CESAG Centre Africain d'Etudes Supérieures en Gestion

Institut Supérieur de Comptabilité, de Banque et de Finance (ISCBF)

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

Promotion 22

(2010-2011)

Mémoire de fin d'étude

THEME

ANALYSE DE LA GESTION DES RISQUES OPERATIONNELS LIES AUX SYSTEMES DE PAIEMENT: CAS DE LA CBAO

Présenté par :

M. Frédéric Aristide Gnaba BOMBO

Dirigé par :

M. LOKOSSOU H. OSCAR

Contrôleur de gestion

Enseignant associé au CESAG

Octobre 2012

DEDICACE

Nous dédions ce mémoire à :

- notre frère aîné pour le soutien matériel et financier inestimable et indispensable à notre formation ;
- notre épouse pour son amour et son soutien malgré la distance qui nous sépare l'un de l'autre ;
- nos frères et sœurs, et surtout notre mère, que ce diplôme nous soit bénéfique dans un avenir proche.
- monsieur Martial TURPIN pour son soutien.
- tous ceux qui nous ont soutenu de près ou de loin,

REMERCIEMENTS

Nous saisissons l'occasion d'adresser nos remerciements à tous ceux qui ont aidé à la réalisation de ce mémoire.

Nos remerciements vont particulièrement à l'endroit de :

- monsieur Abdelkrim RAGHNI, Administrateur Directeur Général de la CBAO pour nous avoir accepté au sein de son entreprise ;
- monsieur François SENE, Responsable du Contrôle Budgétaire, notre maître de stage pour ses orientations et conseils ;
- monsieur Mbaye FAYE, Responsable du Contrôle de Gestion, pour nous avoir permis de comprendre l'activité bancaire ;
- monsieur Souleymane DIAW, Responsable Adjoint de l'Audit Général et de l'Inspection, qui malgré ses multiples occupations, nous a orienté et a mis à notre disposition, des informations nécessaires à la réalisation du mémoire ;
- l'ensemble du personnel de la Direction des Opérations pour son accueil, sa disponibilité et son ouverture professionnelle ayant contribué à nous faciliter la tâche pour rédiger notre mémoire ;
- monsieur Hugues Oscar LOKOSSOU, mon Directeur de Mémoire pour ses conseils avisés, sa rigueur et sa disponibilité qui nous ont aidé pour la rédaction du mémoire ;
- monsieur Moussa YAZI, Directeur de l'Institut Supérieur de Comptabilité, de Banque et de Finance pour ses conseils méthodiques qui nous ont guidé dans notre rédaction ;
- tout le corps Professoral du CESAG pour ses enseignements de qualité ;
- la 22ème Promotion du DESS Audit et Contrôle de Gestion, pour l'amitié et la convivialité ;
- nos amis, pour les conseils et le soutien moral.

LISTE DES SIGLES ET ABREVIATIONS

ABS: Attijari Bank Sénégal

APBEF: Association Professionnelle des banques et Etablissement Financiers

BAM: Banque Al Magbrib

BAO: Banque de l'Afrique Occidentale

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

BCR: Banque Centrale Russe

BIA: Basic Indicator Approch

BIAO: Banque Internationale de l'Afrique Occidentale

BIC: Bank Identification Code

BOAD: Banque Ouest Africaine de Développement

BRI: Banque des Règlements Internationaux

BRVM: Bourse Régionale des Valeurs Mobilières

CBAO: Compagnie Bancaire de l'Afrique Occidentale

CCP: Compte des Chèques Postaux

CEMAC: Communauté Economique et Monétaire de l'Afrique Centrale

CI: Contrôle Interne

CMF: Code Monétaire et Financier

CODIR: Comité de Direction.

COSO: Commitee of Sponsoring Organisations of the Treadway Commission

CRC: Centrale de Référentiel Client

CRO: Compte Rendu d'Opérations

CRO: Correspondant Risques Opérationnels

CTMI: Centre de Traitement Monétique Interbancaire

DAB: Distributeur Automatique de Billets

DCBR: Dépositaire Central Banque de Règlement

DFC: Directeur Financier et Comptable

DHL: Dalsey, Hillblom & Lynn

ERM: Entreprise Risk Management

FAR: Feuille d'Analyse des Risques

FCFA: Franc de la Communauté Financière Africaine

FIFO: First In First Out

GAB: Guichet Automatique de Billet

GIE:	Groupement d'Intérêt Economique
GIM:	Groupement Interbancaire Monétique
GRO:	Gestion des Risques Opérationnels
IFACI:	Institut Français de l'Audit et du Contrôle Internes
KRI:	Key Risk Indicators
MRO:	Manager des Risques Opérationnels
PAC:	Point d'Accès à la Compense
PCB:	Plan Comptable Bancaire
PME:	Petites et Moyennes Entreprises
PNB:	Produit Net Bancaire
QCI:	Questionnaire de Contrôle Interne
RO:	Risques Opérationnels
RRO:	Relais Risques Opérationnels
RTGS:	Real Time Gross Settlement
SCN:	Système de Compensation National
SICA:	Système Interbancaire de Compensation Automatisé
SMIR:	Système Monétique Interbancaire Régional
SP:	Système de Paiement
STAR:	Système de Transfert Automatisé et de Règlement
SWIFT:	Society For Worldwide Interbank Financial Telecommunication
TFfa:	Tableau des Forces et faiblesses apparentes
UAP:	User Account protection
UEMOA:	Union Economique et Monétaire Ouest Africaine
UMOA:	Union Monétaire Ouest Africaine

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

TABLE DES MATIERES

INTRODUCTION GENERALE

Par définition, les banques sont des établissements financiers qui collectent des dépôts d'argent pour les utiliser sous forme d'investissement ou de crédits accordés aux entreprises et aux ménages. Mais aujourd'hui l'activité bancaire a évolué, s'est largement diversifiée et étoffée, ce qui concourt à la rendre beaucoup plus complexe.

Ainsi, on distingue désormais différentes et vastes activités bancaires qui comprennent entre autres les prestations offertes par les réseaux des agences jusqu'au marché des capitaux, l'investissement, la gestion des actifs et la gestion des titres.

Le financement bancaire est un vecteur moteur de croissance économique et de création de richesse. Les banques sont importantes aussi bien du point de vue microéconomique que pour la stabilité macroéconomique. C'est sans nul doute le cas dans l'espace UEMOA (Union Economique et Monétaire Ouest Africaine) où ce secteur a connu une expansion remarquable.

Le mouvement de diversification du paysage bancaire s'est renforcé par l'agrément de nouveaux groupes bancaires rendant l'activité beaucoup plus concurrentielle et vulnérable.

Pour stabiliser ce secteur important de l'économie sous-régionale, la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a renforcé le cadre réglementaire d'exercice de la profession avec l'adoption de nouveaux textes portant sur :

- les instruments de paiement ;
- le blanchiment des capitaux ;
- le financement du terrorisme ;
- la libéralisation des activités bancaires et financières ;
- la restructuration du système bancaire ;
- la mise en œuvre d'un plan comptable bancaire (PCB) ;
- l'application des recommandations de Bâle I et II ;

Nonobstant toutes ces mesures prises par la tutelle, la profession de banquier et bien d'autres activités du secteur financier restent indissociables de la notion de risque, qui peut être défini comme l'éventualité d'un événement plus ou moins prévisible et susceptible de causer un dommage sur une entité.

Nous avons en mémoire les scandales qui ont secoué le monde de la finance ces dernières décennies notamment la faillite de la Barings[1] en 1995 et l'affaire Kerviel[2] avec la Société Générale, dus à des mauvaises décisions de gestion ou à une absence ou une insuffisance des dispositifs de maîtrise des risques.

Cet état de fait met en évidence la survenance du risque malgré les dispositifs prudentiels, mais il interpelle les banquiers quant à l'impérieuse nécessité de se doter d'un contrôle interne rigoureux pour faire face aux menaces que sont :

- le risque de fraude interne ;
- le risque de fraude externe ;
- le risque de dysfonctionnement de l'activité et des systèmes ;
- le risque de mauvaise ou de non exécution, de livraison et de gestion des processus ;
- le dommage aux actifs corporels ;
- le risque de perte de clientèle due à la mauvaise qualité de service.

L'ensemble des menaces suscitées constituent le risque opérationnel tel que défini par le comité de Bale II (2003 :7) qui stipule que « le risque opérationnel est le risque de perte résultant de carences ou de défauts attribuable à des procédures, personnels et systèmes internes ou à des événements extérieurs ».

Ce risque engage la responsabilité de l'établissement et peut entamer son image de marque, source d'un risque de réputation.

Le risque opérationnel apparaît dès lors comme un risque diffus, omniprésent et endogène ; diffus parce qu'il n'est pas toujours apparent ou directement observable, omniprésent car toutes les activités bancaires en plus de leurs risques spécifiques,

---

[1] En 1995, la banque britannique la Barings a été mise en faillite à cause des placements à découvert réalisés par le trader Nick Leeson, supérieurs aux fonds propres de la banque.

[2] Salarié de la Société générale accusé par son employeur d'être le seul responsable, à hauteur de 4,82 milliards d'euros, des pertes de la banque découvertes en janvier 2008, celles-ci résultant de ses prises de positions sur des contrats à terme sur indices d'actions s'élevant à cette époque à environ 50 milliards d'euros.

comportent un risque opérationnel, endogène en ce sens qu'elle se manifeste au sein de l'entité.

Le système de paiement qui est une procédure permettant l'exécution à titre habituel, par compensation ou non, de paiement ne déroge pas à la règle. En effet, les systèmes de paiement de l'UEMOA ont connu une profonde mutation à la suite de la réforme initiée depuis 1999 par la BCEAO en vue d'accélérer le processus d'intégration économique régionale, de moderniser le système financier et d'amélioration le cadre de la politique monétaire.

Cette réforme procède de la volonté de l'Institution monétaire qui est la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) de parvenir à :

- l'automatisation poussée du circuit de règlement des transactions ;
- la minimisation des risques liés aux opérations financières ;
- la réduction des coûts des transactions ;
- un plus grand accès des populations au système bancaire et au service de paiement.

Les efforts consentis dans ce cadre ont permis de mettre en place les infrastructures ci-après :

- un Système de Transfert Automatisé et de Règlement dans l'UEMOA (STAR-UEMOA) ;
- un Système Interbancaire de Compensation Automatisé dans l'UEMOA (SICA-UEMOA) ;
- un Système Interbancaire de Paiement par carte à l'échelle de l'union : GIM-UEMOA.

Ces systèmes ont connu un début d'application entre 2004 et 2007 et sont soutenus par un cadre juridique et réglementaire ainsi qu'un réseau de télécommunication approprié et un dispositif de centralisation des incidents de paiements, visant à garantir le bon fonctionnement de ceux-ci.

La BCEAO, maître d'ouvrage délégué de ce vaste chantier de réformes a pris des mesures de protection des parties prenantes notamment des banques, mais le métier de banque reste indissociable du risque opérationnel, bien que sa survenance soit imputable la plupart du temps à une carence du dispositif de contrôle interne. A côté des risques opérationnels

afférents aux systèmes de paiement subsistent des risques liés aux supports de ces systèmes à savoir les chèques, les virements, les effets de commerce etc.

L'impact d'un risque non maîtrisé lié aux systèmes de paiement et leurs supports peut dès lors être désastreux pour la banque et ses partenaires. C'est pourquoi il est indispensable au top management d'une banque d'avoir la culture de la gestion des risques, caractérisé par l'existence d'un comité de pilotage des risques permettant de cibler, d'évaluer, d'organiser et de maîtriser les risques opérationnels, et particulièrement ceux liés au système de paiement.

S'agissant de la Compagnie Bancaire de l'Afrique Occidentale (CBAO) du Groupe Attijariwafa Banque, premier réseau bancaire du Sénégal, la gestion des risques opérationnels liés au système de paiement est d'autant cruciale que leur survenance peut entraîner d'importantes pertes pécuniaires et mettre en cause la survie de la banque.

Ainsi selon le journaliste BAMBA (2012) du quotidien sénégalais "Libération", près de 152 millions de FCFA ont été détournés du compte d'un client bien connu du monde du sport. C'est la somme qui a été frauduleusement retirée du compte bancaire d'une société dirigée par une figure du monde sportif. L'opération frauduleuse qui a eu lieu à la CBAO aurait, motivé la mise aux arrêts, du Fondé de Pouvoir à la CBAO Siège, M.D., gardé à vue dans les locaux de la Section de recherches (Sr) de Dakar de la gendarmerie.

Les enquêteurs sont convaincus que c'est une affaire qui est grosse de complicité interne car l'argent a été pompé à coups de chèques…retirés du circuit monétaire. C'est pourquoi plusieurs caissiers ont été entendus. La source informe que bientôt ce sera au tour du grand boss de cette banque. Il a, d'ailleurs, été contacté par les gendarmes pour être auditionné. La victime de cette opération a été ahurie de constater que des retraits d'un montant global de cent cinquante deux millions de francs CFA ont été opérés dans le compte de sa société ouvert dans cette banque.

Face à ce problèmes il y a eu des constats au nombre desquels nous pouvons citer :

- absence de dispositifs de sécurité fiables ;
- absence d'un contrôle interne véritable ;
- cartographie des risques non mis à jour ;
- non maitrise des techniques liées aux systèmes de paiement ;

- non suivi du contrôle interbancaire ;
- non mise en application des mesures édictées par la BCEAO ;
- absence de séparation de fonction dans la gestion du système de paiement ;
- absence de transparence dans la gestion des comptes.

Les conséquences de telles anomalies constatées sont énormes :

- face à ce scandale, plusieurs clients ont fermé leur compte ;
- image de marque de la CBAO ternie ;
- démission de certains cadres vers d'autres banques ;
- affaires connue du monde entier à travers le web ;

Il est primordial pour la CBAO de tenir compte de la dimension des risques opérationnels liés aux systèmes de paiement à travers une démarche logique et cohérente qui permettra de constituer une base de connaissance globale de ces risques, de déterminer les modalités de leur gestion par la mise en place d'un dispositif de contrôle interne efficace et de mobiliser l'ensemble du personnel sur le plan d'action en vue d'améliorer la gestion actuelle.

Au regard de l'immensité de la tâche, on se pose la question de savoir : « Quelle piste faut-il explorer pour une gestion efficace des risques opérationnels liés aux systèmes de paiement ? ».

Les propositions de solutions sont énumérées ci-après :

- rechercher les meilleures pratiques en matière de gestion de ces risques ;
- concevoir la cartographie des risques opérationnels liés aux systèmes de paiement à la CBAO ;
- définir, cerner et expliquer en termes généraux les risques afférents à l'utilisation des systèmes de paiements
- encourager les institutions financières, y compris les membres actuels et futurs de la CBAO, à mettre en œuvre leur propre programme de gestion du risque pour l'utilisation des systèmes appartenant à la CBAO et exploités par elle ;
- analyser le dispositif actuel de gestion des risques opérationnels en vue d'apporter une solution à d'éventuelles insuffisances.

La dernière solution paraît beaucoup plus cohérente car l'analyse et le diagnostic sont un préalable à toute action corrective. Bien plus, le risque opérationnel recouvrant les erreurs humaines, les fraudes et malveillance, les défaillances des systèmes d'information, les problèmes liés à la gestion du personnel, les litiges commerciaux, les accidents, les incendies, les catastrophes naturelles etc., a un champ d'application qui semble tellement large qu'on ne peut en apercevoir d'emblée tous les contours. Il faut nécessairement une gestion méthodique et proactive permettant d'avoir une meilleure connaissance de ces risques, de mettre en place des processus de vérification, ainsi que des stratégies susceptibles de les atténuer, voire les maîtriser.

Au regard de ce qui précède, les questions de recherche que nous nous posons sont les suivantes :

- le dispositif de gestion des risques opérationnels liés aux systèmes de paiement mis en place à la CBAO est-t-il en adéquation avec les défis que suscitent ces risques ?
- quelle est la démarche pour identifier et évaluer les risques opérationnels liés aux systèmes de paiement ?
- le contrôle interne existant à la CBAO couvre t-il globalement ces risques ?
- quel dispositif cible en matière de contrôle interne faut il mettre en place pour une meilleure gestion de ces risques ?
- quel dispositif de sécurité mettre en place pour chaque outil du système de paiement ?
- quel contrôle de prévention adopter ?

C'est la recherche de réponses à ces interrogations qui a suscité notre choix pour le thème : « **Analyse de la gestion des risques opérationnels liés aux systèmes de paiement dans une banque commerciale de l'UEMOA, cas de la CBAO** ».

L'objectif principal de cette étude est d'analyser et d'évaluer les risques liés à la gestion des systèmes de paiement de la CBAO.

Les objectifs spécifiques qui y découlent sont :

- identifier le processus d'émission des ordres de paiement dans les différents systèmes de paiement;
- identifier les outils (moyens de paiement) utilisés dans les systèmes de paiement;

- identifier les risques liés aux outils et aux systèmes de paiement ;
- évaluer le dispositif de maîtrise des risques mis en place afin de juger de son efficacité ;
- faire des recommandations.

L'approche par les risques est la mieux adaptée pour notre étude. Celle-ci dégage donc les centres d'intérêt suivants :

Pour la CBAO

Permettre à la banque de se faire une opinion beaucoup plus réaliste des risques auxquels elle est exposée, singulièrement les risques opérationnels liés aux systèmes de paiement. L'analyse de la gestion de ces risques permettra aux responsables de réorienter leur dispositif de sécurité afin de pérenniser les activités de la banque.

Pour nous-mêmes

Elle va améliorer sensiblement nos connaissances en matière de risques bancaires et particulièrement les risques opérationnels liés au système de paiement.

Notre étude sera organisée comme suit :

- la première partie portera sur le cadre théorique basé sur la revue de littérature où nous présenterons la notion de risque opérationnel, notamment les risques liés au système de paiement, la sécurité des cartes bancaires, la méthodologie de recherche et de recueil des données ;
- la deuxième partie consistera à la description de l'entreprise (Historique, Mission, Objectifs) la gestion des risques liés au système de paiement, l'analyse de l'utilisation de la carte bancaire et les recommandations.

PREMIERE PARTIE : CADRE THEORIQUE

INTRODUCTION PREMIERE PARTIE

Selon Lamarque (2003 : 65), la banque est souvent présentée comme un portefeuille de risques. Ces derniers sont une dimension inévitable et naturelle compte tenu des produits proposés et de la matière manipulée : l'argent.

Leur conséquence principale est de provoquer une perte significative pour l'établissement, soit au travers d'un ralentissement de l'activité voire d'une diminution du Produit Net Bancaire (PNB), soit au travers d'une augmentation des charges à savoir les coûts de réparation, de maintenance, de dédommagement, les sanctions financières ou des provisions. Toutes ces charges aboutissent *in fine* à une altération dangereuse des fonds propres, conduisant à la faillite de l'établissement et pouvant remettre en cause la stabilité du système bancaire dans son ensemble.

La modernisation des systèmes de paiement nécessite la mise en place d'un dispositif complémentaire de sécurisation desdits systèmes qui renforce notamment ses bases juridiques et financières. Ce dispositif complémentaire doit s 'attacher : d'une part, à la sécurisation des paiements électroniques par la reconnaissance dans la zone UEMOA de la preuve électronique relativement à tous les instruments et procédés de paiement électronique, aussi bien ceux déjà existants que ceux à venir; d'autre part, à la sécurisation des transactions financières en permettant aux participants du système de paiement de garantir leurs transactions par la réglementation de la cession temporaire de titres. L'objectif visé consiste à donner une assise juridique suffisante à la cession temporaire des titres, en prévenant le risque de requalification juridique en un autre type d'opération et la remise en cause des transactions du fait du droit des procédures d'apurement du passif et ce, en mettant en place un dispositif fiscal et comptable qui tienne compte de sa spécificité. Autrement dit, il est question de conférer à ce mode de financement une protection juridique de haut niveau pour assurer la sécurité des transactions.

Cette première partie traitera des points ci-après :

- les systèmes de paiements
- la notion de risque opérationnel, notamment les risques liés au système de paiement,
- la méthodologie de recherche et de recueil des données

CHAPITRE 1: LES SYSTEMES DE PAIEMENT

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initié un important projet de modernisation des systèmes de paiement des Etats membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA). La mise en œuvre de ce projet requiert la mise en place d'une nouvelle infrastructure dont la sécurité technique doit aller de pair avec sa sécurité juridique aux plans légal, réglementaire et conventionnel. La réponse aux multiples exigences de sécurité nécessite la modernisation du cadre juridique actuel par l'adoption de nouveaux textes plus appropriés, l'abrogation des textes inadéquats ou l'amélioration des textes insuffisants. C'est la raison pour laquelle, il est apparu opportun de conférer une meilleure lisibilité aux missions de la BCEAO en matière de systèmes de paiement en vue de fonder le pouvoir réglementaire qu'elle sera amenée à exercer dans le cadre de ses interventions au titre de la gestion et du contrôle des systèmes.

1.1 Notion de Systèmes de paiement

Les systèmes de paiement modernes et efficaces qui assurent la célérité des transactions financières et commerciales dans un environnement technique et juridique sécurisé sont une réponse à l'accélération des mouvements de capitaux et la globalisation de l'économie mondiale consécutive aux innovations technologiques, notamment dans le domaine de l'information et des télécommunications. Fortes de cette exigence, les autorités monétaires ne ménagent pas d'effort pour l'amélioration des systèmes de paiement existant ; c'est bien le cas dans l'espace UEMOA. Il est donc important d'avoir une bonne connaissance de la notion de systèmes de paiement.

1.1.1 Définition

Selon Kauffman (2008 : 124), les moyens de paiement sont des infrastructures destinées à traiter, au niveau des banques, les paiements en monnaie scripturale – de gros ou de détail – associés aux opérations entre agents économiques. Ces systèmes sont traditionnellement organisés sur une base nationale ou régionale (dans le cadre d'une union monétaire), la banque centrale en étant généralement l'opérateur et la clé de voûte.

Dans une économie monétaire moderne, l'essentiel des paiements s'effectue en monnaie scripturale. Celle-ci est gérée par les banques et est mobilisable par des instruments tels que les cartes bancaires, les virements, les chèques etc.

Selon le dictionnaire, un « **système de paiement** » est un « système constitué d'un ensemble d'instruments, de procédures bancaires et de systèmes interbancaires de transfert de fonds, destiné à assurer la circulation de la monnaie».

L'expression «**système de paiement** » peut désigner à la fois un système, tel que défini précédemment, ou, au niveau national, l'ensemble constitué par les instruments de paiement, les infrastructures, les établissements, les conventions, les lois, etc., permettant le transfert des fonds.

1.1.2 Les acteurs des systèmes de paiement

Comme il ressort de leur définition, les systèmes de paiement regroupent l'ensemble des établissements, des procédures et des moyens permettant des transferts de fonds entre les différents agents économiques et aboutissant au règlement de leurs opérations (dettes-créances-acquisitions-cessions…). Ces systèmes mettent en relation directe la banque centrale, les établissements financiers, le trésor public de l'Etat ou des Etats dans un système régional et les services financiers de la poste.

Les acteurs sont donc l'ensemble des structures qui participent aux systèmes mais également, celles qui se chargent de les gérer au quotidien et les organes de contrôle et de surveillance.

1.1.2.1 Les participants aux systèmes de paiement

Ils sont globalement au nombre de quatre :

1.1.2.1.1 La banque centrale

De l'avis de Mishkin (2010 : 504), la banque centrale est l'autorité publique chargée de contrôler le financement de l'économie en assurant l'émission des billets de banque et en octroyant des crédits aux banques commerciales dans le cadre de sa politique de:

- surveillance et de gestion des systèmes de paiement liés en particulier à la compensation des chèques et des virements interbancaires ;
- surveillance de la solvabilité du système bancaire et financier.

Plus précisément, une banque centrale joue généralement le rôle de prêteur en dernier ressort ; elle prête des liquidités aux banques secondaires par la politique de refinancement, supervise et règlemente l'activité bancaire, facilite le fonctionnement des systèmes de paiement et régule la masse monétaire et les taux d'intérêt pour atteindre les

objectifs macroéconomiques relatifs à la croissance, à l'inflation, au chômage, au taux de change et à la balance des paiements.

1.1.2.1.2 Les établissements de crédit

Les établissements de crédits regroupent les banques, les établissements financiers et toute autre personne morale qui effectue à titre de profession habituelle les opérations de banque ainsi que des opérations connexes.

Les opérations de banque étant la réception des dépôts du public, la distribution de crédit, la mise à disposition et la gestion des moyens de paiement ; les activités connexes sont liées aux opérations de change, aux opérations sur valeurs mobilières, le conseil en matière de gestion de patrimoine, le conseil en matière de gestion financière, l'ingénierie financière…Coussergues (2007 : 6).

1.1.2.1.3 Le Trésor Public

Vallet (2003 : 31) définit le trésor public comme l'institution de l'état qui effectue les opérations d'exécution des dépenses et de collecte des recettes autorisées par la loi de finances. Il est bon de savoir que le mode de fonctionnement du trésor public peut être différent d'un état à un autre.

Pour ce qui concerne les systèmes de paiement dans la zone UEMOA, la banque centrale représente les trésors publics de chaque Etat membre.

1.1.2.1.4 Les services financiers de la poste

Les services financiers de la poste sont des institutions financières appartenant aux services nationaux de postes. Elles émettent des chèques postaux pour leurs clients.

Ces institutions ont connu des restructurations dans leur ensemble ; en France particulièrement l'ex CCP est devenue la Poste finance et elle offre des services financiers.

1.1.2.2 Les gestionnaires des systèmes

Les gestionnaires des systèmes de paiement ou de règlement et de livraison d'instruments financiers sont des entités responsables de l'exploitation dudit système. Ce sont en général les banques centrales et/ou des sociétés de gestion dont les actionnaires sont des établissements de crédit.

1.1.2.3 Les organes de contrôle et de surveillance

Le dysfonctionnement des systèmes de paiement pourrait avoir un impact majeur sur la stabilité du système financier. En outre, la sécurité des moyens et des systèmes de paiement est essentielle au maintien de la confiance du public dans la monnaie. Il est donc important que les acteurs du système financier soient soumis à un contrôle prudentiel et les systèmes de paiement à une surveillance.

En France, tous les établissements de crédit et institutions financières sont supervisés par la commission bancaire, c'est aussi le cas de la zone UEMOA qui est, du reste, la transcription systématique du modèle français. La Banque de France est chargée par le législateur (Article L 141-4 du code monétaire et financier) dans le cadre des missions du système européen des banques centrales, de la surveillance des moyens et des systèmes de paiement. Il en est de même pour la BCEAO dans l'espace UEMOA.

1.1.3 Les différents types de systèmes de paiement

Selon Sardi (2002 :935), il convient, dans le système de paiement de distinguer les opérations à règlement brut des opérations de règlement net.

1.1.3.1 Les systèmes à paiement brut

Les systèmes de paiements bruts sont nommés communément RTGS (Real Time Gross Settlement). Les ordres sont traités un à un, sans compensation, à mesure de leur arrivée, avec exécution immédiate de tout paiement. Ils sont irrévocables et inconditionnels. Les règlements sont effectués en monnaie de banque centrale.

La condition pour que s'effectue un paiement est la disponibilité des fonds ou que le compte du donneur d'ordre soit assorti d'une possibilité de découvert. Ceci exige un système de prêts interjournaliers ou » ***intradays*** » pour faire face aux découverts occasionnels en cours de journée. Ce circuit de paiement de gros montant est réputé pour sa célérité, sa facilitation des échanges interbancaires en temps réel. Il est utilisé dans les opérations de bourse, notamment les transactions sur les valeurs mobilières.

1.1.3.2 Les systèmes de paiement net

Les systèmes à règlement net enregistrent les ordres de paiement échangés durant la journée. En fin de journée, ou plusieurs fois par jour, la compensation intervient et le

solde net est réglé. L'échange précède donc le règlement. On donne ainsi à chaque participant la possibilité d'être à découvert en cours de journée.

Ce système traite des opérations de masse ou de petits montants par le canal du système interbancaire de télé-compensation, qui a remplacé dans bon nombre de système, les chambres de compensation jugées moins rapides et coûteuses.

1.1.4 La nomenclature des systèmes de paiement dans l'UEMOA

L'UEMOA a été créée par le traité signé à Dakar, le 10 janvier 1994 par les chefs d'Etats et de Gouvernements des sept pays de l'Afrique de l'ouest ayant en commun l'usage d'une même monnaie, le Franc CFA.

Ces pays, à savoir le Bénin, le Burkina Faso, la Côte d'Ivoire, le Mali, le Niger, le Sénégal et le Togo ont ratifié le traité qui est par la suite entré en vigueur le 1er Août 1994. Plus tard, le 02 Mai 1997, la Guinée Bissau est devenu le 8ème Etat membre de l'Union.

L'UEMOA compte en son sein deux institutions financières spécialisées que sont la BOAD (Banque Ouest Africaine de Développement) et la BCEAO. Cette dernière est chargée de réguler le fonctionnement du système bancaire et financier dans l'Union.

Grâce à une coopération régionale de cette nature (UEMOA, CEMAC…), les économies africaines peuvent surmonter le handicap de leurs tailles relativement petites et réaliser des économies d'échelle puisqu'elles ont accès à de plus grands marchés. Les obligations résultant de l'appartenance à certaines de ces organisations permettent plus facilement à chaque pays de continuer d'avancer dans la réforme des lois, de l'appareil de règlement, de rationaliser les systèmes de paiement et d'assouplir les restrictions aux transactions en capitaux et aux flux d'investissement, ainsi que de développer des infrastructures communes.

C'est bien le cas dans l'espace UEMOA où la réforme des systèmes de paiement se traduit par la mise en place de nouveaux circuits automatisés et la dématérialisation des échanges et des règlements interbancaires. D'après le rapport de la BCEAO sur les Systèmes de paiement dans l'UEMOA (2007 : 14), à ce jour les circuits de paiement concernent essentiellement les réseaux intrabancaires, le Système Interbancaire de Compensation Automatisée (SICA-UEMOA), le Système de Transfert Automatisé et de Règlement (STAR-UEMOA) pour les paiements de grande valeur et les réseaux de correspondant internationaux à travers SWIFT (Society for Worldwide Interbank Financial Telecommunication).

Pour les paiements avec les cartes bancaires, il a été mis en place une structure technique, le Centre de Traitement Monétique Interbancaire de l'UEMOA (CTMI-UEMOA) connu désormais sous l'appellation de Groupement Interbancaire Monétique de l'UEMOA (GIM-UEMOA).

1.1.4.1 Réseaux intra bancaires pour les groupes

Les réseaux intra bancaires sont utilisés pour les règlements des valeurs pour lesquelles le débiteur et le créancier sont domiciliés dans le même groupe bancaire.

Le système intra bancaire d'échange et de compensation correspond donc aux activités et moyens mis en œuvre au niveau des groupes pour assurer des fonctions analogues à celles du système interbancaire d'échange et de compensation géré par la banque centrale, mais en utilisant des moyens techniques propres à des établissements impliqués dans l'échange.

Ce système est envisageable exclusivement pour les flux d'échange bilatéraux, internes au groupe.

1.1.4.2 Le Système de Transfert Automatisé et de Règlement (STAR)

STAR-UEMOA est le premier système régional de règlement conçu pour les virements interbancaires de gros montants et dans lequel chaque transaction est réglée sur une base brut et en temps réel.

Il est opérationnel depuis le 25 juin 2004 et fonctionne à la satisfaction de l'ensemble des participants.

1.1.4.2.1 Caractéristiques du STAR-UEMOA

Les caractéristiques sont pour l'essentiel en rapport avec les conditions de participation au système et les différents types d'opérations qui y sont effectuées.

Les participants éligibles au système sont : la BCEAO, les banques et établissement financiers, le dépositaire central banque de règlement de la Bourse Régionale de Valeurs Mobilières (BRVM), les sociétés de gestion et d'intermédiation de la BRVM, le CTMI-UEMOA et toute autre structure agréée par la BCEAO.

Par ailleurs, la participation à STAR nécessite le strict respect des règles de fonctionnement du système.

Le mode de participation est défini comme suit :

- la participation directe, où le participant est raccordé au système depuis une plate forme installée dans ses locaux et gère lui-même l'émission de ses ordres dans le système et le suivi de sa position ;
- la participation indirecte, où le participant accède au système via un service bureau installé dans les locaux de l'Agence Principale de la BCEAO.

STAR-UEMOA traite principalement les opérations ci-après :

- les virements, pour compte propre de l'établissement donneur d'ordre ou pour compte de sa clientèle, pour lesquels cet établissement est désireux d'obtenir la finalité en temps réel ;
- le règlement des échanges de titres conservés à la banque centrale sur le marché secondaire soit pour compte propre des banques, soit pour compte de leurs clients ;
- les ordres des participants à STAR-UEMOA à destination des établissements non éligibles au système, qui sont débités dans STAR et reçu par le participant BCEAO, qui les impute au système de gestion des comptes courants ;
- les opérations traitées par la banque centrale, à savoir, la politique monétaire, le refinancement, le marché primaire de titres de créances publiques, les opérations fiduciaires aux guichets de la BCEAO, ou par son intermédiaire (transferts internationaux en devises) passent par le participant BCEAO pour la couverture en franc CFA dans STAR-UEMOA ;
- les retraits et dépôts fiduciaires dans l'ensemble des agences principales ;
- le règlement des soldes de compensation, également réalisé au niveau national selon les règles de calcul décrites dans la convention de compensation.

1.1.4.2.2 Fonctionnement du STAR-UEMOA

La transmission des instructions de paiement sur STAR obéit aux principes ci-après :

- l'irrévocabilité de la transaction ;
- le traitement des ordres suivants les niveaux de priorité et l'ordre d'arrivée ;
- le contrôle automatique de la provision dans le compte règlement du participant donneur d'ordre ;
- l'imputation immédiate des opérations dans le compte de règlement des participants concernés.

L'irrévocahilité de la transaction s'entend par l'engagement irrévocable de l'émetteur de l'instruction à régler au destinataire de l'opération le montant convenu dès l'instant où son ordre a été transmis, reçu et accepté par STAR-UEMOA. Toutefois, en cas d'erreur, la

BCEAO dispose en tant qu'opérateur du système, de l'habilitation technique nécessaire pour l'annulation des instructions de paiement restées en file d'attente.

A la réception de l'instruction de paiement, le système vérifie l'existence de la provision au compte de règlement du participant et crédite le compte du bénéficiaire par le débit du compte de règlement de l'émetteur.

Le transfert de propriété de fonds entre le participant émetteur et le participant récepteur devient alors irrévocable et inconditionnel. En cas d'insuffisance de provision, l'opération est placée en file d'attente et traitée selon les règles de gestion des files d'attente et des liquidités pour une imputation ultérieure lorsque des fonds suffisants sont apportés au compte de l'émetteur.

Les ordres d'attente sont gérés selon la méthode FIFO en tenant compte du niveau de priorité d'exécution défini par le participant qui est tenu de définir un niveau de priorité pour chacune de leurs opérations transmises à STAR-UEMOA.

Il existe deux niveaux de priorité d'importance graduelle :

- le niveau de priorité « Normale» est le niveau de priorité par défaut de toute opération transmise par un participant sans indication ;
- le niveau de priorité « Urgent » qui définit une priorité plus élevée ; toute opération transmise avec ce niveau est présentée au règlement avant les opérations de niveau « Normal » qui se trouvaient déjà en file d'attente du participant.

Les niveaux de priorité associés aux opérations en file d'attente peuvent être modifiés par le participant en vue de prévenir tout risque de blocage du système. Par ailleurs, il existe un troisième niveau de priorité supérieur mais à l'usage exclusif de la BCEAO.

En fin de journée, les instructions de paiement qui n'ont pu être exécutées pour défaut de provision sont rejetées par STAR-UEMOA.

1.1.4.2.3 Architecture du STAR-UEMOA

L'architecture peut être définie comme l'option technique la mieux adaptée aux objectifs opérationnels et commerciaux du système, elle dépend des technologies disponibles et des besoins des clients qui ont des ordres de priorité variables.

Deux domaines technologiques sont particulièrement concernés :

- le réseau des télécommunications pour assurer la transmission des ordres ;

- le traitement des données pour effectuer les opérations de compensation et de règlement dans les meilleures conditions de coût, de rapidité et de sécurité (degré d'informatisation du réseau bancaire).

L'architecture de STAR-UEMOA est marquée par les caractéristiques suivantes :

- un système central localisé au siège de la BCEAO à Dakar ;
- les participants directs sont connectés au système central via le réseau SWIFT pour l'envoi et la réception des messages ou via le réseau VSAT de la BCEAO ;
- chaque agence principale de la BCEAO dispose de postes de travail pour procéder à la supervision du système au niveau national et des postes de travail spécifiques pour participer aux échanges ;
- le siège de la banque centrale assure la gestion opérationnelle et technique centralisée du système ;
- les règlements des soldes de compensation des paiements de masse et des opérations de la BRVM à travers le Dépositaire Central Banque de Règlement (localisé à Abidjan) sont effectués par STAR-UEMOA. De même, les soldes des opérations monétiques régionales sont réglés dans ce système depuis le 15 juin 2005.

1.1.4.3 Le Système Interbancaire de Compensation Automatisé de l'UEMOA

SICA-UEMOA est un outil automatisé d'échange et de règlement des opérations de paiement de petits montants entre les établissements participants au niveau national et régional.

1.1.4.3.1 Caractéristiques de SICA-UEMOA

Les caractéristiques ont trait aux conditions de participation et aux conditions relatives aux opérations admises par le système.

Les seuls participants agréés sont : la BCEAO, les hanques, le trésor public et les services financiers de la poste.

La participation à SICA-UEMOA requiert le strict respect des engagements ci-après :

- être titulaire d'un compte de règlement ouvert dans les livres de la BCEAO et disposant d'effets mobilisables dont la valeur équivaut au solde débiteur maximum de compensation ;

- le respect des règles interbancaires d'échange des chèques et autres effets de commerce ;
- le respect du format, des règles d'échange et les normes techniques de SICA-UEMOA, décrites dans les manuels techniques ;
- l'acceptation du support électronique comme fondement de règlement.

Le mode de transmission des fichiers au système central détermine le mode de participation à SICA-UEMOA. Il existe actuellement deux modes de participation :

- la participation directe : le participant transmet directement ses remises à la banque centrale ;
- la participation indirecte : ce mode de participation permet au participant d'utiliser les services techniques d'un et d'un seul participant direct afin de présenter ses remises au système.

Seuls les instruments scripturaux de paiement en vigueur dans les états membres de l'UEMOA (le chèque, la lettre de change, le billet à ordre, les ordres de virement, les avis de prélèvement) libellés en FCFA sont admises en compensation. Un montant maximal de cinquante millions de FCFA est fixé pour les virements présentés à SICA-UEMOA. Au-delà de ce montant, le participant est tenu d'utiliser STAR-UEMOA.

Les valeurs nationales, sur place ou déplacées peuvent être présentées à tous les points d'accès à la compense. Quant aux valeurs régionales, elles peuvent être uniquement présentées à la compensation dans une Agence Principale de la BCEAO.

1.1.4.3.2 Fonctionnement de SICA-UEMOA

Avec ce nouveau système de compensation, les banques peuvent depuis leurs locaux transmettre des fichiers électroniques de leurs opérations sur chèques, virements, lettre de change et billet à ordre, en compensation et ne plus se déplacer dans les locaux de la BCEAO comme auparavant.

Les calculs des soldes de compensation se font sur la base des présentations électroniques, avec en appui l'échange d'images scannées des valeurs ayant comme support le papier.

Le traitement et la comptabilisation de compensation sont effectués uniquement à partir des fichiers de remise numériques représentant les opérations des participants présentées en compensation.

Les fichiers sont constitués par les établissements participants ou par un tiers, sous leur responsabilité, selon les normes et règles de sécurité figurant dans le manuel technique. Ils sont transmis au système de compensation par une liaison informatique ou des supports physiques (disquettes ou CD-ROM) remis et lus au guichet du point d'accès à la compensation selon les normes indiquées dans le manuel technique intitulé «Interface participant-caractéristiques techniques ».

Le système de compensation vérifie la validité technique des fichiers et de leur contenu et peut rejeter des remises, des lots ou des enregistrements pour non-conformité technique et envoie des comptes rendus aux participants remettants.

Par ailleurs, un participant peut, selon les règles définies dans les manuels techniques, rejeter ou annuler une opération.

En termes d'organisation de la journée de compensation, on distingue deux profils de journée à savoir, une journée à séance unique et une autre à deux séances.

La communication et la modification de la journée sont du ressort de la BCEAO.

Pendant la journée d'échanges et selon les choix de participation, le système de compensation transmet aux sièges des établissements participants ou leurs agences sises dans les points d'accès à la compensation, des informations, des copies de résultats et des statistiques.

SICA-UEMOA est un système de calcul de soldes nets multilatéraux, nationaux, d'une part, et régionaux, d'autre part.

Un délai est accordé aux établissements participants entre la transmission des soldes à régler et l'heure fixée pour le règlement effectif, afin de leur permettre de rechercher en cas de besoin, les liquidités nécessaires à la couverture de leur solde de compensation. Le règlement du solde de compensation s'effectue par imputation au compte de règlement de chaque participant dans STAR-UEMOA.

1.1.4.3.3 Architecture de SICA-UEMOA

SICA-UEMOA se compose de neuf systèmes de compensation, un système national pour chacun des huit états membres du l'UMOA et un système de compensation régional. Chaque Système de Compensation National (SCN) se compose d'un système central installé au niveau de l'agence principale et d'un ou plusieurs Points d'Accès à la

Compense (PAC). Les PAC sont des systèmes informatiques qui permettent l'échange des fichiers entre les participants et la BCEAO.

1.1.4.4 Le Système Monétique interbancaire Régional (SMIR-UEMOA)

Un système monétique est un système informatique qui permet la dématérialisation du paiement scriptural. Il se compose de matériels, avec généralement des bornes de paiement, et de logiciels permettant la gestion du paiement par la monnaie électronique.

Le support de la monnaie dématérialisée est généralement constitué par une carte de paiement électronique.

Dans le cadre de la mise en place du système interbancaire de paiement par carte de l'UEMOA, la BCEAO a un rôle de fédérateur et d'impulsion, la gestion administrative et technique du système est assurée par les banques au travers de deux structures interbancaires distinctes :

- Une structure de gouvernance, sous forme de GIE et dénommée le Groupement Interbancaire Monétique de l'Union Economique et Monétaire de l'Afrique de l'Ouest (GIM-UEMOA) ;

La banque centrale assure le contrôle des orientations stratégiques de cette structure par sa participation, en tant qu'administrateur et membre de droit du comité de direction du GIM-UEMOA.

Les objectifs principaux sont la dématérialisation des moyens de paiement, mais surtout une volonté de promouvoir l'usage de la carte de paiement à l'échelle de l'Union, de telle sorte que la carte puisse jouer un rôle d'instrument de paiement largement accepté par les commerçant et dans tous les distributeurs automatiques de billets de banque de la région.

1.1.4.5 Le Réseau SWIFT

SWIFT est une coopérative bancaire détenue par des membres par l'intermédiaire de laquelle le secteur financier effectue ses transactions financières avec rapidité, assurance et en toute confiance. Autrement dit, SWIFT est un réseau interbancaire qui offre une palette de services extrêmement diversifiés : transferts de compte à compte, opération de devises ou titres, recouvrement

SWIFT a un double rôle :

- mettre à disposition une plate forme, les produits et les services de communication interne permettant aux utilisateurs (clients) de se mettre en relation et d'échanger des informations financières en toute sécurité et fiabilité ;
- agir comme un catalyseur qui rassemble la communauté financière pour travailler en collaboration, déterminer les pratiques du marché, définir ses standards et envisager des solutions aux questions d'intérêt commun.

L'intérêt de SWIFT est d'assurer la non répudiation des échanges : aucun tiers ne peut nier avoir effectué une transaction. SWIFT réalise l'équivalent d'un acte notarial sur l'ensemble des transactions effectuées et ce, quel qu'en soit le montant. Ceci naturellement afin de protéger les participants. Si une banque a payé à une autre banque (lors des mécanismes de compensation par exemple), la banque payeuse exige la garantie du reçu de ce paiement.

SWIFT garantit l'intégrité et l'archivage de tous les reçus qui sont décryptés au sein des serveurs d'archivage du système. Il permet à ses clients d'automatiser et de standardiser les transactions financières afin de réduire les coûts, de minimiser le risque opérationnel et d'éliminer les erreurs relatives aux transactions (Thunis, 1996 :148).

Les ordres SWIFT font l'objet d'une normalisation poussée afin d'automatiser au maximum leur traitement, et ainsi les exécuter dans les meilleurs délais. Les données classiques d'un virement bancaire à savoir : coordonnées bancaires de l'émetteur et du récepteur, un libellé de motif et des zones de service (commissions, type de message, etc.), sont rigoureusement codifiées. Les banques y sont identifiées par leur code BIC, que SWIFT gère, c'est pour cette raison que le code BIC est aussi appelé code SWIFT.

SWIFT a été crée en 1977 pour remplacer le réseau Télex, jugé trop lent et pas assez fiable. Son siège social est situé en Belgique et il possède des bureaux dans les principaux centres financiers mondiaux. Plus de 9 000 organismes bancaires, établissements financiers et clients d'entreprises dans 209 pays font confiance à SWIFT au quotidien pour échanger des millions de messages financiers standardisés.

Il faudra cependant retenir que SWIFT est juste un dispositif de support pour les systèmes de paiement STAR et SICA car c'est à travers ce réseau que les messages liés aux transactions sont émis.

1.1.5 Les moyens de paiement

Presque toutes les opérations des activités bancaires génèrent des flux de règlement qui sont pilotés par la trésorerie en temps réel via des systèmes de règlement variés.

Les moyens de paiement sont donc des supports financiers, mais aussi des supports de flux commercial (entre le débiteur et le créancier) ou des supports de flux juridiques (autorisation de débit du compte).

Les établissements de crédit sont les seuls habilités à la mise à disposition et à la gestion des moyens de paiement.

Les instruments de paiement usuels sont les chèques, les cartes de paiement ou de débit, le porte-monnaie électronique, les effets de commerces, les virements, les transferts (Valin, Gérard & Al, 2006 : 286).

Conclusion Chapitre1

Ce chapitre nous a permis de connaître les caractéristiques et le fonctionnement des nouveaux systèmes de paiement mise en place par la BCEAO pour moderniser les transactions dans l'Union Monétaire.

Le prochain chapitre traitera des risques liés au système de paiement.

CHAPITRE 2 : LA GESTION DES RISQUES LIES AUX SYSTEMES DE PAIEMENT

La banque est souvent présentée comme un portefeuille de risques. Ces derniers sont une dimension inévitable et naturelle compte tenu des produits proposés et de la « matière » manipulée : l'argent.

Les risques ont pour conséquence de provoquer une perte significative pour l'établissement soit au travers d'un ralentissement, soit par une augmentation des charges. Ils aboutissent *in fine* à une altération dangereuse des fonds propres conduisant à la faillite de la banque et pouvant remettre en cause la stabilité du système bancaire dans son ensemble (Lamarque, 2008 : 77).

S'agissant des systèmes de paiement, la masse des traitements et la complexité des circuits internes ou externes entrainent des risques opérationnels.

La banque doit se doter d'un dispositif et des méthodes dont le but serait de juguler ces risques pour s'assurer une compétitivité dans ce métier très concurrentiel.

Ce chapitre traitera des risques, plus particulièrement des risques liés aux systèmes de paiement et des dispositifs de sécurité afférents.

2.1 Notion de risque

Dans son lexique « **Les mots de l'audit** », l'IFACI définit le risque comme étant « un ensemble d'aléas susceptibles d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer autant que faire se peut la maîtrise » (in Jacques Renard, 2010 : 155). Cette définition a été complétée par celle de Dominique Vincenti (in revue Audit, n° 144) : « le risque c'est la menace qu'un événement ou une action ait un impact défavorable sur la capacité de l'entreprise à réaliser ses objectifs avec succès».

2.2 Le risque bancaire

Les domaines d'activités des banques se sont fortement étendus et les produits offerts largement étoffés. Les attentes des clients sont devenues plus élevées, les bourses ont connu des volatilités de plus grande ampleur, la pression sur le secret bancaire devient plus forte et la concurrence nationale et internationale plus vive. Pour survivre et croître, les banques doivent sans cesse augmenter la valeur ajoutée, satisfaire aux exigences

croissantes des régulateurs et des marchés, tout en minimisant en même temps les coûts et les risques.

2.2.1 Typologie des risques bancaires

Le risque bancaire peut se définir synthétiquement comme « l'incertitude temporelle d'un évènement ayant une certaine probabilité de survenir et de mettre en difficulté la banque » (Desmicht, 2004 : 239).

Selon Sardi (2002 : 39) les risques bancaires se classe en quatre catégories :

- le risque de crédit ;
- les risques de marché ;
- le risque opérationnel ;
- et les autres risques (risque de liquidité, risque de transformation, risque global de taux d'intérêt, risque de réputation, risque stratégique, risque systémique).

2.2.1.1 Le risque Opérationnel

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

Le comité de Bâle II (2003 :7) définit le risque opérationnel comme le risque direct ou indirect de perte résultant de processus internes, de personnes et de systèmes défaillants ou inadéquats, ou d'évènements externes.

King (2001) définit le risque opérationnel comme le risque qui « ne dépend pas de la façon de financer une entreprise, mais plutôt de la façon d'opérer son métier » et « le risque opérationnel est le lien entre l'activité du travail d'une entreprise et la variation du résultat du travail ».

Vanini (2002) quant à lui définit le risque opérationnel comme « le risque de déviation entre le profit associé à la production d'un service et les attentes de la planification managériale. Le risque opérationnel correspond à l'écart enregistré, positif ou négatif, par rapport au profit attendu ». Cette définition fait ressortir une dimension positive du risque opérationnel.

La particularité de ce risque est qu'il n'est pas concentré dans un secteur d'activité particulier ; il est partout présent ! Une perte de crédit peut avoir pour cause la défaillance d'un emprunteur, mais aussi une cause opérationnelle : erreur, négligence, fraude etc.

2.2.1.1.1 Typologie des risques opérationnels

Les différents types de risques opérationnels sont les suivantes :

- le risque juridique ;
- le risque de déontologie ;
- le risque règlementaire ;
- le risque de blanchiment ;
- le risque sur le patrimoine ;
- le risque comptable ;
- le risque sur les systèmes d'information ;
- le risque informatique.

2.2.1.1.2 Bâle II et les risques opérationnels

Selon Bâle II (2003 :7), le risque opérationnel se défini comme « tout risque de perte résultant de la défaillance ou de l'inadéquation des processus internes, des ressources, des systèmes ou d'évènements extérieurs ».

Est inclus dans cette définition le risque juridique, en sont exclus les risques stratégiques et de réputation.

De cette définition adaptée au secteur bancaire, et afin de mieux cerner les types d'évènement de risques concernés, sept catégories de risques ont été définies, elles même détaillées en sous catégories. Dans cette perspective, les catégories les plus concernées seraient essentiellement la fraude interne et externe suivant que l'agent agit de l'intérieur ou de l'extérieur de la banque.

La catégorie « clients, produits et pratiques commerciales» concerne notamment les cas d'atteinte à la confidentialité ou ceux de violation du secret professionnel, et dans une moindre mesure, la catégorie « pratique en matière d'emploi et de sécurité sur le lieu de travail » peut mettre en évidence tous les cas de litiges dans le domaine des ressources humaines.

Enfin, dans le cas extrême de terrorisme international tel qu'il s'est développé depuis le 11 septembre 2001, des attaques organisées ayant pour conséquence des destructions directes d'actifs seraient classifiées dans la catégorie « Dommage aux actifs corporels », voire dans la catégorie « destruction malveillante de biens » compte tenu du caractère intentionnel et de la volonté de nuire directement à certaines entreprises.

La même logique pourrait s'appliquer en cas de sabotages par rapport à la catégorie « dysfonctionnement de l'activité et des systèmes ». Mais s'il était reconnu que le délit est intentionnel, cette catégorie ne serait pas appropriée, et l'évènement de risque initial mettrait en évidence une fraude d'origine interne ou externe (Bouchet ; 2007 : 81).

2.2.2 Les risques liés aux systèmes de paiement

L'efficacité et la sécurité des systèmes de paiement constituent des éléments clés pour la stabilité d'un système financier.

D'après Valin & al. (2006 : 286), les risques liés aux systèmes de paiement regroupent les risques de règlement-livraison, les risques de contrepartie ou de liquidité, d'une part, les risques opérationnels, d'autre part, et enfin les risques liés aux transferts sur internet.

2.2.2.1 Le risque de contrepartie

Le risque de contrepartie est le risque de défaut des clients, c'est-à-dire le risque de pertes consécutives aux défauts d'un emprunteur face à ses obligations. Encore appelé risque de crédit, il est le premier risque auquel est confronté un établissement financier (Bessis, 1995 :15).

Lorsque nous rapportons ces risques aux systèmes de paiement, les clients sont les différents participants, dont la défaillance est source de préjudice.

2.2.2.2 Le risque systémique

Le risque systémique est une dérivée du risque de contrepartie. En effet, lorsqu'un participant aux systèmes de règlement est défaillant, cela se propage par contagion sur toute la place pour se transformer en risque systémique. L'ensemble des participants pourraient ainsi se trouver affectés par l'insolvabilité d'un seul.

2.2.2.3 Le risque de liquidité

Le risque de liquidité représente pour une banque la possibilité de ne pas pouvoir faire face, à un moment donné, à ses engagements ou à ses échéances par la mobilisation de ses actifs (Mathieu, 2005 : 152).

La défaillance d'un participant à un système peut être source de risque de liquidité.

2.2.2.4 Les risques de règlement-livraison

Le règlement-livraison est un système informatisé de paiement contre livraison des valeurs mobilières de la bourse, de manière simultanée, fiable et rapide dans un délai normalisé de 3 jours après la date de négociation (2 pour les opérations de gré à gré). Ce délai résulte des normes de pratiques internationales (Lehmann & Macqueron, 1995 :239).

Le règlement livraison s'appui sur un système informatisé auquel tous les intermédiaires doivent être connectés. Les opérations de règlement et de livraison s'effectuent simultanément auprès du dépositaire central banque de règlement.

Il existe un risque de défaillant de l'un ou l'autre des participants ; il s'agit soit d'un défaut de provision en titres du vendeur, soit d'un défaut de paiement de l'acheteur.

2.2.3 Les risques opérationnels liés aux systèmes de paiement

La masse des données traitées et la complexité des circuits internes ou externes entraînent forcement des risques opérationnels. Ce sont entre autres :

- les fraudes externes ;
- les détournements internes ;
- les erreurs d'imputation des ordres dans les systèmes ;
- la négligence dans le traitement des données ;
- l'usage des moyens de paiement à des fins de blanchiment ;
- la défaillance du système informatique ;
- l'insuffisance d'efficacité du système informatique ;
- le risque comptable (lié à la masse importante des opérations) ;
- le risque de perte de piste d'audit (lié au risque comptable) ;
- la perte due à des paiements non autorisés par l'établissement ou le client.

2.2.4 Les risques spécifiques liés aux transferts sur internet

Le risques sur internet sont les mêmes mais amplifiés par plusieurs facteurs :

- traitement automatisé des transferts sans qu'un gestionnaire puisse opérer un contrôle de vraisemblance de l'ordre de transfert par rapport au profil du compte ;
- clientèle plus largement cosmopolite, comprenant potentiellement une part importante de non-résidents qui pourraient être tentés de chercher à bénéficier d'une certaine opacité des opérations à travers des processus automatisés.

2.3 Dispositifs de maîtrise des risques opérationnels des SP

Ces dispositifs permettent de cerner les risques en ayant une meilleure compréhension, et en évaluant leur impact sur les activités de la banque.

La bonne mise en place de ces dispositifs ne saura se faire sans l'implication des organes dirigeants. Ceci est même un préalable afin de définir les objectifs et d'allouer les moyens nécessaires à la structure dédiée à la gestion des risques.

2.3.1 Objectifs du dispositif des SP

La finalité de la mise en œuvre 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 société ou tout du moins sa sensibilité en cas de survenance d'événements non souhaités (Jimenez, 2008 : 127).

2.3.2 Prise de connaissance des SP

De l'avis de Renard (2010 :224), il n'y a pas de méthode d'audit qui ne commence par une prise de connaissance des procédures ou des activités que l'on doit auditer.

Le fait d'imaginer qu'il soit possible de réaliser l'audit comptable et financier ou l'audit de la trésorerie d'une banque, sans rien connaitre de la comptabilité ni de la gestion de trésorerie, serait évidemment un leurre.

Sans connaître 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.

Cette prise de connaissance doit permettre d'avoir une bonne compréhension du fonctionnement des systèmes de paiement et de détecter les risques opérationnels y afférents.

2.3.3 Identification des risques

Pour Coopers & Lybrand (2000 : 59), « l'identification des risques n'est pas un exercice limité dans le temps. C'est un exercice permanent car les risques évoluent avec les changements de l'environnement interne ou externe ».

Il est donc important que dans l'identification des risques, on tienne compte des risques possibles par anticipation de l'évolution future de l'environnement interne et externe.

En effet, l'identification des risques est un processus itératif qui est souvent intégré au processus de planification. Dans la mesure où le pilotage bancaire s'inscrit dans une suite d'amélioration continue, les risques doivent être sans cesse identifiés au niveau de l'organisation dans son ensemble, mais également dans chacune de ses opérations.

Le but de l'identification est d'évaluer l'impact du risque opérationnel en l'absence de tout dispositif de contrôle interne se rapportant aux systèmes de paiement. Pour ce faire, il faut nécessairement décrire de façon précise, les différentes étapes d'émission d'ordre dans les systèmes de paiement.

Plusieurs auteurs ont élaboré des techniques d'identification des risques à savoir :

- l'identification sur les actifs créateurs de valeurs ;
- l'identification basée sur l'analyse de l'environnement ;
- l'identification basée sur les check-lists ;
- l'identification basée sur l'atteinte des objectifs ;
- l'identification par analyse historique ;
- l'identification basée sur les tâches élémentaires.

Pour notre étude, nous allons combiner les deux derniers points énumérés.

L'identification basée sur les tâches élémentaires part du principe que les activités sont à découper en plusieurs tâches élémentaires.

Pour Renard (2004 : 76), il suffit après, de se demander : « qu'est ce qui se passerait si la tâche est mal exécutée ou n'est pas du tout exécutée ? »

L'identification par analyse historique permet quant à elle de faire une analyse en se basant sur les risques opérationnels déjà survenus au sein de l'entreprise.

Pour l'identification des risques liés aux systèmes de paiement, nous ferons usage de ces deux approches.

2.3.4 Évaluation des risques

Selon Maders & Masselin (2004 : 51), une fois que les risques sont identifiés, il est nécessaire d'évaluer leur impact en cas de survenance. Cette évaluation est une

combinaison de 3 facteurs : sa probabilité d'apparition, sa gravité en cas de survenance et la durée pendant laquelle les conséquences de l'évènement ont un impact sur l'entreprise.

Pour évaluer l'exposition d'un établissement bancaire aux risques opérationnels, le comité de Bâle propose trois (03) approches, par ordre croissant de complexité et de sensibilité aux risques mais la Commission Bancaire de l'UEMOA incite à adopter la méthode la plus avancée, ce sont :

- **l'approche de l'indicateur de base (Basic Indicator Approch ou BIA)**

Le capital règlementaire en couverture du risque opérationnel est égal à 15% du revenu annuel brut moyen de l'établissement sur les trois derniers exercices. Celui-ci est défini comme la somme des intérêts créditeurs nets et autres produits d'exploitation. Il exclut les provisions, les plus ou moins values liées au portefeuille-titres, et les clients exceptionnels.

- **l'approche standard**

C'est un prolongement plus fin de la BIA en déclinant ce type de calculs par type de métier ou activité. Le capital réglementaire est ici fonction d'un pourcentage du produit brut établi à 12%, 15% ou 18% selon le niveau de risque opérationnel estimé de chaque activité.

- **l'approche avancée**

Il ne s'agit plus d'une approche unique, définie par le régulateur, mais plutôt d'un régime optionnel. Le choix de la méthode d'évaluation est laissé à la discrétion de la banque, pourvu qu'elle satisfasse aux critères qualitatifs et quantitatifs énoncés par les accords de Bâle II.

2.3.5 La cartographie des risques

Véritable inventaire des risques de l'organisation, la cartographie des risques permet d'atteindre 3 objectifs :

- inventorier, évaluer et classer les risques de l'organisation ;
- informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités ;
- permettre à la direction générale, avec l'assistance du Risk Manager, d'élaborer une politique de risque qui va s'imposer à tous :

- aux responsables opérationnels dans la mise en place de leur système de contrôle interne ;
- aux auditeurs internes pour élaborer leur plan d'audit, c'est-à-dire fixer les priorités.

Pour élaborer une cartographie des risques, il faut garder présent à l'esprit que les méthodes sont multiples, allant du plus élémentaire au plus complexe. Les différentes étapes successives sont (Renard, 2010 : 157):

- **l'élaboration d'une nomenclature de risques**

Il s'agit ici de lister toutes les natures de risques susceptibles d'être rencontrés dans l'organisation. Cette liste sera plus ou moins détaillée selon que l'on veut dresser une cartographie plus ou moins sommaire.

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

Il faudra faire une liste couvrant toutes les activités de l'organisation. Elle sera plus ou moins détaillée selon les objectifs. Cependant le bons sens recommande que chaque rubrique soit dimensionnée de telle façon qu'elle puisse faire l'objet d'une mission d'audit.

- **l'estimation de chaque risque pour chacune des fonctions/activités**

Cette estimation présentée sous la forme d'un tableau à double entrée va porter sur deux points que sont l'appréciation de l'impact du risque (gravité) et l'appréciation de la vulnérabilité estimée (probabilité d'occurrence).

Pour cette double évaluation, il faut se contenter en général d'une échelle de cotation à trois positions (faible, moyen, élevé).

- **l'appréciation globale de chaque risque dans chaque activité**

C'est le résultat du produit des deux appréciations spécifiques. On aura donc :

- Gravité x Vulnérabilité = Criticité

- **le calcul du risque spécifique de chaque activité**

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

2.3.6 Surveillance des risques

Les banques doivent mettre en œuvre, sur une base continue, un système de suivi de l'exposition aux risques opérationnels et des évènements de pertes par grands secteurs d'activité.

Outre le suivi des cas de pertes opérationnelles, l'entreprise met en place des indicateurs d'alerte avancés, ce qui permet d'identifier les sources potentielles de risques opérationnels (taux de croissance anormalement élevé, lancement de nouveaux produits, rotation des employés, rupture de transactions, pannes de système…). Ces indicateurs comportent généralement des seuils dont le dépassement déclenche la mise en œuvre d'actions préventives.

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 aux organes dirigeants. Le suivi régulier des évènements de pertes opérationnelles liées aux systèmes de paiement présente l'avantage de détecter rapidement les déficiences dans les procédures, les processus, les systèmes et les hommes. Il est alors possible de les analyser et d'y porter remède. Ce qui peut réduire significativement les pertes potentielles.

Le système de reporting doit inclure les statistiques et les analyses des évènements de perte ainsi que la sévérité des pertes.

Le contrôle régulier du risque opérationnel par la fonction risk management, traduit par des rapports, renforce l'efficacité du système de surveillance. L'audit interne doit mener des interventions régulières pour couvrir de manière adéquate le risque opérationnel (Sardi ; 2002 : 313).

2.3.7 Dispositifs de gestion des risques opérationnels des SP

Le dispositif de management des risques liés aux systèmes de paiement est :

- un processus permanent qui irrigue toute la banque;
- mis en œuvre par les acteurs intervenant dans le traitement des ordres de transfert, de virement et de compensation ;

- mis en œuvre à chaque niveau du processus de traitement des ordres afin d'obtenir une vision globale d'exposition aux risques ;
- destiné à identifier les évènements susceptibles d'affecter le processus d'émission des ordres et à gérer les risques dans le cadre de l'appétence pour le risque ;
- donné par la Direction et le Conseil d'Administration pour une assurance raisonnable (quant à la réalisation des objectifs des services en chargé de la gestion des systèmes de paiement).

2.3.7.1 Le système de contrôle des risques opérationnels des SP

Le dispositif de contrôle comprend l'ensemble des méthodes de contrôle mis en œuvre par les responsables de la banque à tous les niveaux pour maitriser le fonctionnement des systèmes de paiement.

2.3.7.2 Les méthodes de contrôle des risques opérationnels des SP

Selon l'Association Canadienne des paiements (2005 :39), le système de contrôle et d'atténuation des risques comporte plusieurs méthodes à savoir :

- déterminer le seuil approprié des montants pouvant être retirés d'un compte sur des chèques qui peuvent être en transit;
- surveiller en permanence les clients présentant un risque élevé;
- établir de saines politiques d'identification et d'acceptation des clients;
- éduquer les clients pour garantir que les effets inadmissibles ou frauduleux tirés sur leur compte sont signalés en temps opportun;
- élaborer des politiques et procédures pour aider à gérer les risques et garantir qu'elles sont intégralement conformes aux procédures opérationnelles existantes relatives à la détection et au retour en temps opportun de ces effets;
- examiner les rapports de crédit des institutions financières (actuelles et nouveaux membres), afin d'évaluer la stabilité financière des adhérents et sous-adhérents;
- établir des plans d'urgence efficaces, des systèmes de rechange (p. ex., deux systèmes d'acheminement) et des programmes exhaustifs de formation du personnel au traitement des chèques;
- adhérer aux lignes directrices de sécurité et aux procédures établies par les institutions financières et examiner les opérations afin de déceler des anomalies dans les effets papier (p. ex., signatures) ;
- garantir que les parties sont dûment authentifiées;

- faire en sorte que les appareils utilisés pour enclencher des opérations procurent une sécurité suffisante pour atténuer les possibilités d'une infraction qui mettrait en péril l'intégrité de l'appareil ou de l'information qui y est contenue;
- faire en sorte que des méthodes de substitution pour effectuer les opérations en cas de panne du système soient en place;
- assurer l'intégrité de l'émission et du traitement du code, y compris la séparation appropriée des fonctions entre l'émission de la carte et du code;
- faire en sorte que les renseignements privés et la confidentialité soient sauvegardés en faisant en sorte que seule l'information financière et d'autre information à l'appui, qui est nécessaire pour effectuer, tracer et corriger une opération soit communiquée aux autres participants impliqués dans l'opération;

2.4 Le contrôle interne des systèmes de paiement

Pour Maders & Masselin (2004 : 57), les fondamentaux du contrôle interne sont les suivants :

- politique définie, connue et appliquée ;
- préparation des fonctions ;
- réalité des informations ;
- pistes d'audit ;
- habilitations, délégations, autorisations ;
- codes d'accès informatiques ;
- manuels de procédures...

Le dispositif de contrôle interne permet de ramener le risque inhérent au niveau du risque résiduel, il consiste à diminuer la probabilité et l'impact du risque.

2.4.1 Définition du CI des SP

Selon Amblard (2003 : 121), le contrôle interne se définit comme un dispositif permanent, comportant des aspects formels et des aspects informels (ou visibles et invisibles) qui permet à une organisation de s'assurer que les décisions et comportements développés en son sein sont en cohérence avec ses finalités. Parmi les finalités, nous trouvons la réalisation et l'optimisation des opérations, la fiabilité des informations financières, la conformité aux lois et règlements en vigueur.

Le dispositif est permanent en ce que le contrôle interne n'est pas vu comme une fonction. Il ne se résume pas à l'aspect formel du contrôle (règles écrites, procédures…) mais il comprend aussi le contrôle informel ou le contrôle social.

Le comité de Bâle II a publié en septembre 1997, un document intitulé « Principes fondamentaux pour un contrôle interne efficace » et en septembre 1998 un autre document «**Framework for internal control Systems in organisations** ». Ces travaux rejoignent les réflexions menées au niveau européen dans le cadre du sous comité de surveillance bancaire de l'institut monétaire européen, qui a publié en 1997, un rapport intitulé « les systèmes de contrôle interne des établissements de crédit ».

L'une des idées directrices des réflexions menées par le comité de Bâle II et le sous comité de surveillance bancaire est que le contrôle interne n'est pas une simple procédure ou une politique appliquée à un certain moment, ni même simplement une fonction d'audit mais un système qui fonctionne en continu à tous les niveaux de l'établissement.

Selon Hamzaoui (2008 : 80), le COSO (***Committee Of Sponsoring Organizations of the Treadway Commission)*** définit le contrôle interne dans son référentiel intitulé « Internal Control-Integrated Framework » comme un processus mis en place par le conseil d'administration, les dirigeants et le personnel de l'entité, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- la réalisation et l'optimisation des opérations ;
- la fiabilité des informations financières ;
- la conformité aux lois et règlements.

Les définitions du contrôle interne sont nombreuses mais l'accord se fait sur l'essentiel, c'est-à-dire que le contrôle interne n'est pas une fonction mais plutôt un ensemble de dispositions en vue d'aider l'entreprise à atteindre ses objectifs.

2.4.2 Objectifs du contrôle interne

Le contrôle interne a les objectifs ci-après :

- sécurité des actifs ;
- qualité des informations ;
- respect des directives ;
- optimisation des ressources.

Le COSO I assignait au contrôle interne 3 catégories d'objectifs :

- les objectifs dits opérationnels (réalisation et optimisation des opérations qui se traduisent par l'amélioration des performances et la sécurité des patrimoines. L'optimisation des ressources qui passe par une utilisation économique et efficace des ressources aussi bien financières, humaines, informationnelles, matérielles que structurelles notamment les performances se mesurant en termes quantitatifs et qualitatifs) ;
- la fiabilité des informations financières ;
- la conformité aux lois et règlements en vigueur c'est-à-dire le respect de toutes les dispositions législatives, règlementaires, de toutes les dispositions internes et externes qui s'imposent à l'organisation.

Face à un environnement (économique, juridique, financier, technologique) incertain, porteur d'importants risques et suite aux scandales financiers retentissant qui ont émaillé le début des années 2000, et aux appels visant à renforcer la gouvernance des entreprises et la gestion des risques d'entreprise, le nouveau référentiel COSO II élargit le concept de contrôle interne à celui de management des risques d'entreprise (ERM) en assignant au contrôle interne un quatrième objectif ; celui de la maîtrise des risques liés à la stratégie de l'entreprise (Mandzila ; 2006 : 91).

Pour Renard (2010 : 143), le contrôle interne concourt à la réalisation d'un objectif général que l'on peut décliner en objectifs particuliers. L'objectif général c'est la continuité de l'entreprise dans le cadre de la réalisation de buts poursuivis.

Pour atteindre cet objectif général, on assigne au contrôle interne des objectifs permanents. La norme d'audit interne 2120.A1 définit les aspects sur lesquels doit porter l'évaluation du contrôle interne et qui sont donc autant d'objectifs à atteindre :

- fiabilité et intégrité de l'information financière et opérationnelle ;
- efficacité et efficience des opérations ;
- protection du patrimoine ;
- respect des lois, règlements et contrats.

Face à ses objectifs la démarche du Contrôle Interne se base essentiellement sur les points ci-après :

- appréciation des préalables
- identification des dispositifs spécifiques :
    - découper l'activité
    - identifier et évaluer les risques
    - identifier les dispositifs

- qualifier les dispositifs

- validation de la cohérence

2.4.3 Le dispositif de Contrôle Interne des SP

Selon Sardi (2002 : 952), il existe un dispositif général de contrôle interne lié aux systèmes de paiement, décliné en des dispositifs spécifiques de contrôle pour chaque activité des systèmes de paiement.

La complexité de l'activité bancaire, et les risques qui s'y attachent, rendent impérative l'existence d'un manuel de procédures dans lequel sont confinées toutes les procédures d'exécution des différentes activités. Ce principe est unanimement admis. Tous les organes de contrôle bancaire en prescrivent l'existence.

2.4.3.1 Le dispositif général de contrôle interne des SP

Le dispositif général doit s'assurer que tous les décaissements sont justifiés et autorisés, et que tous les encaissements sont promptement mis à la disposition du bénéficiaire légitime. Il doit ensuite s'assurer de l'efficacité des procédures internes pour réaliser les transferts dans les meilleures conditions de coût et de délais.

2.4.3.1.1 La sécurité des systèmes de paiements

La sécurité et l'efficacité des systèmes de paiement sont essentiellement de la responsabilité des banques centrales et ensuite de la place toute entière.

La Banque des Règlements Internationaux (BRI) pose les principes à respecter par tous les systèmes de paiement.

Dans sa publication sur les Règlements Internationaux de décembre 2009, la BRI a énuméré dix principes fondamentaux destinés à assurer la sécurité et l'efficacité des systèmes de paiement :

- sécurité juridique du système ;
- règles et procédures destinées à maîtriser les risques ;
- règlement définitif le jour même ;
- règlement en monnaie banque centrale ;
- haut degré de fiabilité opérationnelle ;
- transparence du système.

2.4.3.1.2 La sécurité informatique

Les procédures doivent prévoir un ensemble de mesures pour se prémunir contre les risques :

- le système informatique doit comporter les sécurités nécessaires, et faire l'objet d'audits réguliers ;
- les stations d'émission et de réception des messages doivent être protégées : accès limité aux personnes autorisées, codes d'accès et sécurités logiques interdisant un usage non autorisé, station de secours (back up) disponible et régulièrement testée ;
- le système doit être en mesure d'automatiser au maximum les opérations, afin d'offrir une efficacité optimale ;
- les fichiers de valeur doivent être identifiés, et comporter toutes les sécurités attachées aux valeurs ;
- les procédures doivent s'assurer que l'intégralité des opérations traitées à l'aller comme au retour.

2.4.3.1.3 Un reporting des évènements de perte

L'activité des moyens de paiement est particulièrement exposée au risque opérationnel. Il convient pour le qualifier de recenser de manière exhaustive et intégrer tous les évènements de perte et pour chacun d'eux la sévérité de la perte.

La collecte des évènements de perte poursuit deux objectifs :

- gérer le risque opérationnel en permettant de le mesurer et de mettre en place des parades face à des pertes dont la fréquence et l'impact seraient trop élevés ;
- calculer l'exigence de fonds propres pour risque opérationnel.

2.4.3.2 Les systèmes de paiement électronique

Les systèmes de règlement électronique sont articulés autour des virements et des prélèvements.

2.4.3.2.1 Les virements

Les virements doivent se faire dans le respect des procédures et méthodes ci-après :

- le traitement des virements, fréquemment automatisé, doit être fiable et rapide ;
- le virement doit être autorisé par une personne habilitée qui vérifie l'existence d'une provision sur le compte ;

- la signature du client doit être vérifiée pour éviter des paiements non autorisés ;
- en cas d'instructions téléphoniques, l'identité du donneur d'ordre doit être assurée et une confirmation par écrit obtenue pour assurer la non répudiation de l'ordre ;
- une demande de virement par un client de passage, qui règle en espèces, doit être autorisée par une personne habilitée qui effectue notamment les diligences relatives au blanchiment ;
- un virement permanent, ordonné par un client, doit être préalablement autorisé par une personne habilitée, en fonction du montant, de la situation du compte et de la qualité du client. Ensuite à chaque échéance, le système doit identifier les virements qui auraient pour conséquence de rendre un compte irrégulièrement débiteur, permettant ainsi leur blocage ;
- la différence entre la date de valeur appliquée par le système de paiement et celle appliquée aux clients doit être positive pour rémunérer la banque ;
- les commissions, frais et dates de valeur doivent être appliqués conformément aux conditions générales ou particulières dûment approuvées.

2.4.3.2.2 Les prélèvements

Au titre des prélèvements nous notons :

- les demandes de prélèvement reçus doivent être comparées aux autorisations pour s'assurer que le client les a bien autorisées, car un prélèvement non autorisé serait susceptible de mettre en jeu la responsabilité de l'établissement. C'est un contrôle qui devrait être réalisé automatiquement par le système informatique ;
- les demandes ou autorisations de prélèvement qui parviennent doivent être signées par le client, et autorisées par une personne habilitée, ceci pour les mêmes raisons que les virements permanents ;
- ces autorisations doivent être classées et conservées, car elles constituent la pièce justificative de l'instruction reçue du client (piste d'audit) ;
- les anomalies (absence d'autorisation, montant ou date non conforme, autorisation échue) doivent être résolues par une personne habilitée après un éventuel contact avec le client qui accepte ou refuse le prélèvement ;
- les domiciliations de lettres de change relevé et assimilés (LCR) doivent être préalablement autorisées par le client, au cas par cas ou dans le cadre d'une autorisation globale. Si cette autorisation n'est pas parvenue, il convient de la demander au client.

2.4.3.3 La compensation

La chambre de compensation est réduite à sa simple expression du fait de la dématérialisation des échanges qui transitent par SICA-UEMOA. Le dispositif décrit ci-après tend à prémunir la banque contre certains risques :

- les valeurs reçues aux guichets doivent être immédiatement endossées au profit de l'établissement pour éviter tout risque d'usage frauduleux en ces de perte ou de vol ;
- les valeurs doivent être protégées contre le risque de perte et de vol ;
- l'acheminement exhaustif de l'ensemble des valeurs vers le service chargé de la compensation ;
- l'encaissement des valeurs doit se faire rapidement.

2.4.3.4 L'échange de fichiers images et numériques

Les images-chèques et les fichiers numériques (effets) obéissent à certaines règles.

Les procédures doivent être aptes à assurer que :

- toutes les valeurs sont saisies, et transmises pour encaissement, dans les meilleures délais ;
- toutes les valeurs sont à rejeter le sont effectivement dans les délais impartis par le système ;
- les comptes clients sont crédités suivant les dates de valeurs spécifiées dans les conditions générales ou particulières dûment approuvées ;
- le système d'archivage garantit pendant dix ans la production de l'original du chèque ou de sa copie recto/verso.

Les procédures doivent être aptes à assurer que :

- toutes les valeurs sont imputées sans délais au débit des comptes clients ;
- les valeurs à rejeter pour insuffisance de provision ou anomalie le sont dans les délais impartis par le système ;
- en cas de rejet, les formalités légales nécessaires sont accomplies notamment en cas de chèque sans provision ;
- les dates de valeurs appliquées doivent tendre à dégager un solde positif pour rémunérer la banque.

2.4.3.5 Les cartes bancaires

Une carte de paiement est un moyen de paiement se présentant sous la forme d'une carte plastique mesurant 85,60 × 53,98 mm, équipée d'une bande magnétique et/ou puce électronique (c'est alors une carte à puce), et qui permet :

- le paiement, auprès de commerces physiques possédant un « terminal de paiement » ou virtuels sur Internet ;
- les retraits d'espèces aux distributeurs de billets.
- La carte de paiement est associée à un réseau de paiement, tel que le Groupe Carte Bleue, VISA, MasterCard, *American Express*, JCB. Une carte de paiement peut être à « débit immédiat », à débit différé ou une carte de crédit.

Les cartes bancaires, du fait de leur utilisation de plus en plus fréquente sont exposées au risque de fraudes. Le dispositif ci-après doit être adopté pour y faire face :

- le code secret de la carte et l'avis de mise à disposition doivent être adressés directement au client par le centre de traitement, sans transiter par l'établissement bancaire.
- de strictes précautions doivent entourer les cartes reçues du centre de traitement, et tenues à la disposition des clients :
- centralisation ;
- protection contre les risques de perte ou de vol ;
- justification du retrait au moyen de l'avis de mise à disposition signé et daté par le client.
- les commissions doivent être intégralement perçues à la bonne date ;
- signaler rapidement au service compétent ou à l'émetteur, les cartes déclarées perdues ou volées, par les clients pour lui permettre de faire opposition.

2.4.3.6 La sécurité des systèmes de transmission

A partir des systèmes de communication, sont émis et reçus des ordres de paiement à destination ou en provenance de l'étranger. Ce sont donc des centres névralgiques qu'il convient de protéger :

- la salle de transmission SWIFT ou autres moyens de transmission doivent avoir un accès protégé, et limité aux personnes habilitées. Ils doivent notamment être fermés en dehors des heures de travail ;
- les messages seront envoyés rapidement, car la rapidité est à l'origine du choix de ces moyens de communication. Tout retard peut avoir des conséquences

financières ou commerciales importantes, notamment les intérêts de retard pour les ordres de paiement ;

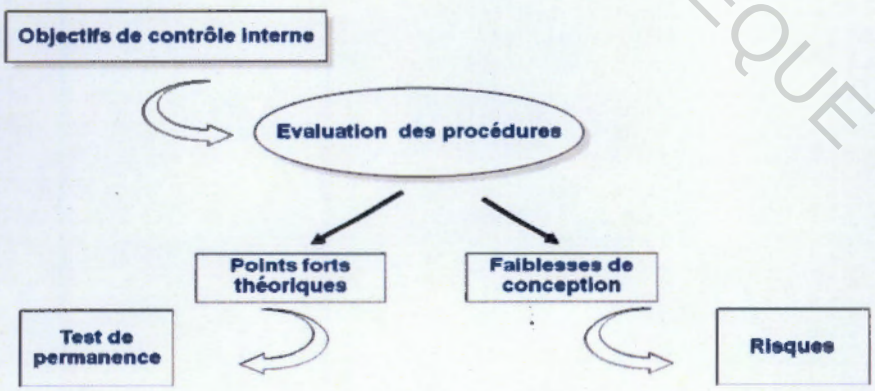
- avant d'être envoyés, les messages doivent être vérifiés pour s'assurer de l'existence et de la validité des signatures autorisées ;
- une personne habilitée vérifiera ces signatures, et apposera son visa sur le support du message avant sa transmission ;
- le dispositif de sécurité adopté doit être en mesure d'interdire l'usage frauduleux du système SWIFT ou de permettre de détecter rapidement ces usages frauduleux pour tenter de les annuler.

2.4.4 Évaluation du dispositif de Contrôle Interne

La plupart des établissements bancaires ont déjà initié leurs démarches de gestion des risques opérationnels, plus par la volonté de mieux maîtriser ces risques que par souci de préserver leurs fonds propres.

Evaluer le dispositif de contrôle interne revient à examiner chaque point des dispositifs présentés ci-dessus, à vérifier son fonctionnement par des tests et sondages appropriés, à porter une appréciation sur son efficacité et à émettre des recommandations à l'organe de direction pour son amélioration.

Figure 1: démarche d'évaluation du contrôle interne



Source : IFACI (2004)

2.4.4.1 Objectifs de l'évaluation

Le système de contrôle interne est constitué de l'ensemble des politiques et procédures (eontrôles internes) mises en œuvre par la direction d'une entité en vue d'assurer, dans la mesure du possible, la gestion rigoureuse et efficace de ses activités. Ces procédures impliquent :

- le respect des politiques de gestion,
- la sauvegarde des actifs,
- la prévention et la détection des fraudes et erreurs,
- l'exactitude et l'exhaustivité des enregistrements comptables,
- l'établissement en temps voulu d'informations comptables et financières fiables.

Le système de contrôle interne est une composante essentielle de la gestion de la banque et constitue le fondement d'un fonctionnement sûr et prudent de l'organisation bancaire. Ainsi les dirigeants doivent appliquer et surveiller l'ensemble des mesures de contrôle qui sont sous leur responsabilité afin d'assurer la protection du patrimoine et la fiabilité de l'information financière. La norme d'audit interne 2120.A1 définit les aspects sur lesquels doit porter l'évaluation du contrôle interne qui sont donc autant d'objectifs à atteindre :

- fiabilité et intégrité de l'information financière et opérationnelle ;
- efficacité et efficience des opérations ;
- protection du patrimoine ;
- respect des lois, règlements et contrats.

Le système de contrôle interne s'entend au-delà des questions directement liées au système comptable. Il comprend :

- l'environnement général de contrôle interne ;
- les procédures de contrôle qui désignent les politiques et procédures définies par la direction afin d'atteindre les objectifs spécifiques

Le système de contrôle interne est constitué de l'ensemble des politiques et procédures (contrôles internes) mises en œuvre par la direction d'une entité en vue d'assurer, dans la mesure du possible, la gestion rigoureuse et efficace de ses activités. Ces procédures impliquent le fait qu'un système de contrôle interne efficace attenu forcement les risques opérationnels, notamment ceux liés aux systèmes de paiement.

2.4.4.2 Les différentes phases de l'évaluation

Selon Sardi (2002 :117), les entreprises doivent organiser leur système de contrôle interne de sorte à se doter de dispositifs :

- qui assurent un contrôle régulier avec un ensemble de moyens mis en œuvre en permanence au niveau des entités opérationnelles pour garantir la régularité, la sécurité et la validation des opérations réalisées et le respect des autres diligences liées à la surveillance des risques de toute nature associés aux opérations ;
- qui vérifient selon une périodicité adaptée, la régularité et la conformité des opérations, le respect des procédures.

L'évaluation consistera donc à identifier les points forts et les points faibles des procédures.

Les points forts relevés devront faire, si nécessaire, l'objet d'un examen complémentaire (test de permanence) pour s'assurer qu'ils sont réellement appliqués d'une manière constante. Dans la négative, le point fort se transforme en point faible.

Les points faibles relevés pourront, suivant leur importance, faire l'objet d'investigations approfondies, ceci dans un double but :

- s'assurer que la faiblesse n'a pas d'incidences significatives ;
- dans le cas inverse, évaluer les incidences de cette faiblesse : pertes financières, comptes injustifiés, fraudes etc.

Le dispositif de contrôle doit être conçu de manière à assurer une stricte indépendance entre les unités chargées de l'engagement des opérations et celles chargées de leur validation. Il s'agira ici d'user d'outils permettant de se rendre compte d'une séparation de tâches ou non.

2.4.4.3 Les limites du contrôle interne

Au titre des limites naturelles du contrôle interne, citons les plus classiques :

- le coût d'un contrôle interne (qui ne doit pas excéder les avantages escomptés du dispositif) ;
- la plupart des opérations internes de vérification portent sur des opérations répétitives et non sur des opérations non récurrentes, peu habituelles et non familières ;
- la possibilité d'erreur humaine (négligence, distraction, erreurs de jugement, mauvaise compréhension des instructions) ;

- les collusions internes ou externes à l'entité, mettant en échec le dispositif,
- l'abus éventuel par une personne de ses prérogatives pour ne pas se soumettre au dispositif ;
- l'inadaptation des procédures à la situation ;
- la non-application des procédures.

Conclusion Chapitre 2

Ce chapitre nous a permis de vulgariser les notions en rapport avec les systèmes de paiement interbancaires et le processus d'émission des ordres de paiement, la notion de risque en général et de risques opérationnels liés aux systèmes de paiement en particulier.

En plus des notions précitées, on a eu une vue d'ensemble sur le dispositif de maîtrise des risques liés aux systèmes de paiement et les bonnes pratiques en matière de gestion de ces risques dont on peut aisément apprécier l'importance dans le secteur bancaire.

CHAPITRE 3 : METHODOLOGIE DE L'ETUDE

Le risk management vise à identifier et anticiper les évènements, actions ou inactions susceptibles d'impacter la mise en œuvre de la stratégie dans un horizon donné, définir les options de traitements et s'assurer qu'une option optimale est choisie, mettre en œuvre cette option et contrôler l'efficacité de la solution retenue par rapport aux attentes».

Pour le Cabinet Ernst & Young Plus généralement appliquée aux entreprises, la gestion des risques s'attache à identifier les risques qui pèsent sur les actifs (financiers ou non), les valeurs ainsi que sur le personnel de l'entreprise. La gestion des risques dans l'entreprise passe par l'identification du risque résiduel, son évaluation, le choix d'une stratégie de maîtrise et un contrôle.

Aujourd'hui, l'attention portée à la gestion des risques dans l'entreprise s'est accrue. Ceci se traduit simultanément par un cadre réglementaire renforcé et par une pression grandissante des marchés pour une prise de conscience des entreprises de la nécessité de maîtriser leurs risques.

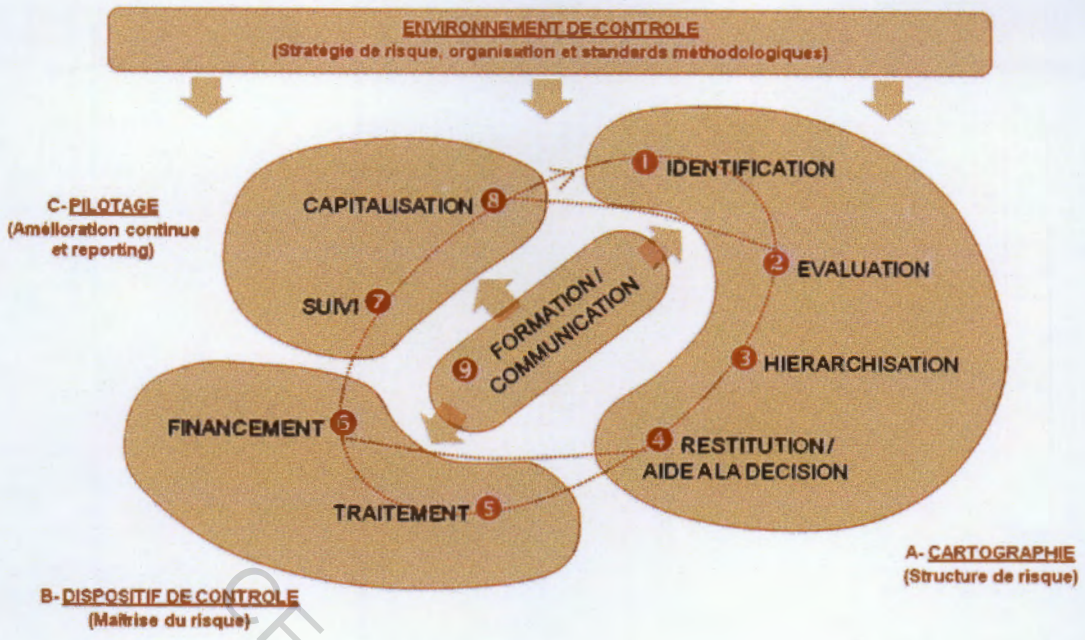
Les deux premiers chapitres nous ont aidé à mieux appréhender les systèmes de paiement ainsi que les risques opérationnels qui s'y attachent. A travers le présent chapitre, nous présenterons notre méthode de recherche ainsi que les outils de collecte et d'analyse des données utilisées.

Nous avons fait le choix de l'approche par les risques pour l'analyse de la gestion des risques opérationnels liés aux systèmes de paiement, dans le cadre de cette étude.

3.1 Le modèle d'analyse pour la gestion des risques

A travers notre modèle d'analyse (Figure 2), il s'agira pour nous de décrire les différentes phases et étapes se rapportant au processus de management des risques.

Figure 2: Analyse autour du processus du management des risques



Source : Management de Risques (COSO2-ERM-2005)

3.1.1 Détail des phases du modèle d'analyse

Le modèle d'analyse se décline en plusieurs phases.

3.1.1.1 L'environnement de contrôle

L'environnement de contrôle englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'entité, et plus particulièrement la conception du management et son appétence pour le risques, l'intégrité et les valeurs éthiques ;

L'environnement de contrôle formalise l'organisation des organes de management des risques et les méthodologies et standards de maîtrise des risques, et définit un langage commun ;

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

3.1.1.2 L'identification et l'analyse des risques

Le préalable à toute démarche de Management des risques consiste à répertorier, de manière la plus complète possible, tous les évènements générateurs de risques pour une

organisation et pouvant conduire à sa remise en cause ou au non respect des objectifs (ainsi que les opportunités).

Pour entreprendre ce recensement, plusieurs technique peuvent alors être utilisées, puis combinées (chacune d'elles ayant ses propres limites) : l'analyse de la documentation existante, l'interview d'experts, la réalisation de réunions de brainstorming, l'utilisation d'approches méthodologiques spécifiques (AMDEC, APR, ACC), la consultation de bases de données de retour d'expérience ou encore l'utilisation de référentiels préétablis.

Concernant les approches méthodologiques, les outils les plus largement utilisées diffèrent selon la nature du problème posé et l'information disponible.

Cette étape est la plus importante, car elle conditionne l'efficacité de toutes les autres.

3.1.1.3 L'évaluation et la hiérarchisation des risques

Selon (Coso 2005) La gestion des risques ne doit pas se limiter uniquement à une simple identification, c'est-à-dire à un recensement plus ou moins exhaustif des risques potentiels et pertinents et à une analyse plus ou moins approfondie de leurs caractéristiques. Elle doit s'appuyer également sur une analyse (qualitative ou quantitative) pour mieux appréhender et estimer leur probabilité d'occurrence et la gravité de leurs conséquences.

Il s'agit, tout d'abord de bien distinguer parmi les risques préalablement identifiés, ceux qui n'en sont pas, ou qui sont non fondés (qu'il convient par conséquent de rejeter de l'analyse), de ceux qui sont réels et susceptibles d'affecter la performance de l'organisation, qui demandent alors une attention constante et qui doivent faire l'objet d'un traitement et d'un suivi particulier.

3.1.1.4 Le traitement et le financement des risques

Le management des risques d'un projet repose non seulement sur leur identification et sur leur évaluation, mais également sur leur prise en compte. En effet, il ne suffit pas de balayer l'ensemble des risques encourus (ou qui pourraient être encourus), de les estimer et de les hiérarchiser. Il faut également les maîtriser, c'est-à-dire définir et mettre en œuvre les dispositions appropriées pour les rendre acceptables. Cela nécessite donc de définir des réponses types et de mettre en œuvre, risque par risque, un certain nombre d'actions visant soit à supprimer ses causes, soit à transférer ou partager sa responsabilité ou le coût du dommage à un tiers, soit à réduire sa criticité (en diminuant sa probabilité

d'occurrence ou en limitant la gravité de ses conséquences), soit à accepter le risque tout en le surveillant ;

L'objectif de l'étape de maîtrise n'est pas de supprimer tous les risques potentiels afférents à l'activité de l'organisation, ce qui semble totalement illusoire, puisqu'il existera toujours des évènements imprévisibles ou non prévu qui échapperont au contrôle des acteurs et qui contribueront au succès ou à l'échec de l'organisation ou du projet. L'objectif est plutôt de savoir comment il est possible de mieux maîtriser les risques majeurs associés au projet pour les ramener à un niveau acceptable et les rendre ainsi plus supportables.

3.1.1.5 Le suivi et le contrôle des risques

Au fur et à mesure que le projet se déroule, le portefeuille des risques potentiels doit être réajusté en fonction des nouvelles informations recueillies. Certains risques pouvant disparaître, d'autres apparaître ou d'autres encore, considérés initialement comme faibles, pouvant devenir rapidement inacceptables pour l'entreprise dès lors qu'ils n'ont pas été maîtrisés, le niveau d'exposition aux risques de l'organisation ou du projet est amené à changer. C'est pourquoi il est important de procéder périodiquement au suivi et au contrôle des risques encourus.

L'objet de cette étape est de mettre à jour la liste des risques identifiés (par la quête d'information complémentaires), d'affiner les données caractéristiques des risques déjà connus (en particulier leurs probabilité et leurs conséquences potentielles), de réévaluer leur criticité, de contrôler l'application des actions de maîtrise, d'apprécier l'efficacité des actions engagées, et de surveiller le déclenchement des évènement redoutés et de leurs conséquences.

3.1.1.6 La capitalisation et la documentation des risques

Le management des risques nécessite enfin de capitaliser le savoir-faire et les expériences acquises et d'établir une documentation rigoureuse sur les risques associés à l'organisation. Même si la plupart des évènements dommageables ne se reproduisent jamais à l'identique, il n'en demeure pas moins que l'accumulation de connaissances et les retours d'expériences doivent permettre d'enrichir la connaissance des risques potentiels et dommageables, d'accroître la réactivité à chaque niveau d'intervention, de faciliter la prise de décision et d'améliorer l'efficacité des actions de maîtrise.

3.2 Les outils de collecte et d'analyse des données

Notre étude a nécessité l'implication de la direction de l'audit et de la direction des opérations de la CBAO. Cela nous a permis de rencontrer plusieurs personnes ressources directement concernées par la gestion des moyens de paiement. Nous avons utilisé différentes méthodes de collecte d'informations à savoir : l'interview, l'observation physique, le questionnaire de contrôle interne, le diagramme de circulation etc.

Ainsi les données suivantes ont fait l'objet d'analyse :

- interview ;
- le questionnaire de Contrôle Interne (QCI) ;
- l'observation physique ;
- l'analyse documentaire ;
- la grille de séparation des tâches ;
- le diagramme de circulation ;
- le Tableau des Forces et faiblesses apparentes (TFfa) ;
- la Feuille d'Analyse des Risques ;
- le test de conformité / de permanence.

3.2.1 L'interview

L'interview est un entretien avec une personne en vue de l'interroger sur ses activités, ses idées, etc. dans le but de recueillir ses opinions. Cet outil est très déterminant dans notre étude pour une fiabilité des informations recherchées. L'interview nous permettra de décrire le processus d'émission d'ordres de paiement dans les systèmes, et d'appréhender les risques et les dispositifs de contrôle interne existants. Pour réaliser les entretiens, nous prendrons rendez-vous avec certains acteurs du processus en vue de leur proposer un questionnaire se rapportant au fonctionnement et à la gestion d'incidents qui surviennent lors du traitement des informations relatives aux systèmes de paiement.

Aussi, nous prévoyons dans la phase pratique de rencontrer :

- le responsable du département traitement des chèques et effets ;
- le trésorier ;
- le responsable de l'Audit Général (Audit Interne);
- le responsable du traitement monétique.

3.2.2 Le questionnaire

Il existe deux sortes de questionnaires :

- les ***Questionnaires de Prise de Connaissance*** intervenant lors de la phase de préparation ;
- les ***Questionnaires de Contrôle Interne*** intervenant lors de la phase de réalisation. Ces questionnaires ne sont pas constitués de questions que l'on pose mais de questions que se pose l'auditeur. Celui-ci va y répondre en utilisant divers outils (interviews, observations, documents).

3.2.2.1 Le Questionnaire de Prise de Connaissance (QPC)

La prise de connaissance du domaine ou de l'activité à auditer ne doit pas se faire dans le désordre, c'est pourquoi l'auditeur va utiliser un questionnaire dénommé « Questionnaire de Prise de Connaissance » récapitulant les questions importantes dont la réponse doit être connue si on veut avoir une bonne compréhension du domaine à auditer. C'est un moyen efficace pour organiser la réflexion et les recherches et surtout pour :

- bien définir le champ d'application de sa mission,
- prévoir en conséquence l'organisation du travail et en particulier en mesurer l'importance ;
- préparer l'élaboration des Questionnaires de Contrôle Interne.

3.2.2.2 Le Questionnaire de Contrôle interne (QCI)

L'élaboration du questionnaire du contrôle interne intervient juste après le questionnaire de prise de connaissance. Ce questionnaire sera administré à un échantillon des agents de la banque intervenant dans la gestion des moyens de paiement. L'échantillon que nous avons retenu portera sur :

- le responsable du département traitement des chèques et effets ;
- le trésorier ;
- le responsable de l'Audit Général (Audit Interne);
- le responsable du traitement monétique
- les agents travaillant sur les systèmes de paiements

Au total 20 personnes seront retenues pour ce questionnaire.

Ce questionnaire sera composé de questions fermées en vue d'analyser les opérations « à risque », et d'évaluer le dispositif de contrôle interne.

Une réponse « oui » à une question constitue une force du dispositif de contrôle interne ; par contre une réponse « non » présage d'une zone potentiellement à risque dans ce dispositif.

Cette méthode nous permet d'avoir des réponses assez précises et concises sur le sujet traité (voir Annexe 3).

3.2.3 L'observation physique

L'observation physique nous permettra de comprendre et de valider les informations recueillies lors des interviews. Elle consiste à suivre le déroulement effectif des opérations d'émission d'ordre dans les systèmes de paiement. Cela est un moyen sûr de vérification de ce qui a été dit lors des entretiens. Pour ce faire nous prendrons attache avec la direction des opérations pour suivre le parcours de traitement des chèques, effets et ordres de virement depuis leurs réceptions jusqu'à leurs validations.

3.2.4 L'analyse documentaire

Cette étape nous permettra de prendre connaissance du manuel de procédure de traitement des données se rapportant aux systèmes de paiement.

L'analyse des documents portera sur les documents suivants :

- les chèques ;
- bordereaux de remise de chèque ;
- les effets de commerce ;
- les ordres de virement et de transfert ;
- les formulaires de demande de cartes bancaires.

Ceci forgera notre opinion sur l'importance des systèmes de paiement à la CBAO, ainsi que les risques qui lui sont liés et le mode de gestion de ces risques.

3.2.5 La grille de séparation des tâches

Elle relie l'organigramme fonctionnel à l'organigramme opérationnel, et comme son nom l'indique, elle permettra de respecter le principe de séparation des tâches. Elle permettra ainsi de déceler les incompatibilités, les cumuls de fonctions, les surcharges des agents pouvant les rendre *de facto* inefficace ; de façon spécifique, l'analyse de la grille de séparation des tâches à la CBAO nous permettra de voir le mode de répartition des responsabilités et des tâches au sein de la banque (voir Annexe 4).

3.2.6 Le diagramme de circulation

Selon Renard (2004 : 156) « Le diagramme de circulation ou Flow-chart est un outil qui permet de retracer les modes opératoires d'un processus ou d'une fonction sous la forme de représentations symboliques ».

Le diagramme nécessite que le processus d'émission d'ordre dans les systèmes de paiement soit découpé en tâches (voir Annexe 2).

3.2.7 Le Tableau des Forces et faiblesses apparentes (TFfa)

Le TFfa servira à identifier, le risque qui est susceptible de se produire à chaque tâche. Devant chaque tâche, il y a l'objectif fixé, le risque encouru et les pratiques communément admises (voir Annexe 5).

3.2.8 La Feuille d'Analyse des Risques (FAR)

C'est un outil mis à la disposition des responsables pour permettre le suivi permanent des risques. Il faut décrire sur cette feuille, les risques opérationnels associés à chaque tâche liée aux systèmes de paiement, les causes de ces risques, les conséquences et les recommandations pour une amélioration (voir Annexe 6).

3.2.9 Le test de conformité / de permanence

Ces tests seront très utiles pour s'assurer d'une part que les dispositifs de contrôle interne ont été appliqués, et que toutes les opérations ont été traitées conformément à ce qui a été décrit lors des interviews et dans le manuel de procédure. (Annexe 7)

Conclusion du chapitre 3

Ce chapitre est le squelette de la conception et de la réalisation effective de notre travail. Depuis le modèle d'analyse jusqu'aux outils de collecte de données, toutes séquences sont très importantes pour avoir l'information juste et pertinente. Ce qui nous permettra *in fine* d'avoir un assez satisfaisante.

CONCLUSION DE LA PREMIERE PARTIE

Dans sa fonction d'intermédiation financière, la banque joue un rôle important dans l'activité économique par la satisfaction des besoins d'investissement et de fonctionnement des entreprises mais aussi par l'aide à l'épanouissement des ménages. Cette activité qui met en relation étroite la banque et les agents économiques se fait par le moyen de systèmes de paiement qui sont sources de divers risques.

La gestion des risques opérationnels, au-delà d'une simple formalité, est source de création de valeur pour la banque ; elle permet de réduire les pertes, de préserver les fonds propres et de protéger l'image de la banque.

La revue de littérature nous a permis de cerner le fonctionnement des systèmes de paiement et l'analyse de la gestion des risques ainsi que les dispositifs appropriés pour assurer leur maîtrise.

La deuxième partie de notre étude traitera de la description de la CBAO et la gestion des risques liés aux systèmes de paiements effectués par la CBAO

DEUXIEME PARTIE : CADRE PRATIQUE

INTRODUCTION DE LA DEUXIEME PARTIE

Le secteur bancaire et financier de l'UEMOA est en pleine mutation. Le nombre des établissements de crédit est croissant. Mais les services financiers demeurent inaccessibles pour la grande majorité de la population. La faiblesse du niveau de bancarisation reste inquiétante et la monnaie fiduciaire est très prisée dans le règlement des transactions ; cela engendre bien évidemment des problèmes important tant au niveau de la mobilisation de l'épargne que du financement de l'activité économique.

A l'analyse de tout ce qui précède, et dans le souci de booster l'activité, l'autorité monétaire de l'UEMOA a pris la décision de vulgariser le secteur bancaire par des campagnes de promotion, et surtout de le moderniser avec l'automatisation des transferts, le déploiement de la télé-compensation et l'introduction de la carte bancaire sous-régionale (GIM-UEMOA).

La caractéristique de l'activité bancaire est le nombre important de risques opérationnels engendrés. La modernisation du secteur voulue par la banque centrale génère aussi des risques opérationnels dont la maîtrise requiert l'adoption d'instruments d'appréciation et de suivi appropriés. Il est dès lors impératif de prendre connaissance des systèmes de paiement à la CBAO et de recommander, si nécessaire, un bon dispositif de gestion des risques opérationnels qui y sont associés.

CHAPITRE 4 : PRESENTATION DE LA CBAO

La CBAO Groupe Attijariwafa Bank est née de la fusion entre la Compagnie Bancaire de l'Afrique Occidentale et Attijariwafa Bank Sénégal (ABS) en décembre 2008.

La CBAO est donc une filiale du Groupe Attijariwafa, présente dans plusieurs pays du Maghreb et en Europe, dont le siège social est à Casablanca au Maroc.

Depuis un peu plus de trois ans, la banque a amorcé son installation en Afrique subsaharienne, principalement dans la zone UEMOA par des opérations de fusion, de rachat ou d'implantation.

4.1 Historique

Créée il y a un siècle et demi, en 1853, la Compagnie Bancaire de l'Afrique Occidentale (CBAO) dénommée à cette époque Banque du Sénégal est la Banque la plus ancienne de l'Afrique de l'Ouest.

La CBAO Groupe Attijariwafa est issue de la fusion entre la Compagnie Bancaire de l'Afrique de l'Occidental (Créée il y a un siècle et demi) et Attijari Bank Sénégal, qui est le fruit de la fusion par création de nouvelle société entre la Banque Sénégalo Tunisienne et Attijariwafa Bank Sénégal. La Compagnie Bancaire de l'Afrique Occidental(CBAO) est la plus ancienne banque de l'Afrique de l'Ouest et sa création date de 1853. Elle a réalisé ses premières opérations sous le nom de Banque du Sénégal. Elle deviendra ensuite la Banque de l'Afrique Occidentale puis la Banque Internationale pour l'Afrique Occidentale, capitalisant une vaste expérience tant dans le domaine du financement des économies africaines que dans des opérations internationales, notamment du commerce intra africain et avec le reste du monde.

Elle a de nouveau changé de dénomination en Janvier 1993 devenant la Compagnie Bancaire de l'Afrique Occidentale. Ce changement traduit une nouvelle mutation de la banque ainsi que ses nouvelles ambitions dans le sens de la constitution d'un grand groupe financier à vocation régionale. Il n'est cependant pas inutile de rappeler que la décennie qui suivit la création de la filiale sénégalaise fut douloureuse. L'environnement économique international s'est détérioré à la suite du second choc pétrolier. Une nouvelle période de sécheresse sévit.

Les institutions bancaires de la place traversent de durs moments, la BIAO n'est pas épargnée.

La gestion de l'institution laisse à désirer, les pertes s'accumulent rendant indispensable la mise en œuvre d'un plan de restructuration en 1988.

Le capital de la banque fut alors reconstitué et porté à 1,1milliard de F CFA et des particuliers y feront leur entrée. A la faveur de cette restructuration, la taille de la banque fut fortement réduite à deux agences et bureaux. Une solution est trouvée aux problèmes de charge d'exploitation, cependant le bilan de la banque reste lourdement compromis. Au même moment, la notoriété de la BIAO- S également entachée avec le projet de la liquidation de la maison mère la BIAO- SA.

Pour pallier la gravité de la situation, une politique de redressement dénommée OUATTARA fut adoptée par le BCEAO (Banque Centrale des Etats de l'Afrique de l'Ouest).L'Etat du Sénégal dans le cadre d'une convention datée du 14 Septembre 1990 décide de prendre en charge les besoins complémentaires en capital. Le Capital fut doublé conformément aux dispositions de la loi bancaire et dans le souci du respect des ratios prudentiels de la BCEAO.

La configuration immédiate du capital après sa libération fut la suivante :

- Etat du Sénégal 10%
- Portage par l'Etat / Compte futur bolding du réseau 19%
- Groupe MIMRAN 46%
- Autre privés 25%

Le redressement des années précédentes se poursuit avec une stratégie de restructuration avancée qui passe par :

- la modification profonde de la structure
- l'établissement d'un nouveau réseau de correspondance
- la rupture de tous liens juridiques avec la BIAO-SA son ancienne maison mère.

Cette politique visait à restaurer la rentabilité de la banque perdue pendant plusieurs exercices et à donner une nouvelle image à la BIAO-SA qui a eu à monter une volonté de changement durant ces dernières années.

C'est dans ce sens que l'assemblé générale extraordinaire des actionnaires de la BIAO Sénégal réunie le 25 Novembre à par conséquent décidé le changement de la dénomination de la banque à l'occasion de son 140 ème anniversaire.

C'est ainsi que ce changement dans le souci d'une réelle continuité a été effective en Janvier 1993 avec la modification de la raison sociale de l'ancienne BIAO Sénégal qui

devient CBAO (Compagnie Bancaire de l'Afrique Occidentale) avec un nouveau capital porté à 9 000 000 000 F CFA et la part des actionnaires se présente comme suit :

- Groupe MIMRAN 72%
- Etat du Sénégal 9%
- Actionnaires privés 19%

Enfin, en Novembre 2007 le groupe Attijariwafa Bank accompagné par ses actionnaires de référence (ONA, SNI) a amorcé l'acquisition de 79,15% du capital de la CBAO auprès du Groupe MIMRAN. Cette opération a été effective en Avril 2008 suite au Conseil d'Administration de la CBAO qui a constaté la composition du capital.

Le groupe Attijari Bank par cette acquisition réitère ainsi sa volonté de disposer des atouts nécessaires au déploiement de son projet de développement au Sénégal et dans l'ensemble des pays de la région de l'Afrique de l'Ouest. Ce développement avait d'ailleurs commencé par la création d'Attijariwafa Bank Sénégal en Juillet 2006 première filiale du groupe en Afrique Occidentale suivi de l'acquisition de la Banque Sénégalo-Tunisienne(BST) en 2007 donnant naissance à Attijari Bank Sénégal. Le capital social de la CBAO est détenu à hauteur de 79,15% par le groupe Attijariwafa Bank, 9% par l'Etat du Sénégal et 12% par les privés. La CBAO Groupe Attijariwafa Bank est dirigée depuis Mi-Juillet 2008 par le Marocain M. Abdelkrim RAGHNI.

Après cette longue historique, nous pouvons clairement voir que pour arriver à ce stade dans le domaine bancaire, la CBAO a eu à relever plusieurs défis, qui lui ont permis d'avoir plus d'expérience et de mieux se positionner dans le secteur bancaire.

4.2 Mission et objectifs de la banque

A l'instar de toutes les institutions bancaires, la CBAO a défini une mission et des objectifs sur lesquels elle s'appui pour planifier ses activités et réaliser ses ambitions.

4.2.1 Mission

Dans un monde en perpétuelle mutation, le rôle d'une Institution quelle qu'elle soit est de s'adapter aux réalités économiques.

En effet, avec la pléthore d'entreprises prestataires de services, des contraintes macro-économiques nouvelles sont apparues à savoir une concurrence nationale et internationale accrue, des fluctuations plus marquées de la demande et des attentes de différenciation des produits et services.

Ainsi, afin d'être compétitive sur le marché, toute entreprise doit donner une importance capitale à la qualité du service offert.

C'est dans cette optique, que la **CBAO** en tant qu'Institution Bancaire fait **des opérations de banque, d'épargne, de crédits et de la gestion des moyens de paiement,** sa mission principale.

Par la même occasion, l'ambition de la CBAO est de devenir un partenaire incontournable d'une part pour les africains originaires des pays membres de l'Union Economique et Monétaire de l'Afrique de l'Ouest (UEMOA), quel que soit leur lieu de résidence et d'autre part pour les investisseurs opérant au Sénégal, quelle que soit leur origine.

4.2.2 Objectifs

Pour réaliser cette ambition, la banque s'est fixé les objectifs suivants :

- développer les activités de marché ;
- dynamiser le secteur des PME
- développer la banque privée ;
- dynamiser le réseau Jeune ;
- proposer des produits différenciés par cible de clientèle ;
- élargir la gamme de produits proposés à la clientèle ;
- développer la proximité avec les clients ;
- optimiser les délais de traitement des dossiers de crédit ;
- développer les crédits aux particuliers via l'industrialisation des prêts aux particuliers ;
- amorcer la commercialisation des produits islamiques ;
- développer une politique innovante de recouvrement.

4.3 Les activités de la CBAO

La CBAO Groupe Attijariwafa est une institution bancaire qui a pour mission principale de faire des opérations de banque, d'épargne, de crédit et de la gestion des moyens de paiement.

Cependant, l'ambition de la CBAO est de devenir un partenaire incontournable d'une part pour les africains originaires des pays membres de l'UEMOA quelque soit leur lieu de résidence et d'autre part pour les investisseurs opérant au Sénégal quelle que soit leur origine.

C'est dans cette optique que la CBAO a développé des produits et services répondant à la demande et aux attentes des clients.

Nous pouvons citer comme produits : le compte épargne, le compte chèque, le compte courant, Avenir logement(AVL), Dépôt à terme(DAT), le bon de caisse(BDC), la carte épargne, la Mastercard, la Business Card, le visa électron. Ses activités s'inscrivent dans le cadre du financement du commerce international, le crédit privé aux particuliers, la collecte de l'Epargne.

Nous pouvons aussi voir que la CBAO Groupe Attijariwafa Bank est une banque qui se veut proche de ses clients et reste compétitive grâce à ses services tant diversifiés.

4.4 Le Fonctionnement de la CBAO

L'organisation de la CBAO Groupe Attijariwafa Bank repose sur une structure en réseau composée de plus de 1000 agents. Ces hommes et femmes ont choisi de partager librement des valeurs sûres et intègres à savoir :

- le professionnalisme : c'est-à-dire une certaine exigence de compétence, de rigueur et d'expertise, d'amour du métier et du travail bien fait.
- l'esprit d'équipe : c'est privilégier l'équipe et l'entreprise par rapport à l'intérêt personnel, en instaurant un climat social favorable.
- avoir envie de voir gagner le groupe grâce au travail collectif et organisé.

Ces agents sont répartis en fonction de leur domaine d'activité dans les 11 Départements que compte la CBAO à savoir :

Les départements juridique Contentieux et Recouvrement, Audit et inspection, Contrôle interne et conformité, Gestion Globale des Risques sont rattachés à la direction Générale.

Ces différents départements coiffent des directions Générales Adjointes à savoir la Direction Générale Adjointe Exploitation et la Direction Générale Adjointe Administration.

Devant les impératifs de la fusion effective, le Président du Conseil d'administration a décidé de mettre en place un organigramme provisoire de fusion afin que la Direction Générale puisse assurer l'exécution correcte des opérations de la nouvelle banque CBAO Groupe Attijariwafa Bank. Cet organigramme provisoire a été remplacé le 03 Septembre 2010 par un autre définitif approuvé par le conseil d'Administration. Nous présentons aux points suivants la structure organisationnelle de la banque.

4.4.1 La Direction Générale

C'est elle coiffe tous les autres départements et directions. Elle se charge de diriger la banque et de rendre compte au Conseil d'Administration.

4.4.2 La Direction Juridique Contentieux et Recouvrement

Ce département se charge de gérer les contentieux de la banque ainsi que le recouvrement des créances.

4.4.3 La Direction de l'Audit et Inspection

Il a en charge le contrôle des caisses et de faire les inspections dans tous les services de la banque. Elle vérifie la régularité et la sincérité des opérations effectuées et participe à la maitrise des risques quantifiables.

4.4.4 La Gestion Globale des Risques(GGR)

Elle est chargée de conseiller la Direction Générale sur les aspects juridiques et fiscaux auprès de la clientèle, d'assurer l'exécution de la bonne gestion des engagements pris par la banque et les clients, du recouvrement des créances et de la gestion des risques.

4.4.5 Le Contrôle interne et Conformité

Se charge de contrôler les activités de la banque et de voir si elle répond aux exigences de la réglementation bancaire.

4.4.6 La Direction Générale Adjointe(DGA) en charge de l'Exploitation

Elle comprend :

- la Direction Clientèle : Elle supervise l'ensemble des services rendus à la clientèle, à savoir la clientèle entreprise, privée et institutionnelle, Elle est chargée du développement de l'activité commerciale de la CBAO sur le marché des entreprises tant du point de vue quantitatif que qualitatif. La direction doit également, en relation avec le département marketing, participer activement à la stratégie produite en ayant le souci d'innover et de rentabiliser ces derniers, de même que les services offerts ;
- la Direction des Opérations qui supervise les opérations sur le plan local, international, les cartes bancaires, les cautionnements et le crédit bail. Elle est en charge de l'exécution des opérations et du traitement des produits et services offerts par la

banque à la clientèle en ayant le souci permanent de la qualité, de la rentabilité et de la fiabilité des prestations rendues ;

- la Direction Activité de marché-change-Trésorerie.

La Direction Générale Adjointe seconde la Direction Générale dans la gestion de la banque.

- la Direction Générale Adjointe en charge de l'Administration : elle supervise l'administration de la banque à travers ;
- la Direction des finances qui comprend le service de la comptabilité et fiscalité, contrôle de gestion, gestion budgétaire et la gestion des filiales;
- la Direction Supports et Moyens qui gère les moyens généraux, le nouveau siège, le Capital humain, l'académie de formation;
- la direction Service informatique et Monétique chargée de garantir une adéquation permanente entre les moyens de traitement de l'information et des besoins liés à l'activité, ainsi qu'à la monétique;
- la direction Organisation et Qualité qui s'occupe de la honne organisation des activités de la banque ainsi qu'un service de qualité à ses clients.

4.5 Régime juridique de la fusion CBAO-ATTIJARI BANK SENEGAL

Il y a deux régimes juridiques qui s'appliquent à une opération de fusion : La fusion par création d'une nouvelle société et la fusion absorption. Le régime juridique qui a été appliqué à la fusion de a CBAO et de Attijari Bank Sénégal est celui de la fusion absorption.

Selon l'Article 192 de l'AUDSC-GIE, la fusion prend effet à la date de la dernière assemblée générale ayant approuvé l'opération, sauf si le contrat prévoit que l'opération prend effet à une autre date, laquelle ne doit être ni postérieure à la date de clôture de l'exercice en cours de la ou des sociétés bénéficiaires ni antérieure à la date de clôture du dernier exercice clos de la ou des sociétés qui transmettent leur patrimoine. La date d'effet de notre fusion est celle du 22 Décembre 2008.

Ci-après, quelques chiffres clés de la banque au cours des deux dernières années en millions de F CFA :

Tableau 1: Quelques chiffres clés de la CBAO (en millions de FCFA)

INDICATEURS	2009	2010
Dépôts de la clientèle	409 336	523 029
Créances nettes sur clientèle	351 034	356 832
Total du bilan	626 882	650 220
Capitaux propres après répartition	68 234	69 176
Produit Net Bancaire	45 303	43 268
Effectif au 31 Déc.	1 029	1 060
Hors Bilan		
Engagement par Signature Donnés	135 100	151 503
Engagement par Signature Reçus	117 852	109 859

Source : Rapport annuel de la CBAO au 31 déc. 2010

Ce chapitre nous a permis de comprendre de façon succincte l'historique, l'organisation et le fonctionnement de la CBAO.

Conclusion Chapitre 4

La fusion n'a pas seulement eu de bons impacts sur la CBAO puisque les clients qui n'étaient pas très bien avisés sur la fusion ont pensé à sa faillite et ils ont du se retirer. Mais ils sont revenus plus tard puisque cette fusion a permis à la CBAO d'être plus puissante pour faire face à ses nombreux concurrents.

Par rapport aux associés de l'ABS, en application de l'Article 191 de l'AUDSC-GIE, la fusion entraine simultanément l'acquisition par les associés de la société absorbée la qualité d'associé de la société bénéficiaire dans les conditions déterminées par le contrat de fusion. Cela veut dire que les associés de l'ABS sont immédiatement devenus ceux de la CBAO par rapport au contrat de fusion, car l'ABS a disparu.

Selon l'alinéa 2 de cet article, ils doivent recevoir une soulte dont le montant ne peut dépasser les 10 % de la valeur d'échange des actions attribuées. Dans cette fusion, la valeur d'échange était de Deux(2) cela veut dire qu'une action CBAO de 10 000F CFA est égale à 2 actions de 10 000 FCFA de l'ABS.

CHAPITRE 5 : LA GESTION DES RISQUES LIES AUX SYSTEMES DE PAIEMENT A LA CBAO

Les systèmes de paiements sont des procédures permettant d'exécuter à titre habituel, par compensation ou non, des paiements.

Les différentes transactions financières entre la CBAO et ses partenaires commerciaux et non commerciaux se font à travers les systèmes de paiement en vigueur dans la zone UEMOA et pilotés par la Banque Centrale. Le volume des flux financiers générés par ces transactions sont sources de risques opérationnels potentiels.

Il est important, pour traiter ces risques, de prendre connaissance du processus permettant l'émission d'ordre dans les systèmes de paiement à la CBAO et appréhender la gestion des risques associés.

5.1 Description des systèmes de paiement à la CBAO

Le processus d'émission ou de réception des ordres de paiement est différent d'un système à l'autre selon que l'on est dans STAR-UEMOA ou SICA-UEMOA.

5.1.1 Le processus de paiement dans STAR-UEMOA

STAR-UEMOA est le système régional de règlement brut en temps réel des transactions d'importance systémique (notamment les gros montants). Son démarrage opérationnel est intervenu le 25 juin 2004.

5.1.1.1 Objectifs visés par la mise en place de ce système de paiement

Ces principaux objectifs sont listés ci-après :

- assurer la célérité des paiements ;
- réduire leurs coûts de gestion des opérations ;
- favoriser le développement et l'intégration des marchés de capitaux régionaux ;
- maîtriser les risques.

Avant la mise en place de STAR-UEMOA, les instructions de paiement entre deux pays de l'UEMOA transitaient par le circuit des comptes courants de la BCEAO à travers les mises à disposition de fonds d'une Direction Nationale à une autre. Le traitement des mises à dispositions permettait une imputation à J+1 en cas de validation immédiate de l'ordre de transferts, à j+2 ou j+5 en cas de défaillance dans la transmission de l'ordre. Avec la mise en production de STAR-UEMOA, une nette réduction du délai de traitement

des opérations est observée. Ainsi, au cours de l'année 2009, le délai moyen de dénouement des paiements s'est établi à 41 secondes.

Le STAR-UEMOA permet à la CBAO :

- d'optimiser la gestion de leur trésorerie grâce à la réduction des intermédiaires et à la célérité du système ;
- des échanges interbancaires en temps réel dans la région ;
- de réduire les risques de paiement et de rendre les transactions interbancaires plus fluides ;
- de réduire le délai des transferts intra-UEMOA de 3 semaines à moins d'une minute ;
- de régler les soldes de compensation dans un délai plus court.

5.1.1.2 Participation à STAR-UEMOA

STAR-UEMOA est un système central auquel les participants directs sont connectés via les réseaux SWIFT ou privé de la BCEAO.

Les participants éligibles au système sont : la BCEAO, les banques et établissements financiers, le Dépositaire Central / Banque de Règlement de la Bourse Régionale des Valeurs Mobilières (BRVM), le Groupement Interbancaire Monétique de l'UEMOA (GIM-UEMOA) et la Banque Ouest Africaine de Développement (BOAD).

La participation à STAR-UEMOA nécessite, le strict respect des règles de fonctionnement du système.

Il existe deux modes de participation au système :

- la participation directe, où le participant est raccordé au système depuis une plate-forme installée dans ses locaux et gère lui-même l'émission de ses ordres dans le système et le suivi de sa position ;
- la participation indirecte, où le participant accède au système via un service bureau installé dans les locaux de l'Agence Principale de la BCEAO.

5.1.1.3 Types d'opérations réalisées avec STAR-UEMOA

Le système STAR-UEMOA traite principalement les opérations ci-après :

- les virements, pour compte propre de l'établissement donneur d'ordre ou pour le compte de sa clientèle, pour lesquels cet établissement est désireux d'obtenir le règlement en temps réel ;

- le règlement des échanges de titres conservés à la Banque Centrale sur le marché secondaire soit pour compte propre des banques, soit pour compte de leur clientèle ;
- les ordres des participants à STAR-UEMOA à destination des établissements non éligibles au système, qui sont débités dans STAR-UEMOA et reçus par le Participant BCEAO, qui les impute au système de gestion des comptes courants ;
- les opérations traitées avec la Banque Centrale (Politique Monétaire, refinancement, marché primaire de titres de créances publiques, opérations fiduciaires aux guichets de la BCEAO) ou par son intermédiaire (transferts internationaux en devises) passent par le Participant BCEAO pour la couverture en FCFA dans STAR-UEMOA ;
- les retraits et dépôts fiduciaires dans l'ensemble des Agences Principales ;
- le règlement des soldes de compensation de SICA-UEMOA, de la monétique interbancaire et de la Bourse Régionale des Valeurs Mobilières de l'UEMOA.

5.1.1.4 Règles de fonctionnement dans STAR-UEMOA

STAR-UEMOA repose sur la transmission des ordres de paiement au format SWIFT et sur les principes ci-après :

- l'irrévocabilité de la transaction ;
- le traitement des ordres suivant les niveaux de priorité et l'ordre d'arrivée ;
- le contrôle automatique de la provision dans le compte de règlement du participant donneur d'ordre ;
- l'imputation immédiate des opérations dans le compte de règlement des participants concernés.

L'irrévocabilité des transactions s'entend par l'engagement ferme de l'émetteur de l'instruction à régler au destinataire de l'opération le montant convenu dès l'instant où son ordre a été transmis, reçu et accepté par STAR-UEMOA.

5.1.1.5 Gestion des risques dans STAR-UEMOA

La prévention des risques dans STAR-UEMOA se traduit par un contrôle préalable du solde du compte de règlement avant l'exécution de l'ordre de paiement, ce qui permet de prévenir notamment le risque de crédit et contribue à la réduction du risque systémique.

La prévention du risque de liquidité est prise en charge d'une part, par le double mécanisme d'une file d'attente associé à un niveau de priorité de règlement et d'autre part,

par la possibilité d'avances intra-journalières garanties par des titres. Toutefois, le dispositif des avances intra-journalières est en cours de conception et permettra de rendre fluide les échanges.

5.1.1.6 Les acteurs impliqués

La plateforme STAR-UEMOA et les services utilisateurs sont tous logés à la direction des opérations. Cependant, les ordres de virement impliquent d'autres services de la banque selon la nature des opérations à traiter. Ce sont entre autres :

- le service courrier
- le secrétariat de la direction des opérations
- les conseillers clientèle
- le service des virements
- le service Visa
- le trésorier

5.1.1.7 Les différentes étapes du processus

Le système de paiement STAR-UEMOA, traitant exclusivement les ordres de virement, s'articule autour de deux types d'opérations à savoir, les opérations de clientèle et les opérations de banque à banque.

Ces opérations sont un ensemble de tâches juxtaposées gérées par plusieurs services et dont le couronnement est d'aboutir à la fiabilité des ordres de paiement.

5.1.1.7.1 Les opérations de clientèle

Ce sont en général les nivellements, les règlements de factures, et toutes autres opérations commerciales dont l'ordre émane des clients de la banque sous diverses formes.

De ce fait, des courriers de demande de virement sont déposés soit au service courrier, pour la clientèle entreprise, soit directement chez le gestionnaire du compte pour la clientèle particulier.

a) Le sous-processus « gestion des ordres de virement »

La gestion des ordres de virement est un ensemble de tâches et de diligences mises en œuvre par le service courrier et le service clientèle dans la procédure de traitement des courriers d'ordre et des bordereaux de virement reçus.

- **Réception des ordres de virement**

  - **Courriers**

L'agent qui réceptionne le courrier de demande de virement procède à la vérification du montant et du numéro de compte du client pour s'assurer de leur conformité avec ceux figurant sur la décharge à viser. Par la suite, les courriers sont rangés dans une chemise « courrier de virement » et leurs références sont portées dans le registre de transmission interne du service, daté et signé.

  - **Bordereaux**

Le bordereau de virement est rempli et déposé à son conseiller (gestionnaire) par le client. Le gestionnaire procède à une vérification pour s'assurer que toutes les rubriques à renseigner le sont effectivement ; c'est ainsi qu'il transmet le bordereau au service clientèle afin d'être acheminé à la direction des opérations.

- **Transmission du courrier**

  - **Courriers**

La plupart des courriers de virement sont transmis le jour même de leur réception au secrétariat de la direction des opérations ; ils sont accompagnés du registre de transmission interne pour décharge.

Cependant, les courriers reçus en fin de journée sont transmis à J+1 pour éviter d'éventuelles erreurs de précipitation.

  - **Bordereaux**

La démarche de transmission des bordereaux de virement est pareille à celle des courriers.

Les documents sont rangés dans un registre de transmission et transportés au secrétariat de la direction des opérations par le coursier du service clientèle.

- **Réception par le secrétariat de la direction des opérations**

Les ordres de virement reçus par la secrétaire, après vérification des montants et numéros de compte, sont immédiatement passés dans l'horodateur, dont le rôle est d'indiquer de façon précise l'heure et la date de réception. Elle procède par la suite à la décharge du registre de transmission des services déposants pour matérialiser la réception.

Les courriers reçus sont rangés dans le parapheur du directeur des opérations et acheminés à son bureau pour une prise de connaissance.

- **Transmission aux différents chefs de service**

Les courriers sont ensuite renvoyés chez la secrétaire qui les dispatche selon que les ordres de virement sont des opérations locales (en FCFA), ou des opérations internationales (en Devises). Ainsi, les courriers de virements locaux sont transmis au responsable des opérations locales et les courriers de virements hors UEMOA sont transmis au responsable des opérations internationales.

b) Le sous-processus « traitement des ordres de virement »

Il faut comprendre par traitement, toutes les tâches techniques exécutées durant la procédure en vue de rendre effectif le virement.

- **Vérification de conformité au service Visa**

Les responsables des opérations locales et internationales, après avoir pris connaissance des ordres de virement les font converger vers le service Visa chargé de vérifier la conformité des signatures.

Il est impératif que ceux qui signent les ordres de virement soient effectivement des signataires légaux des comptes, reconnus comme tels dans la banque par la présence d'une copie scannée de leurs signatures dans les fichiers de la CBAO. Toute altération de signature ainsi qu'une différence entre le montant en chiffre et le montant en lettre, entrainent le rejet de l'ordre.

Ces tâches de contrôle sont exécutées minutieusement par les agents de ce service, qui apposent le visa donnant ainsi l'accord pour l'exécution de l'opération. Le contraire est synonyme de rejet de l'ordre de virement.

Les ordres de virement sont retournés aux responsables des opérations qui se chargent à leur tour de les retranscrire dans un registre de rejet en direction du gestionnaire du client, le cas échéant, ou de les transmettre aux agents du service des virements, chargés de les traiter s'ils sont validés.

- **Imputation des comptes par le service des virements**

Les comptes des clients sont débités des montants figurant sur les ordres de virements reçus, dans le logiciel Delta Bank par les agents de ce service.

Si le compte du client n'est pas suffisamment provisionné pour couvrir le montant du virement, Delta rejette la saisie ; dans ce cas, le gestionnaire du client est saisi pour s'assurer qu'il existe des autorisations de dépassement de solde tels que les découverts et autres avantages ponctuels.

- **Emission de l'ordre de virement**

L'ordre de virement est saisi par l'agent sur un premier poste opérateur de la plateforme STAR-UEMOA, installé dans les locaux du service des virements. Il s'agit d'un message codé émis en direction d'un confrère bénéficiaire de la place ou d'ailleurs, comportant toutes les références du donneur d'ordre, à savoir les nom et prénoms, raison sociale, numéros de compte, montant, code du type d'opération etc. L'ordre est émis via le réseau SWIFT et acheminé vers le poste opérateur du trésorier pour un contrôle de second niveau, suivi de l'envoie d'un support physique composé des documents de virement déposés par le client et d'une copie de l'ordre traité par l'agent du service des virements.

- **Validation et émission définitive de l'ordre de virement**

Le contrôleur (trésorier) après avoir procédé à quelques vérifications d'usage sur le visa d'autorisation de paiement, le montant, la raison sociale, les nom et prénoms, le numéro de compte, se charge de router l'ordre vers le système (STAR-UEMOA) qui le traite en un temps record. Il s'en suit naturellement un message d'envoi SWIFT qui est un accusé de réception que le trésorier prend soin d'imprimer et d'archiver.

- **Traitement des ordres de virement reçus**

Des ordres de virement en provenance des confrères sont reçus de façon progressive sur le poste opérateur du trésorier. Celui-ci se charge de transmettre les fichiers reçus aux agents du service virement, qui à leur tour créditent les compte des bénéficiaires

5.1.1.7.2 Les opérations de banque à banque

Ce sont essentiellement des opérations de trésorerie qui couvrent des transactions entre la CBAO et la BCEAO, puis entre la CBAO et ses confrères.

a) Le sous-processus « Blocage de fonds »

C'est une réservation de fonds destiné à l'approvisionnement des caisses pour faire face aux retraits. Le caissier central émet un mail en direction du trésorier pour exprimer ses besoins.

Il est alors établi une fiche de retrait remise à la SAGAM en direction de la banque centrale, qui après le décaissement, débite le compte de la CBAO et émet un message via SWIFT sur le système STAR.

b) Le sous-processus « Opérations de trésorerie interbancaires »

Ce sont des opérations de prêt et d'emprunt entre les confrères de la place pour combler un besoin ponctuel de trésorerie. Dans le cas où la CBAO est prêteur, à l'échéance et selon les termes de la convention de prêt, la Banque Centrale crédite le compte de la CBAO et lui émet un message sur STAR via SWIFT.

5.1.2 Le processus de paiement dans SICA-UEMOA

Le Système Interbancaire de Compensation Automatisé dans l'UEMOA (SICA-UEMOA) est un outil automatisé d'échange et de règlement des opérations de paiement de masse c'est à dire de petits montants, sous forme de virements, de chèques ou d'effets de commerce, entre établissements participants aux niveaux national et régional. SICA-UEMOA se compose de neuf systèmes de compensation, un système national pour chacun des États membres de l'UMOA et un système de compensation régional. Les participants à SICA-UEMOA sont les banques, la BCEAO, la Poste et le Trésor.

5.1.2.1 Avantages attendus de SICA-UEMOA

SICA-UEMOA assure la compensation multilatérale quotidienne des transactions entre les participants et permet ainsi de réduire :

- les délais d'échange et de règlement des valeurs à support papier (nationales et entre les pays de l'UEMOA), avec comme innovation l'acceptation de toutes les valeurs qu'elles soient « déplacées » ou « hors place » à tous les points d'accès à la compensation (PAC), permettant la réduction des délais d'encaissement de plusieurs semaines à un jour au plus ;
- les risques et les coûts liés à ces délais et aux procédures manuelles de manipulation des valeurs et de leur transport ;

- les besoins de trésorerie nécessaires aux opérations de compensation par la détermination d'un solde de compensation de toutes les opérations nationales d'un participant ;
- Le démarrage du Système Interbancaire de Compensation Automatisé dans l'UEMOA (SICA-UEMOA), amorcé le 17 novembre 2005, au Mali, s'est consolidé le 14 février 2008, avec l'entrée en production de la télé-compensation sous régionale pour les échanges inter-pays.

5.1.2.2 Conditions de participation à SICA-UEMOA

Les conditions de participation à SICA-UEMOA sont de deux ordres à savoir les conditions relatives aux participants et celles relatives aux opérations admises.

5.1.2.2.1 Conditions relatives aux participants

Seuls peuvent être agréés comme établissements participants à la compensation, la BCEAO, les banques, le Trésor public et les services financiers de la Poste. La participation à SICA-UEMOA requiert le strict respect des engagements ci-après contenus dans la convention de compensation et ses annexes :

- être titulaire d'un compte de règlement ouvert dans les livres de la BCEAO ;
- se conformer aux règles interbancaires d'échange des chèques et autres effets de commerce ;
- respecter le format, les règles d'échange et les normes techniques de SICA-UEMOA, décrits dans les manuels techniques ;
- accepter le support électronique comme fondement du règlement.

5.1.2.2.2 Conditions relatives aux opérations admises

Seuls les instruments scripturaux de paiement en vigueur dans les Etats membres de l'UEMOA (actuellement les chèques, lettres de change, billets à ordre, ordres de virement, et avis de prélèvement), libellés en FCFA, sont admis en compensation. Un montant maximum de 50 millions de FCFA est fixé pour les virements présentés à SICA-UEMOA. Au-delà de ce montant, le participant est tenu d'utiliser STAR-UEMOA. En ce qui concerne les chèques ou les effets, aucun plafond n'est prévu.

5.1.2.2.3 Modalités de fonctionnement de la compensation

Le traitement et la comptabilisation de la compensation sont effectués uniquement à partir des fichiers de remises numériques représentant les opérations des participants présentées en compensation.

5.1.2.2.4 Organisation de la journée de compensation

Deux profils de journée de compensation peuvent être définis dans SICA-UEMOA :

- une journée à séance unique ;
- une journée à deux séances.

Pour l'heure, la télé-compensation fonctionne sur la base d'une séance unique par journée d'échanges. La communication et la modification de la journée d'échanges sont du ressort de la BCEAO.

5.1.2.2.5 Gestion des risques dans SICA-UEMOA

La BCEAO ne joue pas le rôle de prêteur de dernier ressort. Il est prévu la constitution d'un fonds commun de garantie par l'ensemble des participants de la place, auquel un participant peut faire appel lorsqu'il a épuisé sans succès les autres moyens d'apporter des liquidités à son compte de règlement pour régler son solde de compensation. Par ailleurs, des sanctions sont prévues en cas de défaillance. Il peut s'agir de suspension ou d'exclusion.

De plus, le traitement par la BCEAO des réclamations et litiges est prévu. Les règles d'archivage définies dans la convention nécessitent l'archivage des données par chaque participant.

5.1.2.2.6 Évolutions récentes de SICA-UEMOA

L'adoption, par les Comités Nationaux de Normalisation (CNN), de nouvelles formules de chèque et d'effets de commerce (lettre de change et billet à ordre) dans l'espace UEMOA respectant les normes internationales a conduit la BCEAO à faire évoluer le Système Interbancaire de Compensation Automatisé dans l'UEMOA (SICA-UEMOA) vers une version prenant en compte les modifications apportées à ces moyens de paiement. Ces nouvelles normes ont été homologuées par la Commission de l'UEMOA et s'imposent à tous les acteurs dans les huit pays de l'UEMOA.

L'une des principales innovations concerne le changement des Relevés d'Identité Bancaire (RIB) avec l'introduction de la norme ISO d'identification des pays en lieu et place des lettres d'identification des pays précédemment retenues dans la zone UEMOA. Cette innovation s'est traduite également par la modification du code ''banque'' des participants à SICA-UEMOA.

Cette nouvelle version de SICA-UEMOA a démarré avec succès le vendredi 08 octobre 2010 et de manière simultanée dans l'ensemble des huit (8) pays de l'UEMOA. Depuis le démarrage de cette version de SICA-UEMOA le lundi 11 octobre 2010, aucun incident majeur n'a été constaté.

Une phase transitoire d'une (01) année a été convenue entre les Comités Nationaux de Normalisation (CNN) durant laquelle les anciennes et nouvelles formules de chèque et d'effet de commerce pourront cohabiter sans difficultés. Les participants sont invités pendant cette phase de procéder au retrait progressif des anciennes formules.

5.1.2.3 Les acteurs impliqués

La plateforme SICA est logée à la direction des opérations, précisément au département des Chèques et Effets de commerce, dans toutes les agences CBAO de Dakar et des autres régions du Sénégal. Plusieurs acteurs sont directement impliqués dans la gestion quotidienne de ce système de paiement. Ce sont ;

- le service clientèle ;
- les conseillers clientèles ;
- les coursiers ;
- l'agent de traitement des Chèques ;
- l'agent de traitement des Effets ;
- Les agents chargés du rapprochement ;
- le responsable du département Traitements de Chèques et Effets.

5.1.2.4 Les différentes étapes du processus

Comme indiqué plus haut, le système de paiement SICA-UEMOA, traite concomitamment les ordres de virement, les chèques et effets de commerce.

5.1.2.4.1 La gestion des ordres de virements

La procédure de saisie des ordres de virement est celle décrite précédemment pour le système de paiement STAR-UEMOA **(voir sous-titre 5.1.1)**. Lors de la génération des

fichiers Lot devant être acheminés à la compensation, le responsable du département de traitement des chèques et effets lance une requête sur l'application Delta Bank et récupère les virements qui respectent les restrictions sur SICA-UEMOA.

5.1.2.4.2 La gestion des chèques et effets de commerce

Elle traite du processus allant de la réception des valeurs, de leur traitement et de leur acheminement à la compensation via SICA.

- **Réception des valeurs**

- **Les chèques**

Le dépôt des chèques se fait aux guichets en y joignant un bordereau de remise en trois volets, dûment remplis et signés par le déposant.

Les agents aux guichets vérifient l'endos des chèques pour s'assurer de l'existence des mentions manuscrites à savoir les numéros du compte, les adresses et contact téléphoniques, les nom et prénoms du bénéficiaire, la raison sociale et le cachet s'il s'agit d'une entreprise, et la signature du remettant.

Lorsqu'ils sont satisfaits de l'endossement des chèques, les agents remettent au déposant un volet du bordereau déchargé et agrafent le reste aux chèques qu'ils inscrivent dans un registre au fur et à mesure de leur réception. A une période précise et lorsque ces agents estiment le nombre de chèques est suffisant pour être traités, ils les font transporter au service Visa et ensuite avec le registre au département de traitement des chèques et effets par le coursier.

- **Les effets de commerce**

Les effets de commerce sont traités sur la base de la crédibilité dont jouit le tiré auprès de la CBAO pour certaines opérations comme l'escompte. Mais pour leur dépôt à l'encaissement, ils fonctionnent à peu prêt comme les chèques, à la différence qu'il faut y coller un timbre fiscal après l'endossement, en plus du fait que ces documents mettent en relation directe le client et son gestionnaire (conseiller clientèle).

- **Transmission des valeurs**

Le coursier transporte les chèques et les effets dans des registres distincts vers les bureaux respectifs des agents de traitements des chèques et effets. Ces derniers prennent le soin de

pointer les valeurs pour vérifier leur conformité d'avec les informations inscrites dans les registres avant de les décharger et de les retourner par la suite au coursier.

5.1.2.4.3 Le traitement des chèques et effets

- **Traitement des valeurs**

La toute première étape de cette tâche est la vérification de conformité des valeurs reçues.

Le contrôle portera sur certaines mentions jugées obligatoires ou facultatives, ce sont entre autres :

- les mentions « chèques » ou « traite ou lettre de change » ou « billet à ordre » ;
- les montants en lettre et en chiffre ;
- l'identité du bénéficiaire ;
- la date du chèque ou de l'effet ;
- le lieu de paiement ;
- la banque du tiré pour les effets;
- la signature ;
- l'endos ;
- un avis de domiciliation permanent pour les effets récurrents.

C'est seulement après avoir vérifié tous les éléments susmentionnés, qu'il sera procédé à la saisie des valeurs sur Delta Bank.

Les chèques sont scannés dans un lecteur pour former un **Fichier Images**. Après chaque séquence de scannage, il apparaît un **Numéro de Remise** à l'écran que l'agent inscrit sur le bordereau qui accompagne le chèque.

L'ensemble des moyens de paiements saisis constituent le **Fichier Remise** dont les montants se déversent automatiquement au crédit des comptes des clients en impactant Delta Bank.

C'est ainsi que toutes les valeurs sont saisies dans les autres agences CBAO du Sénégal.

- **Le rapprochement des valeurs saisies**

Au lendemain de la saisie des valeurs, dans la matinée, le responsable du département lance une requête d'extraction des données de la veille, dans Delta Bank.

Ce sont des données de Dakar et de certaines régions du Sénégal à l'exception des zones de Ziguinchor et Kaolack qui dépendent des agences de la BCEAO de ces localités.

Les données extraites constituent, après quelques mises en forme, le fichier de base du rapprochement contenant le détail des informations sur le client, son numéro de compte, le montant et surtout le numéro de remise.

Les agents chargés du rapprochement procèdent à un pointage des valeurs physiques et du fichier pour s'assurer que les chèques ou effets saisis sont les bons, auquel cas l'on procède à une correction des saisies ou une réclamation.

Après les travaux de rapprochement, les valeurs physiques sont regroupées par confrères et acheminées au bureau de la compensation de l'agence nationale de la Banque Centrale.

- **Validation et Routage de lots vers SICA**

Les trois (03) types de saisies (chèques, effets et virements) formant chacun un **Fichier Lot** sont validés après une autre vérification de l'endos, des montants, des numéros etc., par le responsable du service. Ce dernier prend soin de router en fin de journée ces **Fichiers Lots** dans le dispositif de liaison téléinformatique **(UAP)** en direction du serveur de la Banque Centrale.

Dans le même temps, le poste opérateur reçoit des **CRO** (Compte rendu d'opérations) en provenance de la compense et que l'on impacte à Delta Bank.

5.1.3 Le Système Monétique interbancaire Régional (SMIR)

Comme il a été défini plus haut, le système monétique est un système informatique qui permet la dématérialisation du paiement scriptural. Il se compose de matériels, avec des bornes de paiement, et de logiciels permettant la gestion du paiement par la monnaie électronique. Le support de la monnaie dématérialisée est généralement constitué par une carte de paiement électronique.

Le système bancaire de l'UEMOA a un système monétique auquel a adhéré la CBAO dont elle est un membre de la structure administrative dénommée GIM-UEMOA. De ce fait, certaines cartes de paiements différés ou cartes de crédit telles que VISA, MASTERCARD généralement estampillées du logo de GIM-UEMAO, qu'elle émet, fonctionnent sur le réseau et permettent aux clients CBAO de faire des retraits dans les GAB (Guichets Automatiques) des confrères affiliés au système.

GIM-UEMOA se charge de verser le solde du revenu tiré des transactions de la monétique interbancaire à la CBAO, après des opérations de compensation.

La remise d'une carte de paiement à un client est soumise à une procédure dont il convient de décrire les acteurs et les processus.

5.1.3.1 Les services impliqués

La gestion de la monétique à la CBAO implique plusieurs services et compétences de la banque à savoir :

- le service clientèle ;
- la centrale de référentiel client ;
- le service émission de cartes ;
- le service informatique ;
- les agences.

5.1.3.2 Les différentes étapes du processus

Le processus commence à partir de l'ouverture de son compte par le client jusqu'à la réception effective de sa carte bancaire.

5.1.3.2.1 La demande de cartes bancaires

- **Ouverture de compte**

Les personnes désireuses d'ouvrir un compte à la CBAO sont prises en charge par le service clientèle. Elles transportent par devers elles, leurs documents d'identification et de résidence indispensables à l'ouverture du compte. Ensuite, l'agent du service clientèle soumet un formulaire de demande de carte bancaire au client. Ce dernier le renseigne puis le signe pour marquer son adhésion.

- **Transmission des dossiers à la CRC**

Les dossiers d'ouverture de compte et de demande de cartes bancaires sont transmis à la Centrale de Référentiel Client (CRC) pour un contrôle afin de s'assurer qu'ils ne contiennent pas d'erreurs.

Les liasses de dossiers sont acheminées après vérification, au **Service Emission de cartes** au département du traitement monétique.

5.1.3.2.2 Le traitement des demandes de cartes

- **Génération de numéro de carte**

Les dossiers reçus au Service Emission de cartes sont acheminés au service Visa pour la vérification de conformité de signature.

Après cette étape, les dossiers sont retournés au Service Emission en vue de procéder à leur traitement par les agents. Il s'agit de saisir les informations contenues dans le dossier du client dans le logiciel Powercard Production ayant une interface avec Delta Bank; il s'en suit une génération automatique de numéros de cartes, disponibles sur Delta Bank.

Pour les demandes de cartes des autres agences de Dakar et des régions, les dossiers sont transmis à la direction du réseau et à la Direction Générale pour une double validation.

- **Génération de fichier de personnalisation**

En fin de journée, les agents du service informatique lancent une requête de génération de fichiers de personnalisation des clients. Ces fichiers sont stockés quotidiennement pour former un lot dont il achemine une version cryptée (fichier crypté) au fabriquant à la date de commande, et un fichier récapitulatif (fichier Recap) est transmis au service de la Monétique.

Les commandes sont émises chaque mardi et jeudi, la fabrication et la réception effective des cartes se font dans un délai minimal de deux semaines.

5.1.3.2.3 La gestion post-commande de cartes

- **Réception des cartes bancaires**

Le lot de cartes et des codes est transmis sous pli scellé, au service courrier de la CBAO à travers DHL. Les cartes sont acheminées au département de la monétique et réceptionnées par le service Émission, tandis que les codes sont remis au CRC. Ces deux services procèdent au tri par agence des colis reçus et en font le *dispatching*.

- **Remise des cartes aux clients**

Deux personnes dans l'agence sont habilitées à recevoir les codes, ce sont l'agent de guichet et le responsable des opérations ou l'assistant au chef d'agence.

La carte et le code sont remis au client après décharge du registre de retrait des cartes.

- **Perception de commissions sur monétique interbancaire**

Des commissions sont perçues par la CBAO sur les transactions effectuées par les clients des confrères aux GAB de la banque. Les commissions sont perçues par virement interbancaire ou par prélèvement direct sur le compte de GIM-UEMOA ouvert dans les livres de la CBAO.

5.2 La gestion des risques opérationnels liés aux systèmes de paiement à la CBAO

Depuis le début de l'exercice 2010, un dispositif de gestion de Risques Opérationnels a été mis en place au sein de la CBAO, qui devient ainsi la première filiale internationale du Groupe Attijariwafa Bank à être équipée d'un tel dispositif.

Ce type de disposition répond en partie à la directive dite « Bâle II» qui soumet déjà les filiales sœurs du Groupe se trouvant dans la zone Euro à cette obligation.

Bâle II a pour objet de sécuriser le système bancaire international, en obligeant chaque établissement à mettre en œuvre un dispositif de gestion des risques, et à déterminer la part de ses fonds propres devant être allouée à leur couverture.

Au Sénégal, Bâle II n'est pas encore obligatoire, mais la réflexion est d'ores et déjà lancée au niveau de la BCEAO et de l'Association Professionnelle des Banques et Etablissements Financiers (APBEF). On peut donc s'attendre à ce que des dispositions de ce type soient prises dans un avenir proche.

Au-delà de ce volet règlementaire, la Direction Générale de la CBAO a souhaité à travers le projet « Risques Opérationnels », diffuser au sein de l'organisation, une vraie culture de prévention des risques.

5.2.1 Le modèle de gestion des risques opérationnels lié aux SP

A la CBAO, il a été procédé à la mise en place d'un dispositif de gestion des risques pour tous les métiers de la banque, y compris ceux relatifs aux systèmes de paiements. Ce dispositif est articulé comme suit :

- un Manager des Risques Opérationnels (MRO), chargé d'animer et de piloter la filière Risques Opérationnels et est assisté en cela par :
- trois (03) Correspondants Risques Opérationnels (CRO), qui centralisent et enregistrent les incidents et génèrent le « Reporting Incidents » mensuel.

- des Relais Risques Opérationnels (RRO), au niveau des métiers ou foyers à risques afin de détecter et communiquer les incidents survenus aux CRO.

Vu l'importance que revêt la gestion de ces risques, il a été généralement désigné comme RRO les responsables de chaque métier qui représentent dans un autre cadre, le Contrôle Opérationnel de premier niveau.

Les moyens de paiement étant l'apanage de la direction des opérations, les RRO sont le responsable des services de traitement des chèques et effets, celui du service des opérations locales et celui des opérations internationales. Ils sont donc chargés de compiler tous les incidents potentiels ou survenus pour les acheminer aux CRO.

5.2.2 Identification des risques opérationnels liés aux moyens de paiement

L'identification des risques est la toute première étape de la gestion des risques opérationnels.

Elle consiste à prendre connaissance, tout en déclinant les systèmes de paiement en tâches élémentaires, des événements potentiellement dommageables liés à ces tâches et qui peuvent s'avérer plus ou moins coûteux pour la banque en terme financier, d'image, etc.

A la CBAO, le travail consiste donc à identifier et à décrire tous les risques opérationnels liés aux moyens de paiement. Cette tâche incombe généralement à chaque agent de la banque mais elle est particulièrement celle des agents de la direction des opérations qui ont l'obligation de signaler tout incident et toute source de risque potentiel. Ces agents ont en charge la manipulation de valeurs qui sont la raison d'être de l'institution et objet de toutes les convoitises de l'intérieur comme de l'extérieur. Ainsi, toutefois qu'un agent dans l'exécution de ses tâches quotidiennes constate une anomalie en rapport avec des valeurs (chèques, ordres de virement, effet de commerce…), par intuition ou par expérience, il conçoit un tableau Excel dans lequel ces incidents sont logés et transmis par la suite à son responsable de département ou service qui n'est autre que le RRO. Ce dernier compile tous les incidents reçus de ses collaborateurs, les trie par ordre de priorité, élimine ceux qui sont moins pertinents et les remonte vers les CRO. Ceux-ci consolident les informations à leur niveau pour ensuite les transmettre au MRO.

5.2.3 Évaluation des risques opérationnels liés aux moyens de paiements

Après l'étape de l'identification, celle de l'évaluation consistant à répertorier chaque risque opérationnel, en fonction de sa fréquence et de son niveau de gravité, s'est

matérialisée au travers de l'élaboration d'une cartographie des Risques Opérationnels de la CBAO qui n'a malheureusement pas été mis à notre disposition par l'Audit pour une revue complète car n'ayant pas encore été validée et vulgarisée au sein de la banque.

Néanmoins, selon les explications du responsable de l'Audit interne, le dispositif d'évaluation s'appuie sur :

- l'auto évaluation des risques et des contrôles qui a pour but d'identifier et de mesurer l'exposition de la banque aux risques opérationnels liés aux moyens de paiement. Cela permet d'établir la cartographie des risques en définissant une échelle de cotation de 5 points estimant la probabilité de survenance avec les lettres (a, b, c, d, e), et l'impact par des tranches de montant allant de 0 FCFA à plus de 10 Milliards de FCFA ;
- les Indicateurs Clés de Risques ou Key Risk Indicators (KRI), qui alertent sur les risques potentiels de pertes opérationnelles. Ces indicateurs sont des données objectives et mesurables permettant d'évaluer les risques clés.

Parallèlement, une organisation a été mise en place pour assurer le suivi au quotidien de ces risques majeurs, et les enregistrer lorsqu'ils surviendront.

En effet, le but visé est de sécuriser les processus, en réduisant les risques de dysfonctionnement, et contribuer ainsi à minimiser les pertes accidentelles, dont les montants peuvent s'avérer conséquents.

5.2.4 Suivi des risques

La filière Risques Opérationnels est organisée de manière à détecter, à centraliser et à formaliser les incidents au fil de l'eau. Il existe plusieurs intervenants dans le système de collecte des incidents, mais chaque salarié ayant détecté un incident opérationnel, doit en informer sa hiérarchie. Le responsable du service concerné collecte les données et les vérifie avant de les transmettre, sur une fiche, au RRO chargé de sa zone de métier.

Ainsi, il s'assure :

- qu'il s'agit d'un incident liés aux risques opérationnels ;
- qu'il dispose de suffisamment d'informations sur les impacts associés.

Cette dernière étape ne doit cependant pas ralentir le signalement d'un risque opérationnel dont les conséquences seraient potentiellement graves. La fiche doit être sauvegardée dans un répertoire dédié qui au-delà de son traitement dans le cadre de la gestion des risques

opérationnels (GRO), est mis à la disposition du Contrôle de Conformité et de l'Audit Général lors des contrôles sur place.

En sus, le comité Risque Opérationnel, en présence de la Direction Générale, permet de :

- suivre les incidents ;
- proposer et prioriser les plans d'action sur les incidents les plus significatifs afin de ramener les risques à un niveau acceptable ;
- suivre l'avancement des plans d'action déjà définis lors des comités précédents.

5.2.5 Le dispositif de Contrôle Interne

Le contrôle interne est un processus, exercé en commun par le comité de direction, les responsables hiérarchiques et les collaborateurs, pour donner une assurance raisonnable quant à la réalisation des objectifs d'entreprise. Le contrôle interne a une dimension préventive. Il doit de ce fait couvrir le risque de contrepartie, les risques de marché, le risque de liquidité, le risque opérationnel et le risque juridique.

L'organe exécutif est responsable de la mise en place d'un système de contrôle interne. Le système repose notamment sur une formalisation complète des procédures, des modalités de traitement et d'enregistrement des opérations, sur une claire délégation des pouvoirs et des responsabilités, ainsi qu'une stricte séparation des fonctions. Cela suppose que le mode opératoire fasse l'objet d'une documentation suffisamment explicite, régulièrement mise à jour et diffusée aux personnes concernées.

La formalisation des procédures de traitement des opérations est un chantier complété à 99% au 30 Juin 2011 à la CBAO ; cela dit, il apparaît clairement que les différents départements de la banque ne disposent pas encore de manuel de procédure qui érige leurs fonctionnements.

Cependant, les entretiens avec les agents et les responsables opérationnels nous ont permis de savoir que le système de contrôle interne de la banque, consiste généralement en une double validation des opérations les plus risquées, la séparation des tâches, la sécurisation et l'isolement des bureaux abritant les dispositifs de validation définitive des ordres de paiement, les mesures de prévention destinées à réduire les risques en agissant sur la fréquence de survenance des événements générateurs ou sur l'atténuation de l'impact en cas de survenance. Il faut bien citer les contrôles en amont des événements générateurs de risques, les revues du contrôle permanent et du contrôle périodique.

Conclusion Chapitre 5

Ce chapitre nous a permis de prendre connaissance des processus se rapportant aux systèmes de paiement, des dispositifs de gestion des risques opérationnels et de contrôle interne à la CBAO. Il convient, à la suite de ce qui précède, de s'interroger sur la démarche à adopter en vue d'une analyse efficace des risques opérationnels liés aux systèmes de paiement. Nous répondrons à cette question dans la suite de notre étude.

CHAPITRE 6 : ANALYSE DE LA GESTION DES RISQUES OPERATIONNELS LIES AUX SYSTEMES DE PAIEMENT A LA CBAO

Les différents processus liés aux systèmes de paiement sont exposés à des risques variés. On peut dénombrer entre autres les risques de fraude, de perte, de dégradation du système bancaire dus aux agents de la banque qui interviennent dans les processus ou aux procédures mis en place. La survenance de ces risques peut éprouver durement l'équilibre financier de la banque et l'empêcher d'atteindre ses objectifs.

Ainsi, une tâche exécutée ou omise peut comporter soit des risques positifs pouvant être source d'un éventuel profit, soit des risques négatifs par la menace d'une perte. En effet, la gestion des risques opérationnels vise à minimiser la probabilité de survenance de cette perte, mais elle donne la possibilité de saisir des opportunités provenant de l'environnement de la banque. La gestion des risques opérationnels est donc très importante pour la banque car une bonne gestion de ces risques donne a priori aux dirigeants l'assurance de la pérennité de l'activité.

Cependant, la mise en place des seuls outils de contrôle demeure insuffisante pour la gestion des risques opérationnels liés aux systèmes de paiement. D'où la nécessité de procéder à l'analyse de la gestion de ces risques opérationnels.

Ce chapitre est organisé en cinq sections dont la première sera consacrée à l'analyse de la cartographie actuelle des risques, la deuxième concernera l'identification des risques liés à STAR-UEMOA, SICA-UEMOA et à la Monétique, la troisième portera sur l'évaluation de ces risques, la quatrième sur l'évaluation du dispositif de contrôle interne, la dernière sections sera consacrée à l'analyse et aux recommandations.

6.1 Analyse de la cartographie des risques à la CBAO

La gestion des risques liés aux systèmes de paiement passe nécessairement par un minimum de dispositif et d'organisation au sein de la banque. Le premier grand chantier en vue de maîtriser ces risques reste l'élaboration d'une cartographie de risque ; cela donne une vision beaucoup plus précise des menaces auxquelles la banque est exposée et une estimation chiffrée des éventuels préjudices liés à leurs survenances.

Comme indiqué précédemment, la CBAO a vu juste en lançant le projet de réalisation d'une cartographie couvrant les risques potentiels de la banque, avec le concours d'experts internationaux en la matière.

La logique voudrait bien qu'on prenne connaissance de ce document, qu'on en ressorte les insuffisances après l'avoir analysé, pour ensuite faire des propositions d'amélioration.

Malgré le fait que cette cartographie soit en phase terminale de conception (réalisée à plus de 90%), elle demeure un projet qui n'est pas encore en vigueur, car pas encore validé par le comité de direction. Nous ne pouvions fonder nos recherches sur une documentation non officielle. Ainsi n'en avons nous pas tenu compte lors de nos analyses ; nous nous sommes plutôt basé sur les différents processus de la banque se rapportant aux systèmes de paiement pour élaborer une cartographie des risques.

Nos résultats peuvent venir en appoint de ce qui a déjà été réalisé dans la recherche de solutions pour la maîtrise des risques opérationnels liés aux systèmes de paiement.

6.2 Identification des risques opérationnels liés aux systèmes de paiements

Il s'agira de répertorier tous les risques opérationnels associés aux différentes tâches liées aux systèmes de paiement. Ce sont des risques de perte résultant :

- des défaillances d'exécution des tâches telles que les saisies erronées des données, les omissions de données, les erreurs sur les numéros de comptes ;
- des défaillances liées aux procédures ;
- de l'incompétence et l'indisponibilité des ressources humaines, de la fraude interne;
- des défaillances du système informatique.

Cependant, quels sont les risques opérationnels spécifiques aux systèmes de paiement à la CBAO ?

Pour chaque système de paiement, nous avons scindé le processus en tâches distinctes.

Ainsi pour STAR-UEMOA et en accord avec le trésorier et certains de ses collaborateurs, nous avons énuméré et classé selon les opérations, les sous-processus suivants :

- **opérations de clientèle**

  - la gestion des courriers d'ordre de virement ;
  - le traitement des ordres de virement.

- **les opérations de banque à banque**

  - blocage de fonds ;
  - opération de trésorerie interbancaire.

Concernant SICA-UEMOA, en collaboration avec le responsable du service de traitement des chèques et effets, nous avons énuméré les sous-processus suivants :

- la gestion des valeurs (chèques et effets) ;
- le traitement des valeurs (virements, chèques et effets).

Pour ce qui concerne la Monétique, avec la responsable de ce département, nous avons énuméré les sous-processus suivants :

- l'ouverture de compte ;
- traitement des demandes et commande des cartes ;
- la gestion post commande des cartes.

A l'aide des questionnaires administrés aux différents acteurs des processus, nous avons scindé les processus en sous-processus et les sous-processus en tâches. Les travaux effectués nous ont permis de renseigner les tableaux d'identification des risques à cinq (05) colonnes décomposées comme suit :

- la tâche qui correspond au découpage du processus liés à chaque système de paiement en opérations élémentaires ;
- l'objectif de contrôle interne ;
- le risque opérationnel lié à l'exécution de la tâche ;
- l'impact opérationnel qui traduit la conséquence du risque sur l'activité de la banque ;
- le dispositif de maîtrise des risques.

Nous avons ci-après les tableaux d'identification des risques associés à chaque système de paiement et qui sont susceptibles de survenir.

- **Identification des risques opérationnels liés à STAR-UEMOA**

Tableau 2: Identification des risques opérationnels liés aux sous-processus « gestion des ordres de virement »

Sous-processus : gestion des ordres de virement				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Réception du courrier	S'assurer de la traçabilité et de la conformité des informations contenues dans le courrier	1. Non conformité 2. Confusion courriers virements et courriers ordinaires	-dégradation d'image	- Réception et tri des courriers - Sauvegarde dans des casiers distincts
Réception des bordereaux	S'assurer de l'exhaustivité des informations inscrites sur le bordereau	3. Rejet du bordereau 4. Retard de réception	- Retard de virement et mauvaise réputation	Vérification minutieuse du bordereau par le conseiller client et agents de guichet
Transmission des ordres de virement	S'assurer de la transmission effective et à temps des ordres	5. Perte de courriers et de bordereaux 6. Retard de transmission des ordres	- Perte de clients - Perte financière -.Mauvaise réputation	Fixer un délai précis de transmission des ordres de virement reçus

Source : nous-mêmes

Cette étape nous a permis d'identifier la plupart des risques attachés à la gestion des ordres de virement. Ce tableau montre à quel point il est important de gérer de façon diligente ces ordres de virement afin de préserver la collaboration entre la banque et ses clients.

Tableau 3 : Identification des risques opérationnels liés au sous-processus « traitement des ordres de virement »

Sous-processus : traitement des d'ordre de virement				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Vérification de signature	S'assurer de la conformité des signatures	7. Signature non conforme 8. Collusion DFC entreprise et agents Service Visa	- Perte Financière - Litige avec le client - Perte de Confiance	Double vérification de signature avant le visa
Imputation des comptes	S'assurer de la fiabilité des imputations	9. Chevauchement de numéros de comptes 10. Saisie valeurs erronés	- Litige avec clients - Perte Financière	Dispositif de contrôle de deuxième niveau
Saisie de l'ordre de virement	S'assurer de la justesse des données saisies dans SWIFT	11- Erreur de saisie 12- Fraude	- Perte financière - Perte financière	Dispositif de contrôle de deuxième niveau
Validation de l'ordre de virement	S'assurer de la saisie correcte des valeurs	13. Négligence	- Perte financière	Vérification méticuleuse des données saisies
Routage de l'ordre dans le système STAR	S'assurer que l'ordre est acheminé à la BCEAO	14. Omission 15. Perturbation réseau 16. Panne électrique	- Perte financière - Perte Financière	Diligence de traitement des ordres ; source électrique autonome

Source : nous-mêmes

Ce tableau fait ressortir les risques liés au traitement des ordres de virement. Une attention particulière doit être portée sur cette étape car les risques énumérés sont généralement une source de perte financière.

- **Identification des risques opérationnels liés à SICA-UEMOA**

Tableau 4: Identification des risques opérationnels liés au sous-processus « gestion des valeurs »

Sous-processus : Gestion des valeurs				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Réception des chèques et effets	S'assurer de l'exhaustivité et de la conformité des informations inscrites sur le bordereau de remise	1. Non exhaustivité 2. Rejet des bordereaux de remise	- Perte financière - Conflit avec le client	Vérification méticuleuse des bordereaux et des valeurs
Vérification de l'endos des valeurs	S'assurer que toutes les valeurs reçues sont correctement endossées	3. Rejet des valeurs 4. Usage frauduleux en cas de perte ou vol	- Conflit avec clients - Perte Financière	Vérifier immédiatement l'endos des valeurs reçues
Transmission des valeurs reçues	S'assurer de la transmission effective et à temps des valeurs	5. Perte des valeurs 6. Retard de Transmission des valeurs	- Perte de clients - Perte financière -Mauvaise Réputation	Fixer un délai précis de transmission des ordres de virement reçus

Source : nous-mêmes

Cette étape nous a permis d'identifier la plupart des risques attachés à la gestion des valeurs. Ce tableau montre à quel point il est important de gérer de façon diligente ces valeurs afin de préserver la collaboration entre la banque et ses clients.

Tableau 5: Identification des risques opérationnels liés au sous-processus « traitement des valeurs »

Sous-processus : Traitement des valeurs				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Saisie des chèques et effets	S'assurer de l'exhaustivité et de la conformité des saisies	7. Non exhaustivité des saisies 8. Erreurs de saisie 9. Retard de saisie	- Perte financière - Conflit avec le client	Validation des données saisies par un tiers habilité et délai précis de saisie
Scannage des valeurs	S'assurer de la bonne qualité ses images	10. Mauvaise qualité des images	- Perte Financière	Vérifier immédiatement l'endos des valeurs reçues
Transcription du numéro de remise sur le bordereau	S'assurer de la transcription effective du numéro de remise	11. Omission 12. Erreur de transcription	- Difficile rapprochement données saisies et valeurs	Vérifier la conformité du numéro de remise après sa transcription
Validation des données saisies	S'assurer de la fiabilité des données	13. Données non fiables	- Perte Financière	Vérification méticuleuse des données saisies
Génération de Fichiers Lots	S'assurer de la conformité des fichiers lots	14. Non conformité	- Perte Financière	Rapprochement fichiers lots et valeurs par une personne habilitée
Rapprochement des fichiers lots	S'assurer de la conformité des fichiers lots aux valeurs physiques.	15. Non exhaustivité des rapprochements	- Perte Financière	Vérification minutieuse des données
Routage des fichiers lots dans SICA	S'assurer de l'acheminement effectif des fichiers dans le système	16. Instabilité liaison télécommunication 17. Perturbation de l'échange image	- Perte Financière	

Source : nous-mêmes

Ce tableau fait ressortir les risques liés au traitement des valeurs. Une attention particulière doit être portée sur cette étape car les risques énumérés sont généralement une source de perte financière.

- **Identification des risques liés à la Monétique**

Tableau 6: Identification des risques opérationnels liés au sous-processus « demande de cartes bancaires »

Sous-processus : demande de cartes bancaires				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Ouverture de comptes	S'assurer de la bonne identification du client et de l'effectivité de sa demande de carte bancaire	1. Erreur sur l'identité 2. Omission de proposition de fiche de demande de carte	-contestation du client - Perte Financière	Vérification du profil du client par un service ou une personne habilitée
Transmission des dossiers d'ouverture de comptes	S'assurer que tous les dossiers ont été transmis	3. Perte de dossiers 4. Retard de transmission 5. Omission de transmission	- Conflit avec clients - Perte Financière	Fixer un délai précis de transmission des dossiers
Contrôle des dossiers transmis	S'assurer que les dossiers ne sont pas litigieux et ne contiennent pas d'erreur	6. Validation dossiers de clients indésirables 7. Négligence 8. Erreur de pointage	- Image dégradée - Perte Financière	Vérification minutieuse des dossiers

Source : nous-mêmes

A travers cette étape, nous avons déterminé les risques liés à la demande de cartes bancaires des clients. Cela montre qu'il appartient déjà à la banque de prendre certaines dispositions dès que le client exprime le besoin de la carte.

Tableau 7: Identification des risques opérationnels liés au sous-processus « traitement des demandes de cartes bancaires »

Sous-processus : traitement des demandes de cartes bancaires				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Génération de numéros de cartes	S'assurer de la fiabilité des données saisies	9. Erreur de saisie	- Conflit avec client	Dispositif de contrôle par une personne habilitée
Génération de fichier de personnalisation	S'assurer de la fiabilité des fichiers générés	10. Fichiers générés sur la base de saisies erronées	- Perte Financière	Rapprochement dossier clients et fichiers

Source : nous-mêmes

Tableau 8: Identification des risques opérationnels liés au sous-processus « Gestion post commande »

Sous-processus : Gestion post commande				
Tâches	Objectifs de CI	Risques Opérationnels	Impact Opérationnel	Dispositif de maîtrise de risque
Réception des lots de cartes et de codes	S'assurer de l'exhaustivité et de l'intégrité des cartes et codes reçus	11. Perte de cartes / de codes 12. Fraude	-dégradation image - Perte Financière	Désigner des services distincts pour la réception de cartes et codes
Transmission de cartes et codes	S'assurer de la transmission à la bonne agence	13. Se tromper d'agence	Conflit avec clients	Trier et ranger les cartes et codes par agence
Remise des cartes et codes aux clients	S'assurer que les clients ont retirés ou pas leurs cartes et codes	14. réclamation de documents déjà retirés	Conflit avec clients	Avis de mise à disposition signé et daté par les clients
Perception des commissions sur monétique	S'assurer que les commissions perçues sont exactes	15. Perception partielle	- Perte financière	Un agent commis pour calculer les commissions

Source : nous-mêmes

Les deux précédentes étapes montrent bien l'omniprésence des risques depuis la commande des cartes bancaires, leur émission et leur utilisation. A ce niveau, une gestion rigoureuse est préconisée car le risque de fraude est très élevé pour tous les établissements de crédit.

6.3 Évaluation des risques opérationnels identifiés

L'évaluation des risques est le processus qui consiste à déterminer leur probabilité de survenance et leur impact sur l'activité.

L'objectif de cette évaluation consiste à éliminer un danger ou réduire le niveau de risque en adoptant des mesures de maîtrise ou en adoptant des précautions appropriées.

6.3.1 Évaluation de la probabilité de survenance

La fréquence de survenance des risques est évaluée en s'appuyant sur les résultats des tests d'existence et de permanence effectués durant notre stage à la CBAO. L'évaluation est faite à partir du modèle ci-dessous :

Tableau 9: Échelle de cotation de la vulnérabilité estimée au risque

Niveau	Probabilité	Description
3	Forte	Il est bien possible que le risque se produise
2	Moyenne	Il est éventuellement possible que le risque se produise
1	Faible	Il est difficile que le risque se produise

Source : nous-mêmes

Dans cette échelle de cotation, nous avons attribué des notes allant de 1 à 3 en fonction de notre estimation de la probabilité de survenance du risque.

Ainsi nous attribuons la note "3" en vue de montrer que pour une tâche donnée, il est tout à fait possible que le risque se matérialise malgré le dispositif de sécurité mise en place. Pour la note "2", il existe un doute concernant la matérialisation du risque. Pour la note "1", il est difficile de voir le risque se réaliser.

- **STAR-UEMOA**

Tableau 10: Évaluation de la probabilité d'occurrence des risques opérationnels

RISQUES	PROBABILITE
1. Non-conformité des informations	1
2. Confusion courriers de virements et courriers ordinaires	2
3. Rejet du bordereau	1
4. Retard de réception	2
5. Perte de courrier et de bordereaux	2
6. Retard de transmission des ordres	2
7. Validation de signature non conforme	2
8. Collusion DFC entreprise et Agent Service Visa	2
9. Chevauchement de numéros de comptes	2
10. Saisie de montants erronés	2
11. Erreur de saisie de code	2
12. Fraude	3
13. Négligence	1
14. Omission	1
15. Perturbation réseau	1
16. Panne électrique	3

Source : nous-mêmes

Au regard de l'échelle de cotation susmentionnée, puis en se basant sur les entretiens avec les opérationnels, l'analyse des risques susceptibles de se produire nous permet d'attribuer les notes ci-dessus. Il faut par ailleurs relever que la note 3 a été attribuée au risque de panne

électrique à cause de la situation de délestage à Dakar. Les interruptions d'électricités sont y récurrentes.

- **SICA-UEMOA**

Tableau 11: Evaluation de la probabilité d'occurrence des risques opérationnels

RISQUES	PROBABILITE
1. Non exhaustivité	1
2. Rejet des bordereaux de remise	1
3. Rejet des valeurs	3
4. Usage frauduleux	2
5. Perte des valeurs	3
6. Retard de transmission des valeurs	2
7. Non exhaustivité des saisies	2
8. Erreurs de saisie	2
9. Retard de saisie	2
10. Mauvaise qualité des images	1
11. Omission	2
12. Erreur de transcription	1
13. Données non fiables	2
14. Non-conformité des saisies	3
15. Non exhaustivité des rapprochements	3
16. Instabilité liaison de télécommunication	1
17. Perturbation de l'échange image	1

Source : nous-mêmes

Il convient de noter ici que les risques les plus probables sont la perte de valeurs, la non-conformité des saisies comme il a été confirmé par les opérationnels. Un chèque perdu peut être encaissé par une tierce personne et une erreur sur le numéro de compte du bénéficiaire d'une valeur peut engendrer une grosse perte financière pour la banque.

- **MONETIQUE**

Tableau 12**:** Evaluation de la probabilité d'occurrence des risques opérationnels

RISQUES	PROBABILITE
1. Erreur sur l'identité du client	2
2. Omission de proposition de fiche de demande de carte	1
3. Perte de dossiers	3
4. Retard de transmission	2
5. Omission de transmission	1
6. Validation dossiers de clients indésirables	3
7. Négligence	1
8. Erreur de pointage	2
9. Erreur de saisie	2
10. Fichiers générés sur la base de saisies erronées	2
11. Perte de cartes / de codes	2
12. Fraude	3
13. Se tromper d'agence	1
14. réclamation de documents déjà retirés	2
15. Perception partielle	3

Source : nous-mêmes

Les probabilités d'occurrence de risques les plus élevées telles que « la validation de dossiers de clients indésirables » sont dues au fait que ces clients sont répertoriés comme dangereux dans les rapports que les institutions de crédit déposent chez le régulateur. Les avoir comme client et leur éditer une carte bancaire pourraient mettre en péril l'institution.

6.3.2 Évaluation de l'impact des risques identifiés

Cette évaluation nous permettra de déterminer le niveau d'impact sur la base des conséquences engendrées par ces risques. A l'instar de la fréquence de survenance des risques, nous procéderons à une évaluation qualitative de l'impact des risques. Cette évaluation fait appel à l'échelle ci-après :

Tableau 13: Échelle de mesure de la gravité ou de l'impact des risques

Niveau	Impact	Description
3	Important	Incidence élevée en perte financière
2	Modéré	Conséquence moyenne en perte financière
1	Mineur	Incidence négligeable en perte financière

Source : nous-mêmes

Les chiffres attribués tiennent compte de l'importance des pertes financières potentielles engendrées par la survenance d'un risque. Les tableaux ci-dessous présentent les résultats de cette évaluation :

- **STAR-UEMOA**

Tableau 14: Évaluation de l'impact des risques identifiés

RISQUES	IMPACT
1. Non-conformité des informations	1
2. Confusion courriers de virements et courriers ordinaires	1
3. Rejet du bordereau	1
4. Retard de réception	1
5. Perte de courrier et de bordereaux	2
6. Retard de transmission des ordres	2
7. Validation de signature non conforme	3
8. Collusion DFC entreprise et Agent Service Visa	3
9. Chevauchement de numéros de comptes	2
10. Saisie de montants erronés	2
11. Erreur de saisie de code	1
12. Fraude	3
13. Négligence	2
14. Omission	1
15. Perturbation réseau	1
16. Panne électrique	1

Source : nous-mêmes

La collusion entre le DFC d'une entreprise et un agent de la banque pourrait causer un préjudice financier important à la banque.

- **SICA-UEMOA**

Tableau 15: Évaluation de l'impact des risques identifiés

RISQUES	IMPACT
1. Non exhaustivité	1
2. Rejet des bordereaux de remise	1
3. Rejet des valeurs	1
4. Usage frauduleux	3
5. Perte des valeurs	3
6. Retard de transmission des valeurs	1
7. Non exhaustivité des saisies	2
8. Erreurs de saisie	2
9. Retard de saisie	1
10. Mauvaise qualité des images	1
11. Omission	1
12. Erreur de transcription	1
13. Données non fiables	2
14. Non-conformité des saisies	2
15. Non exhaustivité des rapprochements	2
16. Instabilité liaison de télécommunication	2
17. Perturbation de l'échange image	1

Source : nous-mêmes

La perte et l'usage frauduleux d'un chèque imputable à la banque va constituer forcement une perte financière considérable.

- **MONETIQUE**

Tableau 16: Évaluation de l'impact des risques identifiés

RISQUES	IMPACT
1. Erreur sur l'identité du client	3
2. Omission de proposition de fiche de demande de carte	1
3. Perte de dossiers	1
4. Retard de transmission	1
5. Omission de transmission	1
6. Validation dossiers de clients indésirables	3
7. Négligence	2
8. Erreur de pointage	2
9. Erreur de saisie	2
10. Fichiers générés sur la base de saisies erronées	2
11. Perte de cartes / de codes	3
12. Fraude	3
13. Se tromper d'agence	1
14. réclamation de documents déjà retirés	1
15. Perception partielle	2

Source : nous-mêmes

6.3.3 La criticité des risques opérationnels identifiés

La cartographie des risques est un véritable inventaire des risques d'une organisation permettant d'atteindre trois objectifs :

- inventorier, évaluer et classer les risques de l'organisation ;

- informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités ;
- permettre à la Direction générale, et avec l'assistance du risk manager, d'élaborer une politique de risque qui va s'imposer à tous.

La CBAO qui une organisation assez importante par sa taille, doit élaborer une cartographie des risques opérationnels qui est un outil de suivi des activités de la banque. Pour ce faire, elle procède à l'évaluation de ces risques, ce qui lui permettra de voir les risques les plus importants à surveiller et contre lesquels il convient de prendre des dispositions et des procédures efficaces.

- **STAR-UEMOA**

Tableau 17: Criticité des risques identifiés

Risques	Probabilité	Impact	Criticité
1. Non-conformité des informations	1	1	1
2. Confusion courriers virements / courriers ordinaires	2	1	2
3. Rejet du bordereau	1	1	1
4. Retard de réception	2	1	2
5. Perte de courriers et de bordereaux	2	2	4
6. Retard de transmission des ordres	2	2	4
7. Validation de signature non conforme	2	3	6
8. Collusion DFC entreprise et Agent Service Visa	2	3	6
9. Chevauchement de numéros de comptes	2	2	4
10. Saisie de montants erronés	2	2	4
11. Erreur de saisie de code	2	1	2
12. Fraude	3	3	9
13. Négligence	1	2	2
14. Omission	1	1	1
15. Perturbation réseau	1	1	1
16. Panne électrique	3	1	3

Source : nous-mêmes

- **SICA-UEMOA**

Tableau 18: Criticité des risques identifiés

Risques	Probabilité	Impact	Criticité
1. Non exhaustivité	1	1	1
2. Rejet des bordereaux de remise	1	1	1
3. Rejet des valeurs	3	1	3
4. Usage frauduleux	2	3	6
5. Perte des valeurs	3	3	9
6. Retard de transmission des valeurs	2	1	2
7. Non exhaustivité des saisies	2	2	4
8. Erreurs de saisie	2	2	4
9. Retard de saisie	2	1	2
10. Mauvaise qualité des images	1	1	1
11. Omission	2	1	2
12. Erreur de transcription	1	1	1
13. Données non fiables	2	2	4
14. Non-conformité des saisies	3	2	6
15. Non exhaustivité des rapprochements	3	2	6
16. Instabilité liaison de télécommunication	1	2	2
17. Perturbation de l'échange image	1	1	1

Source : nous-mêmes

- **MONETIQUE**

Tableau 19: Criticité des risques identifiés

Risques	Probabilité	Impact	Criticité
1. Erreur sur l'identité du client	2	3	6
2. Omission de proposer la fiche de demande de carte	1	1	1
3. Perte de dossiers	3	1	3
4. Retard de transmission	2	1	2
5. Omission de transmission	1	1	1
6. Validation dossiers de clients indésirables	3	3	9
7. Négligence	1	2	2
8. Erreur de pointage	2	2	4
9. Erreur de saisie	2	2	4
10. Fichiers générés sur la base de saisies erronées	2	2	4
11. Perte de cartes / de codes	2	3	6
12. Fraude	3	3	9
13. Se tromper d'agence	1	1	1
14. réclamation de documents déjà retirés	2	1	2
15. Perception partielle	3	2	6

Source : nous-mêmes

6.4 Évaluation du dispositif de Contrôle Interne existant

Le contrôle interne est l'ensemble des sécurités contribuant à la maîtrise des activités de l'entreprise. C'est à juste titre que le comité de Bâle souligne qu'un système de contrôle interne fort contribue à la réalisation des objectifs de l'organisation en termes de rentabilité.

Le contrôle interne a une dimension préventive. Les banques et établissements financiers doivent ainsi être en mesure d'identifier l'ensemble des facteurs internes et externes, susceptibles de compromettre la réalisation des objectifs fixés par la direction générale.

Cette étape de notre étude vise à évaluer la qualité des contrôles mis en place par le comité de direction de la CBAO dans l'exécution des différentes tâches liées aux systèmes de paiement en vue de maîtriser les risques opérationnels. L'évaluation permet d'établir de manière synthétique que les contrôles mis en œuvre en vue de couvrir les risques majeurs de l'entreprise sont conformes aux attentes de la CBAO.

Cette évaluation se fait sur la base du questionnaire de contrôle interne (annexe 3), du diagramme de circulation (annexe 2), de la grille de séparation des tâches (annexe 4), des tests de conformité et de permanence (annexe 7), et du tableau des forces et faiblesses apparentes (TFfa) (annexe 5).

Les tableaux d'évaluation ci-dessous sont déclinés en trois colonnes :

- tâches : c'est le découpage du processus en a activités élémentaires ;

- dispositif de CI : ce sont les sécurités mises en place pour le contrôle des systèmes ;
- constat : le **oui** constitue une force et le **non** est une faiblesse.

- **STAR-UEMOA**

Tableau 20: Evaluation du dispositif de contrôle interne lié à STAR-UEMOA

Tâches	Dispositif de contrôle interne	Constat
Réception des ordres de virements	- Existence et Application d'un manuel de procédure - Vérification de montants et autres informations contenues dans les courriers et bordereaux - Casiers de séparation des courriers par nature	Non Oui Non
Circuit de transmission des ordres de virement	- Existence de cahiers de transmission - Définition d'une période précise de transmission	Oui Non
Traitement des ordres de virement	- Double validation de signature - Procédure de saisie des ordres - Vérification automatisée des soldes clients	Non Oui Oui
Circuit de validation des ordres de virement	- Procédure de vérification des ordres saisis, par une personne habilitée - Procédure de validation des ordres	Oui Oui
Contrôle des risques	- Recensement rigoureux de tous les risques opérationnels - Dispositif dédié de gestion des risques opérationnels - Surveillance permanente des risques - Tenue trimestrielle du comité de risques opérationnels	Non Oui Oui Oui

Source : nous-mêmes inspiré de Renard (2010 : 239)

- **SICA-UEMOA**

Tableau 21: Evaluation du dispositif de contrôle interne lié à SICA-UEMOA

Tâches	Dispositif de contrôle interne	Constat
Réception des valeurs	- Existence et Application d'un manuel de procédure - Vérification de montants et autres mentions sur les bordereaux de remise de chèques et effets - Vérification de l'endos des valeurs	Non Oui Oui
Circuit de transmission des valeurs	- Existence de cahiers de transmission - Définition d'une période précise de transmission	Oui Non
Traitement des valeurs	- Vérification des valeurs et des bordereaux de remise avant la saisie - Procédure de saisie des valeurs - Maintenance régulière des scanneurs	Oui Oui Oui
Circuit de validation des valeurs	- Procédure de rapprochement des valeurs saisies, par une personne habilitée - Procédure de validation des données saisies	Oui Oui
Contrôle des risques	- Recensement rigoureux de tous les risques opérationnels - Dispositif dédié de gestion des risques opérationnels - Surveillance permanente des risques - Tenue trimestrielle du comité de risques opérationnels	Non Oui Oui Oui

Source : nous-mêmes inspiré de Renard (2010 : 239)

- **MONETIQUE**

Tableau 22: Evaluation du dispositif de contrôle interne lié à la Monétique

Tâches	Dispositif de contrôle interne	Constat
Ouverture de compte	- Vérification de l'identité et d'autres documents fournis par le client	Oui
Circuit de transmission	- Existence de cahiers de transmission - Définition d'une période précise de transmission	Oui Non
Contrôle de dossiers transmis	- Vérification du profil du client par un service habilité - Procédure de validation et de rejet de dossiers	Oui Oui
Traitement des dossiers de demande de cartes	- Double validation de signature - Procédure de saisie des dossiers - Vérification des dossiers avant la saisie	Non Oui Oui
Gestion post commande de cartes	- Réception distinctes des cartes et codes - Tri des cartes par agences et avis de mise à disposition signé et daté - Existence d'une cellule de contrôle des soldes de la compense monétique	Oui Oui Oui Oui
Contrôle des risques	- Recensement rigoureux de tous les risques opérationnels - Dispositif dédié de gestion des risques opérationnels - Surveillance permanente des risques - Tenue trimestrielle du comité de risques opérationnels	Non Oui Oui Oui

Source : nous-mêmes inspiré de Renard (2010 : 239)

Le dispositif de contrôle interne n'est pas un gage de sécurité absolue quelque soit la qualité de sa conception et de son application.

L'atteinte de ses objectifs en termes de rentabilité et de croissance, ne relève pas de la seule volonté de la banque. En effet, il existe en plus d'éventuelles erreurs et défaillance humaines, des facteurs exogènes qui échappent au contrôle de la banque.

Il ressort de notre analyse que le dispositif de Contrôle Interne de CBAO se rapportant aux systèmes de paiement revêt quelques insuffisances car nous notons l'inexistence de certaines composantes essentielles du Contrôle Interne comme en témoignent les différents tableaux d'évaluation.

L'évaluation du dispositif de Contrôle Interne nous conduit à l'élaboration de la cartographie des risques opérationnels liés aux systèmes de paiement. Ci-après, les différentes matrices des risques opérationnels liés aux systèmes de paiement :

Figure 3: Elaboration de la matrice des risques opérationnels liés à STAR-UEMOA

Forte	16. Panne électrique		3. Fraude
Moyenne	2. Confusion courriers virements/courriers ordinaires 4. Retard de réception 11. Erreur de saisie	5. Perte de courriers et de bordereaux 6. Retard de transmission des ordres 9. Chevauchement de numéros de comptes 10. Saisie de montants erronés	7. Validation de signature non conforme 8. Collusion DFC entreprise et agent du service Visa
Faible	1. Non-conformité des informations 3. Rejet du bordereau 14. Omission 15. Perturbation réseau	13. Négligence	
	Mineur	Modéré	Important

Impact

Légende

→	Action immédiate
→	Attention immédiate
→	Contrôle intermittent

Source : nous-mêmes

Figure 4: Élaboration de la matrice des risques opérationnels liés à SICA-UEMOA

Forte	3. Rejet des valeurs	14. Non-conformité des saisies 15. Non exhaustivité des rapprochements	5. Perte des valeurs
Moyenne	6. Retard de transmission de valeurs 9. Retard de saisie 11. Omission	7. Non exhaustivité des saisies 8. Erreur de saisies 13. Données non fiables	4. Usage frauduleux
Faible	1. Non exhaustivité 2 Rejet bordereaux de remise 10. Mauvaise qualité des images 12. Erreur de transcription 17. Perturbation de l'échange image	16. Instabilité de liaison de télécommunication	
	Mineur	Modéré	Important

Impact

Légende

→	Action immédiate
→	Attention immédiate
→	Contrôle intermittent

Source : nous-mêmes

Figure 5: Élaboration de la matrice des risques opérationnels liés à la monétique

Forte	3. Perte de dossiers	15. Perception partielle	6. Validation dossiers clients indésirables 12. Fraude
Moyenne	4. Retard de transmission 14. Réclamation de documents déjà retirés	8. Erreur de pointage 9. Erreur de saisie 10. Fichiers générés sur la base de saisies erronées	1. Erreur sur l'identité du client 11. Perte de cartes/Codes
Faible	2. Omission de proposition de fiche de demande 5. Omission de transmission 13. Se tromper d'agence	7. Négligence	
	Mineur	Modéré	Important

Impact

Légende

	Action immédiate
	Attention immédiate
	Contrôle intermittent

Source : nous-mêmes

Il ressort de l'analyse de cette évaluation que les risques à surveiller sont ceux coloriés en jaune et rouge.

6.5 Analyses et recommandations

Après les séquences d'identification et d'évaluation des risques opérationnels liés aux différents systèmes de paiement, nous allons nous atteler à l'analyse de ces risques et faire des recommandations dans le sens de leur prise en charge.

6.5.1 Analyse de la maîtrise des risques liés aux systèmes de paiement

L'analyse de la maîtrise des risques liés aux systèmes de paiement se fait à deux niveaux : l'analyse selon la cartographie des risques et l'analyse selon la structure organisationnelle de la CBAO.

6.5.1.1 Analyse selon la cartographie des risques

Cette analyse se fait à trois niveaux :

- **le niveau 1** (couleur rouge), caractérisé par des risques élevés et une qualité de contrôle insuffisante ; ce sont des risques inacceptables dont les effets de pertes financières sont importants. De ce fait, ils nécessitent une attention particulière et

immédiate des dirigeants visant à renforcer le dispositif de contrôle interne mis en place ;

- **le niveau 2** (couleur jaune), caractérisé par des risques moyens et des mesures de contrôle insuffisantes ; ce sont des risques acceptables dont les effets de pertes financières sont modérés. Il revient aux dirigeants de décider s'il est nécessaire de prendre de nouvelles mesures ou de renforcer le dispositif existant permettant de les atténuer ;
- **le niveau 3** (couleur verte), caractérisé par des risques faibles et des mesures adéquates ; ce sont des risques dont les incidences financières sont négligeables. Ils ne méritent pas beaucoup d'attention, cependant un suivi périodique de ces risques est nécessaire pour les maîtriser.

Quelques soient les sécurités mises en place, il subsiste toujours des zones à risques. Le seul dispositif de remonté des incidents ne suffit pas ; il faut renforcer le contrôle interne dans ses zones.

6.5.1.2 Analyse selon l'architecture organisationnelle

Nous notons une bonne architecture du dispositif de gestion des risques opérationnels liés aux systèmes de paiement, car organisée par direction et par métier avec une hiérarchisation ascendante de la gestion des incidents. Les agents reportent directement aux RRO, qui à leur tour remontent les incidents aux CRO qui se chargent de les transférer au MRO. Ce dernier reporte à son tour au RO en vue d'une décision de la Direction Générale.

Cette architecture est essentiellement basée sur les opérationnels qui en général n'ont pas la culture du risque opérationnel. Ils préfèrent plutôt se concentrer sur leurs tâches quotidiennes, car selon eux, leur évaluation en vue d'une éventuelle promotion dépend essentiellement de performation dans l'exercice de leurs fonctions (métier) et pas forcement la détection des risques opérationnels.

En plus, les auditeurs internes et contrôleurs sont perçus comme des gendarmes, des ennemis dans les entreprises. Les opérationnels estiment qu'il serait maladroit de leur part de collecter des informations pour des ennemis supposés.

Une bonne gestion de risques est nécessairement soumise à des mécanismes de détection de risques, elle-même basée sur les procédures que l'organisation met en place. Il est

admis que les procédures ne sont pas forcement écrites, mais il est évident que pour une banque, cela est indispensable à cause de la rigueur et les exigences du métier.

6.5.2 Les recommandations

Au terme de notre étude relative à « l'analyse de la gestion des risques opérationnels liés aux systèmes de paiement dans une banque commerciale, cas de la CBAO », il nous paraît judicieux de formuler les recommandations suivantes à différents niveaux de responsabilité de la banque, en vue d'une amélioration du dispositif de contrôle interne mis en place.

6.5.2.1 A l'endroit de la Direction Générale

- Il faut nécessairement faire rédiger par les opérationnels eux-mêmes des manuels de procédure se rapportant aux moyens de paiement ; cela rendra efficace et efficient le traitement des données. Le manuel de procédure déterminera une fourchette précise de temps pour transmettre des documents, car toute perte de temps est synonyme de perte financière à cause de la date de valeur ;
- La cartographie des risques doit être officiellement adoptée pour permettre aux auditeurs de renforcer leurs contrôles dans les zones où le risque est potentiellement élevé et permettre aussi aux opérationnels de prendre des mesures idoines lors de l'exécution de leurs tâches quotidiennes en vue de protéger la banque ;
- Valider un plan de formation des agents aux techniques de détection, de collecte et de remontée des risques opérationnels pour leur permettre d'avoir des aptitudes sur ce sujet. Cela leur permettra d'appréhender l'importance des risques opérationnels dont la gestion est en réalité l'affaire de tous au sein de l'établissement ;
- La collecte des données est inefficace à la base car les agents estiment qu'ils sont beaucoup plus occupés à leurs tâches quotidiennes que par la collecte d'incidents.

  Il faut valider un plan de motivation et d'intéressement des agents ayant collecté et remonté des incidents opérationnels pertinents. Cette mesure va certainement orienter leur attention sur ce sujet.

6.5.2.2 A l'endroit de l'Audit Général

- Soumettre un plan de formation sur les risques opérationnels à la direction générale pour renforcer la capacité des agents. Ce plan doit intégrer les modules de la formation, le budget et le calendrier de la formation, les objectifs et le résultat espérés à court, moyen et long terme ;

- Soumettre à la direction générale, un plan de motivation attractif mais moins onéreux, au profit des agents ayant détecté et remonté des incidents opérationnels ;
- Les agents de la Direction de l'Audit doivent effectuer un tour de banque chaque trimestre pour évaluer les agents formés et s'enquérir des difficultés qu'ils rencontrent quant à la gestion des risques opérationnels.
- Concevoir un fichier partagé avec toutes les Directions dans lequel seront logés directement les incidents, ou les sources potentielles de risques détectées.

6.5.2.3 A l' endroit de la Direction des Opérations

La direction des opérations regroupe l'ensemble des services ayant à charge la gestion opérationnelle des systèmes de paiement. Nos recommandations vont à l'endroit des services suivants :

- **le secrétariat de la direction des opérations**

  Les ordres de virement et les valeurs de montants significatifs doivent transiter par le bureau du directeur des opérations pour une prise de connaissance.

- **le service des opérations locales et internationales**

  Il existe un cahier de transmission entre le service courrier et la direction des opérations. En revanche, il n'en existe pas entre les différents services au sein de la direction des opérations. De ce fait, il est quasi impossible de situer les responsabilités en cas de perte ou de retard de transmission d'un ordre de virement. Il faut donc matérialiser toute transmission de documents importants par un mail avec un accusé de réception ;

- les responsables de service doivent viser les ordres de virement pour donner l'assurance qu'ils en ont pris connaissance et qu'ils ont approuvé leur traitement ;
- la signature et le solde de compte client sont des éléments névralgiques de l'activité bancaire. Pour éviter une collusion entres des cosignataires véreux de compte et un agent du service visa, il faut une double vérification de la conformité de toutes les signatures avant d'apposer le visa.

- **Le service de traitement des chèques et effets**

- le rapprochement des fichiers lots et des valeurs physiques n'est pas exhaustif, car les chèques et effets déposés dans les agences hors de Dakar ne sont pas transportés à

temps au siège. Il faudra transmettre de façon électronique les fichiers lots générés dans ces agences, afin qu'un agent sur place fasse le rapprochement ; cela évitera que les lots émis soient rejetés pour erreur.

- disposer un coffre fort dans le service dans lequel il faut conserver toutes les valeurs avant de les transporter à la compense à la banque centrale.

- **Le service de traitement Monétique**

- Mettre en place un contrôle de deuxième niveau pour la vérification des données saisies par l'agent du service d'émission de carte ;
- Transporter les dossiers physiques de demande de cartes au service informatique afin de permettre un autre pointage des données saisies, cela va éviter à la banque de commander des cartes comportant des erreurs.

6.5.2.4 Service clientèle

- Les conseillers clients doivent remettre dans le respect des horaires indiqués dans le futur manuel de procédure, les valeurs reçues aux coursiers afin de les acheminer à la direction des opérations ;
- Pour les agents du courrier, des casiers doivent leur être aménagés pour ranger efficacement les courriers reçus et à envoyer.

Conclusion du chapitre 6

Ce chapitre nous a permis de nous faire une opinion de l'organisation de la banque en ce qui conceme la gestion globale des risques et particulièrement ceux liés aux systèmes de paiement. Il montre à quel point le risque est omniprésent dans la profession et qu'il faudra nécessairement être prudent à tous les niveaux pour assurer la pérennité de l'activité.

CONCLUSION DE LA DEUXIEME PARTIE

La partie pratique de cette étude a permis de prendre connaissance de la CBAO, et de nous familiariser à l'organisation et au fonctionnement de ses systèmes de paiement, mais aussi d'avoir une idée des méthodes de gestion des risques opérationnels liés à ces systèmes de paiement.

Nous nous sommes fait une opinion de l'efficacité de la gestion de ces risques sur la base des informations collectées grâce aux outils préalablement définis dans notre modèle d'analyse.

C'est fort de cette opinion que nous avons fait des recommandations à l'endroit de certains acteurs bien ciblés de la banque, en vue d'améliorer le dispositif de contrôle interne existant.

La mise en œuvre de ces recommandations nécessite l'implication de tous ces acteurs.

Nous avons pu mettre en application une démarche ayant abouti à l'analyse des risques opérationnels liés aux systèmes de paiement. Le CODIR a la latitude de s'en servir pour corriger les imperfections observées dans les processus inhérents aux systèmes de paiement.

CONCLUSION GENERALE

La gestion des risques opérationnels est une directive de Bâle II en vue de sécuriser le système bancaire international. Pour ce faire, chaque établissement a l'obligation de mettre en œuvre un dispositif de gestion des risques potentiel et de déterminer la part de ses fonds propres qui doit être allouée à leur couverture.

Les systèmes de paiement désignent l'architecture technique, fondée sur un contrat privé ou une loi, permettant à la monnaie d'exercer au sein d'une communauté de paiement forgée autour d'une même unité de compte, sa fonction de moyen de paiement, c'est-à-dire sa fonction d'acquittement des dettes de manière irrévocable, inconditionnelle et définitive. Ces systèmes dans l'espace UEMOA, constituant une composante majeure de l'infrastructure financière de l'Union, ont emprunté les rails de la modernisation à l'instar des systèmes des pays occidentaux. C'est dans le souci d'avoir une vision beaucoup plus critique sur ces deux chantiers innovants (Risques opérationnels et Systèmes de paiement), que nous avons fait le choix de notre thème.

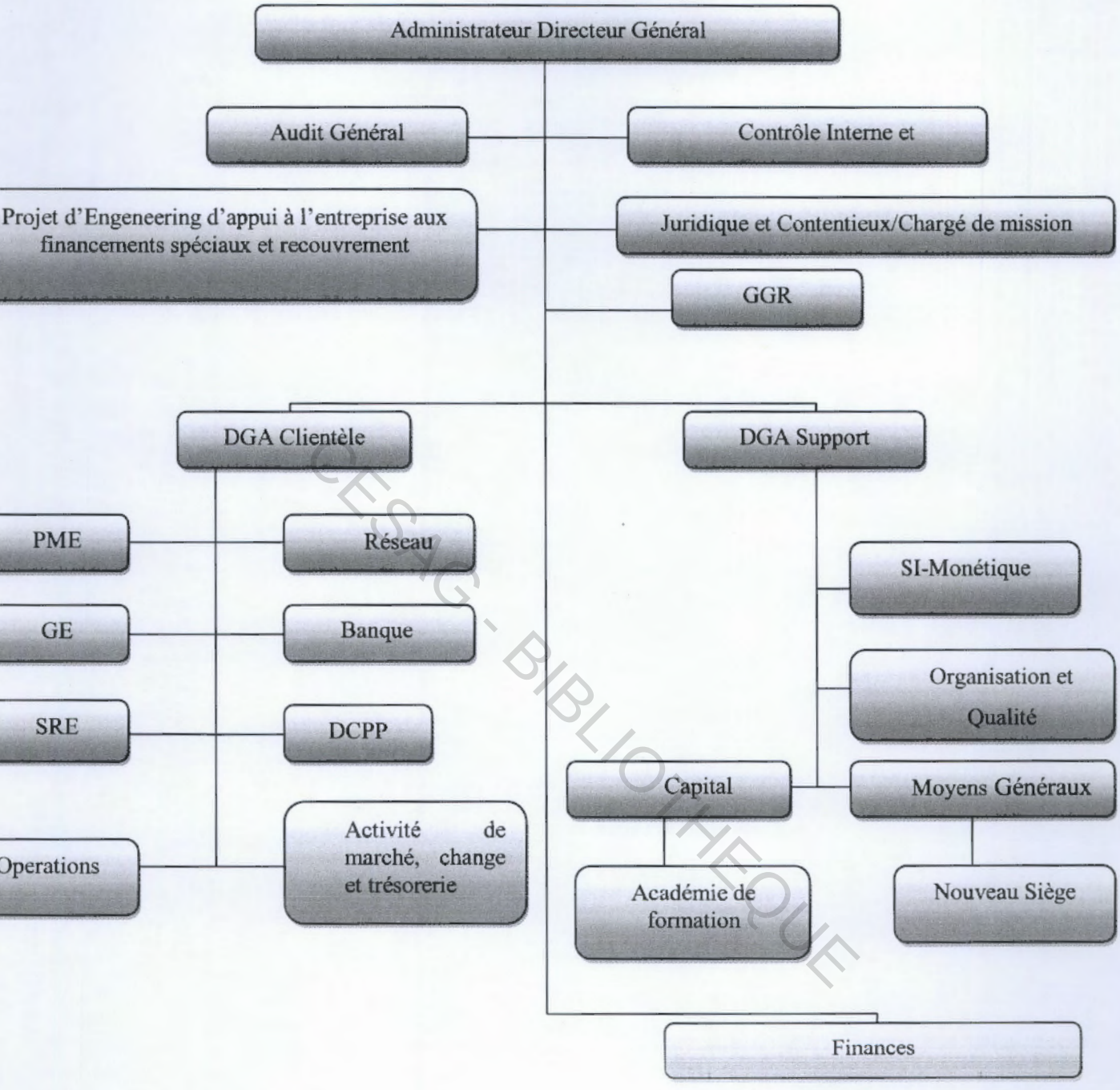
Au cours de notre étude comme dans tous travaux de recherche, nous avons eu quelques difficultés notamment à cause du caractère confidentiel de certaines données de la banque. Bien plus, notre thème couvre t-il plusieurs services dont les responsables, malgré leur bonne volonté, ne sont pas toujours disponibles à cause de leurs tâches quotidiennes. Cela explique forcement la petite taille de notre échantillon sur les dossiers étudiés.

Nous avons essayé d'atteindre nos objectifs. Cependant, tenant compte du fait que toute œuvre humaine reste imparfaite, des insuffisances existent certainement dans notre document ; il appartient au CODIR de la CBAO de l'améliorer pour en faire un bon usage.

Pour cette analyse de la gestion des risques opérationnels liés aux systèmes de paiement, nous avons passé en revue la méthode de gestion des risques et les forces et faiblesses du système de contrôle interne. Nous avons par la suite formulé des recommandations qui pourraient aider à l'amélioration de la gestion des risques opérationnels liés aux systèmes de paiement à la CBAO.

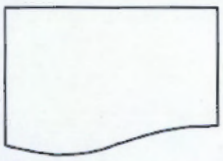
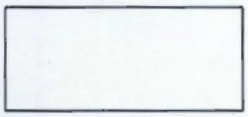
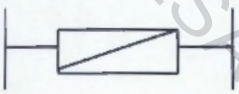
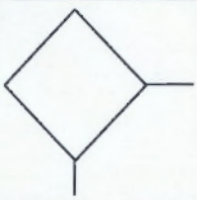
ANNEXES

Annexe 1: Organigramme de la CBAO

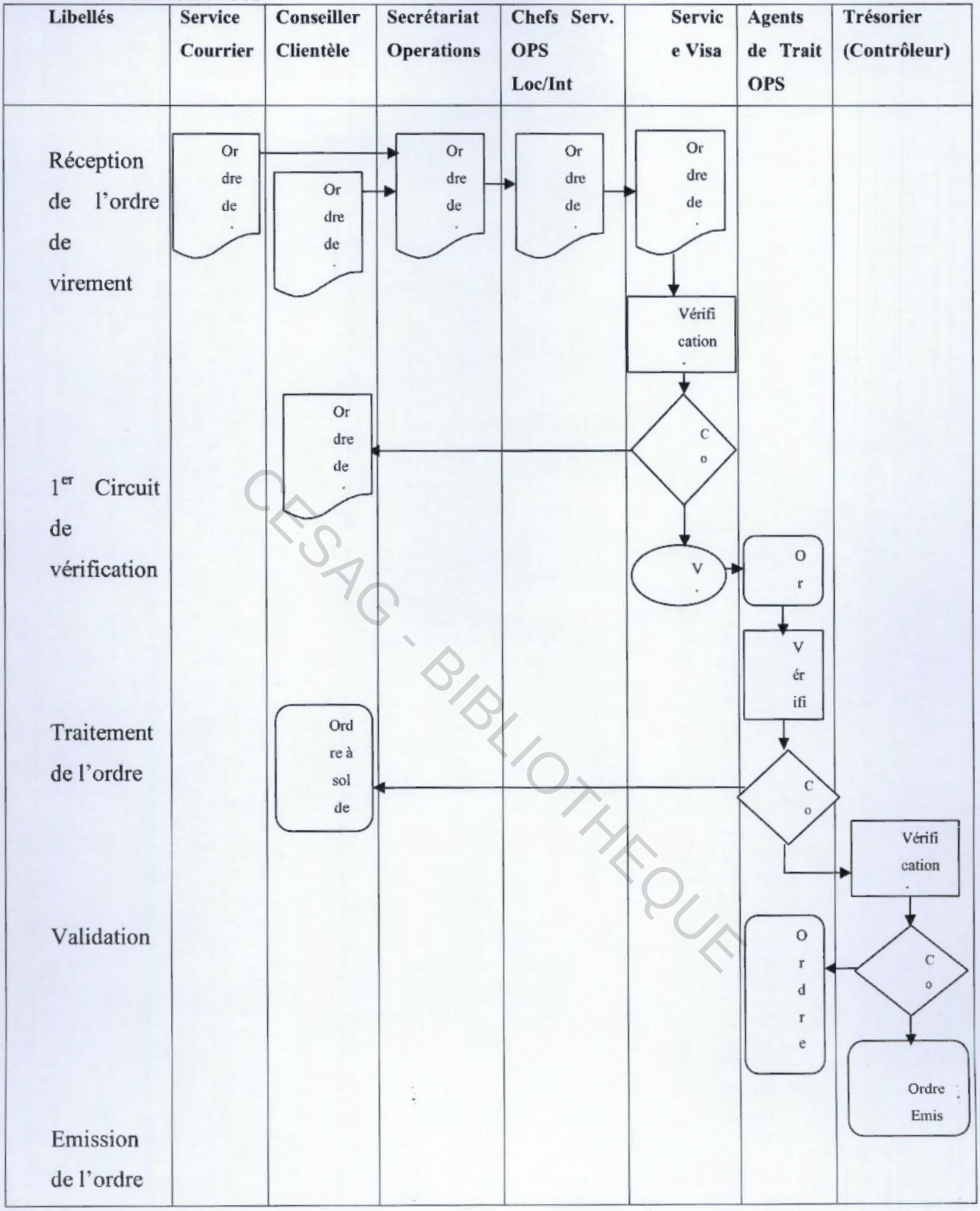


SOURCE : CBAO

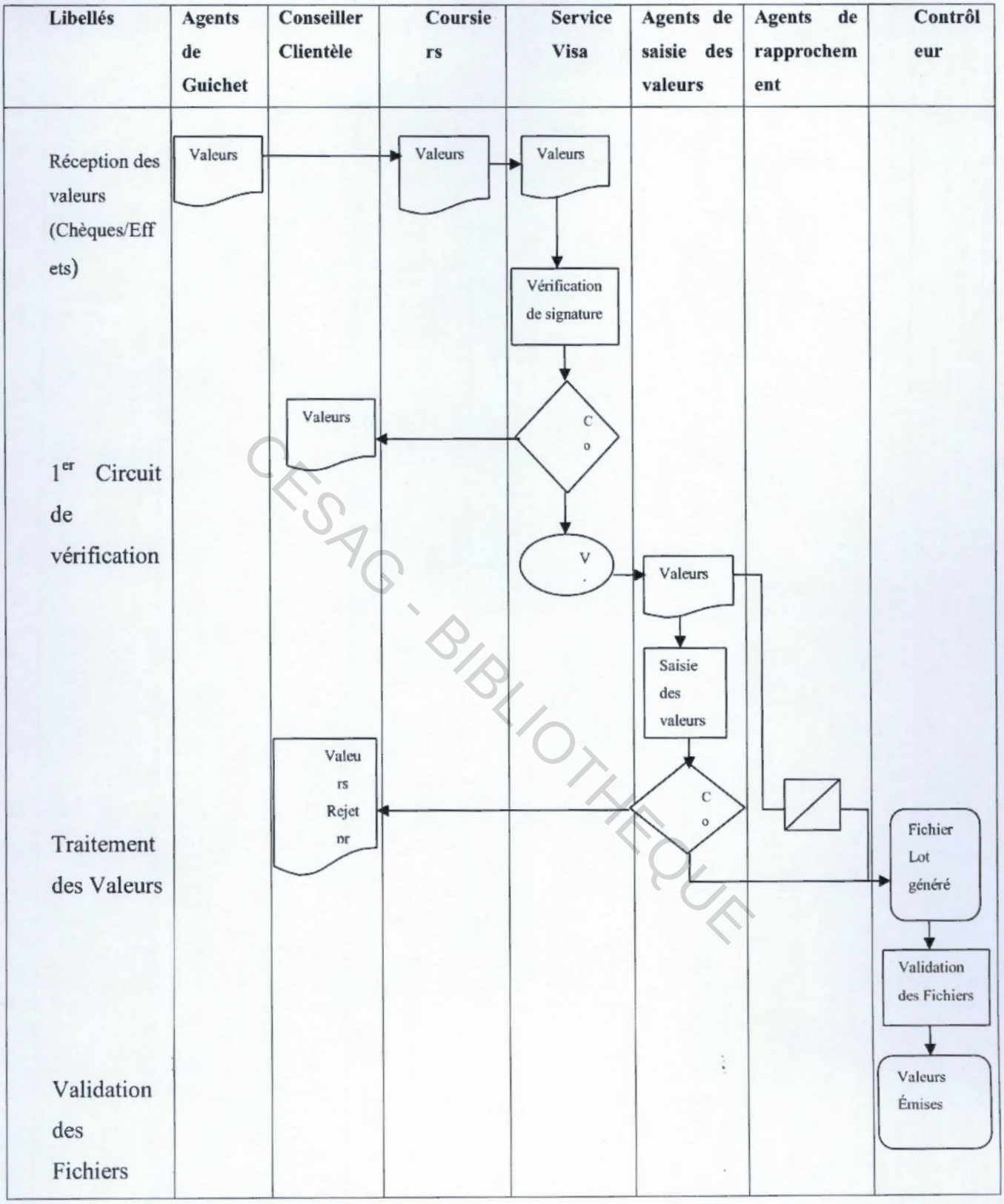
Annexe 2: Flow Chart du processus lié aux systèmes de Paiement

LES SYMBOLES USUELS	
	Symbole de circulation
	Document à traiter
	Traitement
	Archivage
	Comparaison entre deux documents
	Procédure alternative
	Apposition de Visa
	Document traité

STAR-UEMOA



SICA-UEMOA



Annexe 3: Questionnaires de Contrôle Interne

Questionnaire de Contrôle Interne	Section	Entité Auditée : Auditeur : Date :
	Rubrique : Réception et traitement des valeurs et ordres de virement.	

Objectif de Contrôle : s'assurer de l'efficacité de la réception et du traitement des ordres/Valeurs

Questions	Réponses			Commentaires
	Oui	Non	N/A	
1. Existe-il un registre pour inscrire les ordres et valeurs reçus ?	X			
2. Existe-il un casier de rangement des courriers reçus par nature ?		X		
3. Les ordres précisent-ils :				
- Le montant ?	X			
- Le nom du bénéficiaire ?	X			
- Le délai d'exécution ?	X			
4. La transmission des valeurs et ordres se fait :				
- Juste après réception ?		X		
- Quelques temps après ?	X			Selon l'estimation du coursier ou du conseiller client.
- Le lendemain ?		X		
5. Existe-il un registre de transmission aux opérations ?	X			
6. Est-il correctement déchargé ?	X			
7. Lors du traitement des ordres et valeurs, les points ci-après sont-ils saisis ?				
- Montant	X			
- N° titulaire compte	X			
- Nom et N° de compte bénéficiaire	X			
- Banque bénéficiaire	X			
8. Arrivent-ils aux agents de se tromper sur les éléments cités lors des saisis?	X			
9. Existe-il une double vérification ?	X			
10. Les valeurs/ordres sont-ils transmis tout de suite au contrôleur pour validation ?	X			
11. Contrôle-il le fichier avant validation ?	X			
12. Ce dernier procède-t-il à l'archivage des accusés de réception ?	X			

Questionnaire de Contrôle Interne	Section :	Entité Auditée : Auditeur : Date :
	Rubrique : Réception des demandes et émission de cartes bancaires	

Objectif de Contrôle : s'assurer de l'efficacité de la réception des demandes et du processus d'émission des cartes bancaires

Questions	Réponses			Commentaires
	Oui	Non	N/A	
1. Existe-il un registre pour inscrire les demandes de cartes ?	X			
2. Existe-il un casier de rangement des demandes ?			X	
3. Les demandes précisent-elles :				
- Le nom du bénéficiaire ?	X			
- Le N° de compte du bénéficiaire ?	X			
4. La transmission des demandes à la centrale de référentiel client se fait-elle :				
- Juste après réception ?		X		
- 02 heures du temps environ après ?	X			
- Le lendemain ?		X		
5. Existe-il un registre de transmission au service d'émission de carte?	X			
6. Est-il correctement déchargé ?	X			
7. Lors du traitement des demandes les points ci-après sont-ils saisis?				
- N° titulaire compte	X			
- Nom du titulaire du compte	X			
- Type de carte	X			
8. Arrivent-ils aux agents de se tromper sur les éléments cités lors des saisis?	X			
9. Existe-il une double vérification ?		X		
10. Les fichiers référencés et transmis au service informatique le sont-ils avec les documents physiques ?		X		
11. Les fichiers transmis au fabriquant comportent-ils des erreurs quelques fois ?	X			
12. Les cartes fabriquées sur cette base sont-elles détruites ?	X			
13. La réception des codes et cartes se fait-elle de façon séparée ?	X			

Annexe 4: Grilles de séparation des tâches du système de paiement

STAR-UEMOA

- Courriers d'ordre de virement

Tâches		Agent courrier	Resp. Opérations	Agt. Serv. Visa	Agt. De Saisie	Trésorier
Réception de courrier	Ex	X				
Rapprochement Signature	C			X		
Apposition de Visa	A			X		
Transmission à la saisie	A		X			
Saisie des ordres	EN				X	
Rapprochement courriers/ ordres virement saisis	C					X
Émission d'ordres	Ex					X

- Bordereaux de virement

Tâches		Conseiller Clients	Resp. Opérat°	Agt.Serv. Visa	Agt. De Saisie	Trésorier
Réception de bordereaux	Ex	X				
Rapprochement Signature	C			X		
Apposition de Visa	A			X		
Transmission à la saisie	A		X			
Saisie des ordres	EN				X	
Rapprochement Bordereau / ordres virement saisies	C					X
Émission d'ordres	Ex					X

Légende : Ex : exécution C : Contrôle EN : saisie et Enregistrement

A: Autorisation

SICA-UEMOA

Tâches		Agt.Guichet/ Conseiller Clients	Agt. de traitement	Agt. rapprochmt	Resp. Dépt traitement valeurs
Réception des valeurs	Ex	X			
Pointage des valeurs	Ex		X		
Saisie des valeurs	EN		X		
Transcription N° Remise	Ex		X		
Rapprochement	C			X	
Vérification des saisies	C				X
Émission d'ordres	Ex				X

MONETIQUE

Tâches		Agt.Guichet /conseiller clients	CRC	Agt. Serv. Visa	Agt. Serv. Emission	Resp Dépt Mnq	Serv Info	Agence
Ouverture de compte	Ex	X						
Vérification profil client	C		X					
Rapprochement signatures	C			X				
Apposition de Visa	A			X				
Saisie des données clients	Ex				X			
Génération fichier de personnalisation	Ex						X	
Validation des dossiers	A					X		
Commande de cartes	Ex						X	
Réception de cartes	Ex				X			
Réception de codes	Ex		X					
Remise aux clients	Ex							X

Légende : Ex : exécution C : Contrôle EN : saisie et Enregistrement
A : Autorisation

Annexe 5: Tableau des forces et faiblesses apparentes

STAR-UEMOA

Tâches	Objectifs Spécifiques	Risques	POCA Indicateurs	Objet de Contrôle	Test	Conséquences	Comment F / f
Réception des Ordres	Efficacité lors de la réception des ordres	Perte des ordres	Décharge et rangement des courriers par nature	S'assurer que tous les ordres sont déchargés et bien rangés	Echantillon de 8 ordres/15 Et vérification du registre	Tous les ordres sont déchargés mais mélangés aux autres courriers	f
Transmission des Ordres	Efficacité et rapidité de la transmission des ordres	-Perte des ordres -Retard de transmission	-Vérification délai de transmission -Comparer les ordres transmis et ceux du registre de décharge	S'assurer que tous les ordres sont transmis à temps	Echantillon de 8 ordres/15 Et vérifier l'horodatage puis pointage avec le registre	-les ordres arrivent à temps -pas de perte d'ordres	F
Traitement des Ordres	Efficacité et rapidité du traitement des ordres	Non conformité et erreur de saisie	-double vérification -paraphe des agents sur les ordres	S'assurer que tous les ordres sont traités et sont sans erreur	Echantillon de 8 ordres/15 Et vérifier les Montants, référence etc…	Pas d'erreurs sur les ordres	F
Emission des Ordres	Efficacité lors de l'émission des ordres	-Erreur de saisie -Omission d'émission de l'ordre	-saisie conforme aux ordres -validation par personne autorisée	S'assurer que les ordres ont été validés	Vérifier les accusés de réception de 8 ordres/15 générés par le système	Les ordres sont saisis et validés par les personnes indiquées.	F

SICA-UEMOA

Tâches	Objectifs Spécifiques	Risques	POCA Indicateurs	Objet de Contrôle	Test	Conséquences	Comment F / f
Réception des Valeurs	Efficacité lors de la réception des valeurs	Valeurs mal endossées	Vérification de l'endos des valeurs et du bordereau de remise.	S'assurer que toutes les valeurs sont bien endossées	Vérification sur un échantillon de 8 valeurs/15	Toutes les valeurs sont bien endossées	F
Transmission des Valeurs	Efficacité et rapidité de la transmission des valeurs	-Perte des valeurs -Retard de transmission des valeurs	- Vérification délai de transmission -Pointage des valeurs reçues et celles du registre	S'assurer que tous les ordres sont transmis et à temps	Echantillon de 8 valeurs/15 Et vérifier l'horodatage puis pointage avec le registre	-les valeurs arrivent à temps -pas de perte valeurs	F
Traitement des Valeurs	Efficacité et rapidité du traitement des valeurs	Non conformité et erreur de saisie	-double vérification -Inscription de la référence sur les valeurs	S'assurer que toutes les valeurs sont traitées et sont sans erreur	Echantillon de 8 valeurs/15 Et vérifier les Montants, référence etc…	Pas d'erreurs sur les valeurs	F
Validation et routage des valeurs	Efficacité lors de la validation et du routage des valeurs	-validation de valeurs erronées -Omission de validation et de routage des valeurs	-validation conforme aux valeurs -validation par personne autorisée	S'assurer que les valeurs ont été validées correctement routées dans le système	Vérifier un échantillon de 8 valeurs/15	Les valeurs sont validées et routées par les personnes indiquées.	F
Rapprochement	Efficacité du rapprochement	-Non détection d'erreurs	Rapprochement quotidien	S'assurer que les valeurs validées et routées st correctes	Vérifier un échantillon de 8 valeurs/15	Les rapprochements sont bien faits	F

MONETIQUE

Tâches	Objectifs Spécifiques	Risques	POCA Indicateurs	Objet de Contrôle	Test	Conséquences	Comment F / f
Réception des bordereaux de demande de cartes	Efficacité lors de la réception des bordereaux	Perte des bordereaux	Consignation des bordereaux dans un registre	S'assurer que tous les bordereaux sont bien rangés	Echantillon de 8 bordereaux /15 Etvérification du registre	Tous les bordereaux sont bien enregistrés et rangés dans u registre	F
Transmission des demandes de cartes	Efficacité et rapidité de la transmission des ordres	-Perte des bordereaux -Retard de transmission	-Vérification délai de transmission -Comparer les bordereaux transmis et le registre de décharge	S'assurer que tous les bordereaux sont transmis à temps	Echantillon de 8 bordereaux/15 vérifier l'horodatage le puis pointage avec le registre	-les bordereaux arrivent à temps -pas de perte d'ordres	F
Traitement des demandes de cartes	Efficacité et rapidité du traitement des demandes	Non conformité et erreur de saisie	-double vérification -paraphe des agents sur les bordereaux de demande de cartes	S'assurer que toutes les demandes sont traitées et sont sans erreur	Echantillon de 8 ordres/15 Et vérifier les Montants, référence etc…	Pas d'erreurs sur les ordres	F
Transmission de données au fabriquant	Efficacité lors de l'émission des données	-Erreur de saisie -Omission de transmission de données	-saisie conforme aux infos sur le bordereau -validation par personne autorisée	S'assurer que les données ont été validées et transmises	Vérifier les accusés de réception de 8 données/15 générés par le système	Les données transmises au fabriquant sans un pointage avec dossiers physiques.	f

Annexe 6: Feuille d'analyse des risques (FAR).

- **STAR-UEMOA**

Mission :	**Référence :**
Type de risques identifiés : R_3 (Fraude)	
Faits constatés : Signature validée par un seul agent	
Causes explicatives : Carence de la procédure	
Conséquences réelles ou potentielles : - Pertes financières - Mauvaise réputation	
Recommandation : Renforcement de la procédure par l'instauration d'une double validation de signature avant tout apposition de visa.	

- SICA-UEMOA

Mission :	**Référence :**
Type de risques identifiés : R_5 (Perte des valeurs)	
Faits constatés : Survenance de perte de chèques et d'effets de commerce	
Causes explicatives : Précipitation lors du rangement et de la transmission des valeurs	
Conséquences réelles ou potentielles : - Pertes financières - Mauvaise réputation - Perte de client	
Recommandation : Vérification, pointage et rangement rigoureux des valeurs.	

- MONETIQUE

Mission :	**Référence :**
Type de risques identifiés : R_{10} (Génération de fichiers sur la base de saisies erronées)	
Faits constatés : le service informatique génère les fichiers destinés au fabriquant sur la base de saisies du service émission sans rapprochement avec les dossiers physiques.	
Causes explicatives : Carence de la procédure	
Conséquences réelles ou potentielles : - Production de cartes litigieuses - Pertes financières	
Recommandation : Renforcement de la procédure par l'instauration d'un processus de rapprochement au service informatique ou au service d'émission de cartes.	

Annexe 7: Test de conformité et de permanence.

- **STAR-UEMOA**

		Numéros des ordres de Virement							
Tâches	**Vérification**	**118218**	**119869**	**54553**	**119867**	**73723**	**73722**	**119770**	**119871**
Réception Des ordres	Registre de réception signé et daté	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Ordre de virement signé	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Transmission des ordres	Cahier de transmission déchargé	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Paraphe approbation	Oui	Non	Non	Oui	Oui	Non	Non	Non
	Date de réception de l'ordre	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Traitement des ordres	Visa	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Identité et N° compte du donneur d'ordre	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Identité, N° compte et banque bénéficiaire	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Montant	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Emission des ordres	Conformité	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Montant et sens de saisie sur Delta	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Accusé de réception	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

- **SICA-UEMOA**

		Numéros de Remise							
Tâches	Vérification	090322BIS	090320 ECOBK	090369 SGBS	0903261 BICIS	090325 6BOA	0903252 CNCA	0903445 CS	0903282 ICB
Réception des valeurs	bordereau conformes à la norme	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Endos des valeurs	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Transmission des valeurs	Pointage des valeurs	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Décharge registre de transmission	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Existence de bordereaux de remise	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Traitement des valeurs	Endos	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Signature et Montant	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Identité et N° compte du bénéficiaire	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	N° de Remise sur bordereaux	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Validation et rootage	Conformité de saisies	Oui	Oui	Oui	Non	Oui	Non	Oui	Oui
	Montant et sens de saisie sur Delta	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Génération des 3 fichiers Lots	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Rapprochement	Exhaustivité des vérifications	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

- **MONETIQUE**

		Numéros des ordres de Virement							
Tâches	Vérification	004574	004578	004588	004590	004591	004593	004594	004597
Réception Des demandes	Registre de réception signé et daté	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Demande signé et daté par le titulaire compte	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Transmission des demandes de cartes	Cahier de transmission déchargé	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Paraphe approbation	Oui	Non	Non	Oui	Oui	Non	Non	Non
	Date de réception de la demande	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Traitement des demandes	Visa	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Identité et N° compte du donneur d'ordre	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
	Conformité	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Emission des cartes	Accusé de réception	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

BIBLIOGRAPHIE ET WEBOGRAPHIE

BIBLIOGRAPHIE

1. **AMBLARD Marc** (2003), Conventions et management, Edition De Boeck supérieur, 324 pages.
2. **ASSOCIATION CANADIENNE DE PAIEMENT** (2005), Guide du risque afférent aux systèmes de paiement appartenant et exploité par l'ACP, 89 pages.
3. **BALE II (2003),** Nouvel accord sur les fonds propres, Banque des Règlements internationaux, 17 pages.
4. **BESSIS Joël** (1995), Gestion des risques et gestion actif-passif des banques, Edition Dalloz, 574 pages.
5. **BOUCHET Michel-Henry** (2007), Intelligence économique et gestion des risques, Edition Pearson Education France, 248 pages.
6. **BRANA Sophie, MESNARD Mathilde, ZLOTOWSKI Yves** (2002), La transition monétaire russe, avatars de la monnaie, crises de la finance, Edition l'Harmattan, 377 pages.
7. **COOPERS & LYBRAND** (1994), La nouvelle pratique du contrôle interne, Edition d'Organisation, 75008, Paris, 378 pages.
8. **DE COUSSERGUE Sylvie** (2007), Gestion de la banque, 5ème édition, Dunod Paris, 272 pages.
9. **DEGRYSE Christophe** (2005), L'économie en 100 et quelques mots d'actualité, Edition De Boeck, 216 pages.
10. **DESMICHT François** (2004), Pratique de l'activité bancaire, Dunod, 1ère Edition, 320 pages.
11. **GORMAND Claude** (2000), l'Evolution du progrès technique à l'aube du nouveau siècle, Edition l'Harmattan, 222 pages.
12. **GUILLON Bernard** (2008), Méthodes et thématiques pour la gestion des risques, Edition l'Harmattan, 364 pages.
13. **HAMZAOUI Mohamed** (2008), Gestion des risques d'entreprise et contrôle interne, Normes ISA 200, 315, 330 et 500, 2ème Edition, Pearson Education France, 288 pages.
14. **JIMENEZ Christian, MERLIER Patrick, CHELLY Dan** (2008), Risques opérationnels : de l mise en place du dispositif à son audit, Revue banque Edition, 18, rue la Fayette, 75009 Paris, 271 pages.
15. **KAUFFMAN Pascal** (2008), l'Union monétaire européenne, Presse Universitaire de Bordeaux Pessac, 301 pages.
16. **KING Peter** (2001), Understanding housing finance, Routledge Edition, 148 pages.
17. **LAMARQUE Eric** (2003), Gestion bancaire, 1ère édition e-Node & Pearson Education, France, 221 pages.

18. **LAURENT Emmanuel** (2006), Optimiser la gestion de trésorerie par la modernisation économétrique des moyens de paiement, Edition Publibook, 439 pages.
19. **LEHMANN Paul Jacques, MACQUERON Patrice** (1995), Droit des affaires, comptables ; gestion financière, fiscale, Edition Maxima, 765 pages.
20. **LOTH Désiré** (2009), l'Essentiel des techniques du commerce international, Edition Publibook, 167 pages.
21. **MADERS Henri-Pierre & MASSELIN Jean Luc** (2009), Contrôle interne des risques : cibler, évaluer, organiser, piloter, maîtriser, 2ème Edition d'Organisation, Groupe Eyrolles, 261 pages.
22. **MATHIEU Michel** (1995), l'Exploitant bancaire et le risque de crédit, mieux le cerner pour mieux le maîtriser, Edition d'Organisation, paris, 291 pages.
23. **MISHKIN Fréderic, BORDES Christian, HAUTECOEUR Pierre-Cyrille, LACOUE Dominique, RAGOT Xavier (2010)**, Monnaie, banque et marchés financiers, 9ème édition, Pearson Education, Paris, 960 pages.
24. **RENARD Jacques** (2010), Théorie et pratiques de l'audit interne, 7ème Edition, Groupe Eyrolles, 496 pages.
25. **SARDI Antoine** (2002), Audit et contrôle interne bancaire, Afges Edition, 1091 pages.
26. **THUNIS Xavier** (1996), Responsabilité du banquier et automatisation des paiements, Edition Presse universitaire de Namur, Belgique, 362 pages.
27. **VALIN Gérard** (2006) Controlor & Auditor, Dunod, Paris, 457pages.
28. **VALLET Elisabeth** (2003), Les correspondants du trésor, Edition l'Harmattan,5-7, rue de l'Ecole-Polytechnique, 75005 Paris, France, 557 pages.
29. **VAN GREUNING Hennie, BRATANOVIC Brajovic Sonja** (2004), Analyse et gestion du risque bancaire, Edition ESKA, Paris, 324 pages.
30. **VERBIEST Thibault, WERY Etienne** (2002), Le droit de l'internet et la société de l'information, Edition Larcier, 648 pages.
31. **VINCENTI Dominique**, Dresser une cartographie des risques, Revue d'audit N° 12.
32. **WA MADZILA Ebondo Eustache** (2006), La gouvernance d'entreprise, une approche par l'audit et le contrôle interne. Edition l'Harmattan, 349 pages.

WEBOGRAPHIE

1) BCEAO (2007), Rapport sur les systèmes de paiement dans l'UEMOA www.bceao.int
2) SWIFT, Fonctionnement de la plateforme Swift, www.swift.com
3) BAMBA Style (2012) : scandale à la CBAO Dakar; www.seneweb.com du jeudi 18 octobre 2012

Autres Documents

1) Compagnie Bancaire de l'Afrique Occidental (2010), Rapport annuel (2009 ; 2010), CBAO, Dakar, 54 pages.

2) Compagnie Bancaire de l'Afrique Occidental, Plan de stratégie quinquennal (2011-2016), CBAO, Dakar, 26 pages.