CESAG **Centre Africain d'études Supérieures en Gestion**

Institut Supérieur de Comptabilité, de Banque et de Finance

Master Professionnel en Audit et Contrôle de Gestion (MPACG)

Promotion 3
(2008-2010)

Mémoire de fin d'étude

THEME

ANALYSE DE LA GESTION DES RISQUES OPERATIONNELS LIES AUX MOYENS DE PAIEMENT : CAS DE LA BANQUE ATLANTIQUE MALI

Présenté par :

Mlle Salimata DIAKITE

Dirigé par :

Mr. Mohamed Lamine BAMBA

Enseignant associé au CESAG,

Auditeur interne à la BCEAO

AVRIL 2011

DEDICACE

Je dédie ce mémoire :

- A ma mère Mariam SIDIBE, et à mon père Lanceni DIAKITE qui m'ont apporté le soutien moral et financier tout au long de cette formation ;
- A mes frères Sadou Brutus DIAKITE et Souleymane DIAKITE, et à mes sœurs Aissata DIAKITE et Assétou DIAKITE qui n'ont ménagé aucun effort pour me soutenir ;
- A mes beaux frères et sœurs qui m'ont beaucoup soutenu ;
- A tous ceux qui me sont chers.

REMERCIEMENTS

Je rends grâce à DIEU, qui m'a permis de suivre cette formation dans la paix. Que la paix et le salut soient sur son prophète le bienaimé.

J'adresse mes sincères remerciements à :

- Monsieur Moussa YAZI, Directeur de l'ISCBF, professeur au CESAG ;
- Monsieur Mohamed Lamine BAMBA, auditeur interne à la BCEAO, Enseignant associé au CESAG ;
- Monsieur N'gary SOW, auditeur interne, enseignant au CESAG ;
- Monsieur Mahamane DAOU, Directeur du Contrôle et de l'Audit Interne à la BAM;
- Monsieur Afo DIARRA, Chef du Service Contrôle à la BAM ;
- Monsieur Daoud DIARRA, Chef du Service Audit Interne à la BAM ;
- Madame Kadiatou KANTE, agent au Service Contrôle à la BAM ;
- Mademoiselle Fatoumata KEITA, agent au Service Audit Interne ;
- Mademoiselle Nagnouma KEITA, Responsable Monétique à la BAM ;
- tout le personnel de la banque Atlantique MALI ;
- Monsieur Amara Abdel Karim DIARRA, chef d'agence à la Banque Nationale de développement agricole qui m'a beaucoup aidé dans l'élaboration de ce mémoire ;
- tous ceux qui, de près ou de loin, ont contribué à l'élaboration de ce mémoire.

SIGLES ET ABREVIATIONS

AFG: Atlantic Financial Group

BAM: Banque Atlantique Mali

BBA: British Bankers Association

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

CI: Contrôle Interne

CM: Code Monétaire

COSO: Committee of Sponsoring Organizations of the Treadway Commission.

CRBF: Comité de la Réglementation Bancaire Française

CSPL: Chef de Service Portefeuille Local

DFC : Directeur Financier et Comptable

DOP : Directeur des Opérations

FCFA : Franc de la Communauté Financière Africaine.

ISO: International Organization for Standardization

RMS: Robert Morris Association

SICA: Système Interbancaire de Compensation Automatisé

STAR : Système de transfert Automatisé et de règlement

Liste des figures

Liste des annexes

Liste des tableaux

Table des matières

INTRODUCTION GENERALE

L'évolution croissante des activités économiques et l'ouverture quasi-totale des économies ont toujours été tenues comme étant les grands facteurs des bouleversements que nous avons observés durant ces dernières décennies. Ces bouleversements ont eu une grande influence sur la structuration actuelle des institutions financières. C'est dans ce cadre, que ces dernières ont mis en place des règlementations pouvant les mettre à l'abri de certains phénomènes économiques. Ces règlementations consistent en la mise en place de mécanismes et de principes de fonctionnement.

A l'heure où les grandes banques sont interconnectées entre elles et qu'elles essaient de répondre à un certain nombre de standards de fonctionnement, il va de soi de comprendre les réelles inquiétudes de ces dernières. L'amélioration continue et permanente des normes prudentielles est le nouveau défi auquel sont confrontés les établissements de crédit. En effet, dans son activité d'intermédiation financière et afin d'assurer une sécurité financière et une bonne allocation des ressources, la banque doit inscrire dans ses priorités stratégiques la maîtrise des risques auxquels elle se trouve confrontée et ce en adoptant une politique de gestion des risques

La mondialisation des échanges, l'émergence de nouvelles zones économiques à forte croissance nécessitent de la part des banques des prises de risques importants. Mais aussi, la sophistication des produits bancaires, la concurrence accrue dans le secteur, l'ouverture croissante et les innovations financières et technologiques ont grandement accru les risques liés à l'activité bancaire.

Selon SARDI (2002 : 39) « le métier de banquier est le métier du risque. Les risques sont inhérents à l'activité bancaire. L'absence ou l'insuffisance de leur maîtrise provoque inévitablement des pertes qui affectent la rentabilité et les fonds propres. La persistance et la profondeur de ces pertes peuvent conduire à la défaillance, c'est-à-dire l'incapacité de faire face à ses engagements ».

De même, pour GREUNING & al (2004 : 3), « les banques, au cours de leurs activités, sont exposées à une série de risques, qui se classent en général en quatre catégories : risques financiers, risques opérationnels, risques d'exploitation et risques accidentels ».

La gestion des risques opérationnels dans les banques a fortement évolué au cours des dernières années. Elle couvre tous les points susceptibles de poser problème dans une banque.

Elle permet de mettre en place des mesures destinées à limiter les risques liés aux différentes opérations bancaires et à prévoir les fonds propres nécessaires pour faire face aux pertes potentielles. En effet, d'après les résultats [1]d'une enquête internationale sur le risque opérationnel menée par le BBA (British Bankers Association), et le RMS (Robert Morris Association), les pertes dues à une inadéquation ou une défaillance des procédures, des personnels, des systèmes internes ou des événements extérieurs et plus précisément au risque opérationnel sont estimées à plus de 12 milliards de dollars US sur les 10 dernières années. Citons des exemples de pertes opérationnelles énormes subies dans le secteur financier : 2,4 milliards de dollars attribuables aux poursuites subséquentes à l'affaire Enron et une perte de 690 millions de dollars causée par une transaction non autorisée à Allied Irish Bank. Ajoutons le cas de la plus vieille banque du Royaume-Uni, la Barings (233 ans), qui a fait faillite à la suite d'activités non autorisées ayant occasionné une perte de 1,3 milliard de dollars. Plus récemment, l'exercice de collecte de pertes réalisé en 2002 par le groupe Risk Management du Comité de Bâle révèle que les 89 banques ayant participé à cet exercice ont connu sur le seul exercice 2001 plus de 47 000 événements de pertes opérationnelles pour un montant cumulé s'élevant à près de 7,8 milliards d'euros. L'affaire Kerviel en 2008 à la Société Générale qui a occasionné des pertes énormes pour la banque, à hauteur de plus de 4 milliards. Ces exemples montrent l'ampleur de ce risque. Ils constituent également un signal pour alerter les institutions financières qui doivent impérativement le définir, le mesurer et le gérer afin d'éviter les éventuelles pertes colossales qui peuvent en découler.

Si les méthodes de détection et de gestion des risques financiers, accidentels, et risques d'exploitation semblent définitivement acquises, celles concernant les risques opérationnels en sont encore au stade de balbutiements. Les risques opérationnels peuvent provenir de sources internes ou externes. Cependant il est reconnu que la majorité des risques opérationnels serait liée à des événements internes aux banques. Le risque opérationnel touche toutes les activités et les opérations des institutions financières de différentes manières. En effet, nous trouvons des évènements opérationnels attribuables aux personnes, aux processus, aux systèmes et aux événements externes. En revanche, les unités ne sont pas touchées de la même façon par le risque opérationnel. L'impact varie selon la nature des activités et des

[1] Thèse de Ph D de HELA Dahen, HEC Montréal

intervenants. Le risque opérationnel prend donc de plus en plus d'envergure et sa gestion devient une nécessité.

La mise à disposition ou la gestion de moyens de paiement est une activité rigoureuse qui exige la mise en œuvre de moyens de protection fiables, puissants et performants. Leur sécurité est essentielle au maintien de la confiance dans la monnaie. Elle permet aux particuliers d'utiliser les ressources qui parviennent sur leur compte bancaire (salaire, prestations et autres revenus) en émettant des chèques, en effectuant des retraits d'espèces, en réglant par carte bancaire ou en effectuant des virements. Les établissements de crédit doivent assurer une gestion adéquate des risques opérationnels liés à cette activité.

Selon OGIEN (2008 : 465) « Les situations de crise et dysfonctionnements de place sur les moyens de paiement ont participé à l'émergence, puis à la montée en puissance de la notion de risque opérationnel dans le monde bancaire ».

En effet, depuis plusieurs années nous assistons à un certain nombre d'incidents sur les moyens de paiement au sein des établissements de crédit : utilisation des moyens de paiement à des fins de blanchiment, détournement par ordre de virement, falsification de chèque volé ou ramassé, ou fabrication de fausses cartes bancaires etc.

Et pour une banque comme la Banque Atlantique Mali, qui a connu des pertes suite à un certain nombre d'incidents sur les instruments de paiement notamment fraude interne sur les chèques par un agent de la clientèle, prélèvement sur le compte des clients par un agent de la banque qui imitait leurs signatures et faisait des virements à son profit, manipulation frauduleuse des cartes de retrait par certains clients mal intentionnés et bien d'autres[2], adopter une position de gestion des risques opérationnels liés aux moyens de paiement, est d'abord un souci d'efficacité dans la gestion.

Et plusieurs facteurs peuvent nous permettre d'expliquer ces incidents sur les moyens de paiements :

- insuffisance des dispositifs de gestion des risques ;
- faiblesse traditionnelle de la compétence des équipes dédiées aux opérations des moyens de paiements ;

[2] Rapport d'audit 2e trimestre 2010

- évolutions techniques mal maitrisées en interne ;
- défaillance du système informatique.

Les conséquences sont nombreuses pour l'organisation:

- perte financière importante ;
- perte de crédibilité vis-à-vis des clients ;
- difficulté dans la gestion des opérations de moyens de paiement.

Au regard de ces causes, plusieurs pistes de solutions peuvent être envisagées :

- élaboration d'une cartographie des risques opérationnels liés au processus de gestion des moyens de paiement ;
- audit régulier du processus de gestion des moyens de paiement ;
- analyse de la gestion des risques opérationnels liés aux moyens de paiement.

La dernière solution semble être la plus convenable, car cette analyse nous permettra d'apprécier l'efficacité et le niveau de pertinence des dispositifs de gestion des risques opérationnels mis en place dans l'organisation pour assurer la sécurité des moyens de paiement.

La question de recherche à laquelle répondra cette analyse est la suivante : quelle est l'efficacité des dispositifs de gestion des risques liés aux moyens de paiement au sein de la BAM?

Plus précisément :

- quels sont les moyens de paiement ?
- quels sont les risques opérationnels liés aux moyens de paiement?
- quels sont les dispositifs de gestion de risques opérationnels liés aux moyens de paiement?
- Quels dispositifs de contrôle à mettre en place pour une gestion efficace de ces risques opérationnels?

Toutes ces interrogations justifient notre choix du thème « Analyse de la gestion des risques opérationnels liés aux moyens de paiement : Cas de la Banque Atlantique MALI».

L'objectif principal du présent travail est d'apprécier l'efficacité des dispositifs de gestion des risques opérationnels liés aux moyens de paiement.

De cet objectif principal, découlent plusieurs objectifs spécifiques qui sont les suivants :

- prendre connaissance du processus de gestion des moyens de paiement ;
- identifier les risques opérationnels liés au processus de gestion des moyens ;
- apprécier les dispositifs mis en œuvre pour la maitrise des risques opérationnels liés aux moyens de paiement ;
- formuler des recommandations relatives à la maîtrise des risques opérationnels.

Ainsi compte tenu de la volumétrie des opérations sur les moyens de paiement et en raison du temps qui nous est imparti, nous allons nous intéresser aux chèques, aux virements et prélèvements, ainsi qu'aux cartes de paiement en raison de l'importance de leur traitement et du nombre d'incidents survenus sur ces instruments.

L'intérêt du sujet de notre travail de recherche se percevra à 3 niveaux:

Pour la BAM

Au terme de cette étude, la BAM pourrait avoir une idée sur l'efficacité des moyens mis en place pour la gestion des risques opérationnels liés aux moyens de paiement, et ainsi améliorer ces dispositifs en s'appuyant sur les bonnes pratiques en matière de gestion des risques opérationnels.

Pour nous même :

Cette étude nous permettra d'appliquer les connaissances théoriques acquises durant nos deux années de formation, d'appliquer nos connaissances en matière de gestion des risques opérationnels et d'avoir une idée sur la pratique de la gestion des risques opérationnels dans les banques.

Pour le lecteur

A l'endroit du lecteur, nous pensons que ce document pourrait constituer une documentation pertinente sur le sujet traité.

Pour traiter ce thème, nous avons divisé notre travail en deux parties dont la première est consacrée au cadre théorique et la seconde portera sur la pratique :

- le cadre théorique sera basé sur la revue littéraire du thème de notre étude. En effet, le premier chapitre abordera les risques opérationnels liés aux moyens de paiement, le deuxième sera consacré aux dispositifs de maîtrise des risques opérationnels et le troisième chapitre montrera la méthodologie de recherche permettant d'aborder le cadre pratique ;
- le cadre pratique sera axé sur l'aspect pratique de notre travail. Elle sera subdivisée en trois chapitres qui sont respectivement la présentation générale de la BAM, la description des dispositifs de gestion des risques opérationnels liés aux moyens de paiements, et enfin l'analyse de ces dispositifs.

PREMIERE PARTIE : CADRE THEORIQUE

Les risques encourus par les banques constituent un souci majeur pour les autorités monétaires de tous les pays. Soucieux de mettre en place des systèmes bancaires fiables et efficaces pour la collecte des dépôts et le financement de l'économie, les décideurs nationaux ont toujours mis tous les moyens de contrôle envisageables pour limiter les risques liés à l'activité bancaire. L'absence ou l'insuffisance de leur maîtrise provoquera inévitablement des pertes qui affecteront la rentabilité et les fonds propres des banques.

L'identification des risques est une étape importante, car une fois identifiés, il est possible de les mesurer, de mettre en place des mesures destinées à les limiter et de prévoir les fonds propres nécessaires pour faire face aux pertes potentielles. Il est alors indispensable pour les banques de mettre en place les mesures nécessaires pour la maîtrise des risques opérationnels.

Pour mener à bien notre étude, notre cadre théorique sera basé sur les trois chapitres qui sont :

- le chapitre 1 consacré aux risques opérationnels liés aux moyens de paiement ;
- le chapitre 2 axé sur les dispositifs de maitrise des risques opérationnels liés aux moyens de paiement ;
- et le chapitre 3 qui décrit la méthodologie de la recherche.

Chapitre 1: les risques opérationnels liés aux moyens de paiement

Dans ce chapitre, nous allons définir les moyens de paiement, faire leurs descriptions et les risques opérationnels qui y sont liés.

1.1 Les moyens de paiement

La mise à disposition de la clientèle, ou la gestion des moyens de paiement est l'une des trois (3) catégories d'opérations définies par l'article 1 de la loi bancaire[3]. Les deux autres étant la réception de fonds public et les opérations de crédit. C'est une activité qui représente quotidiennement des volumes considérables. Concrètement, pour une banque, ce sont tous les fonds qu'elle décaisse ou encaisse quotidiennement.

1.1.1 Définition des 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, chèques de voyage, cartes de paiement et de retrait, virements ou avis de prélèvement, cartes de crédit et transferts électroniques de fonds.[4]

1.1.2 Les différentes catégories de moyens de paiement

Les principaux moyens de paiement sont : les espèces, les chèques, les effets, les virements, les prélèvements, les cartes de paiement ou de débit.

[3] Loi n°84-46 du 24 janvier 1984 modifiée relative à l'activité et au contrôle des établissements de crédit

[4] Article 7 de la loi portant réglementation bancaire, nouveau texte, UEMOA.

1.1.2.1 Le chèque

1.1.2.1.a Définition

SARDI (2002 : 942), nous définit le chèque « comme un écrit par lequel une personne (le tireur) donne l'ordre à une autre personne (le tiré) de payer une certaine somme à un tiers (le bénéficiaire ou porteur) à concurrence des fonds déposés chez le tiré ».

1.1.2.1.b Descriptif du chèque

Selon le règlement N° 15/2002/CM/UEMOA[5], le chèque doit contenir les éléments suivants :

- la dénomination du 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 (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).

1.1.2.1.c Différentes sortes de chèque mis à la disposition des clients

Comme chèque mise à la disposition des clients, on peut citer le chèque de dépannage, le chèque circulaire, le chèque de guichet, le chèque accréditif, le chèque de voyage, le chèque barré, le chèque de banque, le chèque certifié. Nous allons définir brièvement les trois derniers.

- **Le chèque barré :**

Un chèque est dit barré lorsqu'il est non endossable et payable que dans une banque. (DRAGON & al, 1998 : 98)

[5] Article 48 du règlement N°15/2002/CM/UEMOA portant sur les systèmes de paiement.

- **Le chèque de banque** :

Un chèque de banque est un chèque émis par la banque, tiré sur la caisse centrale de la banque elle-même et qui permettra au client de régler un paiement important. (SIRUGUET, 2001 :470)

- **Le chèque certifié :**

Un chèque est dit certifié si la banque du tireur garantit le paiement du montant tiré. (DRAGON & al, 1998 : 98)

1.1.2.2 Le virement ou transfert

Selon RAMBURE (2008 : 56) « l'ordre de virement (crédit Transfer) émis par le débiteur est adressé à sa banque afin d'effectuer un transfert sur une autre banque ou sur un autre compte de la même banque ».

Nous avons deux types de virement :

- le virement « de compte à compte », lorsque les comptes du donneur d'ordre et du bénéficiaire sont ouverts dans les livres de la même banque ;
- le virement « interbancaire », lorsque le donneur d'ordre demande à la banque un transfert de fonds vers une autre banque de la place. A ce niveau, la banque peut émettre des virements mais elle peut aussi en recevoir.

1.1.2.3 Le prélèvement

SIRUGUET (2001 : 437), « l'avis de prélèvement est un moyen de paiement automatisé, adapté aux règlements répétitifs, dispensant le débiteur de l'envoi d'un titre de paiement lors de chaque règlement ».

1.1.2.4 La carte bancaire

1.1.2.4.a Définition

SARDI (2002 : 945), « une carte de paiement est émise par un établissement de crédit et permet à son titulaire (le porteur) d'effectuer ses règlements au moyen de celle-ci (ce qui

équivaut à un transfert de fonds) ou de retirer des espèces dans les distributeurs automatiques de billets (DAB) ».

1.1.2.4.b Descriptif de la carte bancaire

La carte bancaire est un plastique dont le format et l'emplacement des mentions et composants sont normalises par l'international organization for standardization (ISO). Il comporte notamment :

- le numéro de la carte, le nom du porteur, la date limite de validité en relief (embossage) et sa signature ;
- le logo de l'émetteur, du réseau, et de la catégorie de carte ;
- les pistes magnétiques (pour lecteurs anciens) contenant l'identifiant et les fonctions autorisées ;
- le microprocesseur (pour lecteurs de « puces » en France par exemple) contenant, en plus des informations de la piste, les clés et moyens de contrôle d'accès aux fonctions ;
- un ou plusieurs éléments de sécurité (hologramme par exemple) ;
- un extrait des textes réglementaires et l'indication des moyens de prévenir en cas de difficultés. (DRAGON & al, 1998 : 150 ; DRAGON & al, 2002 : 111).

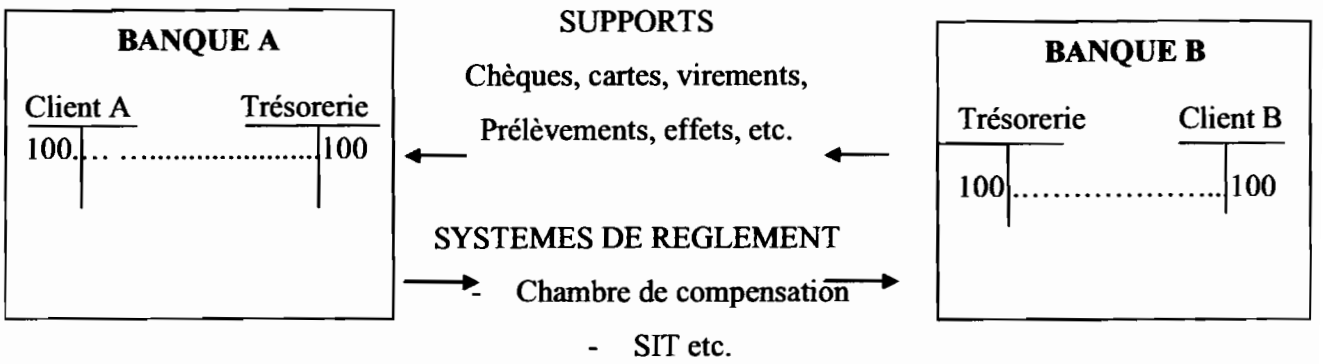
1.1.3 Mécanisme d'un paiement

La problématique d'un paiement est simple dans son principe : il s'agit pour A de transférer au profit de B un montant déterminé. Il peut être illustré par le schéma ci-après.

Le transfert de fonds de la banque de A vers la banque de B pourra se faire par des supports variés – chèque, effet, virement, prélèvement – qui seront encaissés via des systèmes de règlement variés : la chambre de compensation, le système interbancaire de télécompensation, etc.

A noter que A et B peuvent être client d'un même établissement. Dans ce cas, l'opération se traduira pour l'établissement par le débit du compte du client A et le crédit de celui de B.

Figure 1 : Mécanisme d'un paiement



Source : SARDI (2002 : 934).

1.1.4 Le traitement des moyens de paiement

Le traitement des moyens de paiement est complexe, car il fait intervenir plusieurs acteurs. Nous allons décrire brièvement leur traitement.

1.1.4.1 Les principes de traitement des moyens de paiement

Pour SIRUGUET (2001 :438), « l'objectif du traitement des moyens de paiement est de débiter le compte du payeur et créditer le compte du bénéficiaire.

Les moyens de paiements sont émis :

- par un tiers, client ou non de la banque ;
- ou par la banque elle-même.

Ils sont émis au bénéfice :

- d'un tiers, client ou non de la banque ;
- ou de la banque elle-même.

Ils s'échangent :

- à l'intérieur de la banque elle-même ;
- ou entre les banques.

Ils mettent en relation :

- le payeur et son banquier ;
- le payé et son banquier ».

1.1.4.2 Les phases de traitement des moyens de paiement

Pour SIRUGUET (2001 : 439), « Le traitement des opérations « moyens de paiements » comprend généralement 4 phases »

1.1.4.2.a La phase « Aller »

La phase Aller correspond à la réception des moyens de paiements, leur enregistrement en comptabilité générale ou auxiliaire, le traitement approprié de ces moyens de paiement et des données correspondantes, leur envoi aux circuits d'échanges adéquats. Elle comprend les étapes suivantes :

- la banque reçoit du remettant le moyen de paiement ;
- la banque impute le compte du remettant du montant correspondant au moyen de paiement ;
- la banque envoie le moyen de paiement à l'autre banque concernée.

1.1.4.2.b La phase « compensation »

C'est la phase ou les différents remettants se retrouvent et compensent leurs remises et en assurent les règlements suivants.

Il faut noter qu'avec le développement actuel des systèmes de paiement, l'échange des moyens de paiement se fait via des systèmes interbancaires automatisés. Nous avons deux types de systèmes de paiement dans la zone UEMOA, qui sont le système interbancaire de compensation automatisée (SICA), le système de transfert automatisé et de règlement (STAR).

1.1.4.2.c La phase « Retour »

La phase « Retour » qui correspond au traitement des opérations reçues directement des circuits d'échange et leur imputation, les rapprochements des données issues des traitements

avec les totaux de contrôle, ainsi que le traitement des éléments en suspens, rejetés ou retournés. Cette phase comprend les étapes suivantes :

- la banque reçoit du circuit d'échange le moyen de paiement ;
- la banque impute du montant correspondant le compte du client final ou rejette l'opération.

1.1.4.2.d La phase de traitement des rejets et impayés

Eventuellement sont à opérer le traitement des impayés ainsi que les différentes déclarations aux fichiers des incidences pour les opérations liées aux chèques impayés et l'envoi des lettres réglementaires aux clients émetteurs de chèques impayés.

1.1.5 Le droit lié aux instruments de paiement dans l'UEMOA

Dans la zone UEMOA, nous avons le règlement N° 15/2002/CM/UEMOA du 19 Septembre 2002 qui vise la mise en place d'un dispositif juridique relatif aux systèmes de paiement dans les Etats membres de l'UEMOA. Ce règlement prend en compte tous les instruments de paiement notamment les chèques, les effets, les virements, les prélèvements, les cartes de paiement ou de débit, et la porte monnaie électronique.

1.2 Les risques opérationnels liés aux moyens de paiement

Cette section traite du risque opérationnel en général, et des risques opérationnels liés aux moyens de paiements.

1.2.1 Définition du risque opérationnel

La définition des risques opérationnels ne fait pas l'objet d'un consensus. Elle diffère d'un organisme à un autre.

Selon Nicolet (2000 : 44), « la notion de risque opérationnel diffère dans les réglementations nationales et internationales. Un moyen de mieux la cerner serait de la définir par un couple de facteurs /conséquences ». Nicolet poursuit en affirmant que les risques les plus connus sont les risques de fraude, de détournement d'actifs et d'informations financières non fiables.

Cette définition est complétée par celle de Jacob & al (2001 : 32) qui dit que ce sont les pertes occasionnées par la gestion de l'entreprise et non reliées directement au risque de marché ou de crédit. Cette vague définition fait allusion aux risques non couverts par ailleurs.

Le règlement du Comité de Réglementation Bancaire Française (CRBF 97-02) le définit comme étant le risque résultant d'insuffisances de conception, d'organisation et de mise en ouvre des procédures d'enregistrement dans le système comptable et plus généralement dans les systèmes d'information de l'ensemble des évènements relatifs aux opérations de l'établissement.

Le comité de Bâle 2 le définit comme étant le risque de perte résultant d'une inadéquation ou d'une défaillance imputable à des procédures, personnels et systèmes internes, ou à des évènements extérieurs, y compris les évènements de faible probabilité d'occurrence, mais à risque de perte élevée.

Cette définition prend en compte les risques juridiques, et on part des effets quantifiables (perte directe) pour remonter aux causes (évènements de risques). La perte constatée (effet) permet de remonter à l'événement qui lui-même permet de remonter à une ou plusieurs causes (inadaptation des procédures, évènement extérieur, défaillance humaine, etc.).

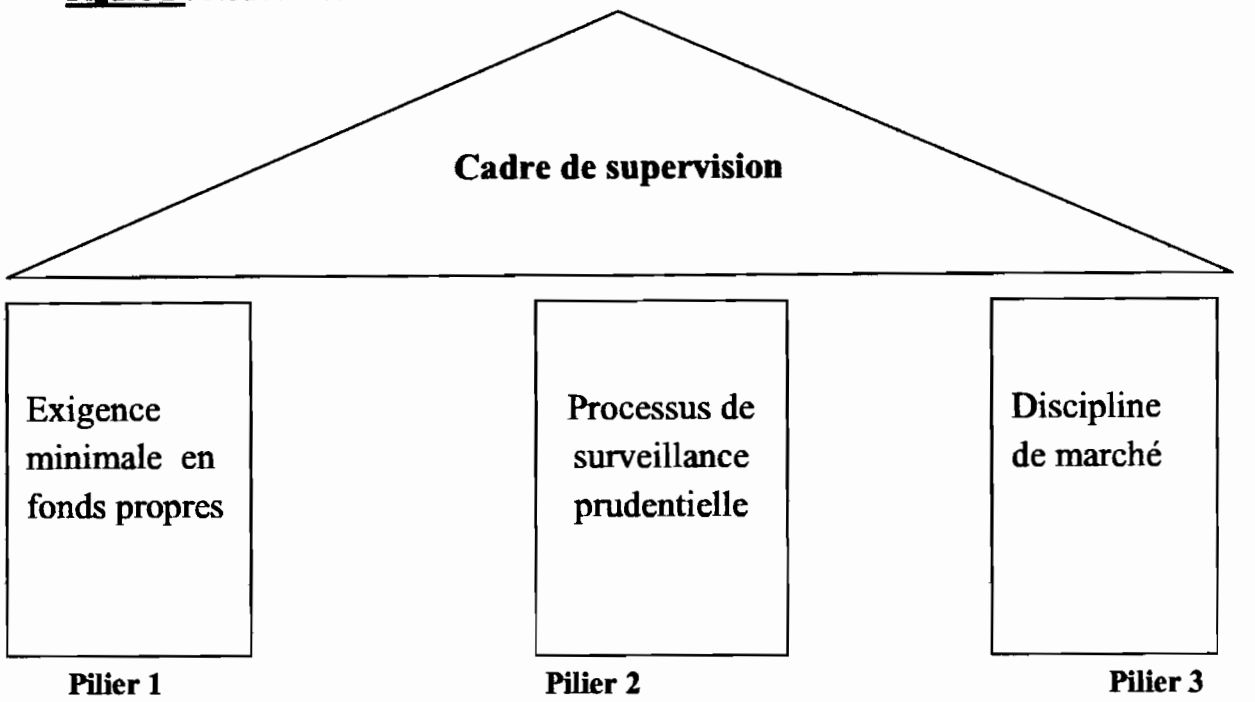
A travers toutes ces définitions, nous pouvons identifier 2 catégories de sources de risques :

- la source interne : le risque opérationnel peut être issu des procédures, du personnel, et/ou des systèmes internes ;
- la source externe à l'entreprise : certains évènements extérieurs tels que les catastrophes naturelles, les lois et réglementations, etc.

1.2.2 Risque opérationnel et Bâle 2

Le nouvel accord sur l'adéquation du capital défini par le comité de Bâle sur la supervision bancaire, a pour principal objectif de s'assurer que les banques disposent de capital minimum pour couvrir les risques. Les dernières révisions incorporent les risques opérationnels dans le calcul de l'exigence des fonds propres. Le nouvel accord repose sur un socle constitué de trois piliers qui y jouent un rôle important.

Figure 2 : Nouvel accord de Bâle 2



Source : DOV (2008 : 406)

- **Pilier 1 :**

Il a pour objectif d'évaluer les risques portés par un établissement et de déterminer les fonds propres minimaux nécessaires à la couverture de ces risques. Il s'agit ici du capital minimum requis par les autorités de régulation de la profession. Plusieurs approches ont été définies par le comité, notamment « l'approche des indicateurs de base », « l'approche standard » et l'approche des mesures avancées ».

- **Pilier 2**

Il a pour objet de renforcer la surveillance prudentielle par les superviseurs nationaux. Il est demandé aux banques de disposer de procédures d'évaluation de leurs fonds propres conformes aux risques portés et d'une stratégie pour le maintien de ces fonds propres. Les superviseurs nationaux doivent évaluer ces procédures et prendre des mesures si elles ne sont pas satisfaisantes. Le superviseur pourra notamment imposer, au cas par cas, des exigences de solvabilité supérieures au minimum réglementaire.

- **Pilier 3**

Il met l'accent sur l'utilisation de la communication financière pour améliorer la discipline de marché (principe de transparence). Il décrit l'ensemble des documents que les banques doivent rendre publics afin de se conformer à la réglementation. Ces documents concernent principalement le calcul des fonds propres et l'exposition aux risques de l'établissement bancaire. Les banques doivent donc diffuser :

- la charge de capital par ligne métier ;
- la description de l'approche utilisée pour déterminer la charge de capital à appliquer par ligne de métier ;
- des informations détaillées sur les procédures utilisées pour gérer et contrôler leur risque opérationnel (y compris l'organisation de leur fonction de gestion de risque et la politique utilisée pour se couvrir contre les risques et éventuellement les réduire).

1.2.3 Typologie des risques de Bâle

Le régulateur a choisi une répartition selon 7 grandes catégories de risques opérationnels :

1.2.3.1 Fraude interne

Pertes liées à des actes commis à l'intérieur de l'entreprise visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou réglementaire, ou à des règles de l'entreprise, à l'exclusion des cas de pratiques discriminatoires ou contraire aux règles en matière d'égalité professionnelle, et imputant au moins un membre de l'entreprise.

1.2.3.2 Fraude externe

Pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif ou à enfreindre une disposition législative ou réglementaire.

1.2.3.3 Insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail

Pertes liées à des actes contraires aux dispositions législatives ou réglementaires, ou aux conventions en matière d'emploi, de santé ou de sécurité, à la réparation de préjudices personnels ou à des pratiques discriminatoires ou contraires aux règles en matière d'égalité professionnelle.

1.2.3.4 Clients, produits et pratiques commerciales

Pertes liées à un manquement délibéré ou non, à une obligation professionnelle envers un client (y compris les exigences en matière de confiance et d'adéquation du service), à la nature ou aux caractéristiques d'un produit.

1.2.3.5 Dommages aux actifs physiques

Pertes liées à la perte ou à l'endommagement d'actifs physiques résultant d'une catastrophe naturelle ou d'autres évènements.

1.2.3.6 Interruption d'activité et dysfonctionnement des systèmes

Pertes liées à des pannes de matériel et de logiciel informatiques, les problèmes de télécommunication, les pannes d'électricité.

1.2.3.7 Dysfonctionnement des processus de traitement (exécution, passation d'ordre, livraison, gestion des processus)

Pertes liées aux lacunes du traitement des transactions ou de la gestion des processus et aux relations avec les contreparties commerciales et les fournisseurs.

1.2.4 Typologie de risques opérationnels liés aux moyens de paiements

Les principaux risques associés aux moyens de paiement sont les suivants.

1.2.4.1 Le risque de fraude interne

Pertes liées à des détournements internes : plus difficiles à identifier, dans la mesure où ils peuvent être opérés dans un environnement parfois instable (DOV, 2008 : 464).

1.2.4.2 Le risque de fraude externe

Pertes liées à des actes de tiers visant à commettre une fraude ou un détournement d'actif (falsification de chèque par exemple), JIMENEZ & al (2008 : 70).

1.2.4.3 Le risque comptable

Difficulté de justifier la masse des paiements entièrement automatisés donc risque de perdre la piste d'audit (SARDI, 2002 : 951).

1.2.4.4 Le risque administratif

Les risques d'ordre administratif relèvent :

- des opérations effectuées avec retard (respect des délais de rejet, remise tardive en compensation, etc.) ;
- des acceptations de paiement sans autorisations, SIRUGUET (2001 : 491).

1.2.4.5 Le risque informatique

Le système de traitement des moyens de paiement est dans la plupart des cas totalement intégré, ce qui engendre des risques spécifiques, notamment liés au niveau de sécurité informatique (SIRUGUET, 2001 : 491).

1.2.4.6 Le risque de blanchiment

L'utilisation des moyens de paiements à des fins de blanchiments. Les banques peuvent s'exposer à des pertes directes dues à la fraude, en acceptant des clients indésirables et par la compromission de certains employés avec des criminels (SARDI, 2002 : 42).

Tableau 1 : Tableau récapitulatif des risques opérationnels liés aux moyens de paiement

Sous-activités	Taches	Risques opérationnels	Dispositifs de maîtrise
Gestion des chèques	-Réception du chèque -Imputation au compte du remettant ou au compte interne -Tri et envoi du chèque à la compensation -Réception des moyens de paiement de paiement du circuit d'échange -Règlement au /du circuit d'échange	-non traitement de la réception ou perte de la valeur reçue -non vérification de la validité de la réception -non enregistrement -erreur d'enregistrement (montant, date, compte) -erreur sur la nature du moyen de paiement -enregistrement fictif	-Vérifier que tous les chèques reçus remplissent les conditions générales de validité ; -Vérifier la conformité du chèque et le correct remplissage du bordereau de remise ; -Vérifier la provision existante sur le compte du client ; -Vérifier que tous les chèques reçus sont bien imputés aux comptes des clients ; -Vérifier que tous les chèques remis à la compensation sont bien réglés, et ce en tenant compte des jours de valeurs.

Gestion des virements et prélèvements	-Réception de l'ordre de virement -Réception d'un avis de prélèvement -Réception d'une opération sur compte client -Envoi de l'ordre de virement ou de prélèvement à la compensation -Réception des moyens de paiement de paiement du circuit d'échange -Règlement au /du circuit d'échange	-Erreur sur les caractéristiques de l'opération ; -Avis de prélèvement sans autorisation -compte clos, sans provision en opposition, etc. -Rejet de l'ordre de virement -Paiements non autorisés - Insuffisance de provision ou non respect de la limite autorisée	-Vérifier que le formulaire d'ordre de virement ou d'avis de prélèvement est bien renseigné - Vérifier que le virement ou l'avis de prélèvement est autorisé par une personne habilitée - Rapprochements des ordres de virements ou prélèvements et des virements existants dans le système
Gestion des cartes	Carte de paiement	-Fraude -Usage abusif -Perte financière -Fraude -perte de crédibilité vis-à-vis du client	-Le code secret de la carte et l'avis de mise à disposition doit être adressés directement au client, sans transiter par l'établissement. -Les cartes reçues du centre de traitement, et tenues à la disposition des clients, doivent faire l'objet de précautions strictes. -Les cartes perdues ou volées, déclarées par les clients doivent être rapidement signalées à l'émetteur pour lui permettre de faire opposition, et dégager ainsi la responsabilité du client et de l'établissement contre d'éventuels usages abusifs. -Les commissions doivent être intégralement perçues à bonne date. -Les codes secrets et les cartes doivent être remis séparément au client.

Source : nous-même à partir de SARDI (2002 : 950-959) ; DOV (2008 : 463-472), SIRUGUET (2001: 449-451).

La gestion des moyens de paiement est une activité très importante de la banque. Leur sécurité est essentielle au maintien de la confiance dans la monnaie. Les établissements de crédit doivent alors assurer une gestion adéquate des risques opérationnels liés à cette activité. Ce chapitre nous a permis non seulement de comprendre le processus de gestion des moyens de paiement, mais aussi de voir les risques opérationnels qui y sont attachés et les dispositifs de maîtrise des dits risques.

Chapitre 2 : La gestion des risques opérationnels liés aux moyens de paiement

La gestion des risques opérationnels est le processus par lequel les risques opérationnels sont évalués en utilisant une approche systématique qui les identifie et les organise par priorité, et qui ensuite met en place les stratégies pour les atténuer. Cette approche comprend à la fois la prévention des problèmes potentiels et la détection au plus tôt des problèmes actuels. C'est un processus itératif qui demande la participation du personnel à tous les niveaux de l'organisation.

L'identification des risques est une étape importante, car une fois identifiés, il est possible de les mesurer, de mettre en place des mesures destinées à les limiter et de prévoir les fonds propres nécessaires pour faire face aux pertes potentielles. Il est alors indispensable pour les banques de mettre en place les mesures nécessaires pour la maîtrise des risques opérationnels.

La conséquence principale des risques est de provoquer une perte significative pour la banque, soit au travers d'un ralentissement, soit par une augmentation des charges (LAMARQUE 2008 :77).

2.1 La politique de gestion des risques opérationnels

Actuellement le problème majeur qui se pose aux dirigeants est l'identification des risques opérationnels pouvant ainsi nuire à l'atteinte de leurs objectifs et d'en apprécier leurs incidences en vue de mettre en place les mesures adéquates pour leur maîtrise. Cela suppose la mise en place d'une politique de gestion des risques opérationnels adéquate, des processus et des procédures adaptés.

La gestion des risques est le processus par lequel les risques sont évalués en utilisant une approche systématique qui identifie et organise par priorité les risques, et qui ensuite met en place les stratégies pour atténuer les risques. Cette approche comprend à la fois la prévention des problèmes potentiels et la détection au plus tôt des problèmes actuels. C'est un processus itératif qui demande la participation du personnel à tous les niveaux de l'organisation.

Selon Jimenez & al (2008 : 113), les objectifs poursuivis par la politique de gestion des risques opérationnels sont au nombre de quatre :

- sécuriser les résultats en assurant une bonne maîtrise des risques opérationnels ;
- se doter de dispositifs et d'outils permettant de mieux gérer leurs activités ;
- optimiser l'allocation des fonds propres par l'amélioration en continu des processus de gestion des risques opérationnels ;
- répondre aux exigences réglementaires.

Il enrichit en donnant les principaux fondements de la politique suivie qui sont les suivants :

- être en mesure de détecter le plus tôt possible les risques ou les incidents ;
- analyser les risques et les incidents ;
- alerter et mobiliser les principaux responsables concernés par lesdits incidents ;
- mesurer les effets de cette politique et disposer d'outils et d'indicateurs de pilotage à destination de la direction générale, des directions de métiers et des différents acteurs du dispositif.

2.1.1 Les acteurs et organes de pilotage du dispositif

Plusieurs acteurs interviennent dans le pilotage du dispositif

2.1.1.1 La direction générale

Selon SARDI (2002 : 312), L'organe délibérant doit être conscient que le risque opérationnel est une catégorie de risque à part entière, distincte et contrôlable. Il doit approuver et revoir périodiquement la stratégie de la banque dans ce domaine. Il doit également approuver la structure dédiée à la gestion de ce risque et s'assurer que l'organe exécutif assume ses responsabilités dans ce domaine.

Jimenez & al (2008 : 114) nous donnent le rôle de la direction générale dans la mise en place de la politique de gestion des risques opérationnels. Elle nomme un responsable risques opérationnels et anime les principaux comités de suivi et de contrôle des risques opérationnels afin :

- de piloter le dispositif ;
- d'adapter la politique du groupe, eu égard à son activité et son organisation, en définissant, en particulier, les objectifs en matière de réduction des risques ;
- de suivre les plans d'action issus des cartographies, des fiches d'incidents et des reportings.

2.1.1.2 Le comité des risques opérationnels

Le comité des risques opérationnels de l'établissement doit se tenir sur une fréquence minimale semestrielle. Il s'appuie sur un tableau de bord risques opérationnels spécifique.

Il doit traiter en particulier :

- les risques majeurs de l'établissement ;
- l'environnement de gestion des risques opérationnels ;
- les indicateurs de risques spécifiques ;
- les incidents avérés -incidents notables et grandes tendances sur la période considérée ;
- les dispositifs assurances existants permettant de couvrir des risques opérationnels.

En outre, le comité des risques opérationnels dispose de prérogatives internes lui permettant :

- de faire évoluer les dispositifs de suivi, de surveillance et de contrôle des risques opérationnels ;
- de décider l'engagement de plans d'actions ;
- de réduire certaines expositions aux risques opérationnels en fixant ou proposant des normes de gestion et des limites (Jimenez & al, 2008 : 114).

2.1.1.3 Les responsables risques opérationnels

Selon Jimenez & al (2008 : 115), l'organe exécutant a la responsabilité de mettre en œuvre la stratégie approuvée par l'organe délibérant. Il a aussi la responsabilité de développer les processus et les procédures pour gérer ce risque dans toutes les activités de la banque.

Le responsable risques opérationnels est rattaché au directeur des risques. Il est en charge :

- de piloter le dispositif « cartographie », « base d'incidents », « plans d'actions », « reporting » au sein de son périmètre ;
- d'assurer le déploiement, auprès des utilisateurs, des méthodologies et outils de l'entité ;
- de garantir l'intégrité des données produites tant en matières de qualité de l'information renseignée qu'en matière d'exhaustivité ;
- d'alerter la direction des risques pour tout incident avéré ou potentiel significatif et/ou dont l'impact pourrait être supérieur à un seuil pour les incidents (montant défini et validé annuellement par le comité des risques opérationnels) ; un seuil brut pour les risques (montant défini et validé annuellement par le comité des risques opérationnels, proportionnel à la capacité bénéficiaire de l'entreprise) ; d'effectuer une revue périodique des bases d'incidents, de la résolution des incidents, de l'état d'avancement des plans d'actions ; de documenter le dispositif de gestion (procédures, contrôles ...).

2.2 Dispositifs de maîtrise des risques opérationnels liés au processus de moyens de paiement

Le dispositif de gestion des risques opérationnels nous permet d'avoir une bonne compréhension de ces risques, un dispositif de détection, de contrôle et de suivi des activités de la banque.

2.2.1 Objectif du dispositif de maitrise des risques opérationnels

Jimenez (2008 :127), la finalité d'un dispositif de maîtrise des risques opérationnels est de pouvoir agir sur les différents éléments identifiés et quantifiés afin de modifier le profil de risques de la banque ou tout du moins sa sensibilité en cas de survenance d'évènements non souhaités.

2.2.2 La prise de connaissance du processus de gestion des moyens de paiement

L'objectif de la prise de connaissance est d'identifier les principales procédures et d'apprécier la fiabilité d'ensemble du contrôle interne (Dov, 2008 : 445).

Renard (2008 : 224), il n'y a pas de méthodes d'audit qui ne commence pas par la prise de connaissance des processus ou des activités que l'on doit auditer. Sans connaitre nécessairement le « métier » de celui qu'il a à auditer, l'auditeur doit au moins en avoir la culture pour être en mesure de comprendre les explications qu'il va chercher et solliciter et, plus généralement pour se faire admettre aisément.

2.2.3 Identification, évaluation et suivi des risques opérationnels à la gestion des moyens

Ici, il s'agit d'identifier, d'évaluer et de faire un suivi des évènements internes et externes susceptibles d'affecter l'atteinte des objectifs de gestion des moyens de paiement.

2.2.3.1 Identification des risques opérationnels liés aux moyens de paiement

Les risques opérationnels sont inhérents à tous les types d'activités, de produits, processus et systèmes doivent être identifiés. Une identification efficace doit comprendre les facteurs internes. L'identification des risques nous permettra d'évaluer l'impact des risques opérationnels. Elle passe nécessairement par une description précise du processus. Le processus d'identification des risques devrait également comprendre la détermination des risques qui sont contrôlables par la banque et ceux qui ne le sont pas. Il n'existe pas méthodes d'identification plus fiables que d'autres ; l'essentiel pour Coopers &al (2000 :60), est que les dirigeants tiennent compte de certains facteurs qui peuvent contribuer à l'apparition d'un risque, voire à son aggravation. Ces facteurs peuvent être :

- la non réalisation d'un objectif par le passé ;
- l'importance de l'activité dans l'organisation ;
- la complexité d'une activité ;
- le niveau de compétence du personnel, etc.

Ils existent plusieurs techniques d'identification des risques.

- **Identification basée sur des actifs créateurs de valeurs**

Selon Mc Namee (1996 : 13), elle consiste à déterminer les actifs constitutifs de valeur de l'organisation et à mettre en évidence les risques qui pèsent sur ces éléments de valeur. La valeur de l'entreprise se trouve souvent sous forme d'actifs intangibles et l'identification des risques nécessite des connaissances et des réflexions approfondies dans ce domaine.

- **Identification basée sur l'atteinte des objectifs**

Très souvent, le risque est défini comme un évènement qui empêche l'atteinte des objectifs de l'organisation. Ainsi, suivant cette approche, selon Bapst (2003: 3), on identifie d'abord les objectifs de l'activité ou de l'organisation, pour ensuite leur adjoindre les menaces qui pèsent sur eux. L'efficacité de cette approche repose sur une identification claire et partagée des objectifs en amont. Quant à sa réussite, elle est fonction d'un langage commun, partagé par les acteurs pour ce qui est des objectifs poursuivis par l'organisation.

- **Identification basée sur les check-lists**

Cette méthode vient en complément des deux précédentes et permet de passer rapidement en revue les risques classiques d'un domaine ou d'un processus (Maders & al, 2006: 50).

- **Identification basée sur l'analyse de l'environnement**

Selon McNamee (1998: 13), L'identification basée sur l'analyse de l'environnement est une technique qui permet de déterminer les risques en fonction des variations que peut subir l'environnement dans lequel se trouve l'organisation. La difficulté dans l'application de cette méthode réside dans le fait que les événements provenant de l'environnement sont toujours difficiles à cerner.

- **Identification par analyse historique+**

Cette approche consiste à identifier les risques opérationnels en se basant sur ceux déjà survenus au sein de l'organisation. L'inconvénient, avec cette méthode, est que les risques peuvent varier avec les variations au plan interne et externe de l'organisation.

- **Identification par tâches élémentaires**

Selon Renard (2006: 220-221), cette approche est basée sur le découpage de la fonction, de l'activité ou du processus en tâches élémentaires. A chaque tâche seront associés les risques essentiels lorsque celle-ci est non ou mal exécutée. Cette méthode est souvent utilisée dans les missions d'audit interne.

- **Identification basée sur les scénarios**

Pour Bernard & al (2006: 75-76), cette approche consiste à décrire d'abord chacune des tâches qui composent l'activité et ensuite imaginer collectivement les menaces qui vont permettre de détecter les risques pèsent sur ces tâches.

En définitive, pour une meilleure appréciation des risques encourus par l'organisation, une utilisation complémentaire ou combinée de deux ou plusieurs de ces méthodes serait souhaitable.

2.2.3.2 Evaluation des risques opérationnels liés au processus de moyens de paiement

Pour évaluer le risque opérationnel, il est nécessaire d'estimer la probabilité d'un évènement de perte et la sévérité de la perte. Il est alors essentiel de se doter d'un système de collecte d'informations sur ces deux paramètres pour constituer un historique de données exhaustif et intègre. Le nouveau ratio de solvabilité propose plusieurs approches pour mesurer l'exigence de fonds propres au titre du risque opérationnel. Trois approches sont retenues pour le calcul de l'exigence de fonds propres au titre du risque opérationnel : l'approche de base, l'approche standard et l'approche mesure avancée.

2.2.3.3 Suivi des risques opérationnels liés au processus de moyens de paiement

Un système de suivi de l'exposition au risque opérationnel et des évènements de pertes par grands secteurs d'activité doit être mise en œuvre sur une base continue. Le suivi est plus efficace lorsque le système de contrôle interne est inclus dans les procédures et produit des rapports réguliers qui sont intégrés dans le système de reporting destiné aux organes dirigeants (SARDI, 2002 : 315).

Ce suivi sera plus efficace si la banque élaborait au préalable une cartographie des risques qui permettra d'identifier les risques pour mieux les aborder et gérer.

Cette cartographie des risques consiste donc à associer aux processus modélisés les évènements de risques qui peuvent entrainer une perte en donnant pour chaque couple ainsi recensé une vision des impacts possibles et le degré de maîtrise estimé. Elle n'est toutefois qu'une photographie des risques à un instant donné.

Les étapes de la démarche de cartographie sont les suivantes :

- définir les couples processus/ risque à évaluer ;
- identifier et évaluer les risques nets (prises en compte de l'existant) ;
- apprécier le dispositif de maîtrise des risques ;
- assurer un contrôle de cohérence avec les risques bruts ;
- classifier et hiérarchiser les risques selon les différents angles d'analyse possibles (risque net, risque brut, impact image ...), Jimenez &al (2008 : 65).

2.2.4 Dispositif de maîtrise des risques opérationnels liés au processus de moyens de paiement

Le dispositif de maîtrise des risques à la gestion des moyens de paiement est :

- un processus permanent qui irrigue toute la banque ;

- mis en œuvre par les acteurs du processus de gestion des moyens de paiement, à tous les niveaux de la banque ;
- mis en œuvre à chaque niveau du processus afin d'obtenir une vision globale d'exposition aux risques ;
- pris en compte dans l'élaboration de la stratégie du processus ;
- donné par la Direction et le Conseil d'Administration pour une assurance raisonnable à la réalisation des objectifs des différents acteurs du processus ;
- destiné à identifier les évènements potentiels d'affecter les objectifs du processus de gestion des moyens de paiement et à gérer les risques qui y sont attachés.

2.2.4.1 Le dispositif de maitrise des risques opérationnels liés au processus de moyens de paiement

Il est composé de l'ensemble des systèmes de contrôle mis en œuvre par les responsables de la banque à tous les niveaux pour une bonne maîtrise des risques opérationnels.

2.2.4.2 Les composantes du dispositif de maîtrise des risques opérationnels liés aux moyens de paiement

Pour le Pricewaterhousecoopers (2005 : 32-33), le dispositif de contrôle des risques opérationnels comprend huit éléments qui résultent de la façon dont l'organisation est gérée et s'intègrent au processus de management :

- l'environnement interne ;
- la fixation des objectifs des évènements ;
- l'identification des risques ;
- l'évaluation des risques ;
- le traitement des risques ;

- les activités de contrôles ;
- l'information et la communication ;
- le pilotage.

2.3 Le contrôle interne du processus de gestion des moyens de paiement

Le contrôle interne concerne la banque dans toutes ses activités. Il s'applique aux biens, aux individus, et aux informations, quelles que soient les circonstances ou l'époque de l'année. Toutefois, on ne peut contrôler que ce qui est organisé. L'ensemble des activités de la banque doit, au préalable, être structuré : définition des niveaux de contrôle, organisation rigoureuse de la fonction (BERTIN, 2007 : 96).

Le COSO définit le contrôle interne dans son référentiel intitulé « *internal control –Integrated Framework* » comme un « processus mise en place par le conseil d'administration, les dirigeants et le personnel de l'entité, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité aux lois et aux réglementations en vigueur ;
- la sécurité des actifs» (Renard, 2006 :123)

Pour SIRUGUET (2001 : 460-462), les fondamentaux du contrôle interne sont les suivants :

- définition des habilitations, délégations, autorisations ;
- limitation des accès ;
- surveillance des conditions de conservation ;
- contrôle de la sécurité des actifs ;
- manuels de procédures ;
- réalité des informations ;
- séparation des fonctions.

Le dispositif du contrôle interne permet de ramener le risque inhérent en risque résiduel, il consiste à diminuer la probabilité de survenance et l'impact du risque. Cependant, le dispositif de contrôle interne ne peut empêcher à lui seul que des personnes de l'institution commettent une fraude, contreviennent aux dispositions légales ou réglementaires, ou communiquent à l'extérieur de la société des informations trompeuses sur sa situation. Il est l'affaire de tous les membres de l'institution de déceler, de prévenir les risques, de réduire les conséquences et d'améliorer les performances.

2.3.1 Objectifs du contrôle interne du processus de moyens de paiement

Selon SARDI (2002 : 952-960), les objectifs du système de contrôle interne des risques opérationnels liés aux moyens de paiement sont les suivants :

- l'endossement immédiat des valeurs reçues ;
- des procédures permettant le traitement exhaustif des valeurs ;
- la protection des valeurs ;
- la célérité et la rigueur dans le recouvrement des valeurs ;
- l'application des dates de valeur permettant d'optimiser la rentabilité des opérations ;
- la séparation des tâches ;
- la sécurité et l'efficacité du système informatique ;
- l'autorisation préalable des décaissements ;
- un système d'information de gestion performant.

2.3.2 Evaluation du dispositif de gestion des risques opérationnels liés aux moyens de paiement

L'évaluation du dispositif de contrôle interne nous permettra de déceler les points forts et les points faibles du système de contrôle interne existant. Evaluer d'une manière efficace un dispositif de contrôle interne revient à adopter une démarche bien structuré et dont la finalité est d'offrir une appréciation synthétique du dit dispositif à la direction générale.

2.3.2.1 Les objectifs de l'évaluation du dispositif de contrôle interne des risques opérationnels

Le contrôle interne est une composante essentielle de la gestion des activités d'une banque et constitue le pilier d'un fonctionnement sur et prudent de l'organisation bancaire. Pour mieux répondre aux objectifs du contrôle interne, les différents acteurs de la banque doivent appliquer et surveiller l'ensemble des mesures prises pour assurer une gestion efficace des différentes opérations mises sous leur responsabilité. Dans la norme 2120.A1, les normes professionnelles définissent les aspects sur lesquels doit porter l'évaluation du contrôle interne qui sont donc :

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité aux lois et réglementations en vigueur ;
- la sécurité des actifs.

En mettant en place un système de contrôle interne rigoureux, la banque pourrait espérer atteindre ses objectifs de performance, de rentabilité et de pérennité et mieux maîtriser les risques opérationnels qui sont liés à ses activités.

2.3.2.2 Les étapes d'évaluation du contrôle interne des risques opérationnels liés au processus des moyens de paiement

Pour OGIEN (2008 :466-467), le contrôle interne doit être approché par processus (et dont de manière transverse sur les différents services), son analyse devant porter en priorité sur ceux qui sont susceptibles de soulever les difficultés. L'identification des dysfonctionnements peut être réalisée à l'aide de la revue du niveau des suspens comptables, des réclamations de la clientèle ou en s'appuyant sur les travaux réalisés par les différents corps de contrôle (audit interne, inspection).

La revue s'opère ensuite selon quatre axes d'analyse :

- la sécurité et l'efficience des systèmes d'information, en s'appuyant sur la revue des cartographies applicatives ;
- le niveau des procédures opérationnelles et leur application effective dans les back-offices et les centres de techniques;

- la compréhension détaillée des schémas comptables ;
- l'analyse du contrôle comptable.

2.4 Les 10 principes de bonne pratique en matière de gestion des risques opérationnels[6]

Le régulateur a développé dix principes de bonnes pratiques nécessaires à la maîtrise des risques opérationnels, rappelant par là l'importance tant de l'implication de l'organe exécutif dans la mise place d'un tel système, que de l'identification des risques opérationnels, notamment au travers d'une cartographie de ces derniers.

Élaboration d'un environnement adéquat pour la gestion du risque opérationnel

- **Principe 1**

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

- **Principe 2**

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

[6] Adapté du "Sound practices for the management and supervision of operational risk" du "Basel Committee on Banking Supervision" (2001: 3-5)

- **Principe 3**

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

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

- **Principe 4**

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

- **Principe 5**

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

- **Principe 6**

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

- **Principe 7**

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

Rôle des superviseurs

- **Principe 8**

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

- **Principe 9**

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

Rôle de la communication financière

- **Principe 10**

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

A travers ce chapitre, nous avons abordé les dispositifs de maîtrise des risques opérationnels liés aux moyens de paiement ainsi que les dix principes de bonnes pratiques en matière de gestion des dits risques. Nous allons maintenant passer à la méthodologie de la recherche de notre travail.

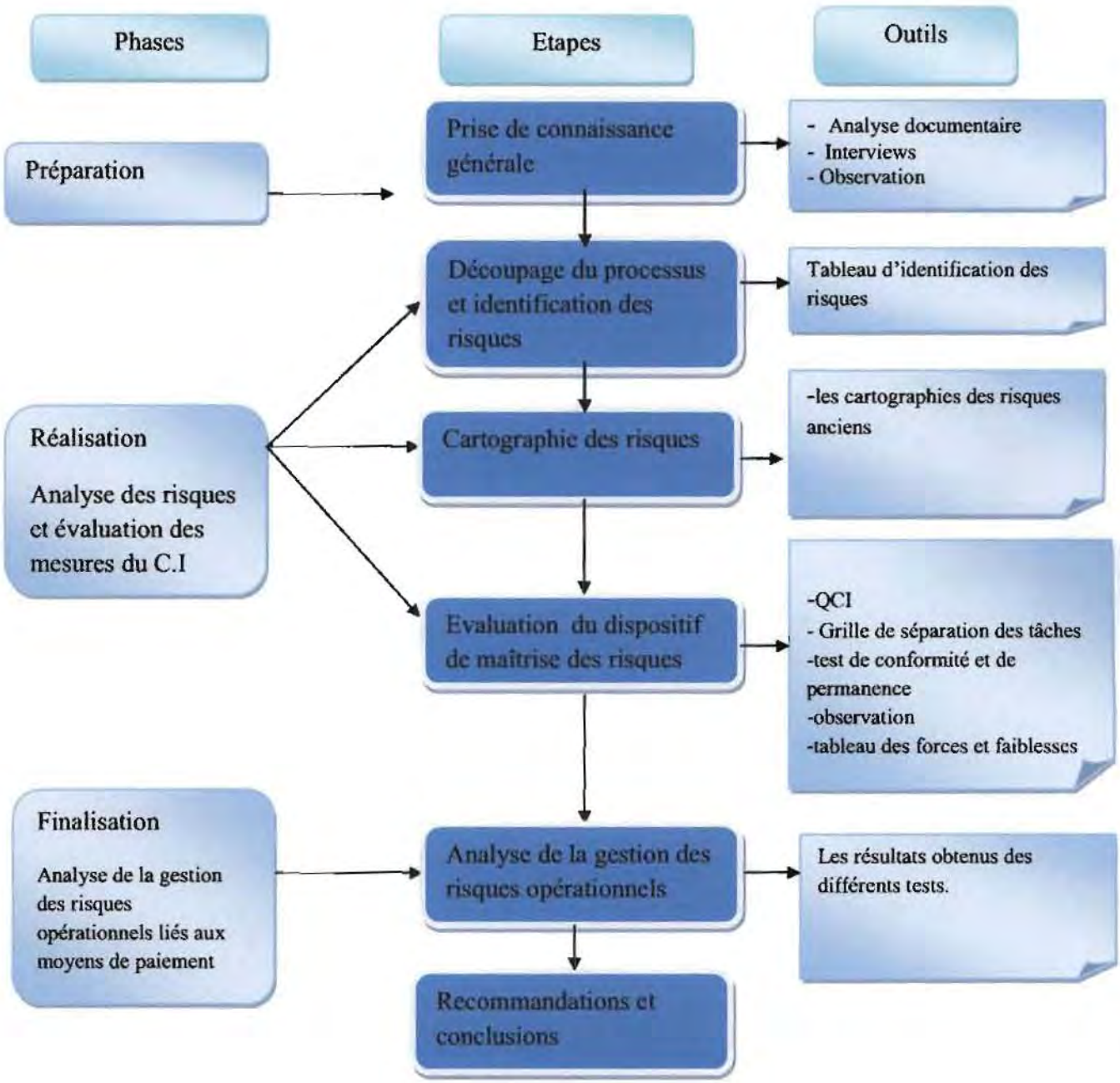
Chapitre 3 : Méthodologie de la recherche

Pour réaliser cette étude, la méthodologie de recherche consiste à la mise en œuvre de notre démarche théorique du processus de gestion des moyens de paiement. Ce chapitre présente, dans un premier temps, un modèle d'analyse, et dans un second temps, les outils de collecte et d'analyse des données.

3.1 Modèle d'analyse

Le modèle d'analyse est la représentation schématique de notre démarche théorique pour l'analyse du dispositif de maîtrise des risques opérationnels liés aux moyens de paiement. Il est composé de la prise de connaissance générale, de l'identification des risques opérationnels, de l'appréciation du dispositif de maitrise et des recommandations.

Figure 3 : Modèle d'analyse de la gestion des risques opérationnels liés aux moyens de paiement à la BAM.



Source : nous-mêmes

3.2 Outils de collecte et d'analyse des données

Ils constituent les méthodes et techniques utilisées pour la collecte et l'analyse des informations concernant le fonctionnement et les procédures de gestion des moyens de paiement d'une entité donnée. Dans l'objectif de maximiser cette collecte d'information, nous allons utiliser l'analyse documentaire, l'entretien, l'observation, le tableau d'identification des risques, le questionnaire de contrôle interne, le test de conformité et de permanence et la grille de séparation des taches.

3.2.1 L'analyse documentaire

Elle consiste à une exploitation des documents existants et nécessaires au fonctionnement de l'organisation. L'analyse documentaire constitue l'acquisition des connaissances générales sur le processus. Notre analyse sera faite en partie sur le manuel de procédures des opérations bancaires.

3.2.2 L'observation physique

Une observation physique est la constation de la réalité instantanée de l'existence et du fonctionnement d'un processus, d'un bien, d'une transaction ou d'une valeur. Elle consiste essentiellement en la vérification détaillée et visuelle d'un descriptif donné. Elle doit permettre de porter un avis sur l'état physique et/ou du fonctionnement apparent du bien à l'instant de l'observation (LEMANT, 1998 : 201-203).

3.2.3 L'interview

Une interview est un entretien avec une personne en vue de l'interroger sur ses actes, ses idées, etc., et de divulguer la teneur de l'entretien. C'est une technique de recueil d'informations qui permet l'explication et le commentaire, et donc apporte une plus value importante à la collecte des informations factuelles et des éléments d'analyse (LEMANT, 1998 :181).

Ainsi, nous allons nous entretenir avec les personnes suivantes :

- les responsables de guichet ;
- l'agent chargé de la clientèle ;
- les responsables du service monétique ;
- les responsables des opérations ;
- le chef d'agence ;
- les responsables de la direction du contrôle et de l'audit interne.

3.2.4 La grille de séparation des taches

C'est un outil de diagnostic qui permet de déceler sans erreurs possibles les manquements au principe de séparation des tâches, d'analyser la charge de travail par agent, d'identifier sa structuration et la manière dont elle est remplie.

Elle va véritablement relier l'organigramme fonctionnel à l'organigramme hiérarchique et justifier les analyses de postes. Sa lecture va permettre de déceler sans erreur possible les manquements à la séparation de tâches et donc d'y porter remède (RENARD, 2007 :347-348).

Elle décrit la répartition du travail et décèle les éventuels cumuls de fonctions incompatibles afin d'y remédier (Obert, 2004 :77).

3.2.5 Le questionnaire de contrôle interne

Le questionnaire de contrôle interne est une grille d'analyse dont la finalité est de permettre à l'auditeur d'apprécier le niveau et de porter un diagnostic sur le dispositif de contrôle interne. Il est généralement composé d'une liste de questions fermées qui servent à recenser les moyens mis en place pour atteindre les objectifs du contrôle interne (LEMANT, 1998 :196).

Ainsi une réponse « oui » correspond à une force apparente du dispositif de contrôle interne et une réponse « non » correspond à une faiblesse de ce dispositif.

3.2.6 Les tests de conformité et de permanence

Le test d'existence et de permanence permet de nous assurer de l'existence des informations recueillies, que l'opération s'effectue effectivement dans la forme.

Lorsque le test d'existence est concluant, nous venons au test de permanence qui nous permettra de nous assurer que les forces théoriques (forces) ont fonctionné de façon permanente, tel que décrit lors des entretiens ou dans le manuel de procédures.

3.2.7 Le tableau des forces et faiblesses apparentes

Le tableau des forces et faiblesses apparentes constitue « l'état des lieux » des forces et faiblesses réelles ou potentiels, et permet de hiérarchiser les risques. Il nous permettra d'identifier à chaque tache, le risque encouru et les pratiques communément admises.

Ce chapitre nous a permis de définir les différents outils et techniques de collectes d'information nécessaires pour mener à bien notre étude. De ce fait, nous allons aborder les aspects pratiques dans la deuxième partie de notre étude.

Conclusion de la première partie

Les banques occupent une place centrale dans notre système économique. Elles ont la responsabilité collective de la gestion des moyens de paiement et elles se présentent comme l'un des principaux garants de la solidité et de la compétitivité de l'économie. Dans le cadre de leur fonction, elles s'exposent à différents risques comme le risque de crédit, le risque de marché, le risque opérationnel, etc.

Et pour assurer leur pérennité et la stabilité du système financier, les banques devraient mettre en œuvre un processus pour contrôler régulièrement les risques auxquels elles s'exposent et les facteurs d'expositions à des pertes.

La revue de la littérature nous a permis de comprendre le processus des moyens de paiement, leur traitement, ainsi que la gestion des risques opérationnels qui y sont rattachés. C'est ainsi que nous avons abordé les risques opérationnels associés au processus, le dispositif de contrôle interne et l'analyse de la gestion des risques opérationnels. Toutes ces dimensions sont importantes pour aborder notre cadre pratique de l'étude.

Quels sont les risques liés opérationnels liés aux moyens de paiement à la BAM ? Quels sont les dispositifs mise en œuvre par la BAM pour la maîtrise de ces risques ?

DEUXIEME PARTIE : CADRE PRATIQUE

Les autorités de contrôle considèrent que les établissements de crédit doivent être dotés de procédures permettant à leurs dirigeants de gérer les risques actuels et de s'adapter aux nouveaux. Un processus de gestion des risques opérationnels réunissant les trois éléments fondamentaux : l'évaluation des risques, le contrôle des expositions et la surveillance des risques aidera les banques et les autorités de contrôle à atteindre ces objectifs. Pour assurer sa pérennité et son développement, la BAM doit toujours améliorer sa performance. Cette amélioration passe par une gestion saine et efficace des moyens de paiement qu'elle gère ou met à la disposition des clients ainsi que les risques opérationnels qui y sont attachés.

Pour ce faire, notre cadre pratique sera basé sur les trois chapitres qui sont :

- le chapitre 4 consacré à la présentation de la Banque Atlantique Mali ;
- le chapitre 5 axé sur la description des procédures de gestion des moyens de paiement et la gestion des risques opérationnels associés ;
- et le chapitre 6 consacré à la mise en œuvre de notre modèle d'analyse.

Chapitre 4 : Présentation de la Banque Atlantique Mali.

Ce chapitre sera consacré à la description générale de la Banque Atlantique Mali. Son objectif est de comprendre l'environnement interne de la BAM afin de mieux cerner l'importance de la mise à disposition ou de la gestion des moyens de paiement.

Plusieurs services interviennent dans la gestion des moyens de paiement, nous allons donc présenter brièvement la BAM, ses organes, son fonctionnement et son organisation.

4.1 Présentation de la BAM

La banque Atlantique Mali est une filiale du groupe bancaire africain « Atlantic Financial Group ». Elle a été agréée en qualité de banque de droit malien par l'arrêté N° 2437/MEF-SG du 12 octobre 2005 du Ministère de l'Economie et des Finances du Mali et immatriculée dans l'ACCRM sous le N° Ma-Bko-2005-1619. La BAM a officiellement ouvert ses portes à la clientèle le 21 mars 2006. En tant que banque, elle opère sous le N° D0135 A. Son siège social est situé à Bamako, Immeuble Baldé, Avenue Cheick Zayed (route de Lafiabougou).

Au terme de l'article 3 des statuts de la loi cadre portant réglementation bancaire, la Banque Atlantique Mali (BAM.SA) a pour objet notamment « de recevoir habituellement au Mali ou dans tout autre pays des fonds dont elle peut disposer par tous moyens de paiement, qu'elle emploie pour son propre compte ou pour le compte d'autrui en opérations de crédits (opérations de prêts, d'escompte, d'acquisitions de créances, de garanties, de financement de vente à crédit et de crédit bail) ou de placement (prise de participations dans les entreprises existantes ou en formation et toutes acquisitions de valeurs mobilières émises par les personnes publiques ou privées) ».

4.2 Les différents organes de la BAM

Nous allons décrire les différents organes de la Banque Atlantique.

4.2.1 Les organes d'administration

- L'Assemblée Générale : Elle représente l'ensemble des actionnaires. Elle permet la prise de décisions collectives et peut revêtir un caractère ordinaire ou extraordinaire

selon la nature des décisions qu'elle est appelée à prendre. Elle se réunit dans les six mois qui succèdent la clôture de chaque exercice social pour statuer sur les comptes de l'exercice.

- Le Conseil d'Administration : Il est composé de six membres et se réunit aussi souvent que nécessaire sur convocation de son président.
- Les commissaires aux comptes : Un commissaire aux comptes titulaire et un commissaire aux comptes suppléant sont nommés.

4.2.2 Les comités de gestion

Indépendamment des organes d'administration légaux, il est institué au sein de la banque six comités de gestion avec un rôle consultatif et décisionnel selon le cas :

- Le Comité de Direction,
- Le Comité de Gestion « Actif Passif »,
- Le comité de Crédit,
- Le Conseil de Discipline,
- Le Comité de Dépenses,
- Le Comité de Suivi des Projets.

- **Le Comité de Direction**

Il comprend le Directeur Général et son adjoint, les directeurs ou les chefs de département da la banque. En tant qu'organe d'information et de coordination des différents services de la banque, il se réunit de façon hebdomadaire et s'occupe du développement de la banque en général.

- **Le Comité de Gestion « Actif Passif »**

Il est composé du Directeur Général, du trésorier, du Directeur Administratif et Financier, du Directeur commercial et du Directeur du risque. Ce comité se réunit une fois par semaine pour statuer sur la gestion des ressources et des emplois de la banque. L'objectif est d'optimiser la gestion de la trésorerie, tout en adaptant les ressources aux emplois. Il est animé par le trésorier.

- **Le comité de Crédit**

Il comprend nécessairement le Directeur Général et son adjoint, le Directeur du Risque et le Directeur commercial.

Le comité de crédit se prononce sur les dossiers de crédits accordés par la banque. Il se réunit une fois par mois pour connaitre l'évolution du portefeuille de la banque, les créances en souffrances, les provisions et le recouvrement.

Il a l'obligation de se réunir aussi souvent que nécessaire. Toutefois, pour des raisons d'efficacité, les décisions de prêts peuvent être fixées dans la limite des pouvoirs du Directeur général de la banque.

Les dossiers dont la limite excède les pouvoirs du Directeur Général et qui relève de la compétence du conseil d'administration ou du siège (AFG) devront faire au préalable l'objet de réunion formelle du comité de crédit suivi d'un procès verbal.

Le responsable du service administration du crédit assure le secrétariat et convoque les réunions en accord avec le directeur du risque.

- **Le Conseil de Discipline**

Sa mission est d'étudier les dossiers faisant l'objet de procédures disciplinaires et de donner un avis motivé à la direction générale.

Il se réunit sur convocation du président après avoir entendu les agents faisant l'objet de procédures disciplinaire au moins 72 heures à l'avance. Les avis du conseil sont consultatifs et adressés au directeur général qui prononce les sanctions en dernier ressort.

Il est composé du directeur administratif et financier, du directeur du contrôle et de l'audit interne, du directeur des opérations, du directeur juridique, du directeur des ressources humaines et moyens généraux et d'un représentant des délégués du personnel.

- **Le comité de dépenses**

Ce comité a pour mission de veiller au respect des procédures et d'approvisionnement ; sélectionner chaque année les prestataires de services ; contenir à tout moment le niveau des dépenses dans la limite du budget ; et veiller au respect du délai de paiement des factures.

Il est constitué par le directeur général adjoint, le directeur du contrôle et de l'audit interne, le directeur des opérations, le service des ressources humaines et moyens généraux.

- **Le comité de suivi des projets**

Il est chargé de suivre et de piloter tous les projets relatifs à l'évolution et au développement normal de la banque. Ce comité est composé de 3 membres nommé par le directeur général en relation avec la nature du projet et en accord avec la direction du groupe.

4.3 Organisation et fonctionnement

Nous allons décrire l'organisation et le fonctionnement des différentes directions de la BAM.

4.3.1 La direction générale

Elle est chargée de suivre, de coordonner et d'orienter les actions de toutes les autres directions de la banque en prenant en compte les rapports de la direction du contrôle et de l'audit interne.

4.3.2 La direction du contrôle et de l'audit interne

La direction du contrôle et de l'audit interne :

- élabore le planning de contrôle et d'audit annuel et veille à son respect ;
- s'assure du respect par tout le personnel du respect des procédures dans l'exécution quotidienne de leur tâche effectue régulièrement des contrôles sur les pièces et sur place de tous les services et de toutes les activités ;
- rédige les comptes rendus de missions faisant état des constats et propose des mesures correctives ;
- veille sur le déroulement courant des activités pour identifier tout risque susceptible d'affecter les actifs de la banque négativement et aviser la direction générale ;
- s'assure que tous les états de déclaration sont faits régulièrement et conformément aux prescriptions des autorités monétaires et de surveillance de l'activité bancaire ;
- veille au respect de tous les ratios prudentiels.

4.3.3 La direction administrative et financière

Elle a pour mission, la coordination et la mise à disposition des équipes de la banque de moyens adéquats en quantité et en qualité pour la bonne exécution de leurs tâches, le contrôle de la qualité de l'information financière et comptable, la gestion de l'actif et du passif, l'élaboration du budget, et de son contrôle, l'application de l'orthodoxie et des principes et règles en vigueur, la production des états financiers de synthèse et le suivi de l'organisation générale de la banque.

4.3.4 La direction commerciale ou de l'exploitation

Cette direction a en charge de développer les relations avec la clientèle cible ; de participer à la conception et au développement des nouveaux produits et services ; d'animer et de superviser toutes les activités de la direction ; de suivre le positionnement de la banque sur les différents créneaux du marché.

4.3.5 La direction des risques

Comme son nom l'indique c'est la direction la plus exposée aux risques car elle a pour fonction d'octroyer des crédits aux clients et de suivre le bon déroulement de ceux-ci ; d'assurer le respect des normes prudentielles et le contrôle et suivi des dossiers en contentieux.

4.3.6 La direction des opérations

Cette direction est la plus impliquée dans les opérations quotidiennes des clients. Elle assure la régularité de toutes les opérations de la clientèle ; elle assure aussi la correcte application de l'ensemble des procédures liées aux opérations, les rapprochements des comptes de liaison et des comptes des correspondants.

La direction des opérations est constituée de trois services, à savoir : le service local ; le service étranger et le service rapprochement.

- **Service portefeuille local** :

Ce service assure la gestion des opérations bancaires locales (paiement de valeurs, réception des valeurs, traitement des opérations avec les autres banques de la place, etc.) ; analyse le niveau de qualité des produits et services distribués par la banque.

- **Service Etranger**

Ce service assure la réception et le traitement de toutes les opérations de la clientèle hors territoire ; traite les opérations bancaires suivantes : crédits et remises documentaires, change, transferts internationaux etc. ; conseille en relation avec le chef de service crédits, les clients sur les transactions qu'ils font avec la clientèle intéressée par les transactions internationales.

- **Service rapprochement**

Il a en charge :

- le rapprochement des comptes des correspondants hebdomadairement et l'apurement des suspens ;
- le rapprochement des comptes de liaison des opérations au jour le jour ;
- la production des statistiques à adresser aux autorités dans les délais requis ;
- le respect des normes et procédures opérationnelles.

4.3.7 La direction des affaires juridiques et du contentieux.

Elle a la responsabilité de donner son avis conforme sur tous les actes contractuels liant la banque ; de s'informer sur les différents transactions en relation avec les chefs de service et prodiguer tous conseils permettant de prévenir les risques ; de prendre toutes les mesures conservatoires susceptibles de préserver les intérêts de la banque ; d'assurer la liaison entre les auxiliaires de justice (notaires, huissier, avocats...) et l'établissement ; d'assurer le suivi des dossiers contentieux de la banque.

4.4 Organigramme

La structure de la banque est présentée à travers son organigramme. (Annexe 1).

Ce chapitre nous a permis d'avoir une vue d'ensemble de la BAM. Après cette présentation, nous allons décrire les procédures existantes en matière de gestion des moyens de paiement et celles de la gestion des risques opérationnels associés au processus.

Chapitre 5 : description des procédures de gestion des moyens de paiement et la gestion des risques opérationnels associés

Dans ce chapitre, nous allons décrire les différentes procédures concernant la gestion des moyens de paiement. Les procédures concernant les chèques, les virements et les prélèvements ont été décrites dans un manuel de procédures, et celles concernant la gestion des cartes n'ont pas encore été élaborées.

5.1 Description de la procédure de gestion des chèques

La constitution de chaque processus dépend de la nécessité et des procédures mise en place pour chaque organisation. Le processus est constitué des fonctions qui sont à leur tour constituées de tâches élémentaires. (BARRY, 2009 :18)

Ces procédures ont été décrites à partir du manuel de procédures de la banque et des interviews faites avec les responsables de la banque.

5.1.1 Demande de chéquiers par le client

Nous allons décrire les procédures concernant la demande de chéquier.

5.1.1.1 Le client

Le client demandeur de chéquier se présente au guichet. Il remplit une demande de carnet de chèques, la signe et la remet à l'Agent du Service Clientèle.

La demande de chéquier peut être adressée sous pli au Gestionnaire de Compte qui la transmet ensuite à l'Agent Service Clientèle.

5.1.1.2 L'Agent Service Clientèle

Il reçoit la demande de chéquier et procède aux vérifications suivantes :

- la conformité de la signature avec le spécimen de signature dans ORION[7] ;
- l'autorisation de délivrer un chéquier selon le compte client (exemple de compte nécessitant une double signature);
- l'existence d'aucune demande en cours dans ORION.

Après contrôle, il procède à la saisie des demandes dans le système et informe le gestionnaire de compte des demandes de chéquiers refusées.

Il procède ensuite à la saisie dans le système du/de: numéro de compte chèque; type de chéquiers; nombre de chéquiers ; la date du jour de saisie est incrémentée automatiquement.

5.1.1.3 Le gestionnaire de compte

Il avise par courrier les clients dont les demandes ont été rejetées en leur précisant le motif.

5.1.2 Commande et réception des chéquiers

Les commandes de chéquiers sont faites directement par le service clientèle, ainsi que la réception de ces commandes.

5.1.2.1 L'agent des moyens généraux

Deux fois par semaine, la Section Moyens Généraux transmet sur une disquette les demandes saisies par agence appuyée d'un listing au service clientèle.

5.1.2.2 Le chef de service clientèle

A la réception des chéquiers, la présence du chef du service clientèle, de l'agent des Moyens Généraux et d'un Auditeur interne est nécessaire. Ceux-ci vérifient que les chéquiers reçus sont conformes à l'état de réception et de la commande.

S'il ne constate aucune anomalie, le chef du service clientèle et l'agent des moyens généraux accusent conjointement réception sur le bordereau de livraison dont ils récupèrent un exemplaire.

Le chef du service clientèle fait parvenir les chéquiers auxquels il joint une copie du bordereau de livraison et une copie du listing aux différents Chefs d'Agence.

[7] Logiciel de gestion de BAM

5.1.3 Enregistrement et conservation des chéquiers reçus

Nous allons décrire les procédures d'enregistrement et de conservation des chéquiers.

5.1.3.1 Chef d'agence

Il accuse réception des chéquiers avant de les transmettre au guichetier qui se chargera de l'enregistrement de la distribution des chéquiers.

5.1.3.2 Le responsable de guichet

A la réception des chéquiers, il procède à la saisie des chéquiers reçus dans le système :

- le numéro du client ;
- le numéro de compte ;
- le nombre de chéquiers ;
- le type de chéquiers ;
- le numéro du 1er chèque et du dernier chèque du chéquier ;
- la date de saisie ;
- Après la saisie, il classe les chéquiers par numéro de compte et les range dans une armoire fermée à clé.

5.1.4 Surveillance des chéquiers conservés

Les procédures de surveillance des chéquiers, qui n'ont pas encore été retirés par les clients, sont décrites ci-dessous

5.1.4.1 L'Agent Service Clientèle

Il doit pointer régulièrement les chéquiers conservés dans l'armoire afin de s'assurer qu'ils ne contiennent pas de chéquiers trop anciens. Pour les chéquiers anciens de trois mois, il élabore une liste des chéquiers incriminés et la transmet aux gestionnaires de compte pour effectuer les relances aux clients.

Après trois relances faites par l'agent clientèle et dans un délai maximum d'un an, tous les carnets de chèques non retirés par les clients sont transmis à la Direction du Contrôle et de l'Audit pour destruction.

5.1.5 Délivrance des chéquiers

Les procédures de retrait des chéquiers par les clients sont décrites ci-dessous.

5.1.5.1 L'agent chargé de la clientèle

Le client se présente de lui-même pour récupérer son chéquier.

Toutefois, il peut mandater quelqu'un pour le retrait. Dans ce cas, le mandaté doit présenter une procuration qui porte les références des pièces d'identités et la signature du client mandataire.

Il vérifie si le chéquier est disponible dans l'armoire. Il ouvre la partie remise de chéquiers dans le système, ensuite il sélectionne la ligne du chéquier à remettre puis renseigne le nombre de chéquiers à remettre.

Il procède à la validation après que les numéros des feuillets se soient affichés.

5.1.5.2 Le client

Le client note sur le 1er feuillet du chéquier qui sert de feuillet de décharge, son nom et prénoms, la date, le numéro de sa pièce d'identité et la signature après avoir vérifié la numérotation des formules de chèques, le nom et le prénom sur le chéquier.

5.1.5.3 L'agent chargé de la clientèle

Il retire le feuillet de décharge, vérifie l'identité de la personne effectuant le retrait du chéquier et la conformité de la signature du client.

Il remet le chéquier au client et procède au classement de la liasse (feuillet de décharge, copie de la pièce d'identité) dans une chemise par date.

L'envoi du chéquier au client entraine la facturation et la comptabilisation des frais d'expédition, qui sont à la charge du client.

En cas d'envoi en recommandé à l'adresse indiquée par le client, les chéquiers sont expédiés au client qui doit accuser réception sur le feuillet de décharge et le renvoyer à la banque. L'envoi du chéquier au client entraîne la facturation et la comptabilisation des frais d'expédition, qui sont à la charge du client.

5.1.6 Destruction des chéquiers à la clôture de son compte

Les procédures de destruction des chéquiers sont décrites ci-dessous.

5.1.6.1 Le responsable de guichet ou l'agent chargé de la clientèle

Lorsqu'un client demande la clôture de son compte, il doit donner à l'agent service clientèle le reliquat des chèques en sa possession et ceux en possession de ses mandataires le cas échéant. A la réception des chèques, il vérifie que les chèques en circulation concernant le client ont été tous reçus à partir d'une consultation du compte client dans le système.

Il porte la mention "ANNULEE" sur tous les feuillets de chèques remis par le client.

Le guichetier remet les chèques annulés au responsable de l'agence qui se charge après vérification de les transmettre à la direction du contrôle et de l'audit interne pour leur destruction.

Il transmet les chéquiers reçus au contrôleur.

5.1.6.2 Le contrôleur

Il reçoit les chéquiers à détruire de son directeur, effectue une seconde vérification dans le système de l'exhaustivité des chéquiers reçus et procède à la saisie de la destruction. ORION : DESTRUCTION DE CHEQUIERS.

La validation de la saisie faite par le directeur de l'audit neutralise les numéros des feuillets concernés.

Ensuite, le contrôleur procède à la destruction physique des chéquiers. La destruction fait l'objet d'un procès verbal dûment classé.

5.1.6.3 Le chef d'agence

A la fin de chaque semestre, le chef d'agence demande au service informatique l'édition de tous les carnets de chèques reçus depuis plus de six mois et qui n'ont pas été retirés par les clients.
A la réception de l'édition, il remet le listing à l'agent service clientèle pour contrôle.

5.1.6.4 L'agent chargé de la clientèle

L'agent chargé de la clientèle procède aux travaux ci après:

- il sort les carnets de chéquiers listés ;
- il pointe les carnets par rapport à l'édition;
- il remet les carnets et l'édition au chef d'agence.

Ensuite le chef d'agence contrôle les carnets par rapport à l'édition, il transmet le listing et les carnets à la direction du contrôle et de l'audit interne qui se chargera de leur destruction.

5.1.6.5 Le contrôleur

Il reçoit les chéquiers à détruire de son directeur et procède à la saisie de la destruction dans le système.

La validation de la saisie faite par l'inspecteur général sort du système les chéquiers préalablement saisis dans le stock.

Le contrôleur procède à la destruction physique des chéquiers.

La destruction fait l'objet d'un procès verbal dûment classé.

5.1.7 Remises de chèques

Chèques sur les caisses

La remise de chèques sur les caisses concerne les chèques déposés par le client pour lesquels l'émetteur et le bénéficiaire sont tous deux clients de la banque.

5.1.7.1 Le client

Il remplit un bordereau de remise de chèques à deux feuillets qu'il signe.

5.1.7.2 L'agent de caisse "Remise de chèques"

A la réception de la valeur à déposer et du bordereau, il vérifie l'existence des mentions obligatoires que sont :

- la somme en chiffres et la somme en lettres. En cas de différence entre ces deux montants, le chèque est systématiquement rejeté ;
- la signature manuscrite du tireur ;
- le nom du tireur et du bénéficiaire ;

- l'indication au verso du chèque, du numéro de compte du tireur.

Si le montant du chèque atteint cinq millions de FCFA (pour les particuliers), il informe le gestionnaire de compte qui appelle le client pour s'assurer qu'il est bien l'émetteur.

Ensuite, le responsable de guichet procède à la saisie de l'opération et adresse un avis de crédit au client.

La validité du chèque requiert l'existence de l'ensemble des mentions énumérées ci avant. S'il n'a pas relevé d'anomalies, il appose le cachet de date de réception et sa signature sur le bordereau dont un feuillet est remis au client.

Si la provision du compte de l'émetteur est insuffisante par rapport au montant du chèque, l'opération doit être approuvée par le Gestionnaire de Compte et le Directeur Commercial avant de procéder à la saisie.

L'opération fait l'objet de validation à plusieurs niveaux selon le montant du chèque :

- par le responsable du Service Portefeuille Local si le montant est inférieur ou égal à cinq millions de FCFA ;
- puis par le Directeur des Opérations si le montant est supérieur à cinq millions de FCFA.

Après la validation de la saisie par les personnes habilitées, l'Agent de la Caisse Remise édite un avis d'opération qui est un avis de crédit.

Chèques sur les confrères

La remise de chèques sur les confrères concerne les chèques réceptionnés par la banque pour lesquels le bénéficiaire est client de la banque et l'émetteur client d'un confrère.

5.1.7.3 Le client

Il remplit un bordereau de remise de chèques à deux feuillets qu'il signe.

5.1.7.4 Le responsable de guichet ou l'agent chargé de la clientèle

A la réception de la valeur à déposer et du bordereau, il vérifie la conformité du chèque et le correct remplissage du bordereau de remise, et s'il n'a pas relevé d'anomalies, il appose le

cachet de date de réception et sa signature sur le bordereau, dont un feuillet est remis au client.

Il joint ensuite l'autre feuillet à la liasse de chèque pour classement.

A la fin de la journée, il fait un récapitulatif de tous les chèques reçus qu'il range par banque. Il les remet ensuite au chef du service portefeuille local qui se charge de les transmettre à l'agent compensation pour traitement.

5.1.8 Opposition sur chèques

Une opposition au paiement d'un ou de plusieurs chèques est une défense de payer faite par l'émetteur du chèque à la banque.

Elle doit être motivée par des causes légales (perte, vol, utilisation frauduleuse du chèque, redressement judiciaire ou liquidation des biens du porteur).

Celui qui paye un chèque sans opposition est présumé valablement libéré. En revanche, celui qui refuse de payer, au motif que le tireur a fait opposition, est en infraction si l'opposition n'est pas conforme aux exigences légales. Ces exigences postulent que l'opposition soit faite par écrit et fondée sur l'un des quatre motifs admis par la réglementation.

Ainsi s'explique que tout banquier doit informer par écrit le tireur du chèque si l'opposition au paiement du chèque émane de lui, qu'il s'est exposé à des sanctions, si elle n'est pas fondée sur un motif admis par la réglementation.

5.2 Description de la procédure de gestion des virements

Ces procédures ont été décrites à partir du manuel de procédures de la banque.

5.2.1 Virement de compte à compte ou inter agences

Le virement de " compte à compte" et "le virement inter agences" sont déclenchés par le client donneur d'ordre.

5.2.1.1 Le client

En effet, le client se présente au guichet de l'agent chargé de la clientèle et dépose une lettre d'ordre de virement.

Ce formulaire est divisé en deux parties : l'une réservée aux informations sur le bénéficiaire et l'autre sur le donneur d'ordre.

Le client donneur d'ordre précise :

- son nom ;
- sa raison sociale ;
- son numéro de compte (le compte à débiter) ;
- son adresse.

Pour le bénéficiaire, le client donneur d'ordre précise :

- le nom ;
- la raison sociale ;
- la banque du bénéficiaire ;
- le numéro de compte du bénéficiaire (le compte à créditer) ;
- l'adresse du bénéficiaire.

Avant d'apposer sa signature et la date, le donneur d'ordre indique le montant du virement en chiffres et en lettres.

5.2.1.2 L'agent chargé de la clientèle

L'agent chargé de la clientèle vérifie que le formulaire est correctement renseigné. Ensuite il met son cachet sur le formulaire et le signe puis remet un exemplaire au client. L'autre exemplaire du formulaire est transmis avec un cahier de transmission à la section transfert local du service portefeuille local.

5.2.1.3 L'agent section transfert local

L'agent section transfert local :

- pointe les ordres de virements reçus avec la liste des ordres reçus;
- vérifie la conformité des renseignements;
- vérifie les signatures ;

- vérifie l'existence de provision.

5.2.1.4 Le gestionnaire de compte ou le directeur commercial

En cas de provision insuffisante, l'agent de la section transfert local soumet le dossier à l'approbation du gestionnaire de compte ou du directeur commercial selon les délégations de pouvoirs.

En cas de rejet de l'ordre de virement, l'agent de la section transfert local retourne le dossier au guichetier qui se charge d'informer le client par courrier.

L'agent section transfert local procède ensuite à la saisie du virement.

5.2.2 Virements interbancaires

Virements émis

La réception des ordres de virement suit la même procédure que dans le cas des virements de compte à compte ou de virement inter agences.

Virements reçus

Les virements sont préalablement reçus via le Système Interbancaire de Compensation Automatisé.

5.2.2.1 L'agent section transfert local

Il reçoit les ordres du guichet et fait une décharge dans le cahier de transmission, puis il saisit les ordres. L'opérateur saisit les éléments concernant le code de l'agence, le bénéficiaire et le montant.

Il saisit ensuite: le numéro de compte du bénéficiaire, son nom, le montant à virer, et le motif.

Après la saisie, il marque à la main la référence automatisée de la saisie sur l'ordre de virement et le transmet à son chef de section.

Au fur et à mesure de leur arrivée au niveau de la Section compensation, l'agent saisit les ordres dans ORION.

L'opérateur saisit les données suivantes :

- le numéro de compte à débiter (l'intitulé est automatique) ;

- le code de la banque du bénéficiaire,
- son code agence et son numéro de compte ;
- le nom du bénéficiaire ;
- le montant ;
- les commissions et taxes.

5.3 Description de la procédure de gestion des prélèvements

Les ordres de prélèvements sont transmis par les autres banques via SICA, si la provision du compte concerné par le prélèvement est suffisante on est tenu de le débiter et d'informer le client.

Au préalable, les clients doivent envoyer les autorisations de prélèvement signées et datées en indiquant le montant et la périodicité.

Pour autoriser un prélèvement, le client donneur d'ordre peut soit envoyer une demande par courrier, ou se présenter sur place au guichet de l'agent clientèle.

5.3.1 Demande de prélèvement automatique

Les procédures de demande de prélèvement sont décrites ci-dessous.

Cas où le client se présente à la Banque

5.3.1.1 Le client

Lorsque le client se présente au guichet, il remplit un ordre de prélèvement automatique. Sur cet ordre de prélèvement automatique, les renseignements à spécifier sont divisés en deux parties.

Une partie où le donneur d'ordre spécifie :

- son nom,
- son adresse
- son numéro de compte,
- le montant à prélever (en chiffres et en lettres),

- La périodicité des prélèvements.

Une autre partie réservée aux renseignements concernant le bénéficiaire qui comprend :

- le nom et l'adresse,
- la banque du bénéficiaire,
- l'Agence du bénéficiaire,
- le code banque et le code guichet,
- le numéro de compte du bénéficiaire et la clé RIB,
- le motif du prélèvement.

Ensuite le client appose sa signature sur la demande.

5.3.1.2 Agent chargé de la clientèle

L'agent chargé de la clientèle vérifie que la demande est correctement renseignée. Puis il met son cachet sur le formulaire et remet une copie au client. Il transmet ensuite l'original à la Direction des Opérations Bancaires.

5.3.1.3 Secrétaire de la direction des opérations

La secrétaire réceptionne les demandes et les transmet au Directeur des Opérations Bancaires qui en prend connaissance et les retourne à la secrétaire. Celle-ci les enregistre dans un cahier et les transmet au Chef de la section transfert local avec un cahier de transmission. Le chef de section affecte enfin le traitement à l'agent de la section.

Cas où la demande est faite par courrier

5.3.1.4 Agent service courrier

Lorsque la demande de prélèvement arrive par courrier, l'agent du service courrier procède à la réception contre décharge, puis la demande est transmise par cahier de transmission au secrétariat de la direction commerciale.

5.3.1.5 Secrétaire de la direction des opérations

La secrétaire réceptionne les courriers et les transmet au Directeur Commercial qui en prend connaissance et le retourne à la secrétaire pour transmission au gestionnaire de compte.

5.3.1.6 Gestionnaire de compte

Le gestionnaire de compte reçoit le courrier et s'assure de la conformité des informations notamment la conformité des signatures. Au besoin, le gestionnaire entrera en contact avec le client. En cas d'acceptation de la demande, le gestionnaire de compte la transmet à la Direction des Opérations Bancaires pour traitement, après avis du Directeur Commercial.

5.3.1.7 Secrétaire de la direction des opérations

La secrétaire réceptionne les demandes et les transmet au Directeur des Opérations Bancaires qui en prend connaissance et les retourne à la secrétaire. Celle-ci les enregistre dans un cahier et les transmet au Chef de la section transfert local avec un cahier de transmission. Celui ci l'affecte à l'agent chargé du traitement.

5.3.1.8 Agent section transfert local

Il renseigne les différentes rubriques de l'écran. Les principaux renseignements sont :

- Nom du donneur d'ordre ;
- Compte du donneur d'ordre ;
- Nom du bénéficiaire ;
- Banque du bénéficiaire et son compte ;
- Montant du prélèvement ;
- Périodicité et durée du prélèvement.

5.3.1.9 Directeur des opérations

Le chef de service ou le Directeur des Opérations contrôle et valide la saisie faite par l'agent.

5.3.1.10 Agent service local

L'avis d'opération est émis automatiquement en deux exemplaires dès que la validation est faite. L'agent récupère ensuite le dossier contenant l'avis.

L'agent agrafe l'original de l'avis à l'autorisation de prélèvement et classe ces documents dans un classeur. La copie de l'avis est retournée au client par courrier.

5.4 Description de la procédure de gestion des cartes

Nous avons décrit cette procédure à partir des entretiens faits avec le responsable monétique.

5.4.1 Demande de carte

Nous allons décrire les procédures de demande de carte.

5.4.1.1 Le client

Le client demandeur se présente au guichet. Il remplit une demande de mise à disposition de carte de paiement, la signe et en remet au guichetier. (Les conditions générales sont jointes au formulaire)

La demande de carte peut être adressé sous pli au gestionnaire de compte qui la transmet ensuite à l'agent service clientèle.

5.4.1.2 Le guichetier

Il reçoit la demande de chéquier et procède aux vérifications suivantes :

- la conformité de la signature avec le spécimen de signature ;
- l'autorisation de délivrer un chéquier selon le compte du client
- l'existence d'aucune demande en cours dans le système.

5.4.2 Commande et réception des cartes

Nous allons décrire les procédures de commande des cartes par la banque.

5.4.2.1 Le service informatique

Deux fois par mois, le service informatique récupère sur une disquette les demandes saisies par agence appuyée du listing.

Il garde une copie et transmet la disquette et le listing au service monétique qui se charge de lancer la commande des cartes chez le fournisseur.

Il met sous pli la disquette et le bon de commande établi conformément au listing qu'il adresse au fournisseur.

5.4.2.2 Le responsable du service monétique

Il lance la commande chez le fournisseur et met sous pli la disquette et le bon de commande établi conformément au listing qu'il adresse au fournisseur.

A la réception des cartes, le responsable du service monétique vérifie que les cartes reçues sont conformes à l'état de réception et de la commande. S'il ne constate aucune anomalie, il accuse réception sur le bordereau de livraison dont il récupère un exemplaire. Il fait parvenir les cartes auxquels il joint une copie du bordereau de livraison et une copie du listing aux différents chefs d'agence.

Les cartes et les codes secrets sont envoyés séparément.

5.4.3 Enregistrement et conservation des cartes

Nous allons décrire les procédures de conservation des cartes.

5.4.3.1 Le chef d'agence

Il accuse réception des chéquiers avant de les transmettre au guichetier qui se chargera de l'enregistrement des cartes.

5.4.3.2 L'agent chargé de la clientèle

Il procède à l'enregistrement des cartes reçues. Toutefois, les cartes et les codes sont conservés séparément dans des armoires par les agents chargés de la clientèle.

5.4.4 Remise des cartes

Nous allons décrire les procédures de remise des cartes.

5.4.4.1 L'agent chargé de la clientèle

Remise de la carte

Le client se présente lui-même pour récupérer sa carte.

Il peut se faire mandater pour le retrait. Dans ce cas, le mandaté doit présenter une procuration qui porte les références des pièces d'identités et la signature du client mandataire. L'agent chargé de la clientèle vérifie si la carte du client est disponible dans l'armoire. Si la carte est disponible, il procède à la remise de la carte.

5.4.4.2 Le client

Il remplit le registre de décharge en renseignant les points suivants : nom, prénom, date, numéro de pièce, adresse, numéro de téléphone, et signature.

5.4.4.3 L'agent chargé de la remise du code secret

Remise du code secret

Le client se présente à l'agent chargé de la remise des codes secrets. Celui-ci vérifie si le code de la carte est disponible dans l'armoire. Ensuite, il remet le code secret au client après décharge.

5.4.5 Opposition

5.4.5.1 Le client

Lorsqu'un client demande une mise en opposition de sa carte, il remplit un formulaire de demande d'opposition, le signe et le remet à l'agent chargé de la clientèle.

Toutefois, il peut faire cette mise en opposition par téléphone, dans ce cas il devrait se présenter le plutôt possible dans une agence de la banque pour matérialiser cette opposition.

5.4.5.2 L'agent chargé de la clientèle

Dès qu'il reçoit la demande d'opposition, il envoie automatiquement un message au responsable du service monétique.

5.4.5.3 Le responsable du service monétique

Il reçoit le message de mise en opposition et procède ensuite à la mise en opposition de la carte du client.

5.4.6 Main levée

Le client qui veut procéder à la levée de la mise en opposition, doit se présenter au guichet de la banque. La main levée suit les mêmes procédures que la mise en opposition. Toutefois, la main levée ne peut être faite qu'en la présence physique du client.

5.5 **Le dispositif de lutte contre le blanchiment** (Cf. Annexe 2)

Le dispositif de lutte contre le blanchiment sera présenté dans les annexes (annexe 2 : 104)

5.6 La gestion des risques opérationnels liés aux moyens de paiement à la BAM

La politique de gestion des risques opérationnels est définie par l'Atlantic Financial Group (AFG), et s'applique à l'ensemble des institutions du groupe.

C'est un processus itératif qui demande la participation du personnel à tous les niveaux de l'organisation.

Pour la gestion des moyens de paiement, elle tourne autour des politiques et procédures mises en place pour la gestion efficace de ce processus et des mesures prises pour maîtriser les risques opérationnels liés au dit processus. Elle consiste à identifier, évaluer et à suivre les risques auxquels la banque est confrontée.

A la BAM, la gestion des risques opérationnels associés au processus de gestion des moyens de paiement consiste à contrôler l'éventualité et la Gravité potentielle d'un incident défavorable, et il comprend trois mécanismes inter-liés :

- **Le dispositif de contrôle interne**

Les moyens de l'institution pour surveiller les risques avant et après les opérations

- **Audit interne**

Une évaluation systématique à posteriori des opérations pour s'assurer que les politiques et procédures sont suivies et respectées au quotidien.

- **Audit externe**

Une évaluation externe des contrôles de l'institution.

Un système de contrôle interne efficace est le mécanisme primaire pour identifier, mesurer, et atténuer les risques opérationnels.

5.6.1 Identification et évaluation des risques opérationnels liés au processus des moyens de paiement

La gestion des risques passe nécessairement par une identification de ceux-ci. C'est une étape qui nous permettra de trouver l'ensemble des risques liés au processus des moyens de paiement. Le dispositif d'évaluation de ses risques opérationnels s'appuie essentiellement :

- l'auto-évaluation des risques qui a pour but d'évaluer les opérations et activités de la banque. ce processus est une dynamique interne qui intègre souvent des listes de

contrôle et/ou des ateliers pour identifier les forces et les faiblesses de l'environnement du risque opérationnel ;

- cartographie des risques, le processus de gestion des moyens de paiement est cartographié. Cet exercice peut révéler des zones de faiblesse et aider à prioriser les mesures de gestion ultérieures ;
- les indicateurs clés de risque ou (KRI : Key Risk Indicators), les indicateurs de risque sont des statistiques et / ou mesures, souvent d'ordre financier, qui peuvent donner un aperçu des risques. Ces indicateurs devraient être examinés sur une base périodique (souvent mensuelle ou trimestrielle) pour alerter la banques sur les changements potentiels qui peuvent être source de risques ;
- tableaux de bord, ceux-ci fournissent un moyen de traduire des évaluations qualitatives en paramètres quantitatifs qui peuvent être utilisés pour répartir le capital économique aux secteurs d'activité par rapport à la performance dans la gestion et le contrôle des divers aspects du risque opérationnel.

5.6.2 Le suivi des risques opérationnels liés au processus de moyens de paiement

Le suivi des risques opérationnels consiste à :

- une évaluation périodique des contrôles mis en place sous la supervision des responsables de risques opérationnels (la direction du contrôle et de l'audit interne) en s'appuyant sur les procédures de contrôle interne ;
- mesurer l'exposition de la banque au risque ;
- procéder aux analyses de scenarii pertinentes ;
- définir les actions nécessaires pour maintenir ou ramener les risques à un niveau acceptable et s'assurer de leur suivi.

Les principales catégories de risques opérationnels sont liées à des défaillances dans la gestion des risques et celles-ci entrainent souvent des pertes financières par suite d'erreur ou fraude, comme exemple d'erreur un guichetier qui débite le mauvais compte ou un encaissement de chèque volé.

Dans ce chapitre, nous avons décrit les différentes procédures concernant la gestion des moyens de paiement. Ensuite nous avons présenté la gestion des risques opérationnels liés aux moyens de paiement au niveau de la BAM. Le chapitre suivant est consacré à l'analyse des risques opérationnels liés à la gestion des moyens de paiement à la BAM.

Chapitre 6 : Analyse du dispositif de maitrise des risques opérationnels liés aux moyens de paiement.

L'activité de gestion des moyens de paiement est une activité rigoureuse qui exige la mise en œuvre de moyens de protection fiables, puissants et performants. Leur sécurité est essentielle. Cette activité peut être exposée au risque de fraude, de dégradation des ressources et du système, ou de pertes. Ces risques peuvent être issus des procédures, du personnel, et/ou des systèmes internes ou de certains évènements extérieurs tels que les catastrophes naturelles, les lois et réglementations, etc. Les établissements de crédit doivent assurer une gestion adéquate des risques opérationnels liés à cette activité. La gestion des risques opérationnels aide les entités à réaliser des objectifs de rentabilité et de performance et constitue une prévention contre la perte de ressources.

Ainsi la maîtrise des risques opérationnels d'une entité peut être perçue comme l'ensemble des initiatives souhaitables qu'elle devrait adopter pour faire face aux principaux risques inhérents à ses activités. (FAUTRAT Michel, 2000 :24)

Et le dispositif de maîtrise des risques opérationnels peut être défini comme l'ensemble des moyens concrets mis en place par les responsables opérationnels pour faire face aux risques inhérents à leurs activités. (FAUTRAT Michel, 2000 :25)

6.1 Identification et évaluation des risques opérationnels

L'identification des risques opérationnels nous permettra d'évaluer l'impact des dits risques. Elle passe nécessairement par une description précise du processus. Cette étape est très importante, il s'agit d'identifier tous les risques liés au processus et d'évaluer leur impact sur les performances du processus.

Nous allons essayer d'identifier les différents risques opérationnels liés à la gestion des moyens de paiement en découpant le processus en sous processus, les sous-processus en activité. Les tableaux comprennent cinq (05) éléments qui sont : la sous-activité, l'objectif de

contrôle interne, le risque opérationnel, la conséquence opérationnelle et enfin le dispositif de maîtrise du risque.

Tableau 2: Identification des risques opérationnels liés à la gestion des chèques

Sous-activité	Objectif de C.I	Risques encourus	Conséquence opérationnelle	Dispositifs de maîtrise
Demande de chéquiers	S'assurer de l'autorisation préalable du client	1) Opérations non autorisées par le client	Perte financière	Les demandes devront faire l'objet d'un contrôle quant à leur régularité: signature, date, forme, autorisations de délivrer un chéquier selon le compte, existante d'aucune demande en cours.
		2) Délivrance de chéquiers à un interdit bancaire	Opération non autorisée	
Commande et réception des chéquiers	S'assurer de la conformité des commandes	3) Non-conformité entre la réception et la commande	Perte financière Litige avec le fournisseur	A la réception des chéquiers l'agent des moyens généraux doit vérifier que les chéquiers reçus sont conformes à l'état de réception et de la commande
conservation des chéquiers reçus	S'assurer de la protection des valeurs	4) Perte, ou vol	Pertes de ressources	Les chéquiers doivent être conservés dans un tiroir fermé à clé par le responsable chargé de la conservation des chéquiers.
Enregistrement des chéquiers	S'assurer de l'enregistrement correct	5) Erreur d'écriture	Perte financière	Vérifier le correct enregistrement des chéquiers
Surveillance des chéquiers conservés	S'assurer du retrait de tous les chéquiers	6) Perte de valeur	Perte financière	Le responsable doit pointer régulièrement les chéquiers conservés dans l'armoire.
Remise de chéquiers	S'assurer du retrait du chéquier par le client	7) Vol	Litiges avec le client Pertes de ressources	Le client doit décharger sur un feuillet en notant son nom, prénom, et la signature.

Récupération des chèques	S'assurer de la récupération du chéquier à la clôture du compte	8) Usage frauduleux	-Pertes de ressources -Perte financière	Le gestionnaire de compte doit récupérer tous les chèques en possession du client.
Destruction des chèques	S'assurer de la destruction des chèques à la clôture du compte	9) Usage frauduleux	-Pertes de ressources -Perte financière	Le contrôleur doit détruire tous les chèques portant la mention "ANNULEE"
Remise de chèques: sur nos caisses	S'assurer que tous les décaissements sont justifiés et autorisés	10) Paiement non autorisé, 11) Acceptation de chèque volé ou ramassé.	-Perte financière -litiges avec le client	Le responsable de guichet vérifie les mentions obligatoires sur le chèque (montant, signature, et l'identité) avant de procéder à la remise. Il remet ensuite un feuillet bordereau de remise au client.
Remise de chèques: sur les caisses	S'assurer de l'existence de provision suffisante sur le compte	12) Paiements de chèques sans provisions	Perte financière	Procéder à une vérification de la provision existante sur le compte du client.
	S'assurer de la validité du chèque	13) acceptation de chèque non valide	Perte financière	Procéder à une vérification des mentions obligatoires sur le chèque. S'assurer de la conformité entre le montant en chiffre et le montant en lettre
	S'assurer que les écritures comptables sont correctes	14) erreur de montant, de date, de compte.	Perte financière	S'assurer du correct enregistrement comptable, autocontrôle
Remise de chèques: sur les confrères	S'assurer de la conformité du chèque et du bordereau de remise	15) erreur sur le montant du chèque	Perte financière	Vérifier la conformité du chèque et le correct remplissage du bordereau de remise.
Mise en opposition	S'assurer que les procédures sont appliquées	16) Usage abusif 17) Négligence	-Perte de ressources -Litiges avec le client	L'avis de mise en opposition doit être directement envoyé au service monétique. Le service monétique prendra les mesures nécessaires.

Main levée	S'assurer que les procédures sont appliquées	18) Négligence	Litiges avec le client	Le client doit se présenter pour procéder à la levée de la mise en opposition faite sur sa carte.

Source: nous-même

Tableau 3: Identification des risques opérationnels liés à la gestion des virements / prélèvements

Sous-activité	Objectif de C.I	Risques encourus	Conséquences opérationnelles	Dispositifs de maîtrise
Compte à compte ou interbancaires	S'assurer de l'autorisation préalable du client	19) Paiements non autorisés	Litiges avec le client	Vérifier que le formulaire d'ordre de virement ou la lettre d'ordre de virement est bien renseigné
Compte à compte ou interbancaires	S'assurer de l'existence d'une provision	20) Insuffisance de provision ou non respect de la limite autorisée	Perte financière	Le virement doit être autorisé par une personne habilitée qui vérifie notamment l'existence d'une provision sur le compte.
Compte à compte ou interbancaires	S'assurer du respect des procédures en matière de blanchiment	21) Blanchiment	Responsabilité de l'entité Mauvaise image	Une demande de virement par un client de passage, doit être préalablement autorisée par une personne habilitée qui effectue les diligences relatives au blanchiment.
Compte à compte ou interbancaires	S'assurer que les écritures comptables sont correctes	22) erreur d'écriture	Perte financière	S'assurer du correct enregistrement comptable, autocontrôle

Réception des demandes de prélèvements	S'assurer de l'autorisation préalable du client S'assurer de la conformité de la signature du client, et de l'existence d'un visa d'approbation	23) Prélèvement non autorisés	Litiges avec le client Perte financière	Les demandes de prélèvements reçus doivent être comparées aux autorisations pour s'assurer que le client les a bien autorisés Les demandes de prélèvements qui parviennent doivent être signées par le client et autorisées par une personne habilitée.
Saisie des autorisations de prélèvements	S'assurer de l'enregistrement correct	24) Erreur d'écriture comptable	Perte financière	

Source: nous-même

Tableau 4 : Identification des risques opérationnels liés à la gestion des cartes

Sous-activité	Objectif de C.I	Risques encourus	Conséquences opérationnelles	Dispositifs de maîtrise
Demande de carte	S'assurer de l'application des procédures	25) opérations non autorisés par le client	-Litiges avec le client	Procéder aux vérifications suivantes: la conformité de la signature, l'autorisation de délivrer une carte.
Commande et réception des cartes	S'assurer de la conformité des commandes	26) non-conformité entre la réception et la commande	Litiges avec le fournisseur	A la réception des cartes, le responsable du service monétique vérifie que les cartes reçues sont conformes l'état de réception et de la commande
Commande et réception des cartes	S'assurer que les codes secrets et les cartes sont envoyés séparément	27) fraude	-Litiges avec le fournisseur -mauvaise manipulation des cartes	Les cartes et les codes secrets doivent être envoyés séparément par le fournisseur.

Enregistrement et conservation des cartes	S'assurer que les codes secrets et les cartes sont bien sécurisés	28) vol, 29) fraude	-Perte de ressources -perte financière	Les cartes et les codes secrets doivent être conservés séparément dans les conditions de sécurité nécessaire.
Remise de la carte et du code secret	S'assurer que les codes secrets et les cartes sont remis au client séparément	30) fraude	Pertes de ressources	Les cartes et les codes secrets doivent être remis pas des personnes différentes dont l'une sera chargé de la remise de carte et l'autre de la remise du code.
Remise de la carte	S'assurer que les cartes sont bien remises au client lui-même.	31) retrait de la carte par un tiers	Perte financière Utilisation frauduleuse Pertes de ressources	Le client présente sa carte d'identité dont une copie sera faite et déchargera dans un registre en renseignant les points suivants: nom, prénom, date, numéro de pièce, adresse, numéro de téléphone, et signature,
Remise du code secret	S'assurer que le code est bien remis au client	32) retrait de la carte par un tiers	-Perte de ressources -Litige avec le client	Même procédure. Le code est remis au client dans une enveloppe fermée.
Mise en opposition	S'assurer que les procédures sont appliquées	33) Usage abusif 34) Négligence	-Perte de ressources -Litiges avec le client	L'avis de mise en opposition doit être directement envoyé au service monétique. Le service monétique prendra les mesures nécessaires.
Main levée	S'assurer que les procédures sont appliquées	35) Négligence	Litiges avec le client	Le client doit se présenter pour procéder à la levée de la mise en opposition faite sur sa carte.

Source : nous-même

6.2 Evaluation du dispositif de contrôle interne

Cette étape vise à évaluer la qualité des contrôles mis en place par la direction de la BAM pour maitriser les risques opérationnels liés à son processus de gestion des moyens de paiement. Nous allons utiliser nos outils de collecte de données et d'information précédemment définis dans la méthodologie de recherche.

6.2.1 Test de conformité et de permanence

Nous avons effectué notre test sur un échantillon d'opérations effectuées en notre présence au cours du mois d'octobre. Nous avons sélectionné dix opérations sur les chèques, dix sur les virements et dix sur les cartes de paiement.

Tableau 5 : Test de conformité et de permanence sur les chèques

	Existence du visa du client	Existence d'un bordereau de remise	Conformité entre le bordereau de remise et le montant du chèque	Conformité entre le montant en chiffre et le montant en lettres	Existence du visa du gestionnaire sur le bordereau de remise
N°1	Oui	Oui	Oui	Oui	Oui
N°2	Oui	Oui	Oui	Oui	Oui
N°3	Oui	Oui	Oui	Oui	Oui
N°4	Oui	Oui	Oui	Oui	Oui
N°5	Oui	Non	N/A[8]	Oui	N/A
N°6	Oui	Oui	Oui	Oui	Oui
N°7	Oui	Oui	Oui	Oui	Oui
N°8	Oui	Oui	Oui	Oui	Oui
N°9	Oui	Oui	Oui	Oui	Oui
N°10	Oui	Oui	Oui	Oui	Oui

Source : nous-même

[8] Le bordereau de remise étant inexistant, on a pas pu vérifier sa conformité.

Tableau 6 : Test de conformité et de permanence sur les virements / prélèvements

	Visa du client sur l'ordre de virement / avis de prélèvement	Visa du gestionnaire de compte	Existence des mentions obligatoires : nom, prénom, numéro de compte du client et du receveur	Envoi de l'ordre /avis de prélèvement au service de la compensation
N° 1	Oui	Oui	Oui	Oui
N° 2	Oui	Oui	Oui	Oui
N°3	Oui	Oui	Oui	Oui
N°4	Oui	Non	Oui	Oui
N°5	Oui	Non	Oui	Oui
N°6	Oui	Oui	Oui	Oui
N°7	Oui	Non	Oui	Oui
N°8	Oui	Oui	Oui	Oui
N°9	Oui	Oui	Oui	Oui
N°10	Oui	Oui	Oui	Oui

Source : nous-même

Ce test a été effectué sur des opérations passées à l'agence Faladié de la banque. Le tableau ci-dessus nous a permis de nous assurer que les procédures concernant les opérations de virements sont bien appliquées et permanente. Nous avons vu que certains ordre de virement ne portait pas le visa du gestionnaire de compte. Des mesures doivent être prise pour les gestionnaires de compte vise tous les ordres de virement et avis de prélèvement.

Tableau 7 : Test de conformité et de permanence sur les cartes de paiement

	Existence d'une autorisation du client sur les demandes	Envoie direct de code et de carte par le fournisseur	Visa du client dans le cahier de décharge	Existence d'un reçu de remise	Remise de la carte et du code par des agents différents de la banque
N°1	Oui	Non	Oui	Oui	Oui
N°2	Oui	Non	Oui	Oui	Oui
N°3	Oui	Non	Oui	Oui	Oui
N°4	Oui	Non	Oui	Oui	Oui
N°5	Oui	Non	Oui	Oui	Oui
N°6	Oui	Non	Oui	Oui	Oui
N°7	Oui	Non	Oui	Oui	Oui
N°8	Oui	Non	Oui	Oui	Oui
N°9	Oui	Non	Oui	Oui	Oui
N°10	Oui	Non	Oui	Oui	Oui

Source : nous-même

Ce test a été effectué sur des opérations passées à l'agence siège de la banque. Ils doivent veiller à ce que le fournisseur envoie séparément les cartes et les codes secrets.

6.2.2 Grille de séparation des taches

Elle va nous permettre de nous assurer que les fonctions d'exécution, de contrôle et d'autorisation ne sont pas cumulées.

Ex : exécution

A : autorisation

C : contrôle

Tableau 8 : Grille de séparation des tâches sur les chèques

CHEQUES		Guichetier / ou agent de la clientèle	Gestionnaire de compte	Service ou Agents moyens généraux	Chef d'agence	Auditeur / contrôleur
Demande de chéquiers	Ex	X				
Vérification des mentions obligatoires.	C	X	X			
Vérification qu'il n y a pas de commande en attente au nom du même client	C		X			
Commande de chéquiers	Ex			X		
réception de chéquiers du fournisseur	Ex			X	X	
Envoi des chéquiers aux agences	Ex			X		
Réception des chéquiers	Ex				X	
Conservation des chéquiers	Ex	X				
Surveillance des chéquiers	Ex	X				
Clôture de compte	Ex	X				
	C		X			
Destruction de chéquiers	C					X
	A					X
	EX					X
Remise de chèques sur les caisses	Ex	X				
	A		X			

Source : nous-même

Les fonctions d'exécution, de contrôle et d'autorisation sont bien séparées.

Tableau 9 : Grille de séparation des tâches sur les virements

VIREMENTS / PRELEVEMENTS		Guichetier	Agent service compensation	Gestionnaire de compte
Ordre de virement et avis de prélèvements	C	X		
	A			X
	Ex		X	
Visa du client	C	X		X
Provision sur le compte du client	A			X
Vérification des mentions obligatoires	C	X		X
Pointage des ordres de virement	C		X	

Source : nous-même

Tableau 10 : Grille de séparation des tâches sur les cartes de paiement

CARTE DE PAIEMENT		Agent service clientèle	Service monétique	Chef d'agence
Demande de carte	Ex	X		
	C		X	
Commande de cartes	Ex		X	
Réception de la commande	Ex		X	
Conservation des cartes	Ex	X		X
Remise de la carte au client	Ex	X		
Remise du code secret	Ex	X		

Source : nous-même

Les fonctions d'exécution, de contrôle et d'autorisation sont bien séparées.

Nous pouvons dire que le système de contrôle interne permet d'assurer une bonne séparation des taches. Cependant, il peut arriver que dans les petites agences qui disposent d'un personnel restreint que certaines fonctions soient cumulées.

6.2.3 Le tableau des forces et faiblesses apparentes

Tableau 11 : Tableau des forces et faiblesses apparentes sur les chèques

Opérations	Objet de contrôle	Indicateurs	Risques	Conséquences	Test à effectuer	Observations F/f	Risques maitrisés
Demande de chéquiers	S'assurer de l'autorisation préalable du client	Demande de chéquiers par le client	Absence d'autorisation du client	Perte financière	Sélectionner un échantillon de 10 opérations sur les chèques et vérifier l'existence de visa.	F Toutes les demandes de chéquiers portent le visa du client	Oui
Enregistrement et conservation des chéquiers reçus	S'assurer de la protection des valeurs	Vérifier la conservation correcte des valeurs	Exposition au risque de vol ou de pertes	Pertes de ressources	Vérifier que les chéquiers réceptionnés sont bien enregistrés et bien conservés	F Ces conditions sont bien remplies	Oui
Surveillance des chéquiers conservés	S'assurer du retrait de tous les chéquiers	Surveiller les chéquiers en instance de retrait	Conservation de chéquiers trop anciens (plus de six mois)	Perte financière	Vérifier dans le cahier de pointage l'existence de tous les chéquiers en attente	F Les chéquiers conservés font l'objet d'un pointage régulier	Oui
Remise de chéquiers	Effectivité du retrait du chéquier par le client	Retrait du chéquier par le client	Retrait par une personne non autorisée	Litiges avec le client Pertes de ressources	Vérifier que tous les retraits de chéquiers ont fait l'objet d'une décharge	f existence de retrait du chéquier sans décharge du client	Non Insuffisamment maitrisé

Source : nous-même

Tableau 12 : Tableau des forces et faiblesses apparentes sur les virements/ prélèvements

Opération	Object de contrôle	Indicateurs	Risques encourus	Conséquences	Test à effectuer	Observation	Risques maitrisés
Compte à compte ou interbancaires	S'assurer de l'autorisation préalable du client	Autorisation du client	Paiements non autorisés	Litiges avec le client Perte de ressources	Vérifier la signature du client sur les ordres de virement / avis de prélèvement sur un échantillon de 10 ordres de virement	F Visa du client sur les ordres de virement	Oui
Compte à compte ou interbancaires	S'assurer de l'existence de la provision	Visa du gestionnaire de compte	Insuffisance de provision	Perte financière	Vérifier le visa du gestionnaire de compte sur un échantillon de 10 ordres de virement	F Visa du gestionnaire sur les ordres de virement	Oui

Source : nous-même

Tableau 13 : Tableau des forces et faiblesses apparentes sur les cartes de paiement

Opération	Object de contrôle	Indicateurs	Risques encourus	Conséquences	Test à effectuer	Observations	Risques maîtrisés
Demande de carte	S'assurer de l'autorisation du client	Vérification du visa du client sur les demandes de carte	Absence d'autorisation	-Litiges avec le client -Perte de ressources	Sélectionner des demandes de carte et vérifier le visa du client	F Toutes les demandes de carte portent le visa du client	Oui
Commande et réception des cartes	S'assurer de la conformité des commandes	Conformité entre la demande et la réception	non-conformité entre la réception et la commande	Litiges avec le fournisseur	Vérifier que les bons de commande sont identiques aux bons de réception	F Pas d'écart entre la commande et la réception	Oui

Gestion des cartes	Réception des cartes	S'assurer que les codes secrets et les cartes sont envoyés séparément	Envoi simultané du code et de la carte	Litiges avec le client	Vérifier que les codes et les cartes ne sont pas réceptionnés au même moment et par la même personne	f les cartes et les codes secrets sont envoyés en même temps par le fabricant.	Non
Gestion des cartes	Enregistrement et conservation des cartes	S'assurer que les codes secrets et les cartes sont bien sécurisés	Vol Usage frauduleux par un tiers	-Perte de ressources -perte financière	Vérifier que les codes et les cartes sont conservés dans des coffres fermés à clé	f les cartes sont conservées dans les tiroirs en bois	Non
Gestion des cartes	Remise de la carte et du code secret	S'assurer que les codes secrets et les cartes sont remis au client séparément	Usage frauduleux par un tiers	Litiges avec le client	Vérifier que les codes et les cartes sont remis séparément	F Un agent remet la carte au client et un autre qui est au back office lui remet le code secret	Oui

Source : nous-même

Ainsi sur la base de la grille de séparation des taches, des tests de conformité et de permanence, du tableau des forces et faiblesses, et du questionnaire de contrôle interne (Annexe 3), nous allons élaborer une cartographie des risques opérationnels.

6.3 Evaluation des risques opérationnels liés à la gestion des moyens de paiement

L'étape d'évaluation des dispositifs de contrôle interne et de maîtrise est une étape particulièrement importante dans la démarche d'évaluation des risques opérationnels. En effet c'est par définition des écarts entre le référentiel-cible et les dispositif existant que seront cotés les systèmes de contrôle interne afin de mettre en place les plans d'action destinés à sécuriser les processus et diminuer les risques. Notre évaluation sera faite par rapport à la

probabilité de survenance et à l'impact des risques identifiés en tenant compte des résultats du test d'existence et de permanence.

6.3.1 Evaluation de la probabilité de survenance

L'évaluation se fait en affectant une cotation de 1 à 5 à l'échelle de la probabilité en appréciant les caractéristiques des dispositifs.

Tableau 14 : Echelle de cotation de la probabilité de survenance du risque

Niveau	Probabilité	Description
5	Très forte	Il est presque certain que le risque se réalise
4	Forte	Il y a de forte chance que le risque se réalise
3	Moyenne	Il est possible que le risque se réalise
2	Faible	Il y a peu de chance que le risque se réalise
1	Très faible	Il y a très peu de chance que le risque se réalise

Source : nous-même

Tableau 15 : Evaluation de la probabilité de survenance des risques identifiés

Risques opérationnels	Probabilité de survenance
1) Opérations non autorisées par le client	1
2) Délivrance de chéquiers à un interdit bancaire	1
3) Non-conformité entre la réception et la commande	2
4) Perte, ou vol	2
5) Erreur d'écriture	1
6) Perte de valeur	2
7) Vol	2
8) Usage frauduleux	2
9) Usage frauduleux	1
10) Paiement non autorisé,	2
11) Acceptation de chèque volé ou ramassé.	3
12) Paiements de chèques sans provisions	2

13) acceptation de chèque non valide	1
14) erreur de montant, de date, de compte.	3
15) erreur sur le montant du chèque	2
16) Usage abusif	3
17) Négligence	3
18) Négligence	3
19) Paiements non autorisés	1
20) Insuffisance de provision ou non respect de la limite autorisée	1
21) Blanchiment	3
22) erreur d'écriture	3
23) Prélèvement non autorisé	3
24) Erreur d'écriture comptable	1
25) opérations non autorisés par le client	2
26) non-conformité entre la réception et la commande	1
27) fraude interne ou externe	3
28) vol,	2
29) fraude interne ou externe	2
30) fraude interne	3
31) retrait de la carte par un tiers	2
32) retrait du code par un tiers	2
33) Usage abusif	4
34) Négligence	2
35) Négligence	2

Source: nous-même

6.3.2 Evaluation de l'impact des risques identifiés

Cette évaluation nous permettra de voir le niveau d'impact des risques identifiés par rapport à leur conséquence. Leur impact sera évalué en fonction de l'échelle ci-après :

Tableau 16 : Echelle de mesure de l'impact des risques identifiés

Niveau	Impact	Description
5	Catastrophique	Conséquences très élevées
4	Elevé	Conséquences élevées
3	Modéré	Conséquences moyennes
2	Mineur	Conséquences faibles
1	Insignifiant	Conséquences négligeables

Source : nous-même

Tableau 17 : Evaluation de l'impact des risques identifiés

Risques opérationnels	Impact
1) Opérations non autorisées par le client	4
2) Délivrance de chéquiers à un interdit bancaire	4
3) Non-conformité entre la réception et la commande	3
4) Perte, ou vol	3
5) Erreur d'écriture	3
6) Perte de valeur	2
7) Vol	3
8) Usage frauduleux	4
9) Usage frauduleux	4
10) Paiement non autorisé,	3
11) Acceptation de chèque volé ou ramassé.	4
12) Paiements de chèques sans provisions	4
13) acceptation de chèque non valide	3
14) erreur de montant, de date, de compte.	3
15) erreur sur le montant du chèque	4
16) Usage abusif	2

17) Négligence	5
18) Négligence	5
19) Paiements non autorisés	2
20) Insuffisance de provision ou non respect de la limite autorisée	3
21) Blanchiment	3
22) erreur d'écriture	3
23) Prélèvement non autorisé	5
24) Erreur d'écriture comptable	4
25) opérations non autorisés par le client	2
26) non-conformité entre la réception et la commande	3
27) fraude interne ou externe	3
28) vol,	4
29) fraude interne ou externe	4
30) fraude	4
31) retrait de la carte par un tiers	5
32) retrait du code par un tiers	5
33) Usage abusif	3
34) Négligence	5
35) Négligence	5

Source : nous-même

6.3.3 Evaluation des risques opérationnels liés aux moyens de paiement

La BAM doit procéder à l'évaluation de ses risques opérationnels à travers une cartographie. Cette cartographie lui permettra de voir les zones de risques importants à surveiller et lui permettra ainsi de prendre les dispositions nécessaires mais aussi de mettre en place les procédures pertinentes pour les réduire.

Tableau 18 : Cotation des risques

Criticité = Probabilité de survenance x Impact

Risques opérationnels	Probabilité de survenance	Impact	Criticité
1) Opérations non autorisées par le client	1	4	4
2) Délivrance de chéquiers à un interdit bancaire	1	4	4
3) Non-conformité entre la réception et la commande	2	3	6
4) Perte, ou vol	2	3	6
5) Erreur d'écriture	1	3	3
6) Perte de valeur	2	2	4
7) Vol	2	3	6
8) Usage frauduleux	2	4	8
9) Usage frauduleux	1	4	4
10) Paiement non autorisé,	2	3	6
11) Acceptation de chèque volé ou ramassé.	3	4	12
12) Paiements de chèques sans provisions	2	4	8
13) acceptation de chèque non valide	1	3	3
14) erreur de montant, de date, de compte.	3	3	9
15) erreur sur le montant du chèque	2	4	8
16) Usage abusif	3	2	6
17) Négligence	3	5	15
18) Négligence	3	5	15
19) Paiements non autorisés	1	2	2
20) Insuffisance de provision ou non respect de la limite autorisée	1	3	3
21) Blanchiment	3	3	9
22) erreur d'écriture	3	3	9
23) Prélèvement non autorisé	3	5	15
24) Erreur d'écriture comptable	1	4	4
25) opérations non autorisés par le client	2	2	4

26) non-conformité entre la réception et la commande	1	3	3
27) fraude	3	3	9
28) vol,	2	4	8
29) fraude	2	4	8
30) fraude	3	4	12
31) retrait de la carte par un tiers	2	5	10
32) retrait du code par un tiers	2	5	10
33) Usage abusif	4	3	12
34) Négligence	2	5	10
35) Négligence	2	5	10

Source : nous-même

Tableau 19 : Hiérarchisation des risques opérationnels selon leur criticité

Nous allons procéder à une hiérarchisation des risques selon leur criticité.

Risques opérationnels	Probabilité de survenance	Impact	Criticité
17) Négligence	3	5	15
18) Négligence	3	5	15
23) Prélèvement non autorisé	3	5	15
11) Acceptation de chèque volé ou ramassé.	3	4	12
30) fraude	3	4	12
33) Usage abusif	4	3	12
31) retrait de la carte par un tiers	2	5	10
32) retrait du code par un tiers	2	5	10
34) Négligence	2	5	10
35) Négligence	2	5	10
14) erreur de montant, de date, de compte.	3	3	9
21) Blanchiment	3	3	9

22) erreur d'écriture	3	3	9
27) fraude	3	3	9
8) Usage frauduleux	2	4	8
12) Paiements de chèques sans provisions	2	4	8
15) erreur sur le montant du chèque	2	4	8
28) vol,	2	4	8
29) fraude	2	4	8
3) Non-conformité entre la réception et la commande	2	3	6
4) Perte, ou vol	2	3	6
7) Vol	2	3	6
10) Paiement non autorisé,	2	3	6
16) Usage abusif	3	2	6
1) Opérations non autorisées par le client	1	4	4
2) Délivrance de chéquiers à un interdit bancaire	1	4	4
6) Perte de valeur	2	2	4
9) Usage frauduleux	1	4	4
24) Erreur d'écriture comptable	1	4	4
25) opérations non autorisés par le client	2	2	4
5) Erreur d'écriture	1	3	3
13) acceptation de chèque non valide	1	3	3
20) Insuffisance de provision ou non respect de la limite autorisée	1	3	3
26) non-conformité entre la réception et la commande	1	3	3
19) Paiements non autorisés	1	2	2

Source : nous-même

Figure 4 : La matrice des risques opérationnels liés aux moyens de paiement

catastrophique		31) retrait de la carte par un tiers 32) retrait du code par un tiers 34) Négligence 35) Négligence	17) Négligence 18) Négligence 23) Prélèvement non autorisé		
Elevé	1) Opérations non autorisées par le client 2) Délivrance de chéquiers à un interdit bancaire 9) Usage frauduleux 24) Erreur d'écriture comptable	8) Usage frauduleux 12) Paiements de chèques sans provisions 15) Erreur sur le montant du chèque 28) vol, 29) fraude	11) Acceptation de chèque volé ou ramassé. 30) fraude		
Modéré	5) Erreur d'écriture 13) acceptation de chèque non valide 20) Insuffisance de provision ou non respect de la limite autorisée 26) non-conformité entre la réception et la commande	3) Non-conformité entre la réception et la commande 4) Perte, ou vol 7) Vol 10) Paiement non autorisé,	14) erreur de montant, de date, de compte. 21) Blanchiment 22) erreur d'écriture 27) fraude	33) Usage abusif	
Mineur		6) Perte de valeur 25) opérations non autorisés par le client 19) Paiements non autorisés	16) Usage abusif		
Insignifiant					
	Très faible	*Faible*	*Moyenne*	*Forte*	*Très forte*

Probabilité de survenance

Zone 1	Zone 2	Zone 3	Zone 4	Zone 5

Après avoir évalué les risques opérationnels liés aux moyens de paiement et sur la base de la grille de séparation des taches, des tests de conformité et de permanence, du tableau des forces et faiblesses, et du questionnaire de contrôle interne (Annexe 3) nous allons faire la synthèse de notre travail dans le tableau ci-dessous.

Tableau 20 : Evaluation du dispositif de contrôle interne

	Dispositif de contrôle interne	Constat
Traitement des moyens de paiement	- Procédure de gestion des chèques	Oui
	- Procédures de gestion des virements/ prélèvements	Oui
	- Procédure de gestion des cartes	Oui
Définition des habilitations	- Définition des normes de gestion	Oui
	- Vérification du traitement des opérations	Oui
	- Procédure de contrôle des opérations	Oui
	- Séparations des taches	Oui
	- Respect du manuel de procédure	Non
Limitations des accès	- Procédure de limitation de l'accès aux moyens de paiement	Oui
	- Procédure de limitation de l'accès aux comptes des clients	Oui
	- Respect du manuel de procédure	Non
Surveillance des conditions de conservation	- Procédure de surveillance par une personne habilitée	Oui
	- Procédure de protection des moyens de paiement	Oui
	- Procédure d'endossement des valeurs détenues par la banque	Oui
	- Souscription d'une assurance contre les risques	Oui
	- Procédure de contrôle des sous-traitants	Oui
Contrôle des risques	- Service de gestion des risques opérationnels	Non
	- Surveillance permanente des risques opérationnels	Non
	- Suivi périodique des risques opérationnels	Oui
	- Service de contrôle et de l'audit interne	Oui
Contrôle de la sécurité des actifs	- Procédure de rapprochement	Oui
	- Procédure d'identification et d'apurement des rejets et des anomalies	Oui
	- Procédure de contrôle	Oui
	- Procédure d'information	Oui
	- Respect des procédures	Oui

Source : nous-même

Les procédures de gestion des cartes existent mais ne sont pas décrites dans un manuel de procédures mis à la disposition des différents acteurs.

Un projet de création d'un service de contrôle permanent des risques au sein de la direction du contrôle et de l'audit interne est en cours.

En contribuant à prévenir et maîtriser les risques de ne pas atteindre les objectifs que s'est fixés la banque, le dispositif de contrôle interne joue un rôle clé dans la conduite et le pilotage de ses différentes activités. Toutefois, le contrôle interne ne peut fournir une garantie absolue que les objectifs de la banque seront atteints, aussi bien conçu et appliqué soit-il.

La probabilité d'atteindre ces objectifs ne relève pas de la seule volonté de la banque. Il existe en effet des limites inhérentes à tout système de contrôle interne. Ces limites résultent de nombreux facteurs, notamment des incertitudes du monde extérieur, de l'exercice de la faculté de jugement ou de dysfonctionnements pouvant survenir en raison d'une défaillance humaine ou d'une simple erreur.

Au terme de notre analyse, nous pouvons dire que le dispositif de maîtrise des risques opérationnels liés aux moyens de paiement à la BAM présente quelques insuffisances quant à sa conception et sa mise en œuvre. Ainsi, nous allons faire des recommandations qui pourront réduire un tant soit peu les pertes liées aux risques opérationnels dans le processus des moyens de paiement.

6.4 Analyse et recommandations

Après avoir identifié et évalué les risques opérationnels liés au processus de moyens de paiement, nous allons procéder à l'analyse de la matrice, et sur la base de l'évaluation du dispositif de contrôle interne formuler les recommandations.

6.3.1 Analyse de la matrice des risques opérationnels liés aux moyens de paiement

La cartographie des risques est divisée en cinq zones réparties comme suit :

- la première zone ou zone 1 est la plus critique car elle regroupe les risques qui ont une forte probabilité de survenance et des conséquences catastrophique sur la banque. Ce

sont les risques à éviter à tout prix et pour lesquels il faut des actions immédiates et une surveillance permanente à travers un dispositif de maitrise adapté.

- la deuxième zone a un niveau de criticité élevé. Elle est constituée des risques dont la probabilité de survenance est faible voire très faible mais qui ont un impact majeur sur les affaires de l'organisation. Du fait de leur impact élevé, ces risques nécessitent un suivi régulier à travers les mesures de protection adéquates et de surveillance à court terme.
- la troisième zone regroupe les risques qui ont une moyenne, voire forte, probabilité de survenance et dont l'impact est majeur voire modéré sur la banque. Ces risques, à travers la lecture de la cartographie sont quasi inexistants. Ainsi, il n'y a pas lieu de mener des actions récurrentes de maîtrise.
- les zones 4 et 5 sont constituées des risques acceptables par l'organisation du fait de leur faible probabilité de survenance et de leur impact négligeable sur les affaires. Ce sont des risques pour lesquels un suivi, de manière périodique, constituerait un gage de leur maîtrise.

6.3.2 Recommandations

Après avoir menés tous les travaux nécessaires pour l'analyse des risques opérationnels liés à la gestion des moyens de paiement à la BAM, nous avons formulé les recommandations suivantes qui sont adressées aux différents acteurs de la banque pour une amélioration des dispositifs de maîtrise des différents risques opérationnels liés à ce processus.

6.3.2.1 A la direction générale

L'efficacité de la gestion des risques opérationnels liés aux moyens de paiement, nécessitent la mise en place d'un dispositif adéquat. Pour cela, certaines propositions seront faites à l'endroit de la direction générale :

- les procédures de gestion des cartes doivent être formalisées dans un manuel de procédures qui sera mis à la disposition de tous les acteurs chargés de la gestion de cet instrument ;

- les manuels de procédures de gestion des chèques, des virements doivent être mis à la disposition des différents services chargés de la gestion de ces instruments de paiement ;

- les modifications concernant ces procédures doivent être diffusées par une communication appropriée aux différents acteurs ;

- la création d'une structure de « Risk Manager » qui sera rattaché à la direction des risques et dont le rôle serait de développer les procédures adéquates pour détecter et gérer le risque opérationnel dans toutes les activités de la banque serait très judicieuse ;

- les outils de suivi de risque opérationnel (tableau de bord, indicateurs de performance, indicateurs clés de risque) pourrait être mise à jour régulièrement ;

- l'externalisation de certaines activités pour réduire le profil du risque ;

- disposer de plans de secours et de continuité d'exploitation concernant la gestion des risques opérationnels;

- améliorer la politique de communication.

6.3.2.2 A la direction des opérations

- une bonne maîtrise des risques opérationnels passe par une bonne application des procédures mis en place. La direction des opérations doit alors prendre les mesures nécessaires pour une application des procédures par le personnel ;

- les valeurs reçues pour encaissements ou décaissements doivent être bien archivés, ils constituent des pièces justificatives des opérations ;

- l'exhaustivité dans le traitement de toutes les demandes d'encaissements et de décaissements pourrait éviter le risque de retards de présentation à la compensation, ou de pertes de jour de valeur.

6.3.2.3 Au service monétique

- les dispositions nécessaires doivent être prises pour que le fabricant envoie séparément les cartes et les codes secrets au service monétique ;

- la distribution des cartes et des codes secrets dans les différentes agences de la banque doivent être faite par des agents différents ;

- une bonne séparation des tâches diminue la possibilité d'erreurs ou d'irrégularités. De ce fait, le responsable du service monétique doit s'assurer que l'agent chargé de la remise des cartes est bien différent de celui qui procède à la remise des codes pour éviter tout risque de fraude sur les cartes ;

- demander à la direction de nommer au sein de chaque agence, un responsable chargé de la remise des cartes et un autre chargé de la remise des codes secrets, des recrutements de personnel pourraient être nécessaires;

- Le processus de gestion des cartes pourrait être amélioré si les procédures étaient décrites dans un manuel de procédures.

6.3.2.4 Au chef d'agence

- une protection adéquate des valeurs pourrait être un dispositif efficace pour éviter les risques de pertes ou de vol. Le chef d'agence pourrait veiller à l'application correcte de ce dispositif ;

- des contrôles inopinés pourraient permettre de s'assurer que les procédures de gestion des instruments de paiement sont bien appliquées au sein des agences ;

- il pourrait s'assurer que les fonctions d'exécution et d'approbation sont bien toujours bien séparées.

Conclusion de la deuxième partie

Cette deuxième partie nous a permis d'avoir une connaissance générale sur la gestion de la BAM, mais aussi elle nous a aussi permis de prendre connaissance du processus de gestion des moyens de paiement au sein de la BAM et du dispositif de maîtrise des risques opérationnels qui lui sont associés. Cela a été possible grâce aux outils préalablement définis dans le chapitre 3.

Notre étude pourrait être utile à la BAM dans la mesure où elle constitue une synthèse des difficultés du processus de gestion des moyens de paiement. Dans le but de réduire les risques opérationnels liés aux moyens de paiement, nous avons formulé des recommandations pour renforcer le dispositif de contrôle interne existant. La mise en application de ces recommandations passe obligatoirement par une implication des différents acteurs du processus de gestion des moyens de paiement.

CONCLUSION GENERALE

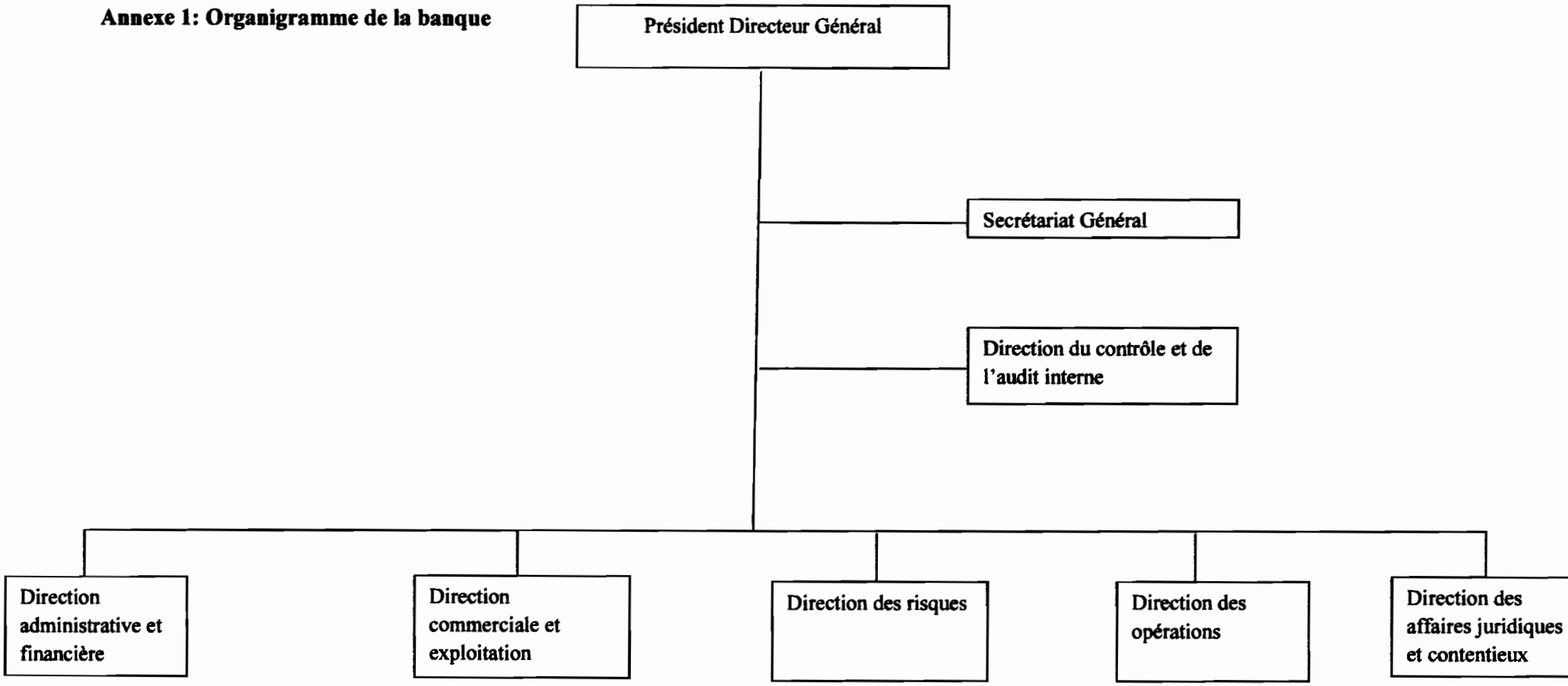
La gestion de ces risques occupe une place d'une importance capitale dans la gestion globale des banques. Cette importance est d'autant plus accentuée par l'interdépendance existant entre les différentes institutions financières. Car la faillite d'une banque, même d'une taille petite, pourrait entrainer un risque systémique et affecter la stabilité de l'ensemble du système de paiement. D'où toute l'importance d'une maîtrise efficace des risques dans le système bancaire. L'atteinte d'un tel objectif passe par le développement de la culture d'une gestion des risques par les organismes de réglementation et de contrôle, mais aussi par une connaissance de la nature de ces risques et la promotion de leur gestion de manière efficace par les contrôles internes des institutions financières. C'est dans cette optique que nous avons retenu notre thème à travers son objectif principal d'apprécier l'efficacité des dispositifs de maîtrise des risques opérationnels liés aux moyens de paiement.

Au cours de nos travaux, nous avons rencontré des difficultés, parmi lesquelles la divergence des points de vue sur la notion de risque opérationnel, les difficultés d'évaluation des risques, le fait que les opérations sur les moyens de paiement soient trop volumineuses. Nous avons donc dû opérer des choix grâce à la revue de la littérature pour aboutir à un modèle d'analyse dans la première partie et sa mise en œuvre effective dans la deuxième partie de notre étude.

Cette analyse nous a permis de montrer comment les risques opérationnels liés à ce processus sont gérés, mais aussi de déceler les forces et les faiblesses du système de contrôle interne. Au bout de notre analyse, nous avons formulé des recommandations. Cependant comme toute œuvre humaine présente des insuffisances et en raison du cours séjour que nous avons eu à faire dans la banque, il appartient aux dirigeants de la banque de prendre les dispositions nécessaires pour enrichir notre étude. L'idéal pour nous serait de contribuer un tant soit peu à la gestion efficace des risques opérationnels liés aux moyens de paiement à la BAM.

ANNEXES

Annexe 1: Organigramme de la banque



Source : manuel administratif 2009-2010, fait le 30 octobre 2010.

Annexe 2 : Le dispositif de lutte contre le blanchiment

La banque a mis en place un certain nombre de mesure pour faire face au risque opérationnel, notamment le dispositif de blanchiment en particulier.

Les obligations mises à la charge de la banque et les diligences qu'elle doit accomplir en matière de lutte contre le blanchiment des capitaux ressortent de la directive N° 07/2002/CM/UEMOA relative à la lutte contre le blanchiment de capitaux dans les États membres de l'Union Économique et Monétaire Ouest Africain (UEMOA).

Les banques exerçant des activités particulièrement vulnérables au blanchiment des capitaux, le législateur a imposé une collaboration entre les différents acteurs de la lutte contre ce phénomène devenu mondial qui peut sur le plan financier entamer la réputation et la crédibilité des établissements de crédit.

Les agents (notamment agents du service clientèle, caissiers, gestionnaires de comptes) en contact avec les clients actuels ou potentiels (déposants, bénéficiaires de concours ou de tout autre service) doivent singulièrement redoubler de vigilance sur :

- **l'identité des clients**

Lors de l'ouverture du compte par la présentation soit d'un document officiel d'état civil (carte nationale d'identité, passeport) portant la photographie de l'intéressé pour les personnes physiques, soit des actes ou extraits (originaux ou copies certifiées) de registre officiel mentionnant la dénomination, la forme juridique, l'objet social pour les personnes morales. Il doit également être fourni pour ces dernières, l'état civil et les actes (statuts, règlement intérieur, procès-verbaux..) constatant l'identité et les pouvoirs des personnes physiques autorisées à agir au nom de la personne morale. Les références et les copies des documents, actes et pièces fournis seront soigneusement conservés dans le dossier juridique ;

- **l'adresse des clients**

Cette vigilance portera sur la vérification par tout moyen de la véracité de l'adresse indiquée, notamment par visite, envoi de lettre d'accueil, de premier relevé de compte ou toute autre correspondance destinée à cette fin avec éventuellement accusé de réception. Le résultat de

cette vérification doit être intégré dans le dossier juridique. De même que tout changement d'adresse spontané ou après investigation ;

- **les mouvements des comptes**

En matière de dépôts ou de retrait d'espèces, de virements, de remise de chèque à l'encaissement, de mise à disposition, de transfert, etc. La vigilance portera plus spécifiquement sur l'origine des fonds, l'identité du bénéficiaire, du remettant, du tireur, du donneur d'ordre dès lors que les montants en cause apparaissent hors de proportion ou sans relation avec l'activité et les revenus de la personne ou les recettes de l'exploitation.

Annexe 3 : Questionnaire de contrôle interne

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°1**
	Questionnaires	**Réponses**			**Observations**
		Oui	**Non**	**N/A**	
	Moyens de paiement				
1	les valeurs reçues sont-elles immédiatement endossées ?	X			
2	existe-t-il un moyen de s'assurer que toutes les valeurs reçues des guichets et des autres services sont bien réceptionnées par le service compensation ?	X			
3	existe-t-il un moyen de s'assurer que toutes les valeurs reçues par le service compensation sont présentées à la chambre de compensation ?	X			
4	les procédures et les circuits permettent-ils de s'assurer que toutes les valeurs sont traitées dans des délais qui évitent des pertes de jours de valeur ?	X			
5	est-il interdit à la section compensation de mouvementer les comptes clients ?	X			Le traitement étant automatisé il n y a pas moyen de mouvementer les comptes.

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°2**
	Questionnaires	**Réponses**			**Observations**
		oui	**Non**	**N/A**	
	Moyens de paiement				
6	les valeurs reçues font-elles l'objet d'un contrôle : - quant à leur régularité ? - quant à la signature du client ?	X			
7	Une autorisation préalable du client est-elle nécessaire avant de débiter son compte ? (à l'exception des chèques).		X		Ca dépend du montant de la transaction.
8	Les gestionnaires des comptes ou exploitants examinent-ils les valeurs reçues (ou les comptes clients après les opérations de compensation) pour décider d'éventuels rejets ?	X			
9	Les temps de traitement et de circulation des valeurs permettent-ils de pouvoir effectuer les rejets dans les délais ?	X			
10	Le rejet est-il approuvé par une personne habilitée qui appose son visa ?	X			
11	Les formalités légales en cas de rejet sont-elles accomplies ?	X			

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°3**
	Questionnaires	**Réponses**			**Observations**
		Oui	**Non**	**N/A**	
	Chèques				
12	Les comptes compensation sont-ils justifiés chaque jour ?	X			
13	Les erreurs sont-elles recherchées et régularisées le jour même?	X			
14	La justification du compte est-elle contrôlée régulièrement par un responsable ?	X			

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°4**
	Questionnaire	**Réponses**			
		Oui	**Non**	**N/A**	
	VIREMENTS EMIS				
	Les signatures des clients figurant sur les ordres de virement sont-elles contrôlées ?	X			
	Les virements sont-ils autorisés par le gestionnaire du compte ou une personne habilitée ?	X			
	Les ordres téléphoniques font-ils l'objet de procédures aptes à authentifier les messages ?			X	la banque n'autorise pas ce genre d'opérations
	Existe t-il un moyen de s'assurer que tous les virements reçus sont traités le jour même ?	X			
	Avant d'être transmis à la compensation les virements sont-ils contrôlés et visés par une personne habilitée, différente de celle qui les traite ?	X			

	Questionnaire de contrôle interne	Processus : gestion des moyens de paiement			Folio n°5
	Questionnaire	**Réponses**			
		Oui	**Non**	**N/A**	
	VIREMENTS				
	Virements reçus				
	Un système permet-il de s'assurer que les virements sont crédités aux clients concernés ?	X			
	Les avis d'opérations sont-ils expédiés indépendamment de la personne, qui a appliqué le virement ?	X			
	La différence entre les dates de valeurs appliquées aux clients par rapport aux dates de valeur appliquées par la chambre de compensation (ou le compensateur) est elle positive ? Est-il possible de l'améliorer ?	X			

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°6**
	Questionnaire	**Réponses**			
	PRELEVEMENT	**Oui**	**Non**	**N/A**	
	Les autorisations de prélèvement reçues des clients sont –elles visées par le gestionnaire de compte ?	X			
	Sont-elles préservées dans un fichier ?	X			
	Les prélèvements reçus sont-ils comparés aux autorisations des clients par le système informatique ?	X			
	Les anomalies (absence d'autorisation, montant ou dates non conformes) sont elles corrigées par une personne habilitée en liaison avec le client ?	X			

	Questionnaire de contrôle interne	**Processus : gestion des moyens de paiement**			**Folio n°6**
	Questionnaire	**Réponses**			
		Oui	**Non**	**N/A**	
	Carte de retrait				
	La délivrance des cartes de paiement fait-elle l'objet d'une autorisation préalable par une personne habilitée ?	X			
	Les codes secrets et les avis de mise à disposition sont-ils directement adressés au client, sans transiter par le service ?		X		Ce sont des agents de la banque qui sont chargés de la conservation des cartes et des codes secrets.
	Les cartes en instance de retrait sont-elles conservées dans des conditions satisfaisantes : Centralisation de l'ensemble des cartes ? Protection adéquate ? Justification des retraits ?	X X X X			Elles sont conservées dans des tiroirs fermés à clé. Notons que ces conditions ne sont pas respectées dans certaines agences de la banque.
	Les commissions sont-elles perçues à bonne date ?	X			Le compte du client est immédiatement débité dès la réception de la demande par le service.
	Les cartes perdues ou volées sont-elles rapidement signalées au centre de traitement pour opposition ?	X			L'opposition est traitée par le service monétique de la banque.

	Questionnaire de contrôle interne	Processus : gestion des moyens de paiement			Folio n°7
	Questionnaire	**Réponses**			
	Carte de retrait	**Oui**	**Non**	**N/A**	
	Les demandes de mise en opposition sont ils immédiatement traitées par le service en charge ?	X			
	Les plafonds sont ils respectés ?	X			
	Les conditions de main levée sont elles respectées ?	X			

	Questionnaire de contrôle interne	Processus : gestion des moyens de paiement			Folio n°7
	Questionnaire	**Réponses**			
	SYSTEME D'INFORMATION	**Oui**	**Non**	**N/A**	
	Le système d'information permet il de mesurer le résultat des moyens de paiement ? - en commissions ? - en date de valeur ?	X X X			
	Des études sont-elles menées pour : - déterminer le cout des moyens de paiement ? - analyser les différents canaux de recouvrement ? - déterminer la rentabilité de chacun d'eux ? - émettre des recommandations ?	 X X X X			

BIBLIOGRAPHIE

1. BARRY, Mamadou (2009), audit contrôle interne, les presses de la sénégalaise de l'imprimerie, 371p.

2. BAPST, Pierre Alexandre & Bergeret Florence (2002), *Pour un management des risques orienté vers la protection de l'entreprise et la création des valeurs*, revue française de l'audit interne, n°161, 157p.

3. BERNARD Fréderic, GAYRAUD Rémy (2006), *contrôle interne, 1ère Edition,* Maxima, Paris, 303p.

4. BERTIN Elisabeth (2007), *Audit interne : enjeux et pratiques à l'international,* EYROLLES, 320p.

5. BILODEAU Yves, POULIOT Daniel (2002), *Mesurer les risques en vue de les contrôler et de les gérer, Audit n°160, p35-37.*

6. BOURDEAUX Gautier, DE COUSSERGUES Sylvie, *Gestion de la Banque : du diagnostic à la stratégie* ,6e Edition, DUNOD, *294p.*

7. BRAJOVIC-BRATANOVIC Sonia, GREUNING Van Henri, ROZERBAUM Marc (2004); *Analyse et Gestion du Risque Bancaire: un cadre de référence pour l'évaluation de la gouvernance d'entreprise et du risque ;* Editions ESKA, 386 p

8. CAMARA Lucien (2006), *la gestion des risques en micro-finance ; comment gérer avec efficacité les risques d'une institution de micro-finance ?* Edition plantation, *175p.*

9. CHELLY Dan, MERLIER Patrick, JIMENEZ Christian (2008), *Risques Opérationnels : de la mise en place du dispositif à son audit,* Revue Banque, 271 p.

10. COOPERS & Lybrand (2000), *la nouvelle pratique du contrôle interne, 5ème* tirage, Editions d'Organisation, Paris, 378p.

11. DALBERA Jean-Louis (2007), moyens paiement : il faut reformer le chèque, *revue banque,* N°696, p.60-63.

12. DOMINIQUE Vincent(1999), *Dresser une cartographie des risques*, Revue Audit n°144, p.26-27.

13. DRAGON Claude, GEIBEN Didier, NALLARD Gilbert, *la carte et ses atouts,* Revue Banque, 126*p.*

14. DRAGON Claude, GEIBEN Didier, KAPLAN Daniel, NALLARD Gilbert, *les moyens de paiement : des espèces à la monnaie électronique,* Revue Banque, *504p.*

15. FAUTRAT Michel (2000), *De l'audit interne au ... management de la maîtrise des risques,* Audit 2000, n°148, p 24-27.

16. HAMZAOUI Mohamed (2005), *audit, gestion des risques et contrôle interne, Normes ISA 200, 215, 330 et 500,* Village Mondial, 243p.

17. HUTIN Herve, *toute la finance, EYROLLES,* France, 951 p.

18. IFACI, PRICE WATERHOUSE COOPERS (2005), *le Management des Risques de l'entreprise, 1e Edition,* Editions d'Organisation, 338 p.

19. LAMARQUE Eric (2008), *gestion bancaire, 2e Edition,* Pearson Education, *240p.*

20. MADERS Henry, MASSELIN Jean-Luc (2006), contrôle interne des risques, 2ème Editions d'Organisation, Paris, 217p.

21. MAIGNON Michel, NICOLET Marie Agnès (2008), *contrôle interne et gestion des risques opérationnels,* Revue Banque, n°668, p (51-52).

22. McNamee, David, CIA, CISA, CFE (1996), *assessing risk,* 1ère edition, *The IIA,* John Wiley & Sons, inc., Floride, 155p.

23. OGIEN Dov (2008), *Comptabilité et audit bancaire,* 2e édition, DUNOD, 532 p.

24. LEMANT Olivier (1995), *la conduite d'une mission d'audit interne*, DUNOD, 279p.

25. NICOLET Marie-Agnès (2000), Risques opérationnels de la définition à la gestion, Banque Magazine, n° 615, p.44-46

26. OBERT, Robert (2004), *Audit et commissariat aux comptes aspects internationaux,* 4ème Edition, DUNOD, 495p.

27. Pricewaterhousecoopers (2005), *la pratique du contrôle interne*, Edition d'organisation, Paris, 337 pages.

28. RAMBURE Dominique (2005), *Les Systèmes de Paiement,* Economica, 288p.

29. Règlement N°15/2002/CM/UEMOA (2002), *Relatif aux systèmes de paiement dans les Etats membres de l'UEMOA*, 57p.

30. RENARD Jacques (2006), *théorie et pratique de l'audit interne, 6ème Edition, Eyrolles, 479p.*

31. RENARD Jacques (2010), *théorie et pratique de l'audit interne, 7ème Edition, Eyrolles, 469p.*

32. SARDI Antoine (2002), *Audit et Contrôle interne bancaires, AFGEE édition, 1099p.*

33. SARDI Antoine (2005), *Pratique de la Comptabilité bancaire, AFGEE édition, 1351p.*

34. SIRUGUET Jean-*Luc (2001), le contrôle comptable bancaire,* Banque éditeur, *562p.*

Site internet

Basel Committee on Banking Supervision (December 2001), Sound practices for the management and supervision of operational risk http://www.fsa.go.jp/inter/bis/bj_20011220a.pdf consulté le 07 Avril 2011.

DAHEN Héla (2006), La quantification du risque opérationnel des institutions bancaires http://neumann.hec.ca/gestiondesrisques/these_Hela%20Dahen_vf.pdf Consulté le 16 novembre 2010.

IFACI (2009), Normes professionnelles de l'audit interne http://www.svir.ch/fileadmin/downloads/revision/iia/081105_Normes_IIA_F_090101.pdf consulté le 10 Novembre 2010.

PIRUS Jean-Luc (2004), L'analyse des risques opérationnels : un enjeu qui dépasse le secteur bancaire http://www.journaldunet.com/solutions/0403/040319_chro_bpms.shtml consulté le 08 Avril 2011.

WIKIPEDIA (Mars 2008), Le risque opérationnel (établissement financier) **http://fr.wikipedia.org/wiki/Risque_op%C3%A9rationnel_(%C3%A9tablissement_financier)** consulté le 19 Avril 2011.