.

5.2.1.2. Le gardiennage

Il est assuré par une société ayant signé une convention avec la Banque Atlantique Sénégal. Après des entretiens avec le personnel de gardiennage et de l'audit interne, nous notons qu'une procédure de contrôle de la prise de fonction effective et de la relève des éléments de surveillance est mise en place. Nous avons pu vérifier l'existence d'un registre de prise de fonction et de départ du personnel de gardiennage.

Par ailleurs, des contrôles inopinés sont effectués afin de s'assurer de la prise de fonction effective des éléments de surveillance particulièrement la nuit.

Nous avons pu observer que les gardiens sont facilement identifiables par des badges et des uniformes et sont géographiquement bien repartis à des endroits stratégiques de la banque notamment. Ils ont des moyens de communication (téléphones).

5.2.1.3. La sécurité des locaux

Pour la sécurité de ses locaux, la BASN a institué un dispositif qui permet d'identifier aisément le personnel à travers le port des badges. Par ailleurs, la circulation dans la banque est réglementée avec des accompagnateurs et des badges visiteurs.

La banque est équipée de moyens de sécurité avec des alarmes, des caméras et des détecteurs d'incendie géographiquement bien repartis. Lors de mission d'audit, les dispositifs sécuritaires font l'objet de tests réguliers de fonctionnement. Les employés sont formés à l'utilisation des extincteurs.

Malheureusement, le système d'alarme de la banque n'est pas relié à un poste de police proche.

5.2.1.4. La sécurité des fonds déposés

Nous avons scindé le processus de collecte de fonds en plusieurs objets auditables. Ainsi nous avons retenus les étapes suivantes : l'ouverture des caisses ; la réception des espèces ; le versement dans la caisse principale (réserve) et le versement à la BCEAO.

- l'ouverture des caisses :

Au cours de notre mission, nous avons pu vérifier que les caissiers ne sont pas autorisés à accéder aux compartiments avec des effets personnels (sac à main, valises...). Il y a une armoire dans laquelle ils les rangent avant d'entrer dans les compartiments. Par ailleurs, chaque caissier possède un compte utilisateur et un mot de passe sécurisé. Nous avons appris du chef de caisse et des auditeurs que ces comptes sont désactivés en cas de démission ou de licenciement du caissier.

- la réception des espèces et des chèques :

Toutes les caisses sont munies de caméras de surveillance et lors des missions menées par les auditeurs de la banque, des tests de fonctionnement de ces caméras sont effectués. Les caissiers ont la possibilité de détecter des fausses signatures par comparaison avec celles intégrées dans le système et ont des monnaies d'appât (bait money) nécessaires à la recherche d'éventuels voleurs.

Malheureusement, toutes les caisses ne sont pas munies de détecteurs de faux billets et les caissiers ne sont pas formés à la détection de chèques falsifiés. Par ailleurs, le personnel de la caisse n'est pas formé sur la conduite à tenir en cas de braquage.

La Banque Atlantique Sénégal possède une procédure de lutte contre le blanchiment d'argent. En effet, les caissiers sont formés à la détection des opérations atypiques et suspectes (versement de montants très élevés par un client qui n'a pas l'habitude de le faire). Par ailleurs, il existe un progiciel dénommé AMAB greffé sur le système de la banque ORION permettant d'identifier les opérations suspectes. Un employé de la banque est spécialement chargé de la détection des opérations de blanchiment d'argent.

- Le versement dans la réserve

Il existe des plafonds d'espèces que les caissiers doivent détenir. Le recomptage des espèces par le chef de caisse avant le transfert à la réserve se fait en présence du caissier. Tous les deux signent le bordereau de versement imprimé en deux exemplaires. La présence d'une troisième personne lors de cette opération serait souhaitable (contrôleur des opérations, chef service caisse ou auditeur par exemple) afin de minimiser les risques de collusion entre des deux.

Les clés et codes d'accès à la caisse principale sont détenus par des personnes distinctes. Toutes les espèces de la réserve sont contenues dans des coffres ignifuges et hydrofuges. En cas de départ en congés du détenteur du code, ce dernier le remet à une autre personne. Malheureusement, en cas d'affectation ou de démission du détenteur des codes, ces derniers ne sont pas toujours modifiés.

- le versement à la BCEAO

Le transfert des espèces à la Banque centrale s'effectue par le biais d'une société de convoi de fonds (SAGAM). Ceci est un point fort pour la Banque Atlantique car en externalisant cette activité, non seulement le risque est transféré à un tiers, mais la Banque bénéficie d'une meilleure qualité du service et d'un gain en productivité.

Nous avons remarqué que non seulement la sortie des fonds de la BASN bien que scellés dans des sacs s'effectue devant les clients assis dans la salle d'attente mais en plus le transfert jusqu'à la BCEAO se fait sans la présence ni d'un agent de la BASN, ni de la Banque Centrale.

5.2.2. Le dispositif d'assurance

Pour couvrir les risques opérationnels se rapportant aux dépôts bancaires, la BASN a souscrit une police d'assurance auprès de la SONAM S.A. et qui couvrent les dégâts causés par les incendies, les inondations, la destruction des locaux suite à un soulèvement des populations (émeutes), les vols commis par les personnes extérieures à la Banque, les vols ou détournements commis par le personnel de la banque, les risques liés au système informatique et le coût de remplacement des matériels détruits.

CESAG - BIBLIOTHEQUE

CHAPITRE 6 : RESULTATS ET RECOMMANDATIONS

Après avoir étudié le processus de réception et de sécurisation des espèces et des chèques des clients, nous avons décrit le système de management des risques opérationnels liés à ce processus. Ce système porte sur le personnel de la caisse, le contrôle au cours de la réception des espèces et des valeurs, la sécurité des locaux, des fonds dans le réserve et le système informatique.

Dans ce chapitre, nous présenterons la suite de notre mission d'audit qui portera tout d'abord sur l'élaboration du tableau des Risques référentiel (TaRiR). A partir de ce tableau, nous listerons les tests à faire qui nous permettrons de relever les forces et les faiblesses du système de management des risques opérationnels liés aux dépôts des clients. Des faiblesses identifiées, nous élaborerons des FRAP (Feuilles de Révélation d'Analyse des Problèmes) et enfin nous présenterons nos recommandations.

6.1. Les résultats

Les résultats de notre analyse seront présentés à travers le tableau de risques référentiels, les tests, la feuille de révélation et d'analyse des problèmes.

6.1.1. L'élaboration du tableau des risques référentiel (TaRiR)

Dans ce tableau, nous allons, pour chaque étape du processus de réception des fonds des clients:

- identifier la finalité de cette étape, c'est-à-dire l'objectif du contrôle interne ;
- définir des scénarii d'empêchement c'est-à-dire les risques que la finalité ne soit pas atteinte ;
- identifier les points de contrôle. Ces points de contrôle décrivent ce que ce que l'auditeur doit contrôler ;
- identifier les impacts de la défaillance ou de la déficience du contrôle interne ;
- énoncer les bonnes pratiques qui décrivent ce que les audités doivent faire pour éviter les scénarii d'empêchement.

Tableau 3 : Tableau des Risques référentiel (TaRiR)

Etapes	Finalités (objectifs de contrôle interne)	Empêchements (scénarii qui empêcheraient l'atteinte des objectifs de contrôle interne)	Points de contrôle	Impacts (conséquences de la défaillance/déficience du point de contrôle)	Bonnes pratiques
Ouverture des caisses	Ouvrir les caisses dans le système en s'assurant que le solde physique de la veille correspond au solde comptable	Détournement, collusion entre le chef de caisse et le caissier	Vérifier que des contrôles inopinés des caisses sont régulièrement effectués	Ecart dans la caisse	Etablir de bordereau de versement en présence d'une troisième personne (chef service caisse ou contrôleur des opérations ou auditeur), désactiver le compte utilisateur d'un caissier quand celui-ci est licencié ou a démissionné
		Vols	S'assurer du contrôle de la prise de fonction effective des gardiens dans la nuit, s'assurer du bon fonctionnement des alarmes.	Atteinte à l'image de la Banque, crainte des clients, écart dans la caisse.	Installer un système d'alarme relié au poste de police le plus proche.

Tableau 4 (suite) : Tableau des Risques référentiel (TaRiR)

Etapes	Finalités (objectifs de contrôle interne)	Empêchements (scénarii qui empêcheraient l'atteinte des objectifs de contrôle interne)	Points de contrôle	Impacts (conséquences de la défaillance/déficiences du point de contrôle)	Bonnes pratiques
Réception des espèces et des chèques par les caissiers	Recevoir la totalité du montant inscrit sur la fiche de versement ou les chèques en s'assurant d'une bonne imputation dans le compte du client	Réception de faux billets/fausses pièces Chèques falsifiés	S'assurer que chaque caisse dispose d'un détecteur de faux billets et d'une caméra de surveillance ; faire des tests réguliers de fonctionnement des appareils de sécurité	inadéquation entre solde physique et solde comptable	Munir toutes les Caisses de détecteurs de faux billets, former les caissiers à la détection de chèques falsifiés
		braquage	S'assurer du bon fonctionnement des caméras de surveillance et du système d'alarme	Atteinte à l'image de la Banque, crainte des clients, écart dans la caisse	Former les caissiers à la procédure à suivre en cas de braquage ; mettre des détecteurs d'armes aux entrées.
		système informatique défaillant	S'assurer que le système informatique fait l'objet de révisions périodiques	remplissage manuel des bordereaux de versement avec des risques d'erreurs (montant, numéros de compte)	Améliorer le système d'informatique en le décentralisant. (donner la possibilité aux personnels du service informatique de résoudre les problèmes liés à la connexion internet)

Tableau 4 (suite et fin) : Tableau des Risques référentiel (TaRiR)

Etapes	Finalités (objectifs de contrôle interne)	Empêchements (scénarii qui empêcheraient l'atteinte des objectifs de contrôle interne)	Points de contrôle	Impacts (conséquences de la défaillance/déficience du point de contrôle)	Bonnes pratiques
Versement des espèces la caisse principale (la réserve)	Reverser la totalité des espèces contenues dans les caisses et les sécuriser	Collusion entre le chef de caisse et le caissier ou entre le détenteur de la clé et celui du code	S'assurer que les clés et les codes de la réserve sont toujours détenus par des personnes distinctes ; s'assurer de la modification des codes en cas de démission ou de licenciement de l'ancien détenteur	Détournements, écart dans la réserve	Faire participer une troisième personne au comptage des espèces (contrôleur des opérations ou chef service caisse ou auditeur) avant le dépôt dans la réserve ; modifier les codes du coffre-fort dès le départ de l'ancien détenteur (licenciement ou démission)

Source : nous-mêmes à partir de SCHICK (2007 :78)

6.1.2. Les tests

Les tests à effectuer au cours de notre mission d'audit découlent des points de contrôle. Il s'agit de vérifications qui nous permettront de nous s'assurer que les objectifs de chaque étape du processus de réception des fonds des clients pourront être atteints.

Tableau 4 : Les tests à effectuer

Etapes	Finalités	Point de contrôle	Tests à effectuer
Ouverture des caisses	Ouvrir les caisses dans le système en s'assurant que le solde physique de la veille corresponde au solde comptable	S'assurer que des contrôles inopinés des caisses sont régulièrement effectués	Consulter les rapports dans de la Direction de l'audit interne de l'effectivité des contrôles inopinés
		S'assurer du contrôle de la prise de fonction effective des gardiens dans la nuit	Consulter le registre de présence des gardiens et vérifier les horaires de prise de fonction
		S'assurer du bon fonctionnement des alarmes	Tester toutes les alarmes des caisses pour s'assurer de leur fonctionnement
Réception des espèces et des chèques par le caissier	Recevoir la totalité du montant inscrit sur la fiche de versement ou les chèques en s'assurant d'une bonne imputation dans le compte du client	S'assurer que les caisses sont munies de détecteurs de faux billets	Vérifier pour chaque caisse l'existence de détecteur de faux billets
		S'assurer que chaque caisse est munie de caméra de surveillance s'assurer aussi que ces caméras fonctionnent effectivement	Vérifier l'existence de caméras de surveillance pour chaque caisse et aller dans le bureau du chef de caisse et si à partir de son écran il peut contrôler toutes les caisses
		S'assurer du fonctionnement du système informatique (ORION)	Sur une période de vingt jours (cinq jours ouvrables de quatre semaines) identifier le nombre d'arrêt du système informatique
Versement des espèces à la caisse principale (la réserve)	Reverser la totalité des espèces contenues dans les caisses et les sécuriser	S'assurer que les clés et les codes de la réserve sont détenus par des personnes distinctes	Vérifier le PV de détention des clés et des codes de la réserve
		S'assurer de la modification du code en cas de licenciement ou de démission de l'ancien détenteur	Vérifier l'existence d'un PV de modification des codes de la réserve

Source : nous-mêmes à partir de SCHICK (2007 : 84)

6.1.3. Présentation des forces et des faiblesses du système de management des risques opérationnels liés aux dépôts bancaires

Les tests effectués nous ont permis de présenter les forces et les faiblesses réelles ou potentielles du système mis en œuvre par la BASN pour la gestion de ses risques opérationnels liés aux dépôts bancaires. Ainsi, nous avons pu mettre en exergue les opportunités découlant des forces et des faiblesses, nous avons émis des recommandations.

Tableau 6 : Tableau des forces et faiblesses du système de management des risques opérationnels liés aux dépôts bancaires

Eléments du système	Forces	Faiblesses	Risques
Identification et hiérarchisation des risques opérationnels		Pas de procédure formalisée d'identification et d'évaluation des risques opérationnels	Négligence des risques prioritaires du fait de l'absence d'évaluation et d'hiérarchisation
Personnel de la caisse	Existence d'une procédure de sélection du personnel de la caisse avec	Absence de formation des caissiers à la détection de chèques falsifiés	Réception de chèques falsifiés
	Formation et évaluation du personnel de la caisse	Pas de formation de caissiers sur la procédure à suivre en cas de braquage	Non application de la part des caissiers des procédures de procédures sécuritaires (activer l'alarme, introduire le bait money dans les sacs avant des le remettre aux voleurs)
Contrôle au cours de la réception des espèces ou des chèques	Toutes les caisses sont munies de système d'alarme et de caméras de surveillance	Toutes les caisses ne possèdent pas des détecteurs de faux billets	Réception de faux billets
	Des tests de fonctionnement des systèmes d'alarme et des caméras de surveillance sont régulièrement effectués		
	Toutes les caisses possèdent des monnaies d'appât (bait money)		
	Les caissiers sont formés à l'identification des opérations suspectes, un progiciel (AMAB) est installé dans le système et permet de détecter des opérations atypiques. Un agent de la banque est chargé de la lutte anti-blanchiment		

Tableau 6 (suite) : Tableau des forces et faiblesses du système de management des risques opérationnels liés aux dépôts bancaires

Eléments du système	Forces	Faiblesses	Risques
Sécurité des locaux	Les gardiens sont repartis à l'intérieur et à l'extérieur de la banque ainsi qu'au niveau des caisses.	Le système d'alarme n'est pas relié à un poste de police proche	Intervention lente de la police en cas de problème (braquage par exemple)
	Contrôles inopinés de la prise de fonction effective du personnel de gardiennage, notamment la nuit	Pas de détecteur d'armes aux entrées de la banque	Entrée de personnes détenant en possession des armes
	Existence de moyens de sécurité (extincteurs et détecteurs d'incendie) géographiquement bien repartis et faisant l'objet de tests réguliers		
	Le personnel est formé à l'utilisation des extincteurs		
Sécurité des fonds dans la réserve	Les clés et les codes de la réserve sont détenus par des personnes distinctes (aucun agent ne détient à la fois la clé et le code de la réserve)		
		Pas de changement des codes de la réserve en cas de licenciement ou de démission de l'ancien détenteur	Détention des codes de la réserve par des personnes extérieures à la banque
système informatique		lenteur dans la résolution des problèmes liés au système informatique car il est centralisé au niveau d'ATECH à Cotonou	Erreurs dans l'enregistrement des opérations qui préalablement ont été effectuées manuellement

Source : nous-mêmes à partir de SCHICK (2007 :89)

6.1.4. Elaboration des Feuilles de Révélation et d'Analyse des Problèmes (FRAP)

A partir des constats que nous avons faits, nous allons déterminer les causes, démontrer ces conséquences et proposer des moyens d'amélioration.

Tableau 6 : Feuilles de Révélation de d'Analyse des problèmes (FRAP N°1)

<p>CONSTATS :</p> <ul style="list-style-type: none">• toutes les caisses ne sont pas munies de détecteurs de faux billets ;• les caissiers ne sont pas formés à la détection des chèques falsifiés ;• les caissiers ne sont pas formés à la procédure à suivre en cas de braquage ;• il n'y pas de détecteurs d'armes aux entrées de la banque. <p>CAUSES :</p> <ul style="list-style-type: none">• absence de procédure formalisée portant sur les braquages• absence de procédure formalisée portant sur la détection de chèques falsifiés• les recommandations faites par les auditeurs au cours des missions précédentes concernant les détecteurs de faux billets n'ont été suivies <p>CONSEQUENCES :</p> <ul style="list-style-type: none">• réception de faux billets ou de chèques falsifiés ;• inadéquation entre solde physique et solde comptable ;• exposition de la banque aux braquages ; <p>RECOMMANDATIONS :</p> <ul style="list-style-type: none">• munir toutes les caisses de détecteurs de faux billets ;• former tous les caissiers à la détection de chèques falsifiés et à la procédure à suivre en cas de braquage ;• relier le système d'alarme de la banque à un poste de police proche
--

Source : nous-mêmes

Tableau 7 : Feuilles de Révélation de d'Analyse des problèmes (FRAP N°2)

<u>FEUILLE DE REVELATION ET D'ANALYSE DE PROBLEME</u>
<p>CONSTATS : les codes d'accès à la réserve ne sont pas modifiés en cas de démission ou de licenciement de l'ancien détenteur</p>
<p>CAUSES : Les employés notamment les chefs de caisse n'ont pas été formés à la modification des codes par les prestataires qui ont installé la réserve</p>
<p>CONSEQUENCES : Des anciens employés pourraient se retrouver en possession des codes de la réserve de la banque</p>
<p>RECOMMANDATIONS :</p> <ul style="list-style-type: none">• former les chefs de caisse à la modification des codes de la réserve ;• établir le cas échéant des procès verbaux de modification des codes de la réserve signés par le nouveau détenteur du code, le Directeur de l'audit interne, et le Directeur Général.

Sources : nous-mêmes

6.2. Recommandations

Dans ce paragraphe, nous formulerons les recommandations par rapport à :

- la gestion des risques opérationnels formalisés ;
- analyse des pertes survenues dans la banque ;
- la sécurité des espèces et des chèques reçus par les caissiers ;
- la sécurité lors des versements à la caisse principale ;
- la sécurité des espèces dans la caisse principale (réserve...)

6.2.1. Gestion des risques opérationnels formalisée

Pour une meilleure gestion des risques opérationnels, la BASN devrait disposer de procédures consignées par écrit portant sur l'identification, l'analyse, la surveillance et le contrôle des risques opérationnels, de même que les mesures visant à atténuer l'exposition à ces risques.

Les risk managers devraient établir une cartographie des risques opérationnels pouvant survenir au sein de la Banque, et ceci pour tous les processus notamment ceux des opérations de caisse (dépôts, retraits...).

Cette cartographie aura l'avantage d'avoir une hiérarchie des risques opérationnels, et ainsi, le programme de travail des risk managers et même des auditeurs sera adapté l'importance accordé à chacun de ces risques (en fonction de l'impact et de la probabilité de survenance).

6.2.2. Analyse des pertes survenues dans la banque

La banque devrait disposer de procédures consignées par écrit portant sur les événements générateurs de pertes survenus en son sein. Pour chacun de ces événements, elle devrait collecter les informations suivantes :

- le montant brut de la perte ;
- la date de l'événement ;
- les mesures d'atténuation de la perte (par exemple du fait de contrats d'assurance) ;
- le dispositif qui a été mis en œuvre pour que l'événement ne survienne plus.

Ainsi, en cas de récurrence, les employés de la banque et les risk – managers en particulier connaîtrons, la conduite à tenir et pourrons le cas échéant améliorer le dispositif de couverture contre ce risque.

6.2.3. La sécurité des espèces et des chèques reçus par les caissiers

Les responsables de la banque doivent veiller à ce que toutes les caisses soient équipées de détecteurs de faux billets qui feront l'objet de tests de fonctionnement réguliers. Par ailleurs, toutes les entrées de la banque doivent être munies de détecteurs d'armes.

Des ateliers de formation portant sur la procédure à suivre en cas de braquage ou sur la détection des chèques falsifiés devraient être organisés pour les caissiers.

Enfin, le système d'alarme de la banque devrait être relié à un poste de police proche. Cette liaison sera telle que en cas de problème (braquage par exemple), l'alarme ne sonnera pas dans la banque mais directement au poste de police. Ainsi, les cambrioleurs ne sauront pas que l'alarme a été déclenchée et pourront être appréhendés plus aisément.

6.3. Sécurité lors des versements à la caisse principale

Les auditeurs devraient de temps en temps faire des contrôles inopinés le matin à l'ouverture des caisses pour s'assurer qu'aucun caissier ne serait rentré avec l'argent dans l'intention de remettre le matin.

6.4. Sécurité des espèces dans la caisse principale (la réserve)

Nous avons constaté que les codes d'accès à la réserve ne sont pas modifiés après la démission ou le licenciement de l'ancien détenteur. Il se pose donc le problème de détention des codes des coffres forts par des personnes extérieures à la banque.

Par ailleurs, lors du départ en congé de l'un des détenteurs du code, ce dernier le remet à un autre employé compte tenu de ce qui est marqué dans les procès verbaux de détention des clés et codes. Malheureusement, au retour des congés du principal détenteur, le code n'est pas modifié. De ce fait, deux personnes se retrouvent avec le code de la réserve, ce qui pose le problème de traçabilité quant à la recherche du responsable en cas de vol dans la réserve.

Nous proposons donc que la société chargée d'installer ces codes de former des personnes extérieures au service de caisse à la modification des codes (les auditeurs par exemple). Ces personnes, pourront procéder au changement des codes chaque fois que le besoin se posera en établissant des procès verbaux de modification des codes signés par l'auditeur (celui qui a modifié le code) et le nouveau détenteur de ce code.

Toutes ces recommandations peuvent être synthétisées dans le tableau 8 suivant.

Tableau 8 : recommandations

Observation/ Problème	Recommandations	Responsables	Période de mise en œuvre
Absence de procédure portant sur la gestion des risques opérationnels	Elaboration d'une procédure portant sur l'identification, l'analyse, la surveillance des risques opérationnels	Direction générale et Risk managers	A partir de l'exercice prochain
Absence de cartographie des risques	Elaboration d'une cartographie des risques opérationnels permettant de les hiérarchiser afin de faciliter le programme de travail des auditeurs et risk managers	Risk managers	A partir de l'exercice prochain
Absence de reporting des incidents (générateurs de pertes) survenus dans la banque	Instaurer un système de reporting des incidents avec comme information : <ul style="list-style-type: none"> • le montant de la perte ; • la date de l'incident • les mesures prises pour l'atténuation de la perte (contrat d'assurance par exemple) • le dispositif mis en œuvre pour que l'évènement ne survienne plus 	Chef d'agence	A partir du mois prochain
Absence de détecteurs de faux billets dans les caisses	Munir toutes les caisses de détecteurs de faux billets qui feront l'objet de tests de fonctionnement réguliers	Direction générale et Business service	A partir du mois prochain
Pas de détecteur d'armes aux entrées de la banque	Installer des détecteurs d'armes aux entrées de la banque	Direction générale et Business service	A partir de l'année prochaine
Pas de liaison entre le système d'alarme et un poste de police proche	Etablir une liaison entre le système d'alarme de la banque et un poste de police proche tel qu'en cas de vol, l'alarme ne sonnera directement au poste de police	Direction générale et Business service	A partir du mois prochain

Tableau : recommandations (suite et fin)

Observation/ Problème	Recommandations	Responsables	Période de mise en œuvre
Pas de contrôles inopinés le matin	Effectuer des contrôles inopinés le matin à l'ouverture des caisses pour s'assurer qu'aucun caissier ne serait rentré avec l'argent dans l'intention de remettre le matin	Contrôleurs opérationnels et auditeurs interne	A partir du mois prochain
Pas de modification des codes d'accès à la réserve	<ul style="list-style-type: none"> • Former des personnes extérieures au service de la caisse à la modification des codes. • Modifier systématiquement les codes en cas de licenciement, de démission ou de retour des congés de l'ancien détenteur 	Contrôleurs opérationnels et auditeurs interne	A partir du mois prochain

En définitive, il ressort de notre mission que le système mis en œuvre par la Banque Atlantique pour le management des risques opérationnels liés aux dépôts se résume aux dispositifs de contrôle interne et d'assurance. Il n'existe pas de procédures écrites d'identification, d'analyse, de surveillance et de contrôle des risques opérationnels. Néanmoins, nous pouvons dire que le dispositif de contrôle interne avec des éléments tels que les systèmes d'alarme, les caméras de surveillance ou encore le progiciel de lutte anti-blanchiment AMAB permettent à la banque d'atteindre ses objectifs de sécurisation des fonds des clients.

Cette partie a été pour nous l'occasion de présenter les étapes de la mission d'audit que nous avons effectuée au sein de la Banque Atlantique du Sénégal portant sur les risques opérationnels liés aux opérations de collecte de l'épargne des clients.

Après une présentation de l'organisation, nous avons décrit le processus de collecte des fonds, puis le système mis en œuvre pour la maîtrise des risques opérationnels de la réception des fonds à la caisse, jusqu'au versement à la BCEAO, en passant par la sécurisation dans les coffres-forts de la banque.

A l'aide des outils que nous avons employés à savoir les questionnaires, les entretiens, les observations et les analyses documentaires, nous avons pu mettre en exergue les forces et les faiblesses de ce système. Par la suite, nous avons établi des Feuilles de Révélation et d'Analyse des Problèmes (FRAP) dans lesquelles nous avons proposé des mesures correctives.

Il ressort de tout cela que

Il revient maintenant aux dirigeants de la banque de prendre en compte les recommandations qui ont été formulées afin d'améliorer leurs résultats en évitant ou en couvrant ces risques.

CESAG - BIBLIOTHEQUE

CONCLUSION GENERALE

Il ressort de notre étude que le système de management des risques opérationnels est constitué de plusieurs activités à savoir l'identification des risques, l'évaluation des risques identifiés, la définition d'un niveau de risque acceptable, la mise en place de stratégie de couverture (contrôle interne, dispositif d'assurance, emprunt, externalisation, automatisations des transactions, franchise, financements alternatifs, captives), l'évaluation du risque net et le reporting.

Selon les travaux du Comité de Bâle portant sur le contrôle bancaire, la méthode de gestion du risque opérationnel choisie par chaque banque dépend d'une série de facteurs à savoir sa taille, le perfectionnement de ses techniques, ainsi que la nature et la complexité de ses activités. Toutefois, au-delà de ces différences, un dispositif efficace de gestion du risque opérationnel se caractérise par des éléments essentiels, quels que soient la taille et le champ d'action des banques. Il s'agit d'une formulation claire des stratégies et surveillance active par le conseil d'administration et la direction générale, et d'une solide culture du risque opérationnel et du contrôle interne (hiérarchie des responsabilités et de la répartition des tâches).

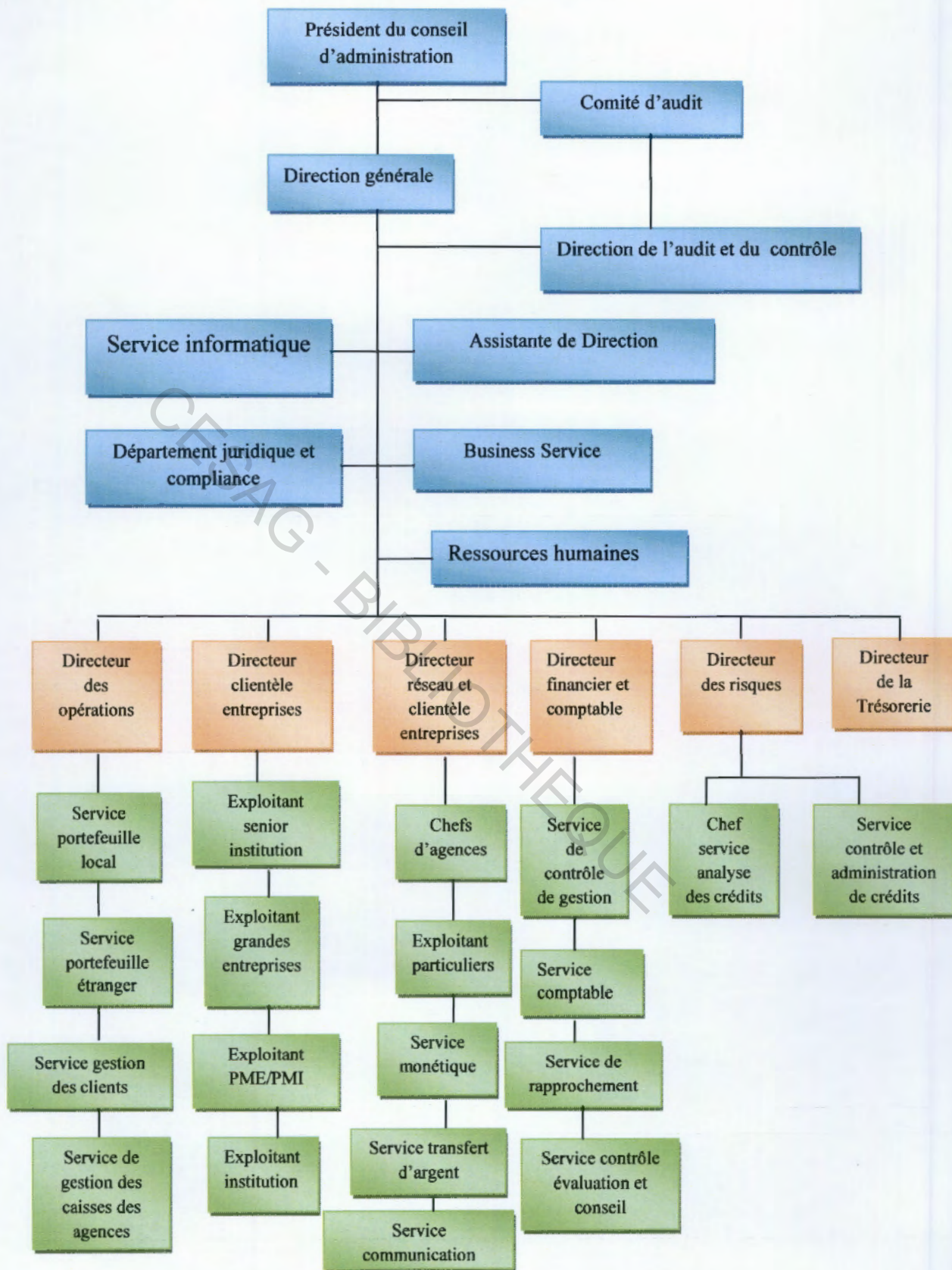
La mission menée au sein de la Banque Atlantique du Sénégal nous a permis de mettre en exergue les points forts, mais aussi les failles du système de management des risques opérationnels. Nous avons pu, à la lumière des bonnes pratiques énoncées par quelques auteurs proposer des recommandations dans l'optique d'une gestion plus saine et plus efficace des risques opérationnels pouvant survenir lors de la collecte des fonds.

La mise en œuvre de ces recommandations pourrait avoir l'avantage d'améliorer la situation financière de la BASN, ainsi que son image de marque, sa capacité de positionnement face à la concurrence ainsi la qualité de son personnel, les produits et les services rendus à ses clients créant ainsi de la valeur ajoutée.

CESAG - BIBLIOTHEQUE











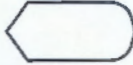
ANNEXES

Annexe 1 : Organigramme de la Banque Atlantique du Sénégal.



Source : Nous-mêmes à partir de l'organigramme de chaque direction de la Banque Atlantique Sénégal

Annexe 2 : Légende du flow-chart de description de processus de collecte de fonds

	Début du processus
	Document
	Liasse de documents
	Traitement
	Entrée manuelle
	Opération manuelle
	Multiple choix (si oui /si non)
	Signature
	Classement provisoire
	Classement définitif
	Vue à l'écran

Source : nous-mêmes à partir de BARRY (2009 : 61)

Annexe 3 : Questions posées au cours des entretiens

- **Avec les risk-managers :**
 - Existe-t-il au sein de votre département un processus de gestion des risques opérationnels ? Si oui ce processus est-il formalisé ?
 - Établissez-vous des cartographies des risques ? Si oui cette cartographie intègre-t-elle les risques opérationnels ?
- **Avec les auditeurs internes**
 - Ya t-il déjà eu des incidents liés aux risques opérationnels au sein de cette banque ?
 - Ces incidents ont-ils fait l'objet de reporting
 - Quelles étaient les mesures correctives appliquées ?
 - Existe-t-il un document mentionnant les noms des détenteurs des clés et des codes de la réserve ? Si oui, est-il précisé les noms des back-up pour chaque détenteur ?
- **Avec le chef de caisse**
 - Que faites vous lorsqu'en fin de journée, vous constatez un manquant ou un excédent dans une de vos caisse ?
- **Avec le gestionnaire de caisse**
 - Quel est le montant maximal que doit contenir une caisse ?
 - Quel est le montant maximal que doit contenir la réserve ?
 - Les caissiers sont ils autorisés à demander aux clients l'origine des fonds pour un dépôt d'un montant très élevé ?
- **Avec les caissiers**
 - Est-il facile pour vous d'identifier des faux billets à vue d'œil ?
 - Êtes-vous formés à la procédure à suivre en cas de braquage ou d'incendie ?
 - Ya t-il un plafond d'espèces que vous devez détenir ? Si oui que faites vous lorsque ce plafond est atteint ?
 - Qu'est ce qui pourrait expliquer les manquants ou les excédents de caisse en fin de journée ?
 - Que faites vous lorsque le système informatique (ORION) ne fonctionne pas ?

- Que faites vous lorsqu'un client vient déposer des biens abimés, déchirés... ?
- **Avec les assistants de la Directrice des Ressources Humaines**
 - Quelles sont pour vous les qualités d'un bon caissier ?
 - Une formation particulière est-elle dispensée aux nouveaux employés de la banque notamment les caissiers ?
 - Les caissiers sont-ils formés à la procédure à suivre en cas d'incendie ? En cas de braquage ?
- **Avec le personnel de gardiennage**
 - Avez-vous des moyens de communication (téléphone, talkie...) ?
 - Y a-t-il des personnes qui viennent vérifier la nuit que vous êtes effectivement en poste ?
 - Que feriez-vous si la personne chargée de vous remplacer au moment de la relève ne se présentait pas ?
 - Quelle est la procédure que vous devez suivre en cas de braquage ? En cas d'incendie ?

Annexe 4 : Questionnaire sur les stratégies de couverture des risques opérationnels liés aux dépôts bancaires

Au cours de notre revue de littérature nous avons recensé huit stratégies de couverture des risques opérationnels liés aux dépôts bancaires. Il s'agit :

- du contrôle interne ;
- du dispositif d'assurance ;
- du recours à l'emprunt ;
- de l'automatisation des transactions ;
- de l'externalisation ;
- de la franchise ;
- des financements alternatifs ;
- des captives ;

A. le contrôle interne

A.1. Le personnel de la caisse :

Nous savons qu'il est nécessaire de mettre l'accent sur la qualité des personnes devant servir à ce point stratégique qu'est la caisse car elle représente le point de contact par lequel le client porte ses premières appréciations sur la banque.

Questions	Oui	Non
a- Existe-t-il une procédure de présélection du personnel de la caisse (interviews, tests, questionnaires) ?		
b- Est-il tenu un fichier des candidats examinés ?		
c- La vérification des « curriculum vitae » par la prise de renseignements extérieurs est elle effective (recommandations, diplômes, expérience dans d'autres établissements...) ?		
d- Existe-t-il un échéancier de périodes d'essai ?		
e- Une évaluation détaillée est-elle établie pendant et après chaque période d'essai ?		
f- Un budget de formation du personnel de la caisse est-il prévu ?		
g- Existe-t-il un plan de formation formalisé pour le personnel de la caisse ?		
h- Une formation particulière est-elle dispensée aux nouveaux employés de la banque ?		
i- Y a-t-il une évaluation de la qualité et des résultats de la formation ?		
j- Les actions de formation sont-elles dispensées par des collaborateurs de la banque ou confiées à des intervenants extérieurs ?		

A.2. Le gardiennage

Questions	Oui	Non
a- Une procédure de contrôle de la prise de fonction effective et de la relève des éléments de surveillance est-elle en place ?		
b- Les gardiens sont-ils identifiables (badges, uniformes) ?		
c- Les gardiens sont-ils géographiquement repartis aux endroits stratégiques notamment la caisse ?		
d- Les gardiens de nuit ont-ils des moyens de communication à leur disposition (téléphone, talkie...) ?		
f- Ont-ils les coordonnées téléphoniques des membres du responsable de sécurité de la banque ?		
g- Des contrôles inopinés sont-ils effectués pour s'assurer de la prise de fonction effective des éléments de surveillance de nuit ?		

A.3. La sécurité des locaux

Questions	Oui	Non
a- Le personnel de la banque est-il facilement identifiable (port des badges) ?		
b- La circulation de la clientèle dans la Banque est-elle réglementée (badges visiteurs, accompagnateurs) ?		
c- La Banque est-elle équipée de moyens particuliers de sécurité (alarme, caméras, détecteurs d'incendie...) ?		
d- Des tests de fonctionnement de ces moyens de sécurité sont-ils régulièrement effectués ?		
e- Les employés de la banque sont-ils formés à l'utilisation des extincteurs ?		

A.4. La sécurité des fonds déposés

A.4.1. Ouverture des caisses

Questions	Oui	Non
a- Chaque caissier utilise-t-il toujours la même caisse ?		
b- Chaque caissier possède-t-il un compte utilisateur des ordinateurs ?		
c- Si oui ces comptes utilisateurs sont-ils accompagnés de mots de passe sécurisés ?		
d- En cas d'affectation ou de démission ou de licenciement du caissier, son compte utilisateur est-il désactivé ?		
d- les caissiers sont-ils autorisés à accéder aux caisses avec des bagages (sac à main, valises...)		
e- Existe-t-il des moyens de contrôle d'accès à la caisse (badges...)?		

A.4.2. Versement des espèces

Questions	Oui	Non
a- Toutes les caisses sont-elles munies d'un détecteur de faux billets ?		
b- Si oui des contrôles des détecteurs de ces faux billets sont-ils régulièrement effectués ?		
c- Toutes les caisses sont-elles munies de caméras de surveillance ?		
d- Toutes les caisses sont-elles munies de système d'alarme ?		
e- le système d'alarme de la banque est-il relié à un poste de police proche de la banque ?		
f- Des tests de fonctionnement des alarmes sont-ils régulièrement effectués ?		
g- Les caissiers sont-ils formés sur la conduite à tenir en cas de braquage ?		
h- Les caissiers sont-ils chargés de demander aux clients l'origine des fonds pour un dépôt d'un montant très élevé ?		
i- Les caissiers sont-ils formés à la détection des chèques falsifiés ?		
j- Existe-t-il un dispositif de détection de falsification de signature ?		
k- Les caissiers sont-ils formés à la détection de fausses signatures ?		

A.4.3. Versement dans la caisse principale

Questions	Oui	Non
a- Ya t-il un plafond d'espèces qu'un caissier doit détenir ?		
b- le recomptage des espèces par le chef de caisse pour le transfert à la caisse principale (réserve) se fait-il en présence du caissier ?		
c- Y a-t-il une autre personne présente lors de ce recomptage ? si oui préciser l'identité de cette personne (un autre caissier, un le chef service caisse...) dans la case observation		
d- les clés et les codes d'accès à la caisse principale sont ils détenus par des personnes différentes ?		
e- Si oui ces personnes font-elles partie du même service ?		
f- En cas de départ en congé d'un détenteur de code de la caisse principale, ce dernier remet-il ce code à une tierce personne ?		
g- A son retour de congés, le code est-il modifié ?		
h- En cas d'affectation ou de démission du détenteur du code, est ce que celui est modifié ?		
i- Tout l'argent de la caisse principale est-il contenu dans des armoires ignifuges ?		
j- Tout l'argent de la caisse principale est-il contenu dans armoires hydrofuges ?		

A.4.4. Versement à la BCEAO

Questions	Oui	Non
a- lorsque le caissier principal remplit le formulaire de versement des espèces, le fait-il en présence d'un agent de la BCEAO ?		
b- l'agent de la BCEAO chargé d'effectuer le versement se rend il à la banque centrale accompagné un agent de la banque atlantique (caissier, ou caissier principal, ou service caisse...)		

B. Le dispositif d'assurance

Questions : existe-t-il une police d'assurance couvant	Oui	Non
les dégâts causés par les incendies ?		
les inondations ?		
la destruction des locaux suite à un soulèvement des populations (émeutes, guerres)		
les vols commis par les personnes extérieures à la banque ?		
les vols ou détournements commis par le personnel de la banque ?		
les risques liés au système informatique ?		
le coût de remplacement des matériels détruits		

C. L'externalisation (outsourcing)

C'est moyen de transfert du risque opérationnel sur un tiers (sous-traitant). « Cette externalisation peut comporter de nombreux avantages : meilleure qualité des services, gain de productivité, rapidité de lancement d'un nouveau produit ou nouvelle activité etc...» (SARDI ; 2002 :316).

Questions	Oui	Non
Y a-t-il des opérations de la banque effectuées par des sous-traitants ?		
Si oui, est ce que cette sous-traitance concerne		
• les opérations de caisse (retraits, dépôts...)		
• les trieurs (dans la réserve) ?		
• Le personnel informatique ?		

D. La franchise

« Le mécanisme de franchise consiste à garder en charge une partie du risque : les pertes inférieures au montant de la franchise sont supportées par la banque, les pertes excédant ce montant étant prises en compte par l'assurance. Le mécanisme de franchise permet à la banque de réaliser une économie de gestion : la prime d'assurance est réduite.» (SIRUGUET & al 2006 :126).

Questions	Oui	Non
Ce mécanisme est-il appliqué au sein de la banque atlantique ?		
Si oui s'applique t-il pour les risques opérationnels ?		

E. Les financements alternatifs

Il s'agit de techniques financières destinées à préfinancer une perte probable dans le temps ; utilisation de produits dérivés et de produits de transfert de risques par exemples.

Questions	Oui	Non
Ces techniques sont-elles utilisées au sein de la BASN ?		
Si oui sont-elles appliquées pour financer des pertes probables dus à la survenance de risques opérationnels ?		

F. Les captives

Ces sociétés sont appelées « captives » pour signaler leur lien avec la société mère. Pour SIRUGUET & al (2006 :127), cette solution est réservée aux banques de taille importante. La création d'une filiale agissant en tant que compagnie d'assurance ou de réassurance est un moyen de participer à la couverture des risques

Questions	Oui	Non
Atlantic Financial Group possède a-t-elle une ou plusieurs sociétés d'assurance ?		
Si oui, est que la BASN a souscrit des polices d'assurance auprès de ces sociétés ?		
Si oui, cette police couvre-t-elle <ul style="list-style-type: none"> • les risques liés aux opérations de caisse ? • les dégâts causés par les incendies ? • les inondations ? • la destruction des locaux suite à un soulèvement des populations (émeutes, guerres...) • les vols commis par les personnes extérieures à la banque ? • les vols ou détournements commis par le personnel de la banque ? • le coût de remplacement des matériels détruits ? 		

Annexe 5 : Questionnaire sur l'identification et l'analyse des risques

1. Existe-t-il au sein de votre département un processus de gestions des risques opérationnels ? oui non

2. Si oui, ce processus présente t-il une méthodologie d'identification des risques ?
oui non

3. Si oui, bien vouloir nous faire une présentation brève de cette méthodologie.

4. Existe-t-il au sein de votre département une cartographie des risques ?
oui non

5. Si oui, cette cartographie intègre-t-elle les risques opérationnels ?
oui non

6. Faites vous des analyses des incidents liés aux risques opérationnels survenus au sein de la banque au cours des années précédentes ?
oui non

7. Si oui quels critères retenez-vous pour l'analyse de ces incidents ?

- le montant de la perte (impact financier)
- la fréquence des incidents
- autres ? Préciser

8. utilisez-vous des outils statistiques (lois statistiques) dans l'analyse des incidents liés aux risques opérationnels ?
oui non

9. Si oui lesquels ?

CESAG - BIBLIOTHEQUE

BIBLIOGRAPHIE

OUVRAGES

1. BARRY Mamadou (2009), Audit et contrôle interne, Presses de la sénégalaise de l'Imprimerie, Sénégal, 371 pages.
2. BARTHELEMY Bernard, COURREGES Philippe, Gestion des risques, éditions d'Organisations, Paris, 472 pages.
3. CLEARY Sean, Thierry MALLERET (2006), risques : Perception, Evaluation, Gestion, éditions Maxima, Paris, 253 pages.
4. DESMICHT François (2007), Pratique de l'activité bancaire, 2^e édition, DUNOD, Paris, 355 pages.
5. DESROCHES Alain, LEROY Alain, FREDERIQUE Vallée (2003), la gestion des risques, LAVOISIER, 286 pages.
6. DOV Ogien (2006), comptabilité et audit bancaires, éditions DUNOD, Paris, 434 pages.
7. DUCLOS Thierry (2005), dictionnaire de la banque, 4^e édition, SEFI, Paris, 464 pages.
8. HAMZOUI Mohamed (2005), Audit : Gestion des risques et contrôle interne, édition Village mondial, 243 pages.
9. HENNIE VAN GREUNING et SONJA BRAJOVIC BRATANOVIC (2004), Analyse et gestion du risque bancaire, les éditions ESKA, Paris, 384 pages.
10. IFACI (2001), Management des risques, édition les cahiers de la recherche, Paris, 59 pages.
11. IFACI (2005), CIA préparation de l'examen : Le rôle de l'audit interne en matière de gouvernance, de risque et de contrôle, Paris, 245 pages.
12. IFACI, PRICEWATERHOUSE/COOPERS, LANDWELL & Associés (2005), le management des risques de l'entreprise, éditions d'organisation, Paris, 339 pages.
13. JIMENEZ Christian, MERLIER Patrick, DAN Chelly (2008), Risques opérationnels : de la mise en place du dispositif à son audit, Revue Banque, Paris, 271 pages.

14. RENARD Jacques (2010), Théorie et pratique de l'audit interne, 7^e édition, éditions d'Organisation, Paris, 472 pages.
15. SARDI Antoine (2002), Audit et contrôle interne bancaire, édition AFGES, Paris, 1099 pages.
16. SCHICK Pierre (2007), Mémento d'audit interne, éditions DUNOD, Paris, 217 pages.
17. SIRUGUET Jean-Luc, FERNANDEZ Emmanuelle, KOESSLER Lydia, (2006), le contrôle interne bancaire et la fraude, éditions DUNOD, Paris, 278 pages.
18. TACONNE Eric (2007), Optimiser la relation avec son banquier, éditions CHIRON, Paris, 240 pages.
19. WILMOTS Hans (2002), Aspects pratiques de l'organisation administrative et du contrôle interne, éditions Standard, Bruxelles, 319 pages.

ARTICLES

20. MAURER Frantz, (2007), les développements récents de la mesure du risque opérationnel, Revue du financier N°163, pages 46-60.
21. BARI Imane, RADI Bouchra, (2011), la gestion des risques opérationnels au terme de la crise financière, la revue du financier N°189, pages 6-17.
22. Consulting and risk services, (2009), maitriser les risques de l'entreprise : un dispositif de gouvernance, acteur de la gestion des risques, publication DELOITTE, 16 pages.

WEBOGRAPHIE

23. Banque et Assurance (2011), le dictionnaire économique, www.banque-et-assurance.com.
24. Comité de Bâle sur le contrôle bancaire (2003), les saines pratiques pour la gestion et la surveillance du risque opérationnel, www.bis.org.
25. Duchâteau Alain (2005), la mesure et la gestion des risques bancaires : Bâle II et les nouvelles normes comptables, www.courdecassation.fr.
26. Fimarkets (2005), Le risque opérationnel, www.fimarkets.com.

27. Organisation Mondiale de la Propriété Intellectuelle (2010), méthodes d'évaluation des risques, www.wipo.int.
28. Micropole-univers (2010), les risques bancaires, un sujet sensible, www.cfo-news.com.
29. SAM Manoo (2009), Le risque opérationnel, www.algofi.fr.
30. Sia-conseil (2008), les clés de la gestion du risque opérationnel, www.sia-conseil.com.
31. Vernimmen (2011), lexicque de finance, www.vernimmen.net.

CESAG - BIBLIOTHEQUE