Centre Africain d'Etudes Supérieures en Gestion

- CESAG -

Master en Banque et Finance

- MBF -

Année académique : 2010 – 2011

Option '' Gestion bancaire et maîtrise des risques''

Projet de mémoire de fin de formation

Thème :

PROPOSITION D'UN DISPOSITIF DE MAITRISE DES RISQUES OPERATIONNELS LIES A LA GESTION DES MOYENS DE PAIEMENTS : CAS DE LA BOA NIGER

Présenté par :
MAHAMAN LAMINOU ATTAOU Abdoulkader
10ème promotion MBF

Sous la Direction de :
TINI Hamadou
Expert-comptable
Enseignant associé au MBF

Dédicaces

Je dédie ce mémoire à :

- ✓ Dieu Tout Puissant qui m'a accordé la force et la santé de pouvoir réaliser ce travail ;
- ✓ Mes parents qui m'ont soutenu financièrement et moralement durant mes études.

Remerciements

Je remercie l'ensemble des personnes qui ont contribué par leur effort et par leurs conseils à m'aider dans la réalisation de ce travail de recherche. Ces remerciements vont particulièrement à :

- Monsieur TINI Hamadou : pour son encadrement tout au long de la rédaction de ce mémoire ;
- Au Directeur Général de la BOA Niger en m'accordant le stage m'ayant permis de réaliser mes travaux ;
- Monsieur MOROU AbdelSalame : pour son encadrement pendant mon stage pratique ;
- L'ensemble du personnel de la BOA Niger pour son accueil ;
- La Direction Générale du CESAG et l'ensemble du personnel pour leur mobilisation pour la réussite individuelle des étudiants en formation ;
- L'ensemble du corps professoral ainsi que les différents intervenants au Master en Banque et Finance du CESAG ;
- Mes collègues masteriens de la 10ème promotion pour les moments conviviaux passés ensemble.

Sommaire

Liste des Sigles et Abréviations

BCEAO : Banque Centrale des Etats de l'Afrique de l'Ouest

BOA : Banque Of Africa

COSO : Committee Of Sponsoring Organizations of the Treadway Commission

DAB : Distributeurs Automatiques de Banque

FERMA : Federation of European Risk Management Associations

QCI : Questionnaire de Contrôle Interne

RTGS : Real Time Gross Settlement ou Système de Règlement Brut en Temps Réel

SICA-UEMOA : Système Interbancaire de Compensation Automatisé de l'UEMOA

STAR-UEMOA : Système de Transfert Automatisé et de Transfert de l'UEMOA

UEMOA : Union Economique et Monétaire Ouest Africaine

UMOA : Union Monétaire Ouest Africaine

Liste des Tableaux et Figures

Tableaux

Figures

Introduction

Les crises majeures récentes parmi lesquelles la crise financière de 2008 déclenchée au Etats Unis ont fait ressortir que dans le contexte économique actuel, un risque mal maîtrisé peut anéantir une entreprise. Dans le domaine bancaire, la notion du risque révèle toute son importance du fait qu'elle caractérise même l'essence de la profession. En effet, dans son métier traditionnel le banquier prête de l'argent et s'expose au risque de ne pas recouvrer sa créance en cas de défaut du débiteur. La banque est exposée à une multitude de risques dont les principaux selon BESSIS Joël (2002 : 12) sont : le risque de crédit, le risque de taux d'intérêt, le risque de marché, le risque de liquidité, le risque de change, le risque opérationnel.

L'occurrence des pertes dues à des dysfonctionnements opérationnels dans le secteur financier a fait prendre conscience aux établissements de crédit de la nécessité d'une meilleure prise en compte du risque opérationnel. A titre d'illustration, nous pouvons citer le cas de la Barings, la plus vieille banque d'Angleterre qui a fait faillite à la suite d'activités non autorisées. Nous avons plus récemment le scandale de la Société Générale en France qui a révélé au grand public les conséquences des risques liés à des dysfonctionnements opérationnels.

Le comité de Bâle[1] définit le risque opérationnel comme « 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. Le risque opérationnel, ainsi défini, inclut le risque juridique, mais exclut les risques stratégiques et de réputation ».

Une des principales innovations de l'accord de Bâle II a été non seulement d'exiger l'allocation de fonds propres à la couverture contre les risques opérationnels mais aussi de prôner un dispositif de gestion des risques opérationnels. Les enjeux liés aux risques opérationnels sont multiples. Comme le souligne JIMENEZ Christian (2008 :21), il s'agit de :

- la sécurisation des résultats en évitant ou en couvrant des risques qui entrainent des pertes nettes ;
- une plus grande compétitivité du fait des améliorations de tarif possible si les pertes constatées sur les évènements à fréquence de survenance élevée sont diminuées ;

[1] Le Comité de Bâle sur le contrôle bancaire, institué en 1975 par les gouverneurs des banques centrales des pays du Groupe des Dix, rassemble les autorités de contrôle des banques. Ses réunions ont habituellement pour cadre la Banque des Règlements Internationaux, à Bâle, siège de son Secrétariat permanent.

- améliorer la productivité en identifiant les processus à risque et en mettant les plans d'actions nécessaires à leur amélioration.

L'évolution de l'environnement financier international a incité les autorités de régulation de la zone UMOA à se conformer aux règles et bonnes pratiques internationales en matière de supervision bancaire et à prendre en compte les recommandations du comité de Bâle à travers le dispositif de Bâle II. Une réforme institutionnelle de L'UMOA en 2007 a renforcé les attributions de la commission bancaire qui est appelée à redynamiser le système de surveillance des établissements de crédits.

La nouvelle circulaire N°003-2011/CB/C de ladite commission, relative à l'organisation du système de contrôle interne des établissements de crédits de l'UMOA, entrée en vigueur en février 2011, fait obligation aux établissements de crédit de mettre en place un dispositif de gestion des risques en général et particulièrement un dispositif couvrant les risques opérationnels. Cette nouvelle circulaire abroge la circulaire N°10-2000/CB du 23 juin 2000 portant réorganisation du contrôle interne des établissements de crédits.

Sur le plan opérationnel, les banques commerciales font face à des dysfonctionnements comme la non-formalisation de certaines procédures, la formation insuffisante de certains agents, la faiblesse du contrôle des opérations, ainsi que des insuffisances dans le dispositif sécuritaire physique. Ces problèmes entrainent des lourdeurs administratives, des erreurs humaines récurrentes ainsi qu'une forte exposition à des risques de fraude.

Les situations de crise et de dysfonctionnement ont placé les moyens de paiements comme accélérateur de la montée du risque opérationnel. Les incidents liés aux moyens de paiement ont pour source comme le décrit OGIEN (2008 : 479) : des évolutions techniques mal maitrisées en interne, la faiblesse traditionnelle de la compétence des équipes dédiées aux opérations des moyens de paiement, une insuffisance des actions anticipant les évolutions et des facteurs externes amplificateurs de difficultés. Ce constat sur les risques opérationnels liés à la gestion des moyens de paiement dans les banques nous amène à nous intéresser à ce cycle. La Banque of Africa Niger n'échappe pas à la règle, ce qui nous amène alors à nous poser la question suivante :

Comment une banque de l'UMOA peut-elle identifier, mesurer, contrôler et suivre les risques opérationnels associés aux moyens de paiement ?

Nous répondrons à cette question à travers le thème « proposition d'un dispositif de maîtrise des risques opérationnels liés à la gestion des moyens de paiements : cas de la BOA Niger ».

L'objectif principal de ce mémoire est de proposer un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiements de la BOA Niger.

De manière plus précise, il s'agira :

- d'identifier les risques opérationnels liés à la gestion des moyens de paiements ;
- d'évaluer et classer les risques identifiés ;
- de formaliser les risques à travers une cartographie ;
- de proposer des mesures de contrôle et de suivi de ces risques.

Pour la BOA Niger, cette étude contribuera non seulement à améliorer son dispositif de maitrise des risques opérationnels, mais aussi aidera la banque à se conformer à la réglementation en vigueur notamment la circulaire N°003-2011/CB/C relative à l'organisation du système de contrôle interne des établissements de crédits. L'étude constituera une démarche pour l'identification, l'évaluation, le traitement et le contrôle des risques opérationnels.

Pour le lecteur, ce sera une occasion de cerner les contours du risque opérationnel dans le domaine bancaire et avoir un aperçu de la mise en place d'un dispositif de gestion des risques opérationnels.

Pour nous-mêmes, cette étude nous permettra d'appréhender les notions de risques opérationnels en milieu bancaire et de se servir des outils permettant d'identifier les processus qui les supportent.

Pour mener à bien notre recherche, nous allons nous appuyer sur le cadre du COSO II[2] de la gestion des risques pour développer notre propre modèle d'analyse. Nous utiliserons des outils et techniques de collecte de données parmi lesquels l'interview, l'observation physique, la revue documentaire, et le questionnaire. Par la suite, nous mobiliserons les outils de la statistique descriptive (tableaux, grapbiques, indicateurs, ...) afin d'analyser le risque opérationnel et aboutir à des recommandations.

[2] COSO est l'acronyme abrégé de Committee Of Sponsoring Organizations of the Treadway Commission, une commission à but non lucratif qui établit en 1992 une définition standard du contrôle interne. Le concept issu des travaux du COSO II est présenté comme un référentiel de gestion des risques.

Notre mémoire sera organisé autour de deux parties :

- La première partie présentera le cadre théorique de la recherche en présentant les différents concepts sous la forme d'une revue de littérature. Ce sera aussi l'occasion de détailler le cadre méthodologique en présentant le modèle d'analyse et les outils utilisés.
- La deuxième partie concernera l'application de la recherche à un cadre pratique qui sera la BOA Niger. Les résultats et les recommandations issues de la recherche seront exposés dans cette partie.

PREMIERE PARTIE : CADRE THEORIQUE DE L'ETUDE

Le risque opérationnel concerne l'ensemble des activités bancaires car c'est le risque né d'une défaillance des processus ou procédures internes, ainsi que des risques liés aux ressources humaines ou à des évènements extérieurs. La gestion des moyens de paiements expose la banque à une multitude de risques dont les risques opérationnels. Cependant, par la complexité des systèmes supportant ces moyens de paiements, il devient difficile pour la banque d'appréhender et de traiter ces risques.

L'objet de cette première partie est de présenter dans un premier temps le concept de risque opérationnel ainsi que la notion de moyens de paiements (chapitre 1). Dans un second temps, nous traiterons de la mise en place d'un dispositif de maitrise des risques opérationnels en milieu bancaire (chapitre 2). Dans un troisième temps, nous présenterons la démarche retenue ainsi que les outils mobilisés pour la mise en place du dispositif de maitrise des risques opérationnels (chapitre 3).

Chapitre 1 : Le risque opérationnel lié à la gestion des moyens de paiement

Dans ce chapitre, nous aborderons en premier lieu la notion de moyens de paiements en décrivant les processus qui les supportent. Nous présenterons ensuite les principaux risques bancaires en dégageant les spécificités du risque opérationnel. Nous terminerons enfin avec la description des aspects pratiques et réglementaires du contrôle interne.

1.1. La gestion des moyens de paiement

Nous décrirons dans cette section les différents moyens de paiement, les systèmes de paiement dans l'UEMOA ainsi que la réglementation sur les moyens de paiement.

1.1.1. Les différents moyens de paiement

La loi portant réglementation bancaire dans l'UMOA définit les moyens de paiement : « sont considérés comme moyens de paiement, tous les instruments qui, quel que soit le support ou le procédé technique utilisé, permettent à toute personne de transférer des fonds. Il s'agit notamment des chèques bancaires, chèque de voyage, cartes de paiement et de retrait, virements ou avis de prélèvement, cartes de crédits et transfert électronique de fonds » (Art. 7). Nous allons présenter dans cette sous-section les chèques, les cartes bancaires et les virements.

1.1.1.1. Les chèques

Le chèque est un écrit qui permet au tireur (celui qui émet le chèque, titulaire ou mandataire du compte) de donner l'ordre au tiré (établissement qui tient le compte) de payer une certaine somme à un tiers ou bénéficiaire dans la limite des avoirs déposés chez le tiré. (MONNIER, 2008). Le règlement N°15/2002/CM/UEMOA relatif au système de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest Africaine précise la forme et les mentions obligatoires du chèque. Le chèque contient :

- la dénomination de chèque, insérée dans le texte même du titre et exprimée dans la langue employée pour la rédaction de ce titre ;
- le mandat pur et simple de payer une somme déterminée ;
- le nom de celui qui doit payer (le tiré) ;
- l'indication du lieu où le paiement doit s'effectuer ;
- l'indication de la date et du lieu où le chèque est créé ;

- la signature manuscrite de celui qui émet le chèque (tireur).

BEGUIN (2008 :51) distingue différentes catégories de chèques : il s'agit du chèque barré, du chèque non barré, du chèque de banque, du chèque certifié, du chèque visé et du chèque de voyage.

- Chèque barré

C'est le chèque le plus répandu et qui est délivré au client sans demande particulière de sa part. Deux traits sont tracés sur le recto du chèque. Seul un établissement de crédit ou assimilé peut l'encaisser directement, à moins que l'émetteur et le bénéficiaire soient clients de la même banque. Le bénéficiaire d'un chèque barré doit l'endosser avant de le remettre à sa banque. Le chèque barré interdit tout paiement en espèces, il faut ainsi attendre que les fonds soient encaissés pour disposer des sommes correspondantes.

- Chèque non barré

Ce type de chèque permet le paiement en espèces. Il est donc utilisé par les entreprises ou les personnes physiques qui souhaitent que les bénéficiaires de leurs chèques puissent être réglés en espèces, sans être obligés de transiter par un compte bancaire.

- Chèque de banque

C'est un chèque établi à la demande du client ou dans certains cas particuliers. L'utilité de ce chèque est de pouvoir régler des montants importants en toute quiétude. La banque se substitue au client en émettant en lieu et place un chèque au nom du bénéficiaire choisi par ce dernier. L'avantage réside dans le fait que le bénéficiaire du chèque est assuré d'être payé, sous réserve toutefois de respecter le délai de validité du chèque.

- Chèque certifié

Moins utilisé que le chèque de banque, il présente, lui aussi, une garantie de paiement mais d'une durée moins importante. Par la certification, la banque atteste l'existence de la provision. Elle va d'ailleurs bloquer la somme correspondante pendant le délai de présentation du chèque qui est de huit jours à compter de la date d'émission.

- Chèque visé

Un chèque visé est tout simplement un chèque dont la provision est garantie le jour de son émission. Par son visa, la banque ne s'engage pas, elle informe seulement le bénéficiaire que la provision existait le jour du tirage du chèque.

- Chèque de voyage

Le chèque de voyage est émis au nom du client en coupure numérotée et montant prédéterminé. Il offre au souscripteur de ce type de moyen de paiement une garantie spécifique en cas de perte ou de vol. Le client peut, en effet, faire opposition à un ou des chèques de banque en cas de perte ou de vol. Il se voit, dans ce cas, intégralement remboursé des sommes en jeu.

1.1.1.2. La carte bancaire

La carte de paiement se présente sous la forme d'un rectangle de plastique rigide comportant, au recto, le nom de la carte, le numéro de la carte, la période de validité, le nom de la banque qui a délivré la carte, le nom du titulaire et une puce électronique, et au verso, une bande magnétique, un spécimen de la signature du titulaire de la carte ainsi qu'un nombre à 3 chiffres : le cryptogramme visuel qui est une sécurité supplémentaire pour les achats à distance. Le titulaire reçoit un code secret qu'il sera seul à connaître et qu'il devra taper pour tout retrait dans un distributeur de billets ou en cas d'achat chez un commerçant utilisant une machine nécessitant la frappe de ce code pour validation. La carte reste la propriété de la banque ; celle-ci dispose du droit de la retirer sans avoir à justifier sa décision (MONNIER, 2008).

On peut distinguer selon l'auteur plusieurs types de cartes bancaires :

- Carte de retrait

Elle sert uniquement à retirer de l'argent dans les Distributeurs Automatiques de Banque (DAB) de la banque teneur du compte ou autorise les retraits auprès de tous les DAB du réseau.

- Carte de paiement

On distingue les cartes nationales et les cartes internationales.

Pour les cartes nationales, on a :

- *Débit immédiat* : cartes qui permettent de retirer de l'argent et d'effectuer des paiements dans la zone et dont les sommes correspondantes sont débitées au comptant.
- *Débit différé* : cartes qui permettent de retirer de l'argent et d'effectuer des paiements dans la zone et dont les sommes correspondantes sont débitées une fois par mois.

Pour les cartes internationales, on a :

- *Débit immédiat et différé* : les cartes internationales se partagent entre deux réseaux (VISA et Mastercard). Elles possèdent les mêmes fonctions que les cartes nationales et permettent en plus d'effectuer des retraits et des paiements à l'étranger.
- *Cartes de prestige* : VISA Premier ou Gold Mastercard ont les mêmes fonctions que les autres cartes de paiement internationales mais offrent des services complémentaires.

▪ Carte de crédit

Certaines cartes de crédit sont adossées à une réserve d'argent. Elles remplissent les fonctions de cartes de retrait, de paiement et permettent également l'accès à un crédit revolving.

1.1.1.3. Le virement bancaire

C'est une opération de transfert de fonds entre deux comptes. Si ces comptes sont domiciliés dans la même banque, il s'agira d'un virement interne, sinon on parlera d'un virement externe ou interbancaire. Dans le premier cas, la gratuité sera de mise, dans le second la banque percevra une commission fixe à chaque virement. Le virement peut être occasionnel ou au contraire permanent. Le virement permanent permet de programmer à une date fixe et selon la périodicité souhaitée, le virement d'une somme d'argent vers un autre compte. Les fonctionnalités de la banque à distance permettent aujourd'hui au client de programmer seul ce mouvement scriptural entre comptes. Pour les virements externes, le client aura préalablement communiqué à la banque sous la forme d'un RIB les coordonnées du compte externe à créditer. Une fois exécuté, le virement est irrévocable. Pour les virements internationaux, les principes de base sont identiques. La seule différence est qu'ils transitent par un autre réseau : le réseau Swift. (MONNIER, 2008).

1.1.2. Les systèmes de paiements dans l'UEMOA

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) avait initié un important projet de modernisation des systèmes de paiement des Etats membres de l'UEMOA. « Un système de paiement est un ensemble de règles, procédures, instruments et infrastructures utilisé pour échanger des valeurs financières entre deux parties s'acquittant d'une obligation contractuelle » (OGIEN, 2008). La réforme a conduit à la mise en place de deux systèmes de paiements : il s'agit du système STAR-UEMOA et du système SICA-UEMOA.

1.1.2.1. Le système STAR-UEMOA

STAR-UEMOA est le Système de Transfert Automatisé et de Transfert de l'UEMOA. C'est la dénomination du Système de Règlement Brut en Temps Réel ou Real Time Gross Settlement (RTGS) de l'UEMOA. Ce système international de règlement est né du constat que les risques de règlement augmentent avec le montant des paiements échangés et le délai de règlement (durée entre l'échange des ordres et la finalité du règlement). L'objectif du système RTGS est donc la réduction du risque de règlement. STAR-UEMOA fonctionne sur la base des messages au format SWIFT et les participants Directs sont connectés au système central de la BCEAO pour l'envoi et la réception des messages.

1.1.2.2. Le système SICA-UEMOA

Le système Interbancaire de Compensation Automatisé de l'UEMOA est un système d'échange des opérations de paiement automatisé qui assure :

- la compensation multilatérale des transactions entre les participants ;
- l'échange d'instruments dématérialisés ;
- la réduction des délais et coûts des échanges interbancaires ;
- le respect du délai maximum de règlement sur le compte de la clientèle.

L'ancien système de compensation était caractérisé par l'existence d'une chambre de compensation dans chaque pays de l'UEMOA, des séances de compensation dans les locaux de la BCEAO, des échanges de support papier ainsi qu'un traitement manuel de la compensation et calcul des soldes. SICA-UEMOA permet une compensation traitée exclusivement à partir des fichiers de remises électroniques des banques et une suppression des séances de compensation avec désormais des échanges d'images scannées des chèques.

1.1.3. La réglementation sur les moyens de paiements

Plusieurs textes réglementent les instruments et moyens de paiements dans l'espace UEMOA.

1.1.3.1. La loi cadre relative à la répression du faux monnayage dans les pays de l'UMOA

Cette loi fixe les sanctions civiles et pénales qu'encourent les auteurs responsables de contrefaçon, de falsification ou d'altération des signes monétaires ayant cours légal sur le territoire national ou à l'étranger.

1.1.3.2. Le règlement N°15/2002/CM/UEMOA relatif au système de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest Africaine

Ce texte abroge la loi uniforme sur les moyens de paiements. Il définit les différents moyens de paiements, les conditions de leur utilisation ainsi que les mécanismes de sécurisation des systèmes qui les supportent.

1.1.3.3. La directive N°08/2002/CM/UEMOA portant sur les mesures de promotion de la bancarisation et de l'utilisation des moyens de paiement scripturaux

Cette directive vise à promouvoir la bancarisation et l'utilisation des nouveaux instruments et procédés de paiement introduits par la réforme dans les relations des Etats et Administrations Publiques avec leurs fonctionnaires et agents ainsi qu'avec leurs partenaires et contribuables.

1.1.3.4. L'instruction N°01/CIP du 1er février 1999 relative au dispositif de centralisation des incidents de paiement dans l'UMOA

Ce texte fait mention obligatoire aux établissements de crédits de consulter la banque centrale avant toute délivrance de formule de chèque ou de carte de paiement à un nouveau client et déclarer les ouvertures de comptes de chèques, les incidents de paiements ainsi que les infractions sur les interdictions bancaires et judicaires.

1.1.3.5. L'instruction N°01/2003 du 8 mai 2003 relative à la promotion des moyens de paiement scripturaux et à la détermination des intérêts exigibles en cas de défaut de paiement.

Cette instruction précise le droit au compte et la mise à disposition d'au moins un instrument de paiement pour les personnes physiques ou morales justifiant d'un revenu régulier supérieur ou égale à cinquante mille (50000) FCFA. Elle fixe le montant de référence pour le paiement en monnaie scripturale des salaires et indemnités dus par l'Administration publique.

1.2. La notion de risque

1.2.1. Définition du risque

D'après HASSID (2008 :14) : « créer une entreprise c'est déjà prendre un risque ». Le risque est donc inhérent à l'entreprise. L'IIA définit le risque comme « la probabilité qu'un évènement ou qu'une action ait des retombées négatives sur l'entreprise ». La norme ISO GUIDE 73 définit le risque comme étant « l'effet de l'incertitude sur l'atteinte des objectifs ». Selon RENARD (2010 : 155) les deux principales composantes du risque sont :

- la gravité ou conséquences de l'impact ;
- la probabilité qu'un ou plusieurs évènements se produisent.

1.2.2. Les différentes catégories de risques bancaires

La banque à l'instar de toutes les entreprises est exposée à des risques divers. Certains sont exogènes tandis que d'autres sont liés à l'activité. En se référant à la typologie de HASSID (2008 :7), on peut distinguer pour toutes les entreprises : les risques politiques, les risques économiques, les risques socioculturelles, les risques technologiques, les risques physiques et moraux ainsi que les risques informationnels. Cependant, la banque ayant une activité spécifique se voit confrontée à d'autres catégories de risques dont BESSIS (2002 :11) nous fait la genèse : il s'agit du risque de crédit, risque opérationnel, risque de liquidité, risque de taux d'intérêt, risque de marché, risque de change, pour ne citer que les principaux.

1.2.2.1. Le risque de crédit

Le risque de crédit est la perte potentielle consécutive à l'incapacité par un débiteur d'honorer ses engagements (on parle également de risque de contrepartie). Les postes de bilan concernés par ce risque sont : les crédits accordés à la clientèle, créances sur les établissements de crédits, les opérations de crédits bail et location simple, les titres d'investissements.

1.2.2.2. Le risque opérationnel

Selon le comité de Bâle, c'est le risque de 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.

1.2.2.3. Le risque de marché

Les risques de marché sont les pertes résultant de la variation des taux d'intérêt, des cours de change, du prix des actions, etc. les postes de bilan concernés sont : le portefeuille de titres de transaction et de placement, les instruments financiers détenus dans le cadre d'une opération de marché, les instruments dérivés.

1.2.2.4. Les autres risques

- Risque de liquidité : risque pour une banque de ne pas pouvoir faire face à ses engagements par l'impossibilité de se procurer les fonds dont elle a besoin ;
- Risque de réputation : atteinte à la confiance qu'une banque doit inspirer à sa clientèle et aux marchés, à la suite d'une publicité portant sur des faits réels ou supposées ;
- Risque stratégique : pertes potentielles résultant de l'échec d'une stratégie adoptée par l'établissement (pénétration d'un marché, lancement de nouveaux produits) ;
- Risque systémique : la défaillance d'un établissement de crédit peut déclencher des difficultés dans d'autres établissements de crédit et risque de mettre en péril tout le système bancaire.

1.2.3. Les risques opérationnels liés aux moyens de paiement

OGIEN (2008 : 463) nous décrit les principaux risques opérationnels liés aux moyens de paiements. Il s'agit : de risques informatiques, de risques liés aux ressources humaines, de risques de fraude et de détournement, et de risques de contrepartie.

1.2.3.1. Les risques informatiques

Les systèmes en charge de la gestion et du traitement des moyens de paiement sont dans la plupart des cas totalement intégrés et de ce fait « opaques » :

- écritures comptables issues de données saisies lors de la constatation d'un acte économique initial dans un sous-système amont ;
- information initiale le plus souvent saisie par un utilisateur non comptable, ou issu de données télétransmises par des systèmes externes (systèmes de place) ;
- dans ce type d'organisation, la pièce génératrice de l'écriture comptable et l'écriture comptable elle-même sont souvent séparées par un processus long et complexe, car faisant l'objet de relais entre les sous-systèmes.

La piste d'audit est, par ailleurs, fragilisée par la tendance des banques à privilégier l'adaptation des systèmes à leurs besoins au détriment des exigences de traçabilité ; par la faiblesse de la documentation existante sur ces systèmes et par le recours à des sous-traitants pas toujours soumis à des contrôles suffisants.

1.2.3.2. Les risques liés aux ressources humaines

Les risques liés au facteur humain sont liés à :

- la fréquente inadéquation des effectifs ;
- le manque de ressources mis en œuvre face à la complexification des opérations ;
- une dépendance possible trop forte à des prestataires externes.

Par ailleurs, l'auditeur se trouve confronté aux risques « exogènes », telle la dépendance à la qualité des traitements des autres établissements partenaires. Le risque administratif et comptable entraîne des défauts de justification de comptes, des pertes de piste d'audit ou des retards dans le traitement des opérations ou absence de traitement complet des opérations.

1.2.3.3. Les risques de fraude et de détournement

Il s'agit d'un risque réel, mais difficile à appréhender compte tenu de la volumétrie des opérations, de la complexité des systèmes et des schémas comptables. Il provient de deux sources en pratique :

- fraude externe (falsification de chèques, cavalerie…) : elle doit pouvoir être détectée et traitée par des procédures ;
- détournements internes : plus difficiles à identifier, dans la mesure où ils peuvent être opérés dans un environnement parfois instable.

1.3. Le système de contrôle interne

Le système de contrôle interne a attiré l'attention des instances de contrôle des banques ainsi que les acteurs de la normalisation comptable depuis le scandale ENRON en 2002. Cela s'est traduit par l'adoption de nouvelles lois telles que Sarbannes Oxley Act aux Etats Unis ou la Loi sur la Sécurité Financière en France. Dans la zone UMOA, de nouveaux textes ont été adoptées par la commission bancaire dont la circulaire N°003-2011 sur le système de contrôle interne des banques. Nous présenterons dans cette section le contrôle interne ainsi que les objectifs qui y sont associés, et nous ferons une synthèse de la nouvelle réglementation en vigueur dans l'espace UMOA.

1.3.1. Définitions et objectifs du contrôle interne

1.3.1.1. Définition du contrôle interne

Le COSO définit le contrôle interne comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation destiné à fournir une assurance raisonnable quant à la réalisation des objectifs. C'est un ensemble de dispositifs mis en œuvre par les responsables de tous les niveaux pour maîtriser le fonctionnement de leurs activités. Il s'assure de:

- la conformité aux lois et règlements ;
- l'application des instructions et des orientations fixées par la Direction Générale ou le Directoire ;

- le bon fonctionnement des processus internes de la société, notamment ceux concourant à la sauvegarde de ses actifs ;
- la fiabilité des informations financières.

Néanmoins, l'application pratique des dispositifs de contrôle interne nécessite avant tout l'affirmation d'une politique et d'une culture générale de contrôle dans l'entreprise (MAZARS, 2005).

1.3.1.2. Les objectifs du contrôle interne

Les objectifs du système de contrôle interne bancaire sont déclinés par l'article 3 de la circulaire N°003-2011/CB. Il s'agit de :

- vérifier que les opérations réalisées, l'organisation et les procédures internes sont conformes aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques ainsi qu'aux orientations des organes délibérant et exécutif ;
- s'assurer que les orientations, les instructions et les limites fixées par l'organe délibérant en matière de risque sont strictement respectées ;
- veiller à la fiabilité de l'information comptable et financière, en particulier aux conditions de collecte, d'évaluation, d'enregistrement, de conservation et de disponibilité de cette information.

1.3.2. Cadre réglementaire de l'organisation du système de contrôle interne

La circulaire N°003-2011/CB de la Commission Bancaire de l'UMOA, entrée en vigueur en février 2011, précise l'organisation du Contrôle Interne des Etablissements de Crédits de la zone monétaire. Elle abroge la circulaire N° 10-2000/CB portant réorganisation du contrôle interne dans les Etablissements de crédits. La nouvelle circulaire impose aux établissements de crédits de l'UMOA de se doter dans les conditions prévues, d'un système de contrôle interne efficace, adapté à leur organisation, à la nature et au volume de leurs activités ainsi qu'aux risques auxquels ils sont exposés. Cette circulaire traite principalement de l'organisation du système de contrôle interne, de l'évaluation et la prévention des risques, de la qualité de l'information comptable et financière ainsi que de la surveillance prudentielle.

1.3.2.1. L'organisation du système de contrôle interne

L'organisation du contrôle interne bancaire est de la responsabilité des organes délibérants et exécutifs qui en assure le bon fonctionnement au sein des établissements de crédit. Le bon fonctionnement du contrôle interne, passe par la mise en place d'un Comité d'Audit ou d'un organe équivalent par l'organe délibérant. Il aura pour tâche d'assurer le suivi, l'organisation et le bon fonctionnement du contrôle interne et de la gestion des risques. Le système repose sur une formalisation complète des procédures destinées à identifier, suivre et maitriser l'ensemble des risques.

1.3.2.2. L'évaluation et la prévention des risques

L'activité bancaire étant par nature très sensible et très risqué, le système de contrôle interne mis en place doit être capable d'assurer l'évaluation et la prévention des risques associés à travers un processus intégré de gestion et d'évaluation des risques.

1.3.2.3. La qualité de l'information comptable et financière

Le système de contrôle interne mis en place doit permettre de veiller à la qualité de l'information comptable et financière. A cet effet, il doit garantir l'existence d'un ensemble de procédures appelées, piste d'audit, et veiller au respect des dispositions du Plan Comptable Bancaire. La piste d'audit doit permettre :

- de reconstituer les opérations dans un ordre chronologique ;
- de justifier toute information par une pièce d'origine à partir de laquelle il doit être possible de remonter, par un chemin ininterrompu, au document de synthèse et réciproquement ;
- d'expliquer l'évolution des soldes d'un arrêté à l'autre, grâce à la conservation des mouvements ayant affectés les postes comptables.

Le système d'information doit permettre la production d'informations fiables, récentes, explicites et conformes aux normes réglementaires. Il doit faciliter la prise de décision rapide afin de corriger les éventuelles faiblesses détectées.

1.3.2.4. La surveillance des Etablissements de Crédit

Dans le souci d'assurer une solidité du système bancaire et d'accompagner les établissements de crédit dans le processus de maitrise des risques, certaines diligences doivent être mise en œuvre par les Etablissements de crédit. Ces diligences sont relatives à la communication de certains documents à la commission bancaire et dans des délais bien précis. C'est ainsi qu'un rapport doit être envoyé à la commission bancaire dans les trente (30) jours suivant la fin de chaque semestre de l'année civile et qui comporte :

- une description de l'organisation et du fonctionnement du contrôle interne au cours de la période sous revue, faisant notamment ressortir les moyens mis en œuvre, les travaux réalisés et les modifications significatives éventuellement intervenues dans les méthodes et l'activité ;
- un inventaire des contrôles effectués par l'audit interne, accompagnés des principaux constats et des mesures correctrices entreprises ;
- un développement sur la mesure et la surveillance des risques auxquels est exposé l'établissement ;
- une présentation du programme d'action pour la période à venir.

1.3.3. La gouvernance des Etablissements de Crédit

Selon la circulaire N°005-2011/CB/C relative à la gouvernance des Etablissements de Crédit de l'UMOA, les outils de gestion ci-après doivent être adoptés par les Etablissements de Crédit :

- un plan d'affaires triennale ou quinquennal, périodiquement actualisé en fonction de l'évolution de l'environnement, de l'activité et des hypothèses ;
- un dispositif de suivi budgétaire incluant une revue analytique trimestrielle des comptes de gestion ;
- un organigramme détaillé et une organisation administrative fonctionnelle, adoptés par le Conseil d'Administration. L'organisation administrative doit notamment comporter une définition précise des fonctions et des postes ;
- des procédures et techniques de gestion des risques comprenant :
  - un système de répartition des pouvoirs en matière de crédit ;
  - des procédures d'évaluation et de cotation des risques aboutissant à une cartographie des risques ;

- des mécanismes de surveillance des grands risques ;
- un processus d'évaluation continue de l'adéquation des fonds propres à l'évolution de leur activité et des risques ;
- un système d'évaluation, de déclassement et de provisionnement des risques, conforme aux dispositions et règles minimales édictées par le PCB et la réglementation prudentielle.

Les Etablissements de Crédit doivent se doter d'outils de contrôle capable de mesurer et d'améliorer les performances à tous les niveaux. Ils doivent particulièrement mettre en place :

- un dispositif de lutte contre le blanchiment des capitaux et le financement du terrorisme conforme aux dispositions légales et réglementaires et permettant notamment une identification rigoureuse de la clientèle, une surveillance accrue de certaines opérations, et une formation continue du personnel ;
- un contrôle interne efficace permettant d'apprécier de manière distincte les conditions d'exercice du contrôle de conformité, conformément à la circulaire de la Commission Bancaire y afférente ;
- des codes de déontologies, applicables aux administrateurs, aux dirigeants et au personnel.

La gestion des moyens de paiements dans la zone UEMOA fait l'objet d'une réglementation spécifique. Les processus et les systèmes qui les supportent sont exposés à des risques parmi lesquels figure le risque opérationnel. L'amélioration du système de contrôle interne est une étape fondamentale dans le processus de maitrise des risques opérationnels liés à la gestion des moyens de paiements. La circulaire N°003-2011/CB de la Commission Bancaire exige dans le dispositif de maitrise des risques, l'élaboration préalable d'une cartographie.

Chapitre 2 : Le dispositif de maîtrise des risques opérationnels

La gestion du risque opérationnel fait encore l'objet de multiples recherches sur le plan de la conception de modèles pour l'évaluation et la mesure ce risque en milieu bancaire. La gestion des risques d'entreprises dans sa généralité nécessite une démarche spécifique, d'où le développement de référentiels de la gestion de risque comme celui du COSO II ou de la FERMA. Ces référentiels tout comme le dispositif de Bâle II préconisent l'identification des risques à travers une cartographie comme préalable à leur maitrise. L'objet de ce chapitre est de présenter d'une part, les référentiels de la gestion des risques d'entreprises du COSO II et de la FERMA ainsi que les instruments de mesure du risque opérationnel du dispositif de Bâle II. D'autre part, définir et décrire la démarche d'élaboration d'une cartographie des risques opérationnels ainsi que le dispositif de contrôle et de traitement de ces risques.

2.1. La gestion du risque opérationnel

La gestion des risques aide une entité à réaliser ses objectifs de rentabilité et de performance et constitue une prévention contre la perte de ressources. Elle fournit une information financière fiable et s'assure que l'entité se conforme aux lois et règlements, lui évitant ainsi de subir des atteintes à sa réputation et d'autres conséquences préjudiciables (FERMA, 2003).

2.1.1. Le référentiel du COSO II

Dans les années 1980, le sénateur américain Treadway a initié une importante recherche sur le contrôle interne. Ainsi, s'est créée aux États-Unis la « Commission Treadway », laquelle a constitué un Comité universellement connu sous le nom de COSO. Ce dernier a initié une réflexion en deux étapes ; le COSO I dans les années 1980 et le COSO II en 2004. Le concept issu des travaux du COSO 2 est défini comme un référentiel de gestion globale du risque élaboré par la direction d'une entité, son management et son personnel en application de la stratégie et visant à identifier les événements qui peuvent l'affecter ; afin de gérer les risques en prenant en compte ce qui est acceptable et ce qui ne l'est pas ; pour fournir une assurance raisonnable quant à la réalisation des objectifs.

Le dispositif de management des risques comprend huit éléments. Ces éléments résultent de la façon dont l'organisation est gérée et sont intégrés au processus de management. Ces éléments sont les suivants :

- *Environnement interne :* l'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'entité, et plus particulièrement la conception du management et son appétence pour le risque, l'intégrité et les valeurs éthiques, et l'environnement dans lequel l'organisation opère ;

- *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. Le management des risques permet de s'assurer que la direction a mis en place un processus de fixation des objectifs et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque.

- *Identification des événements :* les événements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés en faisant la distinction entre risques et opportunités. Les opportunités sont prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs.

- *Évaluation des risques :* les risques sont analysés, tant en fonction de leur probabilité d'occurrence que de leur impact, cette analyse servant de base pour déterminer la façon dont ils doivent être gérés. Les risques inhérents et les risques résiduels sont évalués.
- *Traitement des risques :* le management définit des solutions permettant de faire face aux risques (évitement, acceptation, réduction ou partage). Pour ce faire le management élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec le seuil de tolérance et l'appétence pour le risque de l'organisation.

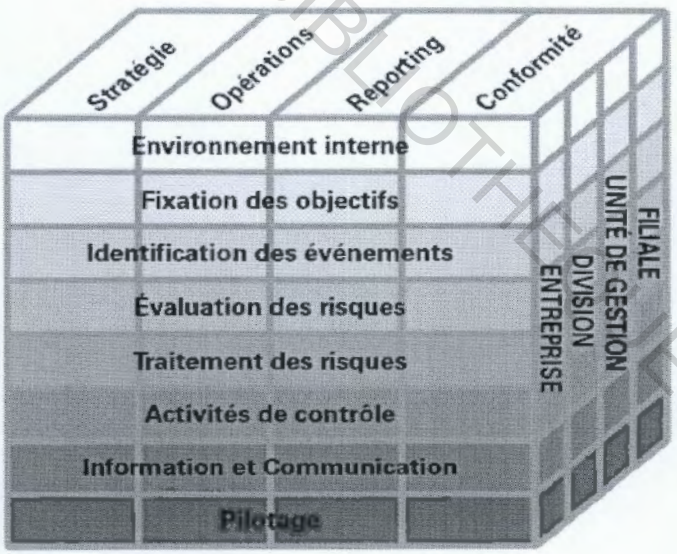
- *Activités de contrôle :* des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques.

- *Information et communication :* les informations utiles sont identifiées, collectées, et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace.

- *Pilotage :* le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

Il existe une relation directe entre les objectifs que cherche à atteindre une organisation et les éléments du dispositif de management des risques qui représentent ce qui est nécessaire à leur réalisation. La relation est illustrée par une matrice en trois dimensions ayant la forme d'un cube.

Figure 1 : Matrice du COSO II



Source : **(IFACI, 2005)**

Les quatre grandes catégories d'objectifs : stratégiques, opérationnels, reporting et conformité sont représentées par les colonnes. Les huit éléments du management des risques par les lignes et les unités de l'organisation par la troisième dimension. Cette représentation illustre la façon d'appréhender le management des risques dans sa globalité ou bien par catégorie d'objectifs, par élément, par unité ou en les combinant.

2.1.2. Le référentiel de la FERMA

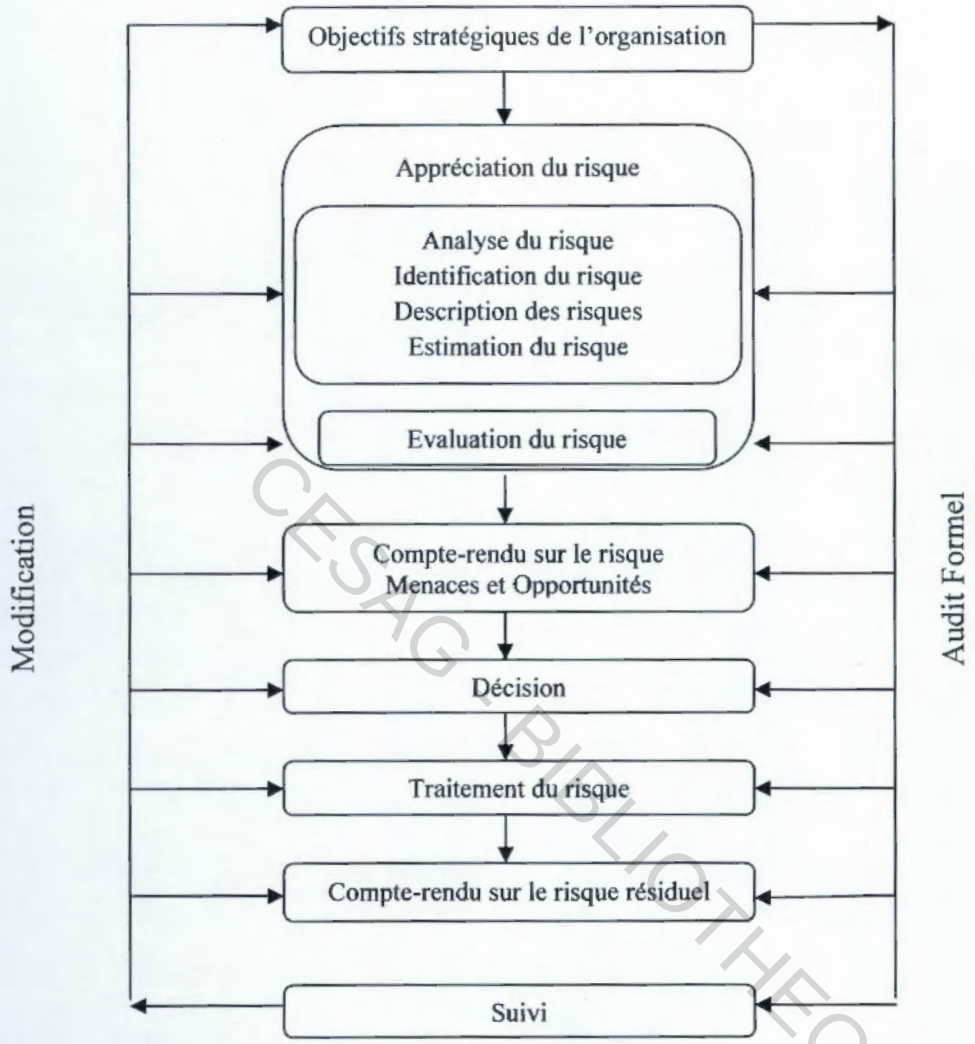
Après le COSO II qui représente pour de nombreuses organisations le cadre de référence pour la gestion des risques, d'autres associations professionnelles comme la Federation of European Risk Management Associations (FERMA), ont élaboré des documents cadres pour la gestion des risques. Selon la FERMA : « La gestion des risques est un processus par lequel les organisations traitent les risques qui s'attachent à leurs activités et recherchent ainsi des bénéfices durables dans le cadre de ces activités ». La gestion du risque protège le patrimoine de l'organisation et crée de la valeur pour celle-ci et ses parties prenantes en:

• fournissant un cadre méthodologique qui permet à toute activité future d'être mise en place de façon cohérente et maîtrisée ;
• améliorant le processus des décisions, leur planification et leur hiérarchisation par une compréhension exhaustive et structurée des activités de l'organisation, de la volatilité de ses résultats et par l'analyse des opportunités ou menaces sur ses projets ;
• contribuant à l'optimisation de l'utilisation/allocation du capital et des ressources dans l'organisation ;
• réduisant la volatilité dans les secteurs non essentiels de l'organisation ;
• protégeant et augmentant le patrimoine et l'image de marque de l'organisation ;
• développant et soutenant le potentiel des employés et le capital de connaissance de l'organisation ;
• optimisant l'efficience opérationnelle.

La gestion des risques passe en premier lieu par l'identification des objectifs stratégiques. Une appréciation du risque est effectué en faisant son identification, son analyse, sa description ainsi que son estimation. Un compte rendu sur le risque analysé est effectué en déclinant les opportunités et les menaces avant la prise de décision sur le mode de traitement de ce risque. Un compte rendu et un suivi sur le risque résiduel est fait après la mise en place des procédures de contrôle.

Cette démarche est illustrée par la figure ci-après :

Figure 2 : Le processus de gestion des risques



Source : (FERMA, 2003)

2.1.3. Le dispositif de Bâle II

Le second accord de Bâle de 2004 sur l'adéquation des fonds propres des banques, dit Bâle II, est entré en vigueur en 2007 en Europe après une période de test. Dans la zone UEMOA, l'application du dispositif issu de Bâle II reste encore au stade embryonnaire. Selon HIMINO (2004 :43), ce nouveau dispositif permet de mettre en rapport les pertes maximales qu'une banque est susceptible de subir au cours de l'année à venir avec les capitaux dont elle s'est dotée pour y faire face ; il offre aux banques une méthodologie pour établir un tel bilan.

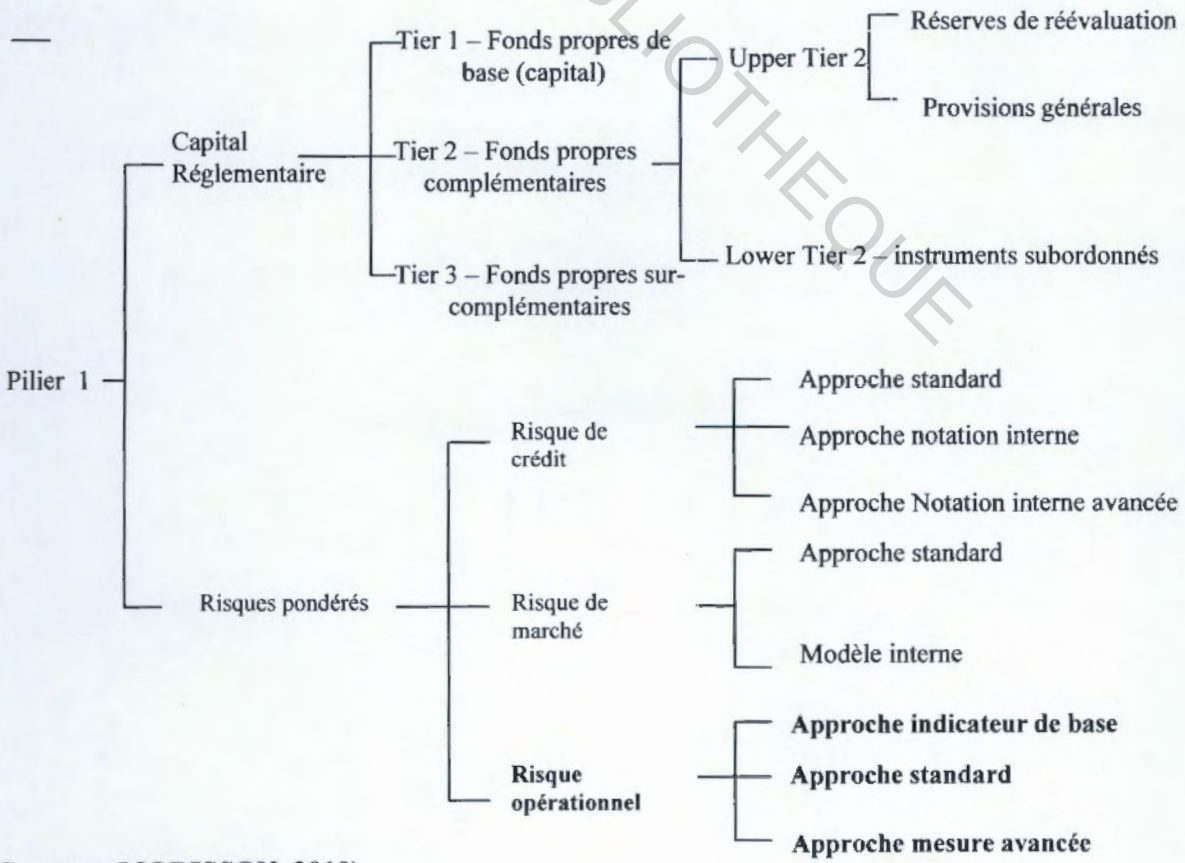
Le second accord de Bâle comprend 3 piliers qui se renforcent mutuellement :

- Pilier 1 : Exigences quantitatives minimales de fonds propres au titre des risques de crédit, de marché et opérationnels ;

- Pilier 2 : Processus de surveillance prudentielle
- Pilier 3 : Discipline de marché

S'agissant du Pilier 1, plusieurs approches de calcul des exigences en fonds propres sont possibles, plus l'approche étant sophistiquée, moins la quantité de fonds propres à constituer étant importante. La prise en compte des risques opérationnels dans le ratio est une avancée.
Le Pilier 2 autorise les superviseurs à demander des fonds propres additionnels pour couvrir notamment les risques de liquidité, les grands risques et le risque de taux d'intérêt sur le portefeuille bancaire.
Le Pilier 3 introduit plus de transparence dans les activités des banques et ouvre la voie à un renforcement de la discipline de marché directe.
Le risque opérationnel est pris en compte dans le pilier 1 du dispositif comme le fait ressortir la figure ci-après :

Figure 3 : Exigences en fonds propres Pilier 1 Bâle II



Source : (MORISSON, 2010)

L'efficacité de la règle d'adéquation des fonds propres dépend du degré de développement de l'infrastructure financière et réglementaire des pays. Comme le souligne MORISSON (2010 :18) cette règle est délicate à mettre en œuvre dans les pays en développement car :

- le capital bancaire accroît le coût des ressources,

- l'environnement est plus risqué et volatil que dans les pays développés et la norme de 8 % s'avère insuffisante,

- les pratiques comptables et d'audit des entreprises sont souvent déficientes et la valeur des portefeuilles d'actifs est sans doute surestimée,

- l'information est asymétrique et l'analyse du risque se limite souvent à l'appréciation des garanties. Les lois sur la faillite sont généralement obsolètes et les procédures de recouvrement aléatoires. Par ailleurs les équipes ne sont pas toujours suffisamment performantes pour apprécier le risque,

- la qualité du capital bancaire est incertaine, faute de marché financier et d'actionnaires fiables.

Le dispositif Bâle II propose trois méthodes de calcul des exigences de fonds propres au titre du risque opérationnel :

- une méthode simple (Basic Indicator Approach ou BIA), consistant en un calcul forfaitaire (alpha = 15 %) des exigences (KBIA) sur la base du produit net bancaire moyen sur les trois derniers exercices de la banque : KBIA = 15% PNB ;
- une méthode standard (The Standardised Approach ou TSA), consistant pour chaque ligne de métiers de la banque en un calcul forfaitaire (bêta = 12 % à 18 % selon les huit lignes définies) des exigences (KTSA) sur la base du produit net bancaire moyen enregistré sur cette ligne sur les trois derniers exercices :
  KTSA =S (PNB1 - 8 x b1 - 8);
- une méthode des mesures avancées (Advanced Measurement Approaches ou AMA), consistant en un calcul des exigences (KAMA) par le modèle interne.

Ces trois approches ont pour objet de quantifier le risque opérationnel avec une sensibilité variable et donc de contribuer à une meilleure surveillance de ce dernier. En effet, un risque ne peut être correctement maîtrisé que s'il est identifié, mesuré, évalué et géré. Parallèlement à ces outils de mesure, le Comité de Bâle a développé les principes nécessaires à une bonne maîtrise des risques opérationnels.

D'une part, il a soumis l'utilisation de l'approche standard et surtout de l'approche des mesures avancées au respect de critères qualitatifs, notamment en matière de gouvernance, d'audit et de contrôle interne. Une banque doit disposer d'une fonction de gestion du risque opérationnel bien identifiée, responsable de la conception et de la mise en œuvre du dispositif de mesure et de gestion de ce risque. Ce dispositif doit être intégré à la gestion quotidienne des risques de l'établissement et le risque encouru doit faire l'objet de comptes rendus adéquats. Il doit aussi faire l'objet d'un examen périodique des auditeurs.

D'autre part, de manière plus générale, le Comité a élaboré des saines pratiques de gestion et de contrôle du risque opérationnel, rappelant l'importance tant de l'implication de l'organe exécutif dans la mise en place d'un tel dispositif que de l'identification des risques, notamment au travers d'une cartographie de ces derniers (MAURER Frantz, 2004).

2.2. La cartographie des risques opérationnels

L'élaboration d'une cartographie des risques au sein des banques est devenue une exigence réglementaire. Cependant, sa mise en place nécessite l'adoption d'une démarche spécifique. Nous présenterons dans cette section la notion de cartographie des risques avant de décrire les étapes de son élaboration.

2.2.1. La notion de cartographie des risques

2.2.1.1. Définition

La cartographie des risques est un mode de représentation et de hiérarchisation des risques d'une organisation. La cartographie des risques constitue la première étape de la gestion des risques (MARESHAL, 2003 :15). Pour HASSID (2008 :145), la cartographie des risques est un processus d'identification, de hiérarchisation et d'évaluation des risques permettant de les positionner sur des échelles afin de les traiter. La cartographie peut représenter soit la

probabilité et l'impact global soit intégrer un élément venant modifier la probabilité ou l'impact (RENARD, 2005 : 221).

On peut donc retenir des différentes définitions que la cartographie des risques est un mode représentation et de hiérarchisation des risques d'une organisation en fonction de leur probabilité de survenance et leur degré de gravité.

2.2.1.2. Les objectifs de la cartographie des risques

Pour RENARD (2010 :157), la cartographie des risques permet d'atteindre trois objectifs :

- inventorier, évaluer et classer les risques de l'organisation ;
- informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités ;
- permettre à la direction générale, et avec l'assistance du risk manager, d'élaborer une politique de risque qui va s'imposer aux responsables opérationnels dans la mise en place de leur système de contrôle interne et aux auditeurs internes pour élaborer leur plan d'audit, c'est-à-dire fixer les priorités.

D'autres objectifs peuvent être assignés à la cartographie des risques, il s'agit :

- la communication sur les risques : selon MARESHAL (2003 :34), la cartographie permet une communication vers les parties prenante notamment la direction générale, les assureurs, les marchés financiers, les régulateurs. Elle répond au souci de transparence sur les risques ;
- répondre aux exigences réglementaires : la commission bancaire de l'UMOA impose aux établissements de crédits de disposer d'un dispositif d'identification et de maitrise des risques (Circulaire N°003-2011/CB/C).

2.2.1.3. Les types de cartographie des risques

Le choix du type de cartographie est lié au profil du risque étudié, ainsi pour MARESHAL (2003 :17), deux options peuvent être envisagées :

- la cartographie globale : elle tend à quantifier et cartographier l'ensemble des risques d'une organisation. Cette démarche permet pour une même entité, de réunir,

hiérarchiser, mais surtout de comparer des risques très différents les uns des autres dans une bonne perspective de gouvernance ;

- la cartographie thématique : c'est l'étude des risques spécifiques liés à un domaine particulier. Le périmètre étudié peut être une unique entité ou bien plusieurs entités d'une même organisation.

2.2.2. Les principales phases d'élaboration de la cartographie

Selon RENARD (2010 : 157), l'élaboration de la cartographie des risques se déroule en cinq étapes successives qui sont décrites comme suit :

- **Première étape** : élaboration d'une nomenclature des risques

On liste toutes les natures de risques susceptibles d'être rencontrées dans l'organisation. Cette liste sera plus ou moins détaillée selon que l'on souhaite dresser une cartographie plus ou moins sommaire ;

- **Deuxième étape** : identification de chaque processus/fonction/activité devant faire l'objet d'une estimation

Cette liste doit couvrir toutes les activités de l'organisation. Elle sera plus ou moins détaillée selon les objectifs ; le bon sens commande que chaque rubrique soit dimensionnée de telle façon qu'elle puisse faire l'objet d'une mission d'audit ;

- **Troisième étape** : estimation de chaque risque pour chacune des fonctions/activités

Cette estimation, présentée sous la forme d'un tableau à double entrée, va porter sur deux points appréciation de l'impact du risque (gravité) ; appréciation de la vulnérabilité estimée (fréquence). Cette appréciation se fait en considérant le risque maximum possible, également nommé risque intrinsèque ou risque spécifique ou risque inhérent (pendant du sinistre maximum possible des assureurs) ;

- **Quatrième étape** : Appréciation globale de chaque risque dans chaque activité

Elle sera le résultat du produit des deux appréciations spécifiques : la gravité et la vulnérabilité en tenant compte d'une échelle numérique mesurant le niveau de gravité et de vulnérabilité.

- **Cinquième étape** : calcul du risque spécifique de chaque fonction/activité

L'appréciation sera égale au cumul de tous les coefficients identifiés pour chaque risque et concernant cette activité. Il est bien entendu que tous les risques figurant dans la nomenclature n'existent pas pour toutes les activités.

2.2.3. Les outils et techniques d'identification des risques

2.2.3.1. Les différentes approches d'identification des risques

Selon NICOLET (2004 : 59), les établissements bancaires et financiers mettant en place des démarches de gestion des risques opérationnels commencent par identifier, pour leurs différentes activités et les produits qu'ils gèrent, les événements de risques par processus.
Cette phase d'identification des risques peut s'effectuer selon plusieurs approches. RENARD (2003 : 100) et LECLERC (2003 : 6) retiennent trois approches pour l'identification des risques. Il s'agit de l'identification bottom-up, l'identification top-down et l'identification combinée.

- l'identification bottom-up

Dans ce cadre, les risques opérationnels sont identifiés et traités dans les unités opérationnelles c'est-à-dire les personnes les plus proches possibles de l'activité, avant d'être communiqués via un dispositif de reporting au management ou aux personnes en charge de l'élaboration de la cartographie.

- l'identification top down

Il s'agit de la démarche inverse à la précédente. L'identification des risques est dans ce cas effectuée de manière plus fermée par les personnes en charge de la cartographie. Ce processus permet de descendre chercher l'information.

- l'identification combinée

Pour RENARD (2003 : 101), la meilleure démarche est celle qui concilie les deux attitudes. Elle consiste pour chaque responsable assisté du risk manager ou de l'audit interne de définir les risques de son activité. En remontant la hiérarchie, on obtient l'ensemble des risques

spécifiques à l'organisation. Dans le même temps, le risk manager ou le responsable de l'audit soumet à la Direction Générale les risques de l'entreprise considérés comme essentiels. Cette liste va redescendre la hiérarchie afin de permettre à chacun de faire une relecture de ses propres risques et s'assurer que tout est bien pris en compte.

2.2.3.2. Les outils d'identification des risques

- Le questionnaire de contrôle interne

Le Questionnaire de Contrôle Interne (QCI) est un outil indispensable dans l'identification des faiblesses au niveau des processus opérationnels. C'est une grille d'analyse dont la finalité est de permettre à l'auditeur d'apprécier le niveau et d'apporter un diagnostic sur le dispositif de contrôle interne, de l'entité ou de la fonction auditée.

- L'interview

L'interview est une technique de recueil d'informations qui permet d'expliquer et de commenter le déroulement des opérations afférentes à un processus. Elle permet à :

- l'auditeur de percevoir les nuances dans l'expression de l'audité
- l'audité de bien comprendre la démarche et les objectifs de l'auditeur

Selon RENARD (2003 : 168), l'interview n'est pas un interrogatoire, ni une conversation, encore moins un discours. Elle doit se dérouler dans une ambiance détendue et refléter une atmosphère de collaboration entre l'auditeur et l'audité.

2.3. Le dispositif de contrôle et de traitement des risques opérationnels

La mise en place de ce dispositif est indispensable après l'élaboration de la cartographie, car il constitue une réponse dans la maitrise des risques identifiés.

2.3.1. Le traitement du risque

Le processus de traitement du risque consiste à sélectionner et mettre en place des mesures propres à modifier le risque. Le traitement du risque a pour principales composantes la

maîtrise et l'atténuation du risque, mais il ne s'y limite pas et s'étend entre autres à l'évitement, au transfert et au financement du risque. (FERMA, 2003).

Tout système de traitement de risque doit assurer au minimum:

- le bon fonctionnement de l'organisation ;
- l'efficacité du système de contrôle interne ;
- la conformité avec les lois et les règlements.

Le processus d'analyse de risque aide au bon fonctionnement de l'organisation en identifiant les risques qui exigent l'attention des responsables. Ceux-ci devront déterminer les actions de maîtrise du risque qui sont prioritaires en termes de bénéfice potentiel pour l'organisation. Pour RENARD (2010 : 160), parmi les deux composantes du risque : impact et probabilité, il faut pour chaque risque identifié, choisir une stratégie :

- minimiser l'impact en développant une politique de protection ;
- ou minimiser la fréquence en développant une politique de prévention.

L'auteur propose alors quatre solutions pour développer ces politiques :

- **Première solution** : l'acceptation

On ne fait rien, c'est-à-dire que l'on accepte de courir le risque. Choix opportun s'il correspond à la stratégie et aux limites de tolérance définies par celle-ci. Mais choix catastrophique s'il n'est que le résultat du hasard ou du manque d'information.

- **Deuxième solution** : le partage

Partager le risque c'est le réduire en souscrivant une assurance ou en mettant au point une joint-venture avec un tiers. Là également on perçoit l'exigence préalable d'une définition des limites de tolérance.

- **Troisième solution** : l'évitement

On fait disparaître le risque en cessant l'activité qui le fait naître.

- **Quatrième solution** : la réduction

On prend les mesures nécessaires pour réduire la probabilité ou l'impact. C'est-à-dire que l'on améliore le contrôle interne. Faire intervenir les auditeurs internes, c'est choisir cette solution. On peut observer que le partage est de même.

2.3.2. Les activités de contrôle

Selon le cadre d'évaluation des systèmes de contrôle interne du comité de Bâle, les activités de contrôle devraient faire partie intégrante des opérations quotidiennes de la banque. La direction générale doit mettre en place une structure de contrôle appropriée pour garantir des contrôles internes efficaces, en définissant les activités de contrôle à chaque niveau opérationnel. Ces activités devraient inclure les éléments suivants: examens effectués au niveau supérieur, contrôles d'activité appropriés pour les différents départements ou unités, contrôles physiques, vérification périodique du respect des plafonds d'engagement, système d'approbation et d'autorisation, système de vérification et de contrôle par rapprochement. La direction générale doit s'assurer régulièrement que tous les domaines de la banque se conforment aux politiques et procédures établies.

La gestion du risque opérationnelle en milieu bancaire peut se faire en se basant sur les référentiels de la gestion des risques du COSO II et de la FERMA. Le dispositif de Bâle II propose des mesures de quantification du risque opérationnel au titre de la dotation en fonds propres du ratio « Mac Donough ». Il est cependant indispensable avant toute démarche de traitement du risque opérationnel, de procéder à son identification à travers une cartographie. Les risques répertoriés seront soumis en fonction de leur gravité et probabilité de survenance à une politique de traitement spécifique à adopter par l'entreprise.

Chapitre 3 : Méthodologie d'approche

Notre travail de recherche nécessite l'adoption d'une démarche pour atteindre les objectifs préalables à la résolution du problème posé. L'objectif principal du mémoire étant de proposer un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiements.

Notre revue de littérature nous a permis d'une part de cerner le concept de risque opérationnel en milieu bancaire ainsi que ses implications sur la gestion des moyens de paiements. D'autre part, nous avons fait ressortir la démarche d'élaboration d'une cartographie des risques opérationnels et le dispositif de contrôle et de suivi à mettre en place en vue de la maitrise de ces risques.

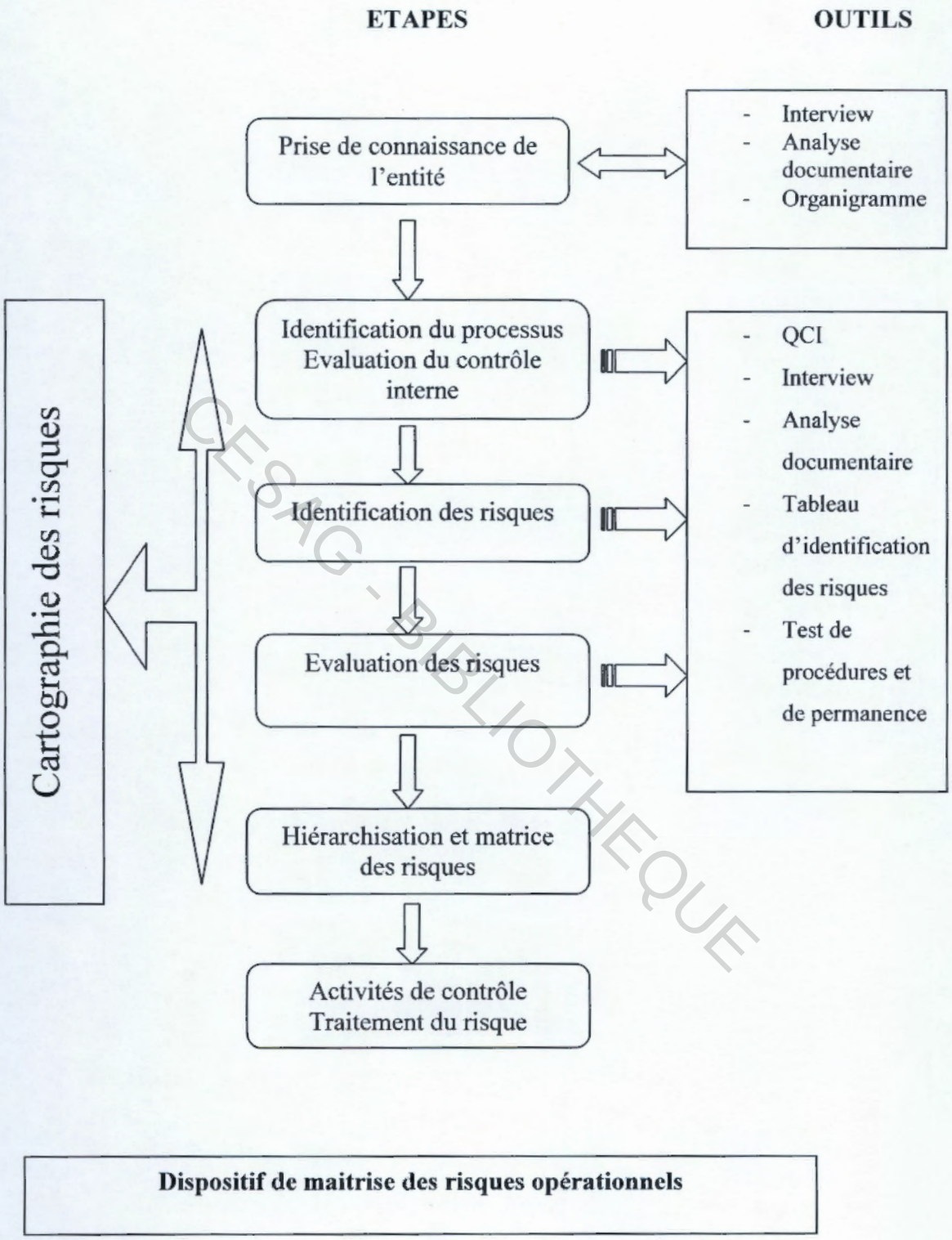
Dans ce chapitre, nous présenterons le modèle d'analyse qui nous servira de référence en vue de la proposition d'un dispositif de maitrise des risques opérationnels. Nous présenterons aussi les outils qui nous ont permis de collecter les données nécessaires à notre travail.

3.1. Le modèle d'analyse

Notre démarche d'analyse du problème étudié commence par la prise de connaissance de l'entité. Nous utiliserons à cet effet des outils comme l'interview, la revue documentaire et l'analyse de l'organigramme. La deuxième étape concerne l'identification des processus sur lesquels seront basés les travaux et l'évaluation du contrôle interne associé. Nous procéderons dans les étapes suivantes à une identification puis à une évaluation des risques identifiés sur les processus choisis. Nous ferons dans la dernière étape une hiérarchisation des risques et la conception de la matrice avant de proposer des mesures de contrôle et de traitement des risques significatifs.

La figure suivante résume notre démarche :

Figure 4 : Le modèle d'analyse



Source : nous-mêmes

3.2. Les méthodes et outils d'analyse

3.2.1. Le questionnaire de contrôle interne

Cet outil nous a permis d'évaluer une partie du système de contrôle interne lié aux processus supportant les moyens de paiements que nous avons retenus pour notre travail. Nous avons à cet effet, testé l'environnement général de contrôle ainsi que la conformité aux dispositions réglementaires des circulaires N°003 et N°005 de la commission bancaire entrées en vigueur en Février 2011.

3.2.2. Les tests de procédures et de permanence

Ces différents tests nous ont permis sur la base d'un échantillon de vérifier l'effectivité des procédures telles qu'elles nous ont été décrites et de nous assurer de leur correcte application sur une période choisie.

3.2.3. Le tableau d'identification des risques

Ce tableau nous a permis de classifier les risques identifiés par processus et selon les catégories définies dans le dispositif révisé du comité de Bâle sur la convergence internationale de la mesure et des normes de fonds propres.

3.2.4. L'analyse documentaire

C'est une étape fondamentale pour comprendre le fonctionnement de l'entité et ses différents services. L'analyse documentaire nous as permis d'enrichir notre travail théorique et de prendre connaissance des différents textes légaux et réglementaires qui régissent l'activité.

3.2.5. Interview

C'est à travers l'interview que les procédures nous ont été décrites. A cet effet, nous avons eu des entretiens avec le responsable du Contrôle Général, le responsable du service monétique, le responsable du service des opérations locales, les agents en charge des opérations de virements et de compensation.

Le cadre théorique de l'étude nous a permis de présenter les différents moyens de paiements ainsi que la réglementation en vigueur qui y est associée. Nous avons définis et décris les risques bancaires en donnant un aperçu sur les risques opérationnels liés aux moyens de paiements.

Nous avons par ailleurs décris la démarche globale de la gestion des risques en nous appuyant sur les référentiels de la gestion des risques du COSO et de la FERMA. Le dispositif de Bâle II nous a éclairés sur les enjeux des aspects réglementaires du risque opérationnels.

Nous avons développé notre propre modèle d'analyse sur l'élaboration d'un dispositif de maitrise des risques opérationnels en nous appuyant sur la revue de littérature que nous avons effectuée.

DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE

La première partie de notre mémoire nous a permis de présenter la notion de moyens de paiement ainsi que celle du risque opérationnel. Nous avons aussi présenté la démarche de mise en place d'une cartographie des risques opérationnels qui constitue la première étape du dispositif de maitrise des risques opérationnels.

Cette deuxième partie du mémoire concernera l'étude d'un cas pratique à travers la proposition d'un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiement à la BOA Niger. Toutefois dans le cadre de notre analyse, nous limiterons notre travail à l'étude de trois processus à savoir le processus de remise de chèques à l'encaissement, le processus d'émission de virements locaux en faveur de la clientèle et le processus de mise à disposition de la carte bancaire à la clientèle. Ces processus concernent essentiellement trois moyens de paiements à savoir les chèques, les cartes bancaires et les virements. La partie sera composée de trois chapitres :

Nous décrirons d'abord l'organisation de la BOA Niger, les moyens de paiement proposés à la clientèle ainsi que les processus identifiés (Chapitre 4).
Nous traiterons ensuite de la conception d'une cartographie des risques opérationnels liés aux processus objets de l'analyse (Chapitre 5).
Nous proposerons un dispositif de traitement et de contrôle des risques significatifs identifiés et nous ferons des recommandations afin d'améliorer le système de contrôle interne liés à la gestion des moyens de paiement (Chapitre 6).

Chapitre 4 : Présentation de la BOA Niger

La BOA Niger est une banque commerciale faisant partie du groupe BOA et a démarré ses activités au Niger en avril 1994. Dans ce chapitre, nous ferons un historique du Groupe BOA et nous décrirons par la suite l'organisation de la BOA Niger.

4.1. Historique et Organisation

Nous allons à travers cette section présenter l'historique du Groupe BOA ainsi que de la BOA Niger, la répartition du capital de la BOA Niger ainsi que la description de son organisation.

4.1.1. Historique du Groupe BOA

La naissance du réseau Bank Of Africa commence avec la création de la BOA Mali en 1982. Le développement de cette banque contribua à la mise en place de la Holding du groupe dénommée « African Financial Holding » (AFH) et à la création de la Bank Of Africa Bénin. La nécessité d'accroitre le capital a conduit le groupe à solliciter l'entrée d'actionnaires de poids comme PROPARCO, le FMO néerlandais et la banque NATEXIS, devenue NATEXIS-BANQUES POPULAIRES. C'est dans ce contexte que le groupe entreprit une forte politique d'expansion, ce qui amènera à l'implantation de la Bank Of Africa Niger en Avril 1994. Avec l'entrée dans le capital de la Banque Marocaine Pour le Commerce Extérieur (BMCE) en 2008, la Holding AFH prendra pour nouvelle dénomination « Bank Of Africa Group ».

4.1.2. Historique et répartition du capital de la BOA Niger

La BOA Niger est née de la reprise des activités de la Nigerian International Bank (NIB) par le groupe Bank Of Africa. Le paysage bancaire était marqué par de nombreuses faillites d'établissements de crédits accentuées par une faiblesse de la réglementation du système bancaire et un contexte économique particulièrement difficile (dévaluation du FCFA en 1994). Le total du bilan d'ouverture de la BOA Niger était légèrement supérieur à douze (12)

milliards de francs CFA, les dépôts de la clientèle environ dix (10) milliards et les créances sur la clientèle quasiment inexistante. La direction qui a été mise en place à la reprise de la NIB a entrepris une forte politique commerciale en vue d'obtenir la confiance de la clientèle locale des grandes entreprises, des institutions gouvernementales et internationales ainsi que des Organisations Non Gouvernementales (ONG).

Le capital social a connu plusieurs augmentations passant de un (1) milliard de FCFA à 1,25 milliard en septembre 1994 ; puis à 1,5milliard de FCFA en 2005, pour se chiffrer à 5milliards en 2011. Ces augmentations ont permis le renforcement des fonds propres et de la solidité financière de l'établissement.

Le capital se répartit en Février 2011 comme suit :

Tableau 1 : Répartition du Capital BOA

Actionnaires	Pourcentage (%)
BOA GROUP SA	22,99%
BOA WEST AFRICA	24,81%
BANQUE OUEST AFRICAINE DE DEVELOPPEMENT	8,78%
ATTICA SA	8,41%
ACTIONNAIRES NIGERIENS	14,19%
PERSONNEL BOA NIGER	0,32%
AUTRES ACTIONNAIRES	20,50%

Source : Rapport d'activité BOA 2010

4.1.3. Organisation de la BOA Niger

La BOA Niger est une société anonyme avec Conseil d'Administration (CA) et une Direction Générale. Nous allons décrire l'organisation de la structure dans cette sous-section.

- Le Conseil d'Administration

Le Conseil d'Administration de la BOA Niger est composé d'administrateurs désignés représentants chaque groupe d'actionnaires. Le CA est responsable devant les actionnaires de la bonne gestion de l'établissement de crédit.

➢ La Direction Générale

La Direction Générale de la BOA Niger est assurée par un Directeur Général qui doit notamment veiller à gérer la société dans le respect de l'objet social fixé dans les statuts et de toutes les dispositions légales qui lui sont applicables. A la Direction Générale de la BOA Niger est rattachée plusieurs départements dont nous ferons la description. Il est à noter aussi la présence d'un Directeur Général Adjoint qui assiste le Directeur Général dans la gestion de l'établissement (voir organigramme détaillé Cf. annexe).

➢ Le Département de Contrôle Général

Le Département Contrôle Général de la BOA Niger, au sein duquel nous avons passé notre stage, est directement rattaché à la Direction Générale et voit ses principales actions s'étendre à l'ensemble des autres départements de l'établissement. En effet, la BOA Niger par le souci de se conformer à la réglementation en vigueur a mis en place cette structure chargée d'assurer le bon fonctionnement du système de contrôle interne. Les principales actions dévolues à ce département sont : de prévenir, d'informer et de corriger les faiblesses constatées dans les procédures.

➢ Le Département des Ressources Humaines

Cette Direction a en charge de mener la politique en matière de ressources humaines de l'établissement. Elle s'occupe du volet paie et suivi du personnel, des prestations sociales ainsi que de la formation et gestion des carrières.

➢ Le Département Analyse et Gestion du Crédit

Ce département s'assure de l'application correcte des politiques et procédures en matière de crédit de l'établissement. Il comprend un service d'analyse du crédit, un service gestion administrative du crédit et un service gestion et prévention des risques en ce qui concerne le risque de crédit.

- Le Département Juridique

Le Département Juridique s'assure du bon recouvrement des créances en cas de contentieux. Il gère les garanties adossées aux différents produits de crédit et assure un contrôle des engagements. Un service compliance est rattaché à ce département pour prendre en compte les risques liés au blanchiment de capitaux.

- Le Département de l'Exploitation et du Réseau

Sous ce département sont rattachées toutes les agences de l'établissement aussi bien ceux de la capitale Niamey que ceux des autres régions. La BOA Niger compte à ce jour un réseau de seize (16) agences dont huit (8) à Niamey et huit (8) dans les régions. Le département comprend aussi le service monétique, le service marketing et communication ainsi que le service commercial.

- Le Département Traitement des Valeurs et des Opérations Locales

Ce département s'assure du traitement quotidien des opérations de virement et prélèvement locales. Il gère le service du portefeuille central ainsi que de la compensation et traite les opérations d'incidents de paiements.

- Le Département Etranger et Trésorerie

Le Service Etranger a vocation de traiter toutes les opérations effectuées vers un pays étranger, ou reçues d'un pays étranger, qu'il s'agisse d'opérations en monnaie locale ou en monnaies étrangères, ce qui inclut donc, en Zone UEMOA, les opérations traitées avec un des pays de cette zone.

- Le Département Comptable et Financier

Le département comptable et financier a en charge le bon respect des procédures et principes comptables réglementaires adoptées par le Direction Générale. Il est responsable de la centralisation de toutes les opérations comptables, de la comptabilisation des écritures de régularisation, du suivi réglementaire ainsi que la production des états financiers périodiques et de synthèse. Le service de contrôle de gestion et suivi budgétaire y est rattaché.

➢ Le Département de l'Administration Générale

L'Administration Générale gère le service achats et prestations internes, le service immobilier, entretien et archives, le service organisation et procédures, le centre de traitement, informatique et télécoms ainsi que le service Swift, standard et courrier. C'est donc un département qui fait des prestations à tous les autres départements.

4.2. La gestion des moyens de paiements de la BOA Niger

La BOA Niger offre à sa clientèle plusieurs moyens de paiements dont nous ferons la description dans cette section. Nous présenterons par la suite les processus supports à notre travail de recherche.

4.2.1. Les moyens de paiements proposés à la clientèle

Nous allons décrire principalement les formules de chèques délivrées par la banque, les types de virements traités ainsi que les cartes bancaires proposés à la clientèle.

4.2.1.1. Les chèques

La clientèle de la BOA Niger est composée de la clientèle institutionnelle, des entreprises et autres organisations, ainsi que des particuliers. La délivrance d'une formule de chèques est conditionnée par l'ouverture préalable d'un compte bancaire. Pour les particuliers, il s'agit d'un compte chèque et pour la clientèle entreprises et autres organisations, il s'agira d'un compte courant. Deux types de formules de chèques peuvent être délivrés par la banque :

- des chèques pré-barrés, non endossables sauf au profit d'une banque,
- des chèques non barrés, soumis à un droit de timbre supporté par le demandeur du chéquier.

4.2.1.2. Les virements et prélèvements

Les virements bancaires proposés aux clients sont de plusieurs natures, on peut distinguer :

- **les virements internes** : les comptes mouvementés du donneur d'ordre et du bénéficiaire sont tous des comptes BOA Niger ;

- **les virements par compensation :** ces virements concernent les mouvements des comptes des clients BOA Niger vers les comptes des tiers dans les autres banques de la place. Ces opérations transitent par le système SICA ;
- **les virements multiples** : ces opérations concernent l'ordre de débit du compte du client BOA Niger vers les comptes de plusieurs bénéficiaires domiciliés ou non à la BOA Niger.
- **les avis de prélèvement** ou **virement permanent** : à la demande du client, un virement est effectué de façon périodique et automatique en prélevant le montant demandé par le client de son compte vers les comptes des bénéficiaires.
- **les virements sur l'étranger** : les ordres de virements des clients BOA Niger vers les comptes des bénéficiaires à l'étranger.

Les virements émis et les virements reçus locaux en faveur de la clientèle sont des opérations traitées par le département des opérations locales. Les virements émis et les virements reçus sur l'étranger sont quant eux gérés par le département étranger.

4.2.1.3. Les cartes bancaires

La BOA Niger propose à sa clientèle sa carte bancaire « sésame ». Cette carte permet d'effectuer des opérations de retrait d'espèce sur ses Distributeurs Automatiques de Banque (DAB). Au-delà du réseau d'agences propres à la BOA Niger, la carte sésame permet à son détenteur de retirer ses fonds au niveau des DAB dans les agences BOA des autres pays de l'UMOA. La carte « sésame » est délivrée sur demande de la clientèle « particulier ». Elle est disponible aussi bien pour les comptes d'épargne que pour les comptes chèques. La carte VISA est aussi proposée à la clientèle.

4.2.2. Description des processus supportant les moyens de paiements

Les moyens de paiements sont supportés par des processus qui sont transverses à plusieurs services. Dans le cadre de notre travail, nous allons nous limiter à la description des sous processus suivants qui constitueront par la suite le cadre de base de l'élaboration de notre cartographie des risques:

- Processus de remise de chèques à l'encaissement (compensation-aller)

- Processus d'émission de virements locaux en faveur de la clientèle
- Processus de mise à disposition de la carte bancaire à la clientèle

4.2.2.1. Opérations de remise de chèques à l'encaissement

Le service courrier reçoit les remises chèques des clients et fait remplir par ces derniers le bordereau de remise de chèques. Les chèques sont reliés au bordereau et le lot est envoyé chaque matin au niveau du service compensation des opérations locales. Le responsable du service compensation décharge sur un registre de transmission dès réception des remises chèques par le service courrier.

Le service compensation débute le traitement en procédant au scannage des chèques reçus et procède à leur enregistrement dans le système. Ce premier enregistrement permet d'obtenir des images chèques que le responsable met en attente de confirmation. Une fenêtre permet de renseigner les informations sur chaque chèque scanné (tireur, bénéficiaire, montant du chèque, date, numéro de chèque, banque).

En fin de journée, le responsable édite la liste des chèques scannés et procède à un pointage afin de s'assurer que tous les chèques en sa disposition ont été scannés et enregistrés dans le système. Une fois cette procédure terminée, le responsable procède à la validation finale des images chèques qui étaient en attente de confirmation. Le responsable prend alors attache avec le service informatique qui sera alors chargé de faire l'intégration des données avec le progiciel de la banque.

4.2.2.2. Opérations d'émission de virements locaux en faveur de la clientèle

Les demandes de virements émis par les clients sont déposées au niveau de la réception qui se charge de leur enregistrement. Les demandes sont ensuite transmises au niveau du service des opérations pour visa de réception dans un registre tenu par le chef de service. La demande est ensuite transmise au responsable chargé du traitement des virements émis. Le responsable vérifie l'exactitude et la conformité des éléments suivants :

- le numéro de compte ;
- la signature du client donneur d'ordre ;
- le montant en chiffres et en lettres ;
- le libellé et le numéro de compte du bénéficiaire ;

- la concordance entre le nom du bénéficiaire inscrit sur la demande et le nom correspondant au compte du bénéficiaire ;
- vérification du solde du client demandeur avant l'opération.

Pour tous les montants supérieurs à trois millions, le responsable appelle le client pour confirmation. C'est seulement lorsque ces différents contrôles sont effectués que le responsable procède à la comptabilisation en débitant le compte du client et en créditant celui du bénéficiaire. En cas de non provision sur le compte du client, une copie de l'ordre du virement est transmise au service de crédit pour l'établissement d'une demande de dépassement qui sera validée par la Direction Générale.

Les ordres de virement peuvent être reçus par fax ou par mail. Dans ce cas, le client signe au préalable une convention avec la banque stipulant que les ordres de virement seront transmis par ces voies. Les ordres de virement par mail ou par fax sont directement envoyés au secrétariat de la Direction Générale qui s'assure de la transmission d'une copie de l'ordre annexé à une copie de la convention au service ces opérations. Le traitement sera le même que la procédure décrite un peu plus haut. Les mouvements supérieurs à cinquante (50) millions transitent par le système RTGS.

4.2.2.3. Opérations de mise à disposition de la carte bancaire à la clientèle

La mise à disposition d'une carte bancaire à la clientèle commence par la demande d'ouverture d'un contrat de carte. A l'ouverture du contrat, l'agent en charge vérifie l'identité du client demandeur. Il vérifie également que ce dernier dispose d'un compte à vue et n'est pas interdit bancaire. Une fiche de demande standard est remise au client afin de renseigner les données utiles et d'apposer sa signature. L'agent procède à la saisie du contrat dans le logiciel qui attribue automatiquement un numéro de carte. Les demandes effectuées au niveau des agences sont transmises au siège pour traitement. Un logiciel permet de traiter et suivre toutes les données relatives aux cartes de la saisie des demandes jusqu'à la transmission au client.

Le service monétique est responsable de la gestion des cartes bancaires. Les cartes sont fabriquées par un fournisseur spécialisé. Après réception des cartes fabriquées, le service monétique s'assure de leur transmission aux différentes agences en prenant soin de faire décharger ces dernières sur un registre de transmission ou faire établir un PV de transmission. Les codes « pins » des cartes bancaires sont transmis séparément des cartes et sont imprimés

sous un format garantissant la confidentialité. Les codes et les cartes sont conservés par des responsables différents dans les agences afin de garantir une séparation des tâches. Les cartes bancaires ne sont activées qu'au moment de la transmission effective au client. Ce dernier décharge sur un registre de transmission pour visa de réception.

La BOA Niger a depuis sa création progressivement accru la taille de son bilan. Avec l'entrée dans le Capital du Groupe Bank Of Africa d'un nouvel actionnaire de taille à savoir la BMCE, la banque s'est fixé de nouveaux objectifs de développement. Sur son activité essentiellement de banque de détail la BOA Niger propose à sa clientèle, divers moyens de paiements parmi lesquels les chèques, la carte bancaire et les virements bancaires.

Chapitre 5 : Cartographie des risques opérationnels liés à la gestion des moyens de paiement

La revue de littérature dans la première partie nous a permis de formaliser une démarche pour l'identification des risques opérationnels dans une banque. L'objet de ce chapitre est de dresser la cartographie des risques opérationnels liés à la gestion des moyens de paiements à la BOA Niger. Sans vouloir nous montrer exhaustif dans la détermination de ces risques, notre démarche se limitera à relever les risques opérationnels liés au processus de remise de chèques à l'encaissement, au processus d'émission de virements locaux en faveur de la clientèle et au processus de mise à disposition de la carte bancaire à la clientèle. Ces processus concernent essentiellement trois (3) moyens de paiements à savoir les chèques, les cartes bancaires BOA et les virements bancaires.

5.1. Evaluation du système de contrôle interne

L'évaluation du système de contrôle interne, au niveau des processus que nous avons identifiés et retenus dans le cadre de notre travail, nous permettra de déceler les forces et les faiblesses des procédures mises en place. Pour ce faire, nous avons effectué des tests de procédures et des tests de permanence. Nous avons aussi testé l'environnement général de contrôle à travers un questionnaire de contrôle interne (cf. annexe). Les résultats issus de nos travaux se présentent comme suit :

5.1.1. Tests de procédure et Tests de permanence

Les tests de procédures nous ont permis valider les procédures telles qu'elles nous ont été décrites et sur la base d'un échantillon, nous avons effectués des tests de permanence afin de vérifier sur une période l'effectivité des contrôles.

- Test de permanence processus d'émission de virements locaux

Les objectifs du test de permanence sur le processus des virements locaux sont principalement de :

- s'assurer de l'existence d'un ordre de virement signé par le client ;
- s'assurer que l'ordre de virement a été correctement saisi dans le logiciel ;
- s'assurer que l'opération a été validée par le responsable concerné ;
- s'assurer des contrôles par l'audit interne à J + 1 de l'opération.

Tableau 2 : Test de permanence processus d'émission de virements locaux

Numéro transaction	Ordre de virement	Concordance Montants Pièce Comptable/Etat comptable	Concordance numéros de comptes crédité/débité	Validation par le responsable concerné	Contrôle par l'Audit à J+1
4452	oui	oui	oui	oui	non
4785	oui	oui	oui	oui	non
4692	oui	oui	oui	oui	non
4782	oui	oui	oui	oui	non
4321	oui	oui	oui	oui	non
5263	oui	oui	oui	oui	non
5832	oui	oui	oui	oui	non
5869	oui	oui	oui	oui	non
5476	oui	oui	oui	oui	non
5364	oui	oui	oui	oui	non

Source : nous-mêmes

NB : à noter qu'avant transmission des journées comptables à l'audit, l'agent qui saisit l'opération effectue un auto-contrôle. L'audit effectue les contrôles à réception des journées comptables (qui ne sont pas transmises toujours à J+ 1 par les départements concernés). Les pièces contrôlées sont ensuite transmises au service des archives qui vérifie l'exhaustivité des pièces avant archivage.

L'analyse des résultats de notre test fait ressortir des insuffisances dans le contrôle des opérations à J+1. Ces faiblesses s'expliquent par l'insuffisance de l'effectif de l'audit interne

mais aussi des retards dans la transmission des pièces comptables à l'audit par les départements concernés.

- Test de permanence processus de mise à disposition de la carte bancaire

Les objectifs de ce test ont été de :

- s'assurer de l'existence d'une demande de carte signée par le client
- s'assurer de la validation par le responsable concerné
- s'assurer de la décharge par le client lors des retraits de carte et code
- s'assurer du contrôle par l'audit interne

Tableau 3 : Test de permanence processus de mise à disposition de la carte bancaire

Référence	Demande de carte	Validation par le responsable concerné	Décharge du client	Contrôle par l'audit
2020	oui	oui	oui	oui
2091	oui	oui	oui	oui
2197	oui	oui	oui	oui
2067	oui	oui	oui	oui
2054	oui	oui	oui	oui
2168	oui	oui	oui	oui
2024	oui	oui	oui	oui
2045	oui	oui	oui	oui
2134	oui	oui	oui	oui
2183	oui	oui	oui	oui

Source : nous-mêmes

Les résultats issus de ce test n'ont pas relevé d'anomalies au niveau de ce processus. Toutefois, nous avons relevé des difficultés dans la gestion des stocks physiques et théoriques des cartes ainsi que dans l'établissement de statistiques permettant des analyses sur les mouvements de stocks de carte.

- Test de permanence processus de remises chèques à la clientèle (compensation- aller)

Les objectifs du test de permanence sur ce processus sont principalement de :

- s'assurer du correct renseignement des bordereaux de remises
- s'assurer de la matérialisation du contrôle par le responsable avant la saisie
- s'assurer de la validation par le responsable concerné
- s'assurer du contrôle à J+1 des opérations par l'audit interne

Tableau 4 : Test de permanence processus de remises de chèque à l'encaissement (compensation- aller)

Référence	Bordereaux de remises	Contrôle avant saisie	Validation par le responsable concerné	Contrôle par l'audit à J+1
1123	oui	oui	oui	non
1245	oui	oui	oui	non
1167	oui	oui	oui	non
1189	oui	oui	oui	non
1109	oui	oui	oui	non
1156	oui	oui	oui	non
1234	oui	oui	oui	non
1221	oui	oui	oui	non
1268	oui	oui	oui	non
1098	oui	oui	oui	non

Source : nous-mêmes

L'analyse des résultats du test fait ressortir des insuffisances dans le contrôle à J+ 1 des opérations. Les mêmes conclusions que celles du test sur le processus d'émission des virements s'applique.

5.2. Identification des risques opérationnels

Nous allons présenter dans cette section la liste des risques opérationnels que nous avons identifiés par processus et les classifier suivant les catégories proposés par le « dispositif

révisé sur la convergence internationale de la mesure et des normes de fonds propres » du comité de Bâle en 2004. Cette identification concerne les risques susceptibles de se produire au niveau des processus.

5.2.1. Identification des risques liés au processus de remises de chèques à l'encaissement

Tableau 5 : Identification des risques liés au processus de remises de chèques à l'encaissement

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
1	Bordereau de remise non rempli	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
2	Registre de transmission non visé	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
3	Perte de chèques reçus	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
4	Mauvaise qualité des images chèques	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
5	Erreur de saisie	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
6	Falsification de cheque	Fraude externe	Vol et Fraude
7	Signature non conforme	Fraude externe	Vol et Fraude
8	Chèque anti daté	Fraude externe	Vol et Fraude
9	Mentions obligatoires incomplètes	Fraude externe	Vol et Fraude
11	Paiement non autorisé	Fraude interne	Activité non autorisé
12	Compte débité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
13	Compte crédité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
14	Montant débité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
15	Montant crédité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
16	Montant en chiffres différent de celui en lettres	Fraude externe	Vol et Fraude

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
17	Suspens non apurés	Exécution, livraisons et gestion des processus	Contreparties commerciales
18	Mauvais archivage des chèques payés	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
19	Scannage non exhaustif des chèques	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
20	Panne du système informatique	Interruptions d'activités et dysfonctionnement des systèmes	Systèmes
21	Commissions non prélevées	Exécution, livraisons et gestion des processus	Gestion comptes clients
22	Commissions prélevées non conformes	Exécution, livraisons et gestion des processus	Gestion comptes clients
23	Manque d'effectifs	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
24	Qualification insuffisante des agents	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
25	Manipulation frauduleuse interne	Fraude interne	Vol et Fraude
26	Non détection erreur/CG	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions

Source : nous-mêmes, inspiré du dispositif de Bâle II (2004)

5.2.2. Identification des risques liés au processus d'émission de virements locaux

Tableau 6 : Identification des risques liés au processus d'émission de virements locaux

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
27	Non enregistrement des demandes de virements	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
28	Registre de transmission au service non visé	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
29	Perte des demandes de virement	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
30	Numéro de compte à débiter non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
31	Montant en chiffres différent de montant en lettres	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
32	Transaction non autorisée	Fraude interne	Activité non autorisé
33	Compte débité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
34	Compte crédité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
35	Montant débité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
36	Montant crédité non conforme	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
37	Absence de convention pour les demandes par mail ou fax	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
38	Client « black listé » non identifié	Fraude externe	Vol et Fraude
39	Trésorerie insuffisante	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
40	Virement permanent non autorisé	Fraude interne	Activité non autorisé
41	Commissions non prélevées	Exécution, livraisons et gestion des processus	Gestion comptes clients
42	Commissions prélevées non conformes	Exécution, livraisons et gestion des processus	Gestion comptes clients
43	Panne du système informatique	Interruptions d'activités et dysfonctionnement des systèmes	Systèmes
44	Erreur de saisie	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
45	Défaillance du système de sauvegarde	Interruptions d'activités et dysfonctionnement des systèmes	Systèmes
46	Manque d'effectifs	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
47	Qualification insuffisante des agents	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
48	Intrusion frauduleuse dans le système	Fraude externe	Sécurité des systèmes
49	Clientèle sous informée	Clients, produits et pratiques commerciales	Conformité, diffusion d'informations et devoir fiduciaire
50	Opération de blanchiment non détectée	Fraude externe	Vol et Fraude

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
51	non détection erreur/CG	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions

Source : nous-mêmes, inspiré du dispositif de Bâle II (2004)

5.2.3. Identification des risques liés au processus de mise à disposition de la carte bancaire

Tableau 7 : Identification des risques liés au processus de mise à disposition de la carte bancaire

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
52	Falsification d'identité	Fraude externe	Vol et Fraude
53	Interdiction bancaire	Fraude externe	Vol et Fraude
54	Non visa du client sur demande de carte	Exécution, livraisons et gestion des processus	Admission et documentation clientèle
55	Erreur de saisie	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
56	Non transmission des demandes au siège	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
57	Panne du système informatique	Interruptions d'activités et dysfonctionnement des systèmes	Systèmes
58	Commande non autorisée	Fraude interne	Activité non autorisé
59	Commande de carte en excès	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
60	Réception tardive des cartes	Exécution, livraisons et gestion des processus	Fournisseurs
61	Facture fournisseur non conforme	Exécution, livraisons et gestion des processus	Fournisseurs
62	Livraison de cartes non conformes	Exécution, livraisons et gestion des processus	Fournisseurs
63	Perte de cartes en stock	Dommages aux actifs corporels	Catastrophes et autres sinistres
64	Mauvaise conservation des cartes	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
65	Mauvaise protection des codes "pin"	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions

Référence	Evénements de risques	Catégories Bâle (niveau 1)	Sous Catégories (niveau 2)
66	Non suivi du stock de cartes non retirées	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
67	Mauvaise séparation des tâches conservation cartes et pin	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
68	Absence de PV de transmission des cartes aux agences	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
69	Activation frauduleuse des cartes	Fraude interne	Vol et Fraude
70	Qualification insuffisante des agents	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
71	Effectif insuffisant des agents de la monétique	Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Relations de travail
72	Absence d'états de suivi des cartes en stock	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
73	Mauvais paramétrage des cartes	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
74	Cartes en stock depuis 6 mois	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
75	Cartes expirées non détruites	Exécution, livraisons et gestion des processus	Saisie, exécution et suivi des transactions
76	Utilisation frauduleuse des cartes	Fraude externe	Vol et Fraude

Source : nous-mêmes, inspiré du dispositif de Bâle II (2004)

5.3. Evaluation et Cotation des risques

Dans cette section, nous allons faire une hiérarchisation des risques en tenant compte de la probabilité de survenance et évaluer ces risques en fonction de leur impact financier. La pondération des indices mesurant la probabilité de survenance et l'impact financier nous permettra de hiérarchiser ces risques sur une matrice. Nous avons évalué la probabilité et l'impact financier grâce à nos différents tests et entretiens avec les responsables, l'analyse des statistiques de correction d'erreurs ainsi que des réclamations des clients.

Le tableau ci-après présente la méthode d'évaluation et de cotation des risques que nous avons retenue :

Tableau 8 : Evaluation et cotation des risques

Impact Financier (Gravité)	Indice	Probabilité de survenance	Indice
Faible	1	Faible	1
Moyen	2	Moyen	2
Fort	3	Fort	3

Source : nous-mêmes

5.3.1. Evaluation des risques liés au processus de remises de chèques à l'encaissement

Nous avons évalué les risques sur ce processus grâce aux différents entretiens que nous avons eu avec les responsables, les résultats de nos tests de permanence, ainsi que l'analyse du contrôle interne à travers un questionnaire (Cf. annexe). Le tableau suivant présente les résultats de nos travaux sur ce processus :

Tableau 9 : Evaluation des risques liés au processus de remises de chèques à l'encaissement

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
1	Bordereau de remise non rempli	1	1	1
2	Registre de transmission non visé	1	1	1
3	Perte de chèques reçus	1	2	2
4	Mauvaise qualité des images chèques	3	1	3
5	Erreur de saisie	2	3	6
6	Falsification de cheque	1	3	3
7	Signature non conforme	1	3	3
8	Chèque anti daté	1	1	1
9	Mentions obligatoires incomplètes	1	3	3
10	Paiement non autorisé	1	3	3
11	Compte débité non conforme	1	3	3
12	Compte crédité non conforme	1	3	3
13	Montant débité non conforme	2	3	6
14	Montant crédité non conforme	2	3	6
15	Montant en chiffres différent de celui en lettres	1	1	1

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
16	Suspens non apurés	1	3	3
17	Mauvais archivage des chèques payés	1	1	1
18	Scannage non exhaustif des chèques	1	2	2
19	Panne du système informatique	1	3	3
20	Commissions non prélevées	1	3	3
21	Commissions prélevées non conformes	1	3	3
22	Manque d'effectifs	1	2	2
23	Qualification insuffisante des agents	2	3	6
24	Manipulation frauduleuse interne	3	3	9
25	Non détection erreur/CG	1	3	3

Source : nous-mêmes

La hiérarchisation de ces risques nous permettra de mieux appréhender les risques significatifs.

5.3.2. Evaluation des risques liés au processus d'émission de virements locaux

Nous avons évalué les risques sur ce processus grâce aux différents entretiens que nous avons eu avec les responsables, les résultats de nos tests de permanence, ainsi que l'analyse du contrôle interne à travers un questionnaire (Cf. annexe). Le tableau suivant présente les résultats de nos travaux sur ce processus :

Tableau 10 : Evaluation des risques liés au processus d'émission des virements locaux

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
26	Non enregistrement des demandes de virements	1	1	1
27	Registre de transmission au service non visé	1	1	1
28	Perte des demandes de virement	1	3	3
29	Numéro de compte à débiter non conforme	1	3	3
30	Montant en chiffres différent de montant en lettres	1	1	1
31	Transaction non autorisée	2	3	6
32	Compte débité non conforme	1	3	3
33	Compte crédité non conforme	1	3	3
34	Montant débité non conforme	1	3	3

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
35	Montant crédité non conforme	1	3	3
36	Absence de convention pour les demandes par mail ou fax	2	3	6
37	Client « black listé » non identifié	1	3	3
38	Trésorerie insuffisante	2	3	6
39	Virement permanent non autorisé	1	3	3
40	Commissions non prélevées	1	3	3
41	Commissions prélevées non conformes	1	3	3
42	Panne du système informatique	1	3	3
43	Erreur de saisie	2	3	6
44	Défaillance du système de sauvegarde	1	3	3
45	Manque d'effectifs	2	2	4
46	Qualification insuffisante des agents	2	3	6
47	Intrusion frauduleuse dans le système	1	3	3
48	Clientèle sous informée	2	2	4
49	Opération de blanchiment non détectée	1	3	3
50	non détection erreur/CG	1	3	3

Source : nous mêmes

La hiérarchisation de ces risques nous permettra de mieux appréhender les risques significatifs.

5.3.3. Evaluation des risques liés au processus de mise à disposition de la carte bancaire

Nous avons évalué les risques sur ce processus grâce aux différents entretiens que nous avons eu avec les responsables, les résultats de nos tests de permanence, ainsi que l'analyse du contrôle interne à travers un questionnaire (Cf. annexe). Le tableau suivant présente les résultats de nos travaux sur ce processus :

Tableau 11 : Evaluation des risques liés au processus de mise à disposition de la carte bancaire

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
51	Falsification d'identité	2	2	4
52	Interdiction bancaire	1	3	3

Référence	Evénements de risques	Probabilité de survenance (P)	Impact Financier (I)	Cotation (P x I)
53	Non visa du client sur demande de carte	1	2	2
54	Erreur de saisie	2	3	6
55	Non transmission des demandes au siège	1	2	2
56	Panne du système informatique	1	3	3
57	Commande non autorisée	1	3	3
58	Commande de carte en excès	1	1	1
59	Réception tardive des cartes	3	2	6
60	Facture fournisseur non conforme	1	3	3
61	Livraison de cartes non conformes	1	3	3
62	Perte de cartes en stock	2	3	6
63	Mauvaise conservation des cartes	1	2	2
64	Mauvaise protection des codes "pin"	1	3	3
65	Non suivi du stock de cartes non retirées	2	1	2
66	Mauvaise séparation des tâches conservation cartes et pin	1	3	3
67	Absence de PV de transmission des cartes aux agences	1	1	1
68	Activation frauduleuse des cartes	1	3	3
69	Qualification insuffisante des agents	2	3	6
70	Effectif insuffisant des agents de la monétique	2	2	4
71	Absence d'états de suivi des cartes en stock	3	2	6
72	Mauvais paramétrage des cartes	1	2	2
73	Cartes en stock depuis 6 mois	3	1	1
74	Cartes expirées non détruites	3	1	3
75	Utilisation frauduleuse des cartes	1	3	3

Source : nous-mêmes

La hiérarchisation de ces risques nous permettra de mieux appréhender les risques significatifs.

5.4. Hiérarchisation et matrice des risques

Dans cette section, nous allons faire une représentation schématique des risques sur un repère comportant deux axes. Sur l'axe des abscisses, nous aurons la probabilité de survenance et l'axe des ordonnées représentera l'impact financier. Nous ferons l'analyse de cette matrice afin de proposer un plan d'action pour les risques les plus significatifs.

5.4.1. Hiérarchisation des risques

Cette hiérarchisation nous permet de classifier les risques en fonction de la cotation (P x I) définie. La cotation la plus élevée correspondra aux évènements à forte probabilité et pouvant générer des pertes élevées. Le tableau suivant fait la synthèse par ordre décroissant de ces facteurs de risques.

Tableau 12 : Hiérarchisation des risques identifiés sur les processus

Référence	Evènements de Risques	P	I	P x I
24	Manipulation frauduleuse interne	3	3	9
5	Erreur de saisie	2	3	6
13	Montant débité non conforme	2	3	6
14	Montant crédité non conforme	2	3	6
23	Qualification insuffisante des agents	2	3	6
31	Transaction non autorisée	2	3	6
36	Absence de convention pour les demandes par mail ou fax	2	3	6
38	Trésorerie insuffisante	2	3	6
43	Erreur de saisie	2	3	6
46	Qualification insuffisante des agents	2	3	6
54	Erreur de saisie	2	3	6
59	Réception tardive des cartes	3	2	6
62	Perte de cartes en stock	2	3	6
69	Qualification insuffisante des agents	2	3	6
71	Absence d'états de suivi des cartes en stock	3	2	6
45	Manque d'effectifs	2	2	4

Référence	Evènements de Risques	P	I	P x I
48	Clientèle sous informée	2	2	4
51	Falsification d'identité	2	2	4
70	Effectif insuffisant des agents de la monétique	2	2	4
4	Mauvaise qualité des images chèques	3	1	3
6	Falsification de cheque	1	3	3
7	Signature non conforme	1	3	3
9	Mentions obligatoires incomplètes	1	3	3
10	Paiement non autorisé	1	3	3
11	Compte débité non conforme	1	3	3
12	Compte crédité non conforme	1	3	3
16	Suspens non apurés	1	3	3
19	Panne du système informatique	1	3	3
20	Commissions non prélevées	1	3	3
21	Commissions prélevées non conformes	1	3	3
25	Non détection erreur/CG	1	3	3
28	Perte des demandes de virement	1	3	3
29	Numéro de compte à débiter non conforme	1	3	3
32	Compte débité non conforme	1	3	3
33	Compte crédité non conforme	1	3	3
34	Montant débité non conforme	1	3	3
35	Montant crédité non conforme	1	3	3

Référence	Evènements de Risques	P	I	P x I
37	Client « black listé » non identifié	1	3	3
39	Virement permanent non autorisé	1	3	3
40	Commissions non prélevées	1	3	3
41	Commissions prélevées non conformes	1	3	3
42	Panne du système informatique	1	3	3
44	Défaillance du système de sauvegarde	1	3	3
47	Intrusion frauduleuse dans le système	1	3	3
49	Opération de blanchiment non détectée	1	3	3
50	non détection erreur/CG	1	3	3
52	Interdiction bancaire	1	3	3
56	Panne du système informatique	1	3	3
57	Commande non autorisée	1	3	3
60	Facture fournisseur non conforme	1	3	3
61	Livraison de cartes non conformes	1	3	3
64	Mauvaise protection des codes "pin"	1	3	3
66	Mauvaise séparation des tâches conservation cartes et pin	1	3	3
68	Activation frauduleuse des cartes	1	3	3
73	Cartes en stock depuis 6 mois	3	1	3
74	Cartes expirées non détruites	3	1	3
75	Utilisation frauduleuse des cartes	1	3	3
3	Perte de chèques reçus	1	2	2

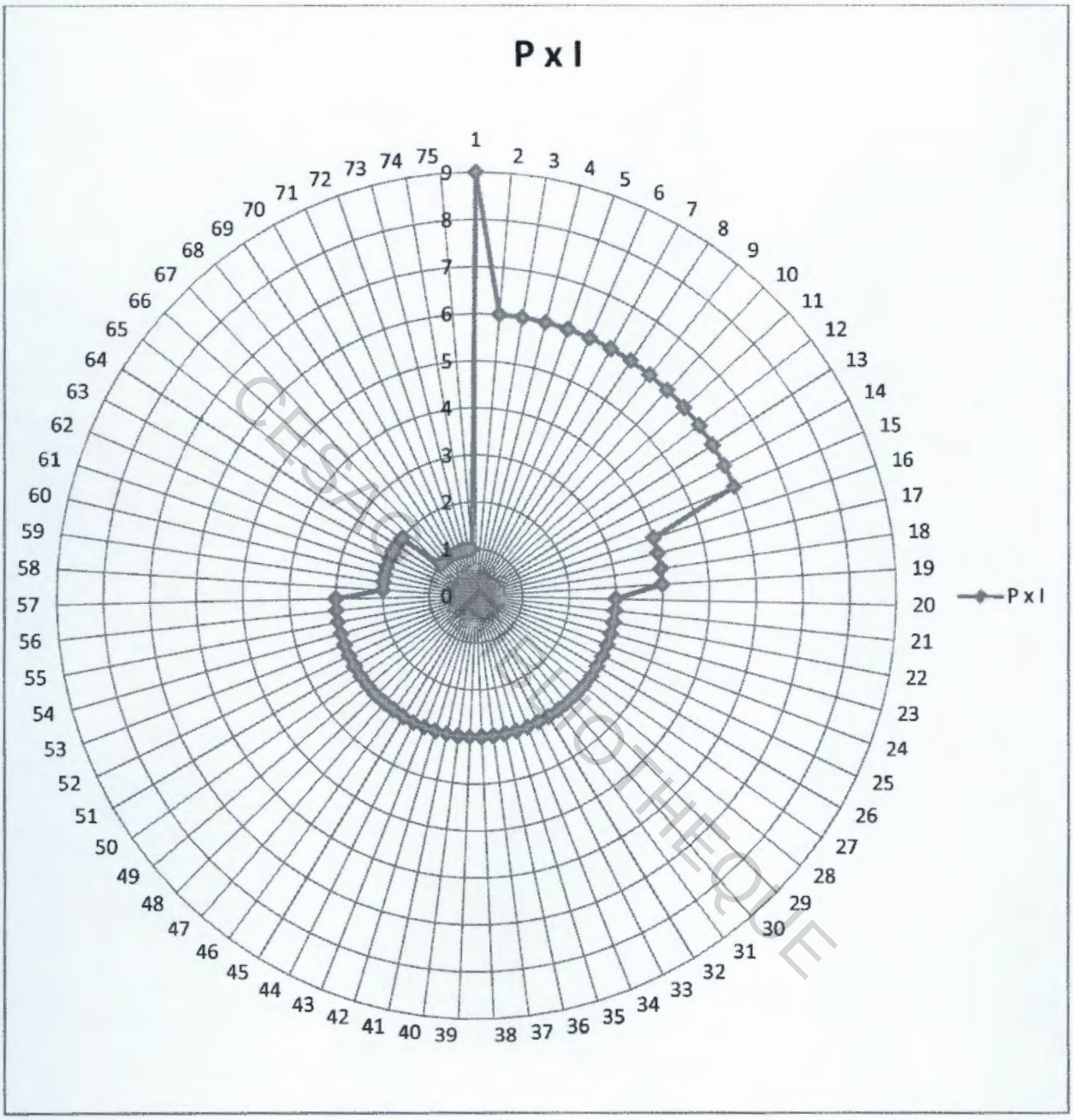
Référence	Evènements de Risques	P	I	P x I
18	Scannage non exhaustif des chèques	1	2	2
22	Manque d'effectifs	1	2	2
53	Non visa du client sur demande de carte	1	2	2
55	Non transmission des demandes au siège	1	2	2
63	Mauvaise conservation des cartes	1	2	2
65	Non suivi du stock de cartes non retirées	2	1	2
72	Mauvais paramétrage des cartes	1	2	2
1	Bordereau de remise non rempli	1	1	1
2	Registre de transmission non visé	1	1	1
8	Chèque anti daté	1	1	1
15	Montant en chiffres différent de celui en lettres	1	1	1
17	Mauvais archivage des chèques payés	1	1	1
26	Non enregistrement des demandes de virements	1	1	1
27	Registre de transmission au service non visé	1	1	1
30	Montant en chiffres différent de montant en lettres	1	1	1
58	Commande de carte en excès	1	1	1
67	Absence de PV de transmission des cartes aux agences	1	1	1

Source : nous mêmes

5.4.2. Matrice des risques

La matrice des risques nous donne une représentation schématique des risques en fonction de leur probabilité de survenance et de leur impact financier. Les figures suivantes décrivent la matrice des risques.

Figure 5 : Hiérarchisation et matrice des risques



Source : nous-mêmes

La figure 5 nous présente une hiérarchisation des risques en fonction de la cotation des risques (Probabilité x Impact). Plus on s'éloigne du centre de la sphère, plus la cotation du risque devient de plus en plus élevée. La cotation va donc du centre de la sphère à la surface, tandis que les risques sont représentés par leurs numéros de référence sur la surface.

Figure 6 : Matrice des risques

Source : nous-mêmes

La figure 6 nous présente une hiérarchisation en fonction de leur probabilité de survenance et de leur impact financier. L'axe des abscisses représente la probabilité de survenance et l'axe des ordonnées l'impact financier.

5.5. Analyse des résultats de la matrice des risques

La hiérarchisation des risques et leur disposition sur une matrice nous donne un aperçu des risques les plus significatifs en fonction des deux critères choisis que sont la probabilité de survenance et l'impact financier. Notre analyse se limitera aux risques ayant un fort impact financier pour la banque en cas de réalisation, car ce sont eux susceptibles d'engendrer de fortes pertes financières. Nous pouvons dès lors faire ressortir que sur un total de 75 risques retenus sur les trois processus, un (1) risque seulement soit 1,33% présente un caractère critique avec une probabilité élevée de survenance et un fort impact financier en cas de réalisation. 16% des risques identifiés soit un total de 12 risques présentent une probabilité moyenne de survenance et un fort impact financier. Les risques ayant une faible probabilité mais avec un fort impact représentent quant à eux 45,33% du total des risques soit 34 risques identifiés.

L'évaluation du contrôle interne nous a permis de faire ressortir les faiblesses liées à trois processus supportant les moyens de paiements : il s'agit du processus de mise à disposition de la carte bancaire à la clientèle, du processus de remise de chèques à l'encaissement ainsi que du processus d'émission de virements locaux en faveur de la clientèle. L'identification des risques qui y sont liés a permis de mettre en évidence 75 risques dont 13 à mettre sous surveillance en raison de leur probabilité de survenance et de leur fort impact financier en cas de réalisation. Le traitement de ces risques nécessite la mise en place d'un dispositif de contrôle.

Chapitre 6 : Dispositif de contrôle et de traitement des risques

Dans ce chapitre, nous ferons un descriptif du dispositif de contrôle à mettre en place ou visant à renforcer le dispositif déjà existant en vue de la maitrise des risques identifiés dans le chapitre précédent. Nous allons aussi présenter nos recommandations en vue de l'amélioration du système de contrôle interne.

6.1. Dispositif de contrôle et de traitement des risques

Le traitement consiste à sélectionner pour chaque risque identifié une méthode visant à atténuer ce risque tant au niveau de sa probabilité de survenance que de son impact financier. Les évènements de risques pour lesquels nous avons choisi une stratégie de traitement sont les suivants :

Tableau 13 : Risques retenus

Référence	Evènements de risques	Risque (P X I)
24	Manipulation frauduleuse interne	9
23	Qualification insuffisante des agents	6
37	Client « black listé » non identifié / Opération de blanchiment non détectée	3
47	Intrusion frauduleuse externe dans le système	3

Source : nous-mêmes

A. Manipulation frauduleuse interne

Cet évènement de risque a une origine interne. Il est le résultat d'une fraude interne, d'une utilisation d'informations à des fins personnelles par les agents de la banque. On peut classifier dans cette catégorie les vols de biens, de données financières, la banqueroute, le recel, la manipulation d'informations visant à contourner les lois et règlements, les détournements, etc. La banque de par son activité est confrontée à ce genre de risque. Pour minimiser ce risque, les mesures ou les contrôles suivants peuvent être initiés :

- renforcer les critères visant à s'assurer de l'intégrité du personnel au recrutement et s'assurer du correct respect des procédures de recrutement mises en place par la banque ;
- adopter un code de déontologie et le faire viser par l'ensemble du personnel et les administrateurs ;
- sensibiliser davantage le personnel sur les enjeux stratégiques et développer une forte culture d'entreprise ;
- renforcer le contrôle hiérarchique des opérations et limiter autant que possible les cumuls de fonction dites incompatibles ;
- favoriser une rotation au niveau des postes opérationnels.

Ces mesures ne sont pas exhaustives mais peuvent donner une assurance raisonnable quant à la limitation du risque de manipulation frauduleuse interne.

B. Qualification insuffisante des agents

Ce risque s'accroit avec l'évolution technologique et la complexité des processus. La non maitrise par les agents en charge des opérations peut entrainer des lourdeurs administratifs et des erreurs récurrentes dans les tâches. Pour couvrir ce risque, on peut mettre en place :

- une identification périodique des besoins de formation du personnel ;
- la mise en place d'un programme de formation par service ;
- encourager le personnel à l'autoformation ;
- le respect des procédures de recrutement définies.

C. Client « black listé » non identifié / Opération de blanchiment non détectée

Ce point concerne les clients identifiés comme susceptibles d'effectuer des opérations de blanchiments d'argent ou une opération de blanchiment non détectée. Ce risque notamment très important révèle d'un enjeu stratégique, en effet la prise en compte de la lutte contre le blanchiment des capitaux doit interpeller au plus haut niveau de l'administration de la banque par la mise en place d'une stratégie. Néanmoins, nous pouvons proposer des pistes de solutions en vue d'une réduction de ces risques :

- la correcte identification des clients avant la relation d'affaires. Cette identification doit permettre de connaitre l'activité précise du client, la justification des flux de son compte ou de ses comptes ainsi que toute autre information susceptible d'éclairer sue les activités du client ;

- le blocage systématique par le système des clients figurant sur la « liste noire » : cela peut se faire par l'intégration de la liste dans le logiciel de la banque ;
- la création d'une fonction de chargé du contrôle des opérations de blanchiments ;
- le blocage des opérations d'un certain montant jusqu'à leur analyse ;
- le filtrage des opérations.

Ce risque est cependant maitrisé au niveau la banque par la mise en place d'un dispositif de lutte contre le blanchiment.

D. Intrusion frauduleuse externe dans le système

Ce risque est relatif aux mesures de sécurités à mettre en place par la banque afin d'éviter une atteinte à son patrimoine par une intrusion externe. Il a été jugé comme faible par sa probabilité de survenance au niveau de la banque, néanmoins en raison de l'impact qui peut être significatif les contrôles et mesures de sécurités à mettre en place ou à renforcer si existantes peuvent être les suivantes :

- renforcement du système de sécurité interne par la mise en place de portiques sécurisés, de dispositif d'alarme et de caméra de surveillance ;
- la présence de forces de sécurité avec moyens dissuasifs ;
- renforcement de la politique de protection du système d'information par la réalisation préalable d'un audit afin d'identifier les faiblesses ;
- le contrôle d'accès au serveur ;
- la sensibilisation du personnel sur ces risques.

6.2. Recommandations

Les recommandations formulées à ce niveau visent à améliorer le système de contrôle interne de la banque et plus spécifiquement celui relatif à la gestion des moyens de paiements

Recommandation 1 : Renforcer l'équipe du contrôle général

Le contrôle des opérations de façon exhaustive ne peut se faire qu'avec la présence d'un personnel suffisant. Ce renforcement du personnel du contrôle permettra à ce département de couvrir un large périmètre de contrôle pour répondre aux objectifs fixés par la direction générale.

Recommandation 2 : Elaborer une cartographie globale des risques

Comme exigé dans la circulaire N°003 de la Commission Bancaire sur le contrôle interne, l'élaboration d'une cartographie globale des risques de la banque devient une nécessité dans l'approche visant à maitriser les risques de l'organisation. Notre travail de recherche pouvant constituer une démarche dans l'élaboration de cette cartographie et la mise en place d'un dispositif complet de gestion des risques.

Recommandation 3 : Nommer un responsable chargé de la gestion des risques (Risk Manager)

Bien que pouvant générer un coût en charge de personnel, il n'en demeure pas moins que cette fonction soit un investissement à très grande valeur ajoutée si les objectifs qui lui sont assignés permettent de prendre en compte la dimension risque de toute l'organisation.

Le traitement des risques nécessite la mise en place de procédures de contrôle spécifiques sur les processus. Notre proposition dans le cadre de ce travail a été de formuler des recommandations visant à instaurer ou à renforcer les pratiques en matière de contrôle pour couvrir quelques risques à fort impact sur les processus retenus. Les recommandations générales visent à renforcer le dispositif de contrôle interne.

Conclusion

Les mutations profondes dans le secteur financier ont contribué un changement d'échelle du risque bancaire. Ces mutations conjuguées aux multiples scandales dans le secteur bancaire et financier ont fait prendre conscience aux autorités de contrôle et des instances de normalisation internationales de la nécessité d'une meilleure prise en compte du risque opérationnel. Ce dernier fait l'objet d'une disposition spécifique dans le premier pilier de l'accord de Bâle II qui y consacre des méthodes d'évaluation et de traitement.

Dans la zone UMOA, les enjeux liés à l'harmonisation des pratiques en matière de contrôle bancaire a incité les autorités de contrôle bancaire de l'UMOA à se conformer aux règles et dispositions des accords de Bâle II. A cet effet, de nouvelles circulaires de la commission bancaires en 2011 sont venus renforcer le système de surveillance des établissements de crédit de la zone. La circulaire N°003/CB sur le système de contrôle interne fait mention et obligation aux établissements de crédits de mettre en place un dispositif de gestion des risques bancaires et particulièrement un dispositif couvrant les risques opérationnels. Cela se traduit par l'élaboration d'une cartographie des risques opérationnels ainsi que des dispositifs de contrôle et de traitement couvrant ces risques.

L'objectif de ce mémoire a été de proposer un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiements au niveau de la BOA Niger. Nous avons dans une première partie dite théorique définis les différents concepts de risques bancaires en insistant sur le risque opérationnel tout en présentant les notions pratiques et les aspects réglementaires des moyens de paiement. Nous avons présenté la démarche d'élaboration d'une cartographie des risques opérationnels ainsi que les dispositifs de contrôle à mettre en place pour atténuer ces risques. Une deuxième partie dite pratique, nous a permis de proposer un dispositif de maitrise des risques opérationnels liés à la gestion de trois processus couvrant les chèques, les cartes bancaires et les virements. Les résultats issus de nos travaux ont montré que seul un faible pourcentage des risques identifiés relevait d'un caractère significatif. Nous avons donc proposé des mesures de contrôles et de traitement tout en faisant des recommandations afin d'améliorer le système de contrôle interne.

Nous osons espérer que notre travail de recherche constituera une démarche pour l'élaboration d'un dispositif complet de gestion des risques opérationnels au niveau de la BOA Niger.

Bibliographie

➢ Ouvrages

1. AHOUANGANSI Evariste, (2006), *Audit et révision des comptes,* éditions mondexperts, 729p.
2. BARTHELEMY Bernard et COURREGES Philippe (2004), *Gestion des risques, Méthode d'optimisation globale,* 2e édition, 409p.
3. BEGUIN Jean-Marc et BERNARD Arnaud, (2008), *L'Essentiel des Techniques Bancaires*, Editions d'Organisation.
4. BERNARD Frédéric et GAYRAUD Laurent, (2006), *contrôle interne : concepts, réglementations, cartographie des risques, guide d'audit de la fraude, méthodologie et mise en place, référentiels, modes opératoires*, Maxima, 303p.
5. BESSIS Joël, (2002), *Risk Management in Banking,* 2nd edition, John Wiley & Sons, 812 p.
6. DE MARESCHAL Gilbert (2003), *La cartographie des risques*, édition AFNOR, 45p.
7. DOV Ogien, (2008), *Comptabilité et Audit Bancaire,* 2e édition, Dunod, 527p.
8. GREUNING Hennie van et SONJA Brajovic (2004), *Analyse et gestion du risque bancaire*, édition ESKA, 384p.
9. HASSID Olivier, (2008), *La gestion des risques,* 2e édition, Dunod, 149p.
10. HAMZAOUI Mohamed et PIGE Benoit, (2005), *Audit : gestion des risques d'entreprise et contrôle interne*, Editions Pearson Education France, 243 p.
11. IFACI (2005), *le management des risques de l'entreprise COSO II*, éditions d'organisation, 338p.
12. JIMENEZ Christian, MERLIER Patrick, CHELLY Dan, (2008), *Risques opérationnels : de la mise en place du dispositif à son audit,* Revue Banque Edition, 271 p.
13. MADERS Henri-Pierre et MASSELIM Jean-Luc (2006), *contrôle interne des risques,* 2e édition, Editions d'Organisation, 261p.
14. MONNIER Philippe et MAHIER-LAFRANCOIS Sandrine (2008), *Les Techniques Bancaires*, Dunod, 298p.
15. MOREAU Franck (2002, comprendre et gérer les risques, Editions d'Organisation, 222p.
16. RENARD Jacques, (2010), *Théorie et pratique de l'audit interne,* 7e édition, Editions d'Organisation, 469 p.
17. RENARD Jacques, (2003), *L'audit interne : ce qui fait débat*, Maxima, 265p.
18. SARDI Antoine (2002), *Audit et Contrôle Interne Bancaires*, édition AFGES, 1065p.

19. SIRUGUET Jean-Luc, (2007), *le contrôle comptable bancaire : un dispositif de maitrise des risques,* 2e édition, Revue Banque Edition, 577 p.
20. THEORET Raymond, (1999), *Traité de gestion bancaire*, Presses universitaires du Québec, 259p.

➢ **Articles**

1. HIMINO Ryozo, (2004), *Bâle II ou la définition d'un langage commun*, Rapport trimestriel BRI Septembre 2004, PP. 43-51
2. MAZARS, (Février 2005), *Bâle II : les principes fondateurs de la réforme,* les cahiers de Mazars, PP. 18-25
3. NICOLET Marie-Agnès (Novembre 2004), *Intégrer l'évaluation des moyens de paiements dans les cartographies des risques opérationnels*, Banque magazine, N°663, PP.58-60.
4. PENNEQUIN Maxime et FRACHOT Antoine, (2003), *Bâle II : vers une convergence des différents méthodologies*, Banque magazine, N°649, PP.60-65.
5. VERET Catherine et NAÏM Patrick, (Mai 2011), *Risk Management : gérer et évaluer les risques opérationnels extrêmes*, Revue Banque, N°736, PP. 46-50.

➢ **Textes réglementaires et rapports institutionnels**

1. BCEAO, (2003), Instruction N°01/2003 du 8 mai 2003 relative à la promotion des moyens de paiement scripturaux et à la détermination des intérêts exigibles en cas de défaut de paiement.
2. BCEAO, (2002), Directive N°08/2002/CM/UEMOA portant sur les mesures de promotion de la bancarisation et de l'utilisation des moyens de paiement scripturaux ;
3. BCEAO, (2002), Règlement N°15/2002/CM/UEMOA relatif au système de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest Africaine qui abroge la loi uniforme sur les moyens de paiements ;
4. BCEAO, (1999), Loi cadre relative à la répression du faux monnayage dans les pays de l'UMOA;
5. BCEAO, (1999), Instruction N°01/CIP du 1er février 1999 relative au dispositif de centralisation des incidents de paiement dans l'UMOA ;
6. Commission Bancaire UMOA, (2011), Circulaire N°003-2011/CB/C relative à l'organisation du système de contrôle interne des établissements de crédits de l'UMOA ;

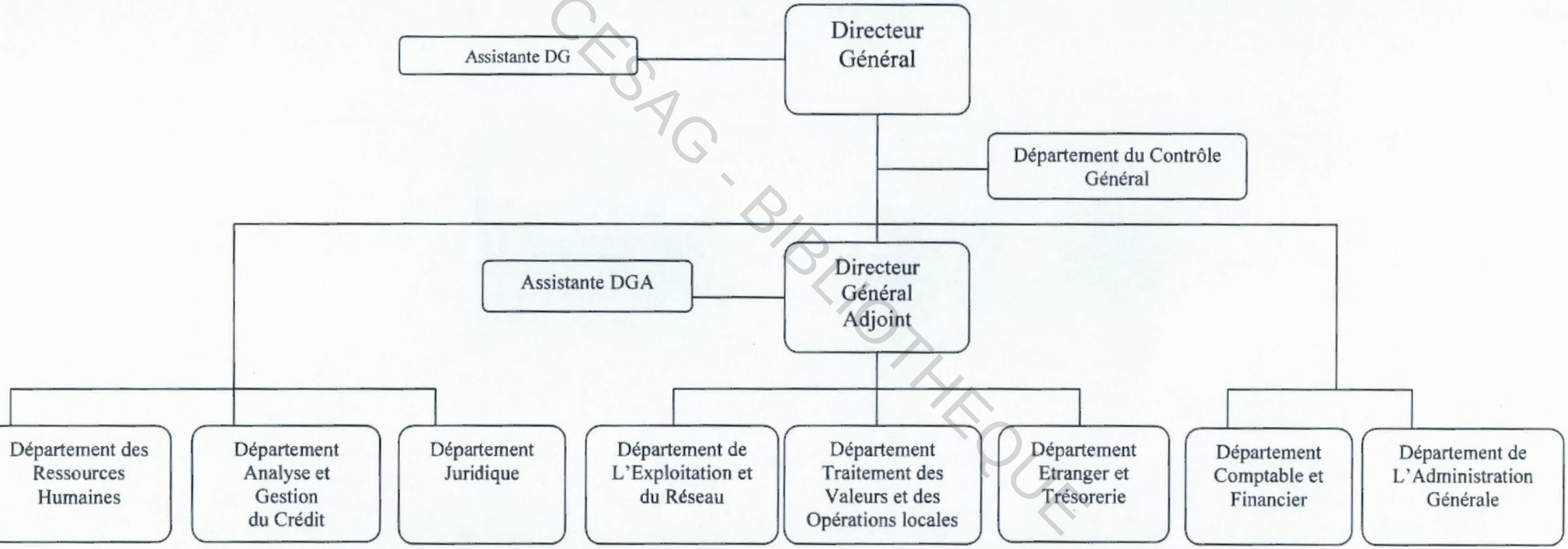
7. Commission Bancaire UMOA, (2011), Circulaire N°005-2011/CB/C relative à la gouvernance des Etablissements de Crédit de l'UMOA ;
8. Commission Bancaire, (2009), Rapport Commission Bancaire UMOA 2009
9. Comité de Bâle, (2004), convergence internationale de la mesure et des normes de fonds propres : dispositif révisé.

➢ **Références Internet**

1. ANDRIES Marc et MARTI Carlos, page consulté le 10 juillet 2011, http://www.banque-france.fr/archipel/publications/bdf_rsf/etudes_bdf_rsf/bdf_rsf_05_etu_3.pdf
2. DELOITTE, page consultée le 10 juillet 2011, http://www.deloitterecrute.fr/sites/www.deloitterecrute.fr/files/etude/111/puttingriskcomfortzone_francais_mars2009.pdf
3. FERMA, page consultée le 15 juillet 2011, http://www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-french-version.pdf
4. MAURE Frantz, page consulté le 10 juillet 2011, http://affi2007.u-bordeaux4.fr/Actes/31.pdf
5. MORISSON Gilles, page consulté le 15 juillet 2011, http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Documents_Economiques/doc-pedagog-num3-situation-financ-banques.pdf
6. NICOLET Marie-Agnès, page consulté le 10 juillet 2011, http://www.audisoft-consultants.com/fichier_pdf/Nicolet%20663.pdf
7. PIERRE-YVES THORAVA, page consulté le 10 juillet 2011, http://www.banquefrance.fr/archipel/publications/bdf_rsf/etudes_bdf_rsf/bdf_rsf_09_etu_6.pdf

ANNEXES

ANNEXE 1 : Organigramme de la BOA Niger



ANNEXE 2 : Questionnaire de contrôle interne

Questionnaire de Contrôle interne	Service :	Rubrique : Systèmes de paiements automatisés	Auditeur : Date :

Objectifs de Contrôle Interne :

- S'assurer de la qualité du traitement des opérations par le service informatique

Questions	Réponses			Commentaires
	Oui	Non	N/A	
1. Le système informatique fait-il l'objet d'audits réguliers ?				
2. Le système informatique permet-il de traiter l'ensemble des opérations, avec le minimum de retraitements manuels ?				
3. Les procédures permettent-elles de s'assurer que toutes les opérations sont transmises au centre de traitement ?				
4. L'organisation des traitements permet-elle de respecter les délais ?				
5. Existe-t-il un plan de reprise en cas de panne du serveur central ?				

Questionnaire de Contrôle interne	Service :	Rubrique : Virements et prélèvements	Auditeur :
			Date :

Objectifs de Contrôle Interne :

- S'assurer de l'autorisation préalable des virements
- S'assurer que les erreurs sont rapidement détectées et corrigées
- S'assurer que les réclamations des clients sont rapidement traitées

Questions	Réponses			Commentaires
	Oui	Non	N/A	
1. Les virements permanents sont-ils préalablement autorisés ? 2. Sont-ils conservés dans des fichiers ? 3. Sont-ils annulés automatiquement à l'échéance fixée par le client ? 4. Les autres virements sont-ils préalablement autorisés par un responsable ? 5. Les autorisations de prélèvement reçues des clients sont-elles visées par le gestionnaire du compte pour accord ? 6. Sont-elles préservées dans un fichier ?				

Questionnaire de Contrôle interne	Service :	Rubrique : Virements et prélèvements	Auditeur :
			Date :

Objectifs de Contrôle Interne :

- S'assurer de l'autorisation préalable des virements
- S'assurer que les erreurs sont rapidement détectées et corrigées
- S'assurer que les réclamations des clients sont rapidement traitées

Questions	Réponses			Commentaires
	Oui	Non	N/A	
7. Les anomalies (absence d'autorisation, montants ou dates non conformes) sont-elles corrigées par une personne habilitée en liaison avec le client ? 8. La différence entre les dates de valeur appliquées aux clients et les dates de valeur appliquées par l'organe de gestion du système est-elle positive ? 9. Existe –il un délai de traitement des réclamations clients ? 10. Le client est-il toujours informé par écrit des suites de sa réclamation ?				

Questionnaire de Contrôle interne	Service :	Rubrique : Correspondants	Auditeur :
			Date :

Objectifs de Contrôle Interne :

- S'assurer de la protection des valeurs contre les risques de perte, de vol et d'incendie
- S'assurer de la qualité de traitement des remises chèques à l'encaissement
- S'assurer que les procédures sont respectées

Questions	Réponses			Commentaires
	Oui	Non	N/A	
1. Les valeurs sont-elles suffisamment protégées contre les risques de perte, de vol et d'incendie ? 2. Les comptes irrégulièrement débiteurs sont-ils promptement identifiés pour permettre un éventuel rejet ? 3. Les procédures en vigueur assurent-elles un encaissement rapide des valeurs remises par les clients ou les correspondants ? 4. Les actions nécessaires sont-elles régulièrement entreprises pour relancer les correspondants et les clients en cas de retard ? 5. Les frais d'encaissement et les dates de valeur appliquées par les correspondants sont-ils vérifiés et conformes aux accords conclus ou aux conditions générales ?				

Questionnaire de Contrôle interne	Service :	Rubrique : Correspondants	Auditeur :
			Date :

Objectifs de Contrôle Interne :

- S'assurer de la protection des valeurs contre les risques de perte, de vol et d'incendie
- S'assurer de la qualité de traitement des remises chèques à l'encaissement
- S'assurer que les procédures sont respectées

Questions	Réponses			Commentaires
	Oui	Non	N/A	
6. Les comptes sont-ils régulièrement justifiés par rapport aux existants et contrôlés par une personne habilitée ? 7. Les valeurs exigibles après encaissement et qui ne sont pas comptabilisées, font-elles l'objet d'un suivi ou d'une comptabilité matière ? 8. La différence entre les dates de valeur appliquées aux clients et les dates de valeur appliquées aux correspondants est-elle positive ? 9. La différence entre commissions perçues auprès du client et commissions payées aux correspondants est-elle positive ?				

TABLE DES MATIERES

RESUME

Proposition d'un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiement : cas de la BOA Niger

Les mutations profondes dans le secteur financier ont contribué un changement d'échelle du risque bancaire. Ces mutations conjuguées aux multiples scandales dans le secteur bancaire et financier ont fait prendre conscience aux autorités de contrôle et des instances de normalisation internationales de la nécessité d'une meilleure prise en compte du risque opérationnel. Ce dernier fait l'objet d'une disposition spécifique dans le premier pilier de l'accord de Bâle II qui y consacre des méthodes d'évaluation et de traitement. La nouvelle réglementation bancaire de la zone UMOA notamment la circulaire N°003 relative au système de contrôle interne fait mention et obligation aux établissements de crédits de mettre en place un dispositif couvrant les risques opérationnels. L'objectif de ce mémoire est de proposer à la BOA Niger un dispositif couvrant les risques opérationnels liés à la gestion des moyens de paiements. La matrice des risques qui en résulte donne un aperçu des risques significatifs sur les processus identifiés en fonction de leur probabilité de survenance et leur impact financier.

Mots clés : moyens de paiements, risque opérationnel, BOA Niger.

ABSTRACT

Proposal of a control device for operational risks associated with managing means of payment: Case of BOA Niger

The profound changes in the financial sector contributed to change the scale of bank risk. These changes combined with multiple scandals in the banking and financial sector have raised awareness to the supervisory authorities and international standardization bodies of the need for greater consideration of operational risk. The latter is the subject of a specific provision in the first pillar of Basel II, which devotes methods of assessment and treatment. The new banking regulations in the WAMU area especially Circular No. 003 on the internal control system mentioned and requires credit institutions to set up a device to cover operational risks. The objective of this paper was to propose to the BOA Niger device covering the operational risk associated with managing means of payment. The risk matrix that results provides an overview of the significant risks identified processes based on their probability of occurrence and their financial impact.

Keywords: means of payment, operational risk, BOA Niger.

RESUME

Proposition d'un dispositif de maitrise des risques opérationnels liés à la gestion des moyens de paiement : cas de la BOA Niger

Les mutations profondes dans le secteur financier ont contribué un changement d'échelle du risque bancaire. Ces mutations conjuguées aux multiples scandales dans le secteur bancaire et financier ont fait prendre conscience aux autorités de contrôle et des instances de normalisation internationales de la nécessité d'une meilleure prise en compte du risque opérationnel. Ce dernier fait l'objet d'une disposition spécifique dans le premier pilier de l'accord de Bâle II qui y consacre des méthodes d'évaluation et de traitement. La nouvelle réglementation bancaire de la zone UMOA notamment la circulaire N°003 relative au système de contrôle interne fait mention et obligation aux établissements de crédits de mettre en place un dispositif couvrant les risques opérationnels. L'objectif de ce mémoire est de proposer à la BOA Niger un dispositif couvrant les risques opérationnels liés à la gestion des moyens de paiements. La matrice des risques qui en résulte donne un aperçu des risques significatifs sur les processus identifiés en fonction de leur probabilité de survenance et leur impact financier.

Mots clés : moyens de paiements, risque opérationnel, BOA Niger.

ABSTRACT

Proposal of a control device for operational risks associated with managing means of payment: case of BOA Niger

The profound changes in the financial sector contributed to change the scale of bank risk. These changes combined with multiple scandals in the banking and financial sector have raised awareness to the supervisory authorities and international standardization bodies of the need for greater consideration of operational risk. The latter is the subject of a specific provision in the first pillar of Basel II, which devotes methods of assessment and treatment. The new banking regulations in the WAMU area especially Circular No. 003 on the internal control system mentioned and requires credit institutions to set up a device to cover operational risks. The objective of this paper was to propose to the BOA Niger device covering the operational risk associated with managing means of payment. The risk matrix that results provides an overview of the significant risks identified processes based on their probability of occurrence and their financial impact.

Keywords: means of payment, operational risk, BOA Niger.