



**Centre Africain d'Etudes Supérieures en Gestion**

**CESAG EXECUTIVE EDUCATION  
(CEE)**

**MBA-Audit et Contrôle de Gestion  
(MBA-ACG)**

**Promotion 25  
(2013-2014)**

**Mémoire de fin d'étude**

**THEME**

**ANALYSE DE LA GESTION DES RISQUES OPERATIONNELS  
DES MOYENS DE PAIEMENTS SCRIPTURAUX PAR LE SICA-  
UEMOA ET LE STAR-UEMOA DANS UNE BANQUE : CAS DE  
LA VERSUS BANK**

**Présenté par :**

**KOUASSI KADJO FIRMIN**

**Dirigé par :**

**Mr. KOUASSI MONDON THIERRY**

**INGENIEUR FINANCIER**

**AUDITEUR INTERNE VERSUS BANK**

**Avril 2015**

CESAG - BIBLIOTHEQUE

## **DEDICACE**

Je dédie ce mémoire :

- A ma mère qui m'a toujours soutenu par ces prières tout au long de cette formation.
- A mes Frères et Sœurs à qui je dis un grand merci pour leur amour et tout leur soutien morale et financier dont j'ai toujours bénéficié ;
- A mes amis de la 25<sup>ème</sup> promotion de MBA Audit & Contrôle de gestion du CESAG-DAKAR pour leur solidarité sans faille à mon égard durant cette formation.

## **REMERCIEMENTS**

---

J'adresse mes sincères remerciements à :

- Monsieur Mr Moussa YAZI Directeur de la formation au CESAG pour sa disponibilité et ses conseils en matière de méthodologie de rédaction de mémoire
- Mr CHABI Bertin Chef de département CESAG EXECUTIVE EDUCATION
- Mr KOIZAN Guy, Directeur général de la VERSUS BANK pour m'avoir accepté au sein de son institution
- Mr KOUASSI Mondon Thierry Auditeur interne chargé de la conformité pour avoir accepté de m'encadrer pour le mémoire durant mon stage au sein de la VERSUS BANK.
- Mme KOUAKOU Mariam pour m'avoir accepté au sein de son département pour le stage
- Tout le personnel de la VERSUS BANK pour leur soutien et leur disponibilité leur de mes investigations dans la banque

## Sigles et abréviations

**Back- Office** : Le Back-office suit le traitement "post-marché" des opérations

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

**CAD** : Service de l'Administration du Crédit

**CRP** : Compte rendu de Paiement

**COSO**: Committee of Sponsoring Organizations of the treadway commission.

**DSI**: Département des Service des Systèmes d'Information

**Front Office** : Le Front Office est littéralement l'interface de la banque avec le marché

**Middle Office**: très proche du Front, assure la validation et l'enrichissement des opérations négociées

**MT202** : désigne un message type 202 et s'effectue par SWIFT lorsqu'il ya plusieurs bénéficiaire domicilié dans une même banque

**SICA**: Système Inter bancaire de Compensation Automatisé

**STAR**: Système de Transfert Automatisé et de Règlement

**SWIFT**: Society for Worldwide Interbank Financial telecommunication

**TIM** : Transfert Initié Manuellement

**UEMOA**: Union Economique et Monétaire Ouest Africain

**UMOA**: Union Monétaire Ouest Africain

**VIB** : virements inter bancaire

## Liste des Figures et Tableaux

### Figures

|                                      |    |
|--------------------------------------|----|
| Figure 1 :Modèle d'analyse.....      | 44 |
| Figure 2 : Matrice des risques ..... | 79 |

### Tableaux

|  |    |
|--|----|
| Tableau 1 :Quelques risques opérationnels liés au processus .....                      | 29 |
| Tableau 2 : Risques opérationnels liés à la gestion des chèques sur confrères .....    | 59 |
| Tableau 3 : Risques opérationnels liés à la gestion des virements et transferts .....  | 61 |
| Tableau 4 : Risques opérationnels liés à la gestion des effets escomptés .....         | 62 |
| Tableau 5 : Test de conformité et de permanence sur les chèques sur confrères .....    | 64 |
| Tableau 6 : Test de conformité et de permanence sur les virements interbancaires ..... | 65 |
| Tableau 7 : Test de conformité et de permanence sur les effets escomptés .....         | 66 |
| Tableau 8 : Grille de séparation des tâches sur les chèques sur confrères .....        | 67 |
| Tableau 9 : Grille de séparation des tâches sur virements interbancaires .....         | 68 |
| Tableau 10 : Grille de séparation des tâches sur les effets escomptés .....            | 69 |
| Tableau 11 : Forces et faiblesses apparents sur les chèques sur confrères .....        | 70 |
| Tableau 12 : Forces et faiblesses apparents sur les virements interbancaires .....     | 71 |
| Tableau 13 : Forces et faiblesses apparents sur les effets escomptés .....             | 72 |
| Tableau 14 : Echelle de mesure de la probabilité de survenance .....                   | 73 |
| Tableau 15 : Tableau d'évaluation de la probabilité de survenance des risques .....    | 74 |
| Tableau 16 : Echelle de mesure de l'impact des risques identifiés.....                 | 75 |
| Tableau 17 : Evaluation de l'impact des risques identifiés .....                       | 76 |
| Tableau 18 : Cotation des risques .....  | 77 |
| Tableau 19 :Hiérarchisation des risques.....   | 78 |
| Tableau 20 : Synthèse du dispositif du contrôle interne .....                          | 80 |

## ANNEXES

|   |    |
|---|----|
| Annexe 1: Organigramme de VERSUS BANK .....                         | 87 |
| Annexe 2: description procedures des chèques sur confrères VB ..... | 88 |
| Annexe 3: description procedures des effets escomptés .....         | 89 |
| Annexe 4: description procedures des VIB .....                      | 90 |
| Annexe 5: description procedures des transferts émis .....          | 91 |
| Annexe 6: symbole .....   | 92 |

CESAG - BIBLIOTHEQUE

## Table des matières

|  |    |
|--|----|
| DEDICACE.....  | 1  |
| REMERCIEMENTS.....   | 2  |
| SIGLE ET ABREVIATIONS .....  | 3  |
| LISTE DES ANNEXES .....  | 4  |
| LISTE DES TABLEAUX & FIGURES .....   | 5  |
| TABLE DES MATIERES .....   | 6  |
| INTRODUCTION GENERALE.....   | 9  |
| PREMIERE PARTIE: CADRE THEORIQUE .....   | 15 |
| CHAPITRE 1: LES RISQUES OPERATIONNELS LIES AUX MOYENS DE<br>PAIEMENT SCRIPTURAUX ET LEURS SYSTEMES DE PAIEMENT ..... | 16 |
| 1.1 Les moyens de paiement scripturaux .....   | 16 |
| 1.1.1 Définitions des moyens de paiement scripturaux .....   | 16 |
| 1.1.2 Les différents moyens de paiement scripturaux au sein de la Zone UEMOA.....                                    | 16 |
| 1.1.2.1 Le chèque .....  | 17 |
| 1.1.2.2 Les virements et transferts .....  | 17 |
| 1.1.2.3 Les effets de commerce.....  | 17 |
| 1.1.2.4 L'avis de prélèvement .....  | 18 |
| 1.1.2.5 La carte bancaire.....   | 18 |
| 1.3.1 Les caractéristiques communes aux moyens de paiements scripturaux .....  | 18 |
| 1.2 Les principaux systèmes bancaires de moyens de paiements scripturaux .....                                       | 19 |
| 1.2.1 Définition de système bancaire de moyens de paiement .....   | 19 |
| 1.2.2 Les acteurs des systèmes de paiement .....   | 20 |
| 1.2.1.1 La banque centrale .....   | 20 |
| 1.2.1.2 Les établissements de credit.....  | 20 |
| 1.2.1.3 Le trésor public .....   | 20 |
| 1.2.1.4 Les services financiers de la poste .....  | 20 |
| 1.2.1.5 Les gestionnaires des systèmes .....   | 21 |
| 1.2.3 La nomenclature des systèmes de paiement dans l'UEMOA.....   | 21 |
| 1.2.3.1 Réseau intra bancaire pour les banques .....   | 21 |
| 1.2.3.2 Système de Transfert Automatisé et de Règlement (STAR).....  | 22 |
| 1.2.3.3 Système Inter bancaire de Compensation Automatisé (SICA-UEMOA).....  | 23 |
| 1.2.4 Les acteurs du processus de règlement des moyens de paiement scripturaux .....                                 | 24 |
| 1.3 Risques opérationnels liés aux processus de règlements des moyens de paiement<br>scripturaux.....                | 25 |
| 1.3.1 Définition du risque .....   | 25 |
| 1.3.1.1 Risques liés à l'activité bancaire.....  | 25 |
| 1.3.2 Définition du risque opérationnel.....   | 26 |
| 1.3.3 Les composantes du risque opérationnel .....   | 26 |
| 1.3.3.1 Le risque lié au système d'information .....   | 26 |
| 1.3.3.2 Le risque lié au processus .....   | 27 |
| 1.3.3.3 Le risque lié aux personnes .....  | 27 |
| 1.3.3.4 Le risque lié aux événements extérieurs .....  | 27 |
| 1.3.4 Quelques risques opérationnels liés au processus de paiements scripturaux.....                                 | 28 |

|  |    |
|--|----|
| <b>CHAPITRE 2 : LA GESTION DES RISQUES OPERATIONNELS LIES AU PROCESSUS DE REGLEMENT DES MOYENS DE PAIEMENT SCRIPTURAUX</b> .....                           | 28 |
| 2.1 La politique de gestion des risques opérationnels .....  | 29 |
| 2.2 Les acteurs et organes de pilotage du dispositif .....   | 29 |
| 2.2.1 Les actionnaires et le Conseil d'Administration .....  | 29 |
| 2.2.2 La Direction générale .....  | 29 |
| 2.2.3 Le comité de risque opérationnels .....  | 30 |
| 2.2.4 Les responsables risques opérationnels .....   | 30 |
| 2.3 Dispositif de maîtrise des risques opérationnels liés aux moyens de paiement .....   | 31 |
| 2.3.1 Objectif du dispositif de maîtrise des risques opérationnels .....   | 31 |
| 2.3.2 La prise de connaissance du processus de gestion des moyens de paiement .....  | 31 |
| 2.4 Identification, évaluation et suivi des risques opérationnels liés au processus de règlement des moyens de paiements scripturaux .....                 | 33 |
| 2.4.1 Identification des risques opérationnels liés aux moyens de paiement scripturaux .....   | 33 |
| 2.4.1.1 Identification basée sur l'atteinte des objectifs .....  | 34 |
| 2.4.1.2 Identification par analyse historique .....  | 34 |
| 2.4.1.3 Identification par tâches élémentaires .....   | 34 |
| 2.4.2 Evaluation des risques opérationnels liés aux processus de moyens de paiement scripturaux .....  | 35 |
| 2.4.3 suivi des risques opérationnels liés aux processus de moyens de paiement scripturaux .....   | 36 |
| 2.5 Le contrôle interne du processus de gestion des moyens de paiement scripturaux .....   | 37 |
| 2.5.1 Le contrôle interne du processus de gestion des moyens de paiement scripturaux .....   | 37 |
| 2.6 Evaluation du dispositif de gestion des risques opérationnels liés aux moyens de paiements scripturaux .....   | 38 |
| 2.6.1 les objectifs de l'évaluation du dispositif de contrôle interne des risques opérationnels liés aux processus de moyens de paiement scripturaux ..... | 39 |
| 2.6.2 Les étapes d'évaluation du dispositif du contrôle interne des risques opérationnels liés aux processus de moyens de paiement scripturaux .....       | 39 |
| 2.6.3 Les dix (10) principes de bonnes pratiques en matière de gestion des risques opérationnels .....   | 39 |
| <b>CHAPITRE 3: METHODOLOGIE DE LA RECHERCHE</b> .....  | 40 |
| 3.1 Modèle d'analyse .....   | 44 |
| 3.2 Outils de collecte et d'analyse des données .....  | 45 |
| 3.2.1 L'analyse documentaire .....   | 45 |
| 3.2.2 l'observation physique .....   | 45 |
| 3.2.3 L'interview .....  | 45 |
| 3.2.4 La grille de séparation des tâches .....   | 46 |
| 3.2.5 Les tests de conformité et de permanence .....   | 46 |
| 3.2.6 Le tableau des forces et faiblesses apparentes .....   | 47 |
| <b>DEUXIEME PARTIE: CADRE PRATIQUE</b> .....   | 48 |
| <b>CHAPITRE 4: PRESENTATION DE VERSUS BANK</b> .....   | 49 |
| 4.1 Présentation générale de l'entreprise .....  | 49 |
| 4.1.1 Historique, Objectifs et Activités .....   | 49 |
| 4.1.1.1 Historique .....   | 49 |
| 4.1.1.2 Objectifs .....  | 49 |
| 4.1.1.3 Activités .....  | 50 |
| 4.2 Organisation , Fonctionnement et Organigramme .....  | 51 |

|   |           |
|---|-----------|
| 4.2.1 Organisation .....  | 51        |
| 4.2.1.1 Organe exécutif .....   | 51        |
| 4.2.2 Organigramme.....   | 52        |
| 4.2.3 Fonctionnement .....  | 53        |
| <b>CHAPITRE 5 : DESCRIPTION DES PROCEDURES DE GESTION DE MOYENS DE<br/>PAIEMENT SCRIPTURAUX TRAITES VIA LE SICA-UEMOA ET LE<br/>STAR-UEMOA ET LA GESTION DES RISQUES ASSOCIES .....</b> | <b>54</b> |
| 5.1 Description de la procédure de traitement des chèques sur confrères .....   | 54        |
| 5.2 Description de la procédure de traitement des effets escomptés .....  | 54        |
| 5.3 Description de la procédure de traitement des virements et transferts .....   | 54        |
| 5.3.1 Procédure de traitement des virements .....   | 55        |
| 5.3.2 Procédures de traitement des transferts émis .....  | 55        |
| 5.4 La gestion des risques opérationnels liés aux moyens de paiement scripturaux à<br>VERSUS BANK .....   | 55        |
| 5.5 Identification et évaluation des risques opérationnels liés au processus des<br>moyens de paiement scripturaux à VERSUS BANK .....  | 56        |
| 5.5.1 Identification des risques opérationnels liés au processus des moyens de<br>paiement scripturaux au niveau de VERSUS BANK .....   | 57        |
| 5.5.2 Le suivi des risques opérationnels liés au processus des moyens<br>de paiement scripturaux au niveau de VERSUS BANK.....  | 57        |
| <b>CHAPITRE 6: ANALYSE DU DISPOSITIF DE MAITRISE DES RISQUES OPERATIONNELS<br/>LIES AU MOYENS DE PAIEMENT SCRIPTURAUX PAR SICA-UEMOA ET<br/>STAR-UEMOA .....</b>                        | <b>58</b> |
| 6.1 Identification et évaluation des risques opérationnels liés aux moyens de<br>paiement scripturaux traités via le SICA-UEMOA et le STAR-UEMOA .....                                  | 58        |
| 6.2 Evaluation du dispositif de contrôle interne.....   | 63        |
| 6.2.1 Tests de conformité et de permanence .....  | 63        |
| 6.2.2 Grille de séparation des tâches .....   | 66        |
| 6.2.3 Forces et faiblesses apparentes .....   | 70        |
| 6.3 Evaluation des risques opérationnels liés à la gestion des moyens de paiement<br>scripturaux par SICA- UEMOA et STAR-UEMOA .....  | 73        |
| 6.3.1 Evaluation de la probabilité de survenance des risques identifiés .....   | 73        |
| 6.3.2 Evaluation de l'impact des risques identifiés .....   | 75        |
| 6.4 Evaluation des risques opérations liés aux moyens de paiement .....   | 76        |
| 6.4.1 Analyse de La matrice des risques opérationnels liés aux moyens de<br>paiements scripturaux par SICA-UEMOA et STAR-UEMOA .....  | 77        |
| 6.4.2 Hiérachisation des risques opérationnels selon leur criticité.....  | 78        |
| 6.4.3 La matrice des risques opérationnels .....  | 79        |
| 6.5 Analyse et recommandations .....  | 81        |
| 6.5.1 Recommandations.....  | 82        |
| Conclusion .....  | 84        |
| Bibliographie .....   | 93        |
| Table des annexes .....   | 05        |
| Table des figures.....  | 04        |
| Table des tableaux.....   | 04        |



**INTRODUCTION GENERALE**

Depuis la crise économique mondiale connue en 2008, L'environnement économique et financier est devenu de plus en plus une source de risque ; cela est dû principalement à son caractère d'instabilité; aux mutations accélérées; à une concurrence accrue dans différents secteurs; à la mondialisation des échanges; à l'émergence de nouvelles zones économiques à forte croissance, à une sophistication incessante des produits financiers, à l'innovation technologique et une forte volatilité de marché...

Le système bancaire international se trouve situé au cœur de ces mutations. Il est au centre des circuits et mécanismes financiers, il représente le partenaire officiel et habituel des acteurs économiques des différents Etats.

Une banque au sens large est un établissement qui facilite les paiements des particuliers ou des entreprises, avance et reçoit des fonds et gère des moyens de paiement. Elle prend donc des risques.

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

L'histoire nous donne un aperçu il suffit en effet de regarder ces différents scandales financiers :

(D'après la revue Jeune Afrique du 10 février 2009) certaines banques africaines se sont vues faire frauder et perdre d'énormes montants :

- par falsification de chèque volé ou ramassé ;
- par de mauvais placements financiers ou fictifs (cas de la BEAC, Banque centrale des états de l'Afrique Centrale)
- par crédit documentaire (import) ; l'agent fraudeur a délivré des documents à l'importateur contre une traite non avalisée, la banque devra payer à celle du fournisseur la marchandise pour 2 milliards de FCFA.
- par chèque interbancaires à compenser : l'agent chargé de la compensation ne retournait pas les chèques impayés et ne les imputaient pas au compte des clients il les plaçait dans des comptes d'attente (14 millions de FCFA de perte).

De plus en France, L'affaire Kerviel en 2008 à la Société Générale qui a occasionné des pertes énormes pour la banque, à hauteur de plus de 4 milliards d'euros.

De telles pertes sont dues généralement à une inadéquation ou une défaillance des procédures, du personnel, des systèmes internes ou à des événements extérieurs et plus précisément au risque opérationnel.

Avec les avancées technologiques et la complexité des processus de gestion, la notion de risque opérationnel s'est particulièrement développée ces dernières années alors qu'elle était auparavant ignorée ou bien gérée d'une manière isolée. Face au développement de nombreux produits bancaires une meilleure maîtrise des risques opérationnels est inévitable.

Aussi, pour faire face et suivre ces mutations, les banques centrales mettent en place des mécanismes afin de maîtriser les risques, favoriser le développement et l'intégration des marchés de capitaux régionaux et assurer la célérité des paiements.

Ainsi donc la BCEAO met en place un certains nombres de systèmes de moyens de paiement tels : Le Système Interbancaire de Compensation Automatisé dans l'UEMOA (SICA-UEMOA) et le système régional de règlement brut en temps réel des transactions d'importance systémique (notamment les gros montants) le STAR-UEMOA. 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 pour ces deux systèmes.

Notre étude se fera au sein de VERSUS BANK qui est une structure au sein de laquelle nous avons fait notre stage académique, elle est une société anonyme de droit ivoirien, Banque à capitaux privés à l'origine, Versus Bank a été reprise par l'Etat de Côte d'Ivoire, comme actionnaire unique depuis janvier 2009.

Sa création, répond à une volonté de voir naître une institution financière qui participe pleinement au dynamisme du marché bancaire ivoirien, de promouvoir l'initiative privée et de développer des produits et services adaptés aux réalités de notre environnement.

le cadre d'exercice de l'activité bancaire des pays membres de L'Union Economique Monétaire Ouest Africaine (UEMOA) est ordonné autour d'une loi bancaire, d'un dispositif prudentiel et des normes comptables uniformes aussi d'une convention portant création de la Commission Bancaire de l'UEMOA chargée de superviser les établissements de crédits et de s'assurer du respect des normes.

Ces dispositions sont renforcées au plan international par les normes éditées par Bâle 2, elles se résument en trois piliers qui sont :

- Pilier 1 Les nouvelles exigences en matière de fonds propres
- Pilier 2 Le rôle du superviseur national en matière de contrôle des activités bancaires
- Pilier 3 la transparence en matière de communication financière

Selon Les dispositions de Bâle 2, le risque opérationnel vient des pertes directes et indirectes pouvant résulter d'une inadéquation ou de défaillances attribuables à des procédures, à des personnels, à des systèmes internes ou à des événements extérieurs. Ces défaillances peuvent être dues à :

- l'absence ou à une faiblesse du dispositif de contrôle interne ;
- l'insuffisance de moyens matériels de contrôle ;
- la négligence des responsables d'exploitations qui n'ont pas mis en œuvre toutes les instructions de contrôle prévues ;
- une défaillance du mode de fonctionnement du système bancaire ;
- une mauvaise supervision du travail de chaque employé de la banque ;

De ce fait, il est donc important pour VERSUS BANK de gérer le risque opérationnel lié aux moyens de paiement scripturaux afin de réduire la probabilité d'une perte au cas où elle surviendrait éventuellement, et limiter son ampleur.

Face à cette situation, quelques solutions peuvent être proposées :

- évaluer les expositions au risque et les incidents à l'échelle de la banque ;
- recruter un personnel qualifié dans le département risk management afin qu'une cartographie des risques susceptibles de survenir soit établit ;
- mettre en place un contrôle interne fiable à tous les niveaux de départements ;
- Analyser les risques liés aux moyens de paiements scripturaux afin de mettre en place un dispositif de gestion du risque opérationnel dynamique répondant aux normes internationales bancaires.

De toutes les solutions proposées celle qui nous semble la plus importante à retenir est la dernière car elle permettra à VERSUS BANK d'avoir une vision claire des risques liés aux processus de règlements scripturaux spécialement les chèques et remises chèques sur confrères, les virements et effets de commerces, afin de mieux les gérer.

De cette solution découle notre question principale : quelle est l'efficacité des dispositifs de gestion des risques liés aux moyens de paiement scripturaux au sein de VERSUS BANK ?

Plus précisément :

- Quels sont les moyens de paiement scripturaux utilisés ?

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

Pour ce faire nous avons choisir d'axer notre réflexion sur le thème : « **Analyse de la gestion des risques opérationnels liés aux moyens de paiement scripturaux traités via le SICA- UEMOA et le STAR-UEMOA : Cas de la VERSUS BANK** »

L'objectif général de ce thème est

- D'apprécier l'efficacité de la gestion des risques opérationnels liés au processus de règlements des moyens de paiements scripturaux via le SICA-UEMOA et le STAR- UEMOA mise en place par VERSUS BANK.

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

- Prendre connaissance du processus de gestion des moyens de paiement scripturaux par ces deux systèmes;
- Identifier les risques opérationnels liés aux processus de gestion des moyens de paiement scripturaux ;
- Evaluer les dispositifs mis en œuvre pour la maîtrise des risques opérationnels liés aux moyens de paiements scripturaux par le SICA-UEMOA et STAR-UEMOA afin de faire ressortir des forces et faiblesses ;
- Formuler des recommandations relatives à la maîtrise des risques opérationnels.

Ainsi compte tenu du nombre élevé des opérations sur les moyens de paiements scripturaux et en raison du temps qui nous est imparti, nous allons nous intéresser aux chèques et remises chèques sur confrères, aux virements et les effets de escomptés en raison de l'importance de leur traitement. Aussi nous allons nous concentrer plus sur le système de télé compensation « aller » et le système RTGS pour les virements et transferts émis

L'intérêt de l'étude de ce thème :

- Pour VERSUS BANK  
Elle pourrait avoir une idée sur l'efficacité des moyens mis en place pour la gestion des risques opérationnels liés aux moyens de paiement scripturaux par SICA-UEMOA et STAR-UEMOA, et ainsi améliorer ces dispositifs en s'appuyant sur les bonnes pratiques en matière de gestion des risques opérationnels.

- Pour nous même

Cela nous permettra d'appliquer les connaissances théoriques acquises durant notre année de formation, d'appliquer nos connaissances en matière de gestion de risques opérationnels dans les banques.

Notre travail se subdivisera en deux grandes parties :

Une première partie axée sur le cadre théorique composée en trois chapitres qui traiteront successivement des risques opérationnels des moyens de paiement scripturaux et des systèmes de paiement, des dispositifs de maîtrise des risques opérationnels, de la méthodologie de recherche permettant d'aborder le cadre pratique.

La deuxième partie axée sur le cadre pratique subdivisée aussi en trois chapitres qui traiteront de la présentation de VERSUS BANK, la description des dispositifs de gestion des risques opérationnels liés aux moyens de paiements scripturaux par la télé compensation « aller » et STAR UEMOA, et enfin l'analyse de ces dispositifs.

**PREMIERE PARTIE : CADRE THEORIQUE**

CESAG - BIBLIOTHEQUE

## **Chapitre 1 : les risques opérationnels liés aux moyens de paiement scripturaux et leurs systèmes de paiement**

### **1.1 Les moyens de paiement scripturaux**

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

#### **1.1.1 Définitions des moyens de paiement scripturaux**

Sont considérés comme moyens de paiement scripturaux, tous les instruments, qui quel que soit le support ou le procédé technique utilisé permettent à toute personne de transférer des fonds. Il s'agit notamment des chèques bancaires, chèques de voyages, carte de paiement et de retrait, virement ou avis de prélèvement, cartes de crédit et transfert électronique de fonds.

#### **1.1.2 Les différents moyens de paiement scripturaux au sein de la Zone UEMOA**

D'après le rapport annuel 2005 de la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) nous disposons au sein de la zone UEMOA, cinq sortes d'instruments scripturaux :

- Le chèque ;
- Le virement ;
- Les effets de commerce (lettre d'échange et le billet à ordre) ;
- L'avis de prélèvement ;
- La carte bancaire.

Les instruments scripturaux encore appelé moyens de paiement scripturaux sont indispensables au fonctionnement du circuit économique. Leur utilisation est généralement adossée à des comptes bancaires à vue ou des comptes d'épargne. Ils ont pour but de simplifier et de limiter les risques liés aux transactions entre les agents économiques.

### **1.1.2.1 Le chèque**

Le chèque est un écrit par lequel une personne (le tireur) donne l'ordre à une autre personne (le tiré) de payer une certaine somme à un tiers (le bénéficiaire ou le porteur) à concurrence des fonds déposés chez le tiré.

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

- Le chèque barré :

Un chèque est dit barré lorsqu'il est non endossable et payable dans une banque.

- Le chèque de banque :

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

- Le chèque certifié :

Un chèque est dit certifié si la banque du tireur garantit le montant du paiement du montant tiré.

### **1.1.2.2 Le virement ou transfert**

L'ordre de virement (crédit transfert) émis par le débiteur est adressé à sa banque afin d'effectuer un transfert sur une autre banque ou sur un compte de la même banque.

### **1.1.2.3 Les effets de commerce**

Nous avons généralement deux types d'effets de commerce qui sont : la lettre de change et le billet à ordre

- La lettre de change

Une lettre de change est un document écrit sur lequel une personne, appelée le tireur (le fournisseur), donne à son débiteur, appelé le tiré (le client), l'ordre de lui payer une somme d'argent déterminée, à une date déterminée (l'échéance).

○ Le billet à ordre

Le billet à ordre est un document par lequel le client reconnaît sa dette et s'engage à payer le fournisseur à la date d'échéance. Il peut être papier ou relevé (billet à ordre dématérialisé sur une bande magnétique).

#### **1.1.2.4 L'avis de prélèvement**

L'avis de prélèvement est un moyen de paiement automatisé adapté aux règlements récurrents, dispensant le débiteur de l'envoi d'un titre de paiement lors de chaque règlement.

#### **1.1.2.5 La carte bancaire**

Une carte de paiement est émise par un établissement de crédit et permet à son titulaire (le porteur) d'effectuer ses règlements aux moyens de celle-ci. (Ce qui équivaut à un transfert de fonds) ou de retirer des espèces dans les distributeurs automatiques de billets (DAB).

### **1.1.3 Les caractéristiques communes des moyens de paiement scripturaux**

L'offre des moyens de paiement scripturaux est variée et le mode d'utilisation de ceux-ci se différencie pour répondre à différents besoins. D'après une étude de Marc Andries et Carlos Martin (2004 :92)<sup>1</sup>, tous moyens de paiement scriptural se caractérisent par la combinaison d'un instrument sur support papier ou informatisé qui permet à l'utilisateur de produire un ordre de paiement tel que : le chèque, la carte bancaire, le virement et un dispositif technique et organisationnel, qui permet le traitement de cet ordre.

En effet la remise d'un ordre de paiement ne suffit pas à transférer les fonds tenu en compte par un intermédiaire financier. Ce dernier doit effectuer un certain nombre d'opérations pour exécuter ce transfert, ce qui requiert la mise en œuvre d'une infrastructure technique et organisationnelle plus ou moins complexe destinée à

- assurer la validité des ordres émis par les utilisateurs ;
- collecter les ordres émis par les utilisateurs ;
- transmettre les informations nécessaires (identifications du compte, par exemple) à l'exécution du transfert.

---

<sup>1</sup> ANDRIES MARC & CARLOS MARTIN (2004), la surveillance des moyens de paiement scripturaux : objectifs et modalités de mise en œuvre, Banque de France, Revue de la stabilité financière N°5, Novembre, P.92

Le transfert de fonds proprement dit c'est lorsque le paiement est réalisé par des fonctions d'échange et de règlement entre les établissements de crédit.

## **1.2 Les principaux systèmes bancaires de moyens de paiement scripturaux**

La Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO) a initiée un important projet de modernisation de ces systèmes de paiement des états membres de l'Union Economique Monétaire Ouest Africaine (UEMOA). Ces 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 à la globalisation de l'économie mondiale consécutive aux innovations technologiques, notamment dans le domaine de l'information et des télécommunications. Fortes de ces exigences, les autorités monétaires ne ménagent pas d'effort pour l'amélioration des systèmes de paiement existants ; c'est bien le cas dans l'espace UEMOA. Il est donc important d'avoir une bonne connaissance de la notion de système de paiement.

### **1.2.1 Définition de système bancaire de moyens de paiement**

Selon KAUFFMAN (2008 : 124)<sup>2</sup>, les systèmes bancaires de moyens de paiements sont des infrastructures destinées à traiter au niveau des banques, les paiements en monnaie scripturale de gros ou 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 les instruments tels que les cartes bancaires, les virements les chèques etc.

Selon le dictionnaire un « système de paiement » c'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 ».

---

<sup>2</sup> KAUFFMAN Pascal (2008), l'union monétaire européenne, Presse universitaire de bordeaux Pesac, P. 124

## 1.2.2 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 aboutissent au règlement de leurs opérations. Ces systèmes mettent en relation directe la banque centrale, les établissements financiers, le trésor public de l'état ou des états dans un système régional et les services financiers de la poste.

### 1.2.2.1 La banque centrale

De l'avis de MISHKIN (2010 : 504)<sup>3</sup>, 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 virements interbancaires ;
- Surveillance de la solvabilité du système bancaire et financier.

### 1.2.2.2 Les établissements de crédit

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

### 1.2.2.3 Le trésor public

Vallet (2003 : 31)<sup>4</sup> définit le trésor public comme l'institution de l'état qui effectue les opérations d'exécutions 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.

---

<sup>3</sup> MISHKIN Frédéric (2010), Monnaie banque et Marchés financiers, 9<sup>ème</sup> édition, Pearson éducation, Paris, P. 439

<sup>4</sup> VALLET Elisabeth (2003), les correspondants du trésor, Edition l'Harmattan, 5-7, rue de l'école-polytechnique, 75005 Paris, France, P.31

#### **1.2.2.4 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

#### **1.2.2.5 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.

### **1.2.3 La nomenclature des systèmes de paiement dans l'UEMOA**

Dans l'espace UEMOA, les réformes dans les systèmes de paiement se sont traduites par la mise en place de nouveaux circuits automatisés et la dématérialisation des échanges et des règlements interbancaires, A ce jour les circuits de paiement concernent essentiellement les réseaux intrabancaires, le Système Interbancaire de Compensation Automatisée (SICA-UEMOA), le Système de Transfert Automatisée 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 Télé communication). Pour les paiements avec les cartes bancaires, il a été mis en place une structure technique, le centre de Traitement Monétaire Interbancaire de l'UEMOA (CTMI-UEMOA) connu désormais sous l'appellation de Groupement Interbancaire Monétique de l'UEMOA (GIM-UEMOA).

#### **1.2.3.1 Réseaux intra bancaires pour les groupes**

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

### **1.2.3.2 Le Système de Transfert Automatisé et de Règlement (STAR)**

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

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, ou le participant est raccordé au système depuis une plateforme installée dans les locaux et gère lui-même l'émission de ces ordres dans le système et le suivi de sa position.
- La participation indirecte, ou le participant accède au système via un service bureau installé dans les locaux de l'agence principale de la BCEAO.

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 de l'ordre d'arrivée ;
- Le contrôle automatique dans le compte règlement du participant donneur d'ordre ;
- L'imputation immédiate des opérations dans le compte de règlement des participants concernés.

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 aux systèmes centrale via le réseau SWIFT pour l'envoi et la réception des messages ou via le réseau VSAT de la BCEAO;
- Le siège de la banque centrale assure la gestion opérationnelle et technique centralisée du système ;

### **1.2.3.3 Système Inter bancaire de compensation Automatisé de l'UEMOA (SICA –UEMOA)**

Le 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.

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

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

- Etre 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 interbancaire 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 du système central détermine le mode de participation au SICA-UEMOA. Il existe actuellement deux modes de participation :

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

Avec ce nouveau système de compensation, les banques peuvent depuis leur locaux transmettre des fichiers électronique de leur 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 de présentations électroniques, avec en appui l'échange d'images scannées des valeurs ayant comme support le papier.

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.

La communication et la modification de la journée sont du ressort de la BCEAO. Le SICA-UEMOA se compose de neuf systèmes de compensation, un système national pour chacun des huit états membres de l'UMOA et un système de compensation régional. Chaque système de compensation national relié à un système centrale installé au niveau de l'agence principale et d'un ou plusieurs points d'accès à la compense (PAC). Ce sont des systèmes informatiques qui permettent l'échange des fichiers.

#### **1.2.4 Les acteurs au processus de règlement des moyens de paiement scripturaux**

Le processus de paiement d'un instrument scriptural fait intervenir les acteurs suivants :

- Le débiteur ;
- L'établissement du débiteur ;
- Le créancier ;
- L'établissement du créancier.

Toutefois, d'autres intermédiaires financiers peuvent s'ajouter à la liste. Cela dépend de l'instrument scriptural émis, et accepté par l'ensemble des établissements financiers intervenant dans le traitement du paiement de l'ordre. (Marc Andrea et Carlos Martin, 2004).

### **1.3 Risques opérationnels liés au processus de règlement des moyens de paiement scripturaux**

La notion de risque opérationnel sera abordée après avoir défini le risque de manière générale.

#### **1.3.1 Définition du risque**

Selon les normes européennes (EN 292-1 et 2 EN 1050) Le risque est défini par : « *Une combinaison de la gravité et de la probabilité d'apparition d'une lésion ou d'une atteinte à la santé, pouvant survenir dans une situation dangereuse* ». Cette Définition est complétée par celle de l'institut Français de l'Audit et du Contrôle Interne (IFACI) qui 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 on notamment pour mission d'assurer autant que faire se peut la maîtrise* ».

### 1.3.1.1 Risques liés à l'activité bancaire

Pour François DESMICHT (pratique de l'activité bancaire, 2004 : 239) <sup>5</sup> 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* » ; le risque est indissociable de l'activité bancaire, il existe à tous les niveaux de la banque.

Les risques inhérents à l'activité bancaire peuvent se classer en quatre catégories selon Hennie VAN GREUNING & Sonja BRAJOVIC BRATANOVIC (analyse de gestion du risque bancaire, 2004) <sup>6</sup>

- Le risque de crédit ;
- Les risques de Marché ;
- Les risques opérationnels ;
- Et autres risques.

Chaque catégories de risques se décomposent en plusieurs sous risques.

Nous traiterons du risque opérationnel en général, et des risques opérationnels liés aux moyens de paiements.

### 1.3.2 Définition du risque opérationnel

La définition du risque opérationnel ne fait pas l'objet d'un consensus. Elle diffère d'un organisme à un autre.

Selon NICOLET <sup>7</sup>, « *la notion de risque opérationnel diffère dans les réglementations nationales et internationales. Un moyen de mieux la cerner serait de la définir par un couple de facteurs/conséquences* ». NICOLET poursuit en affirmant que les risques les plus connus sont les risques de fraude, de détournement d'actifs et d'informations financières non fiables.

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

---

<sup>5</sup> DESMICHT François (2007), la pratique de l'activité bancaire, 2<sup>e</sup> édition Dunod, Paris P354

<sup>6</sup> Hennie Van GREUNING & Sonja BRAJOVIC BRATANOVIC (2004), analyse de la gestion du risque bancaire P.120

<sup>7</sup> Nicolet Marie-Agnès (2000), Risques opérationnels : de la définition à la gestion, banque magazine n°615 P. 44

Cette définition prend en compte les risques juridiques. Et on part des effets quantifiables (pertes directes) pour remonter aux causes (événements du risques). La perte constatée (effet) permet de remonter à l'évènement lui-même permet de remonter à une ou plusieurs causes (inadéquations des procédures événement extérieur, défaillance humaine, etc.)

### **1.3.3 Les composantes du risque opérationnel**

Selon le comité de bale 2 (convergence internationale de la mesure et des normes de fond propres, 2004), le risque opérationnel se décompose en quatre sous ensemble définit comme suit :

#### **1.3.3.1 Le risque lié au système d'information**

Ce risque peut être lié à une défaillance matérielle suite à l'indisponibilité soit provisoire ou prolongé des moyens (installations immobilières matériels, systèmes informatiques ou dispositifs techniques) nécessaire à l'accomplissement des transactions habituelles et à l'exercice de l'activité.

#### **1.3.3.2 Le risque lié au processus**

Ce risque est dû au non-respect des procédures, aux erreurs provenant de l'enregistrement des opérations, la saisie, les rapprochements et les confirmations tels que : un double encaissement de chèque, un crédit porté au compte d'un tiers et non du bénéficiaire, le versement du montant d'un crédit avant la prise effective de la garantie, le dépassement des limites et autorisations pour la réalisation d'une opération.

#### **1.3.3.3 Le risque lié aux personnes**

Ce risque naît lorsque les exigences attendues des moyens humains (exigence de compétence et de disponibilité, exigence de déontologie) ne sont pas satisfaisantes, peut être lié à l'absentéisme, la fraude l'incapacité d'assurer la relève sur des postes clés. Ce risque peut être volontaire ou naît d'une intention délibérée, résultant souvent d'une intention frauduleuse. Les erreurs involontaires sont souvent coûteuses ; leur prévention comme leur détection précoce dépendent de la qualité du personnel, de sa vigilance, comme de sa capacité d'adaptation aux évolutions techniques mais aussi à la technicité des opérations à traiter et de la qualité du matériel et de la logistique utilisés. Quant au « risque volontaire », il va de la simple inobservation des règles de prudence, du conflit d'intérêts entre opérations pour son propre compte et opérations pour le compte de

l'établissement ou du client, jusqu'à la malveillance et la réalisation d'opérations carrément frauduleuses.

### 1.3.3.4 Le risque lié aux événements extérieurs

Ce risque peut provenir des catastrophes naturelles, de l'environnement réglementaire, du risque politique.

### 1.3.4 Quelques risques opérationnels liés au processus de paiements scripturaux

Les risques opérationnels liés au processus de règlement des moyens de paiements scripturaux sont des risques liés à l'organisation et au fonctionnement général du système interne de la banque. Ils sont liés par exemple à l'informatique et aux technologies, à l'adéquation aux pratiques, aux procédures bancaires, et aux dispositions prises contre la mauvaise gestion et la fraude (GREUNING & al, 2004)<sup>8</sup>.

Ces risques sont présentés dans le tableau ci-dessus :

**Tableau 1 : Différents risques opérationnels liés au processus**

| Sous- activité      | Tâches   | Risques opérationnels   | Dispositifs de Maitrise   |
|---------------------|--|---|---|
| Gestion des chèques | <ul style="list-style-type: none"> <li>- réception du chèque</li> <li>-imputation au compte du remettant ou au compte interne.</li> <li>- Tri et envoi du chèque à la compensation.</li> <li>-Réception des moyens de paiement du circuit d'échange.</li> <li>- Règlement au / du circuit d'échange</li> </ul> | <ul style="list-style-type: none"> <li>-Non traitement de la réception ou perte de la valeur reçue</li> <li>-Non vérification de la validité de la réception</li> <li>-Non enregistrement</li> <li>Erreur d'enregistrement (montant, date, compte)</li> <li>-Erreur sur la nature du moyen de paiement</li> <li>-Enregistrement fictif</li> </ul> | <ul style="list-style-type: none"> <li>-Vérifier que tous les chèques reçues remplissent les conditions générales de validité ;</li> <li>- Vérifier la conformité du chèque et le correcte remplissage du bordereau de remise ;</li> <li>- Vérifier que tous les chèques reçus sont bien imputé aux comptes des clients.</li> <li>- Vérifier que tous les chèques remis à la compensation sont bien réglés, et ce en tenant compte des jours de valeurs.</li> </ul> |

<sup>8</sup> GREUNING Van Henri & al (2004), analyse et gestion du risque bancaire : un cadre de référence pour l'évaluation de la gouvernance d'entreprise et du risque, éditions ESKA, P 386

|  |   |  |   |
|--|---|--|---|
| <p>Gestion des virements et prélèvements</p> | <ul style="list-style-type: none"> <li>-Réception de l'ordre de virement</li> <li>-Réception d'un avis de prélèvement</li> <li>-Réception d'une opération sur compte client</li> <li>- Envoie de l'ordre de virement ou de prélèvement à la compensation</li> <li>-Réception des moyens de paiement du circuit d'échange</li> <li>-Règlement au/du circuit d'échange</li> </ul> | <ul style="list-style-type: none"> <li>-Erreur sur les caractéristiques de l'opération ;</li> <li>-Avis de prélèvement sans autorisation</li> <li>-Compte clos sans provision en opposition, etc.</li> <li>-Rejet de l'ordre de virement</li> <li>-Paiement non autorisés</li> <li>-Insuffisance de provision ou non-respect de la limite autorisée</li> </ul> | <ul style="list-style-type: none"> <li>-Vérifier que le formulaire d'ordre de virement ou d'avis de prélèvement est bien renseigné</li> <li>-Vérifier que le virement ou l'avis de prélèvement est autorisé par une personne habilitée</li> <li>-Rapprochement des ordres de virements ou prélèvements et des virements existants dans le système.</li> </ul> |
|--|---|--|---|

**Source : nous même**

Les travaux de normalisation qui ont été menés dans le secteur bancaire ont remis au goût du jour la notion de risque opérationnel. La réglementation bancaire le place au premier rang des préoccupations. La méthodologie unique d'action face au risque n'existe pas. Selon leur but de gestion et leurs modes d'organisation, les entreprises adoptent leur méthode d'action.

## **Chapitre 2 : la gestion des risques opérationnels liés au processus de règlements des moyens de paiement scripturaux**

Le risque est l'exposition à une forte probabilité de perte. Les banques sont menacées par une diversité de risques nuisant à leurs activités et à leurs positions sur le marché financier. Cependant pour qu'une banque puisse atteindre sa mission elle doit être en mesure d'identifier et d'atténuer les risques qui menacent sa santé financière et son existence à long terme. La gestion des risques réduit donc la probabilité de réaliser des pertes et minimise le degré de la perte au cas où celle-ci arriverait, elle réduit la prime d'assurance et baisse les charges en capital.

Pour être mieux géré et appréhendé, les banques de nos jours tentent d'analyser et de mesurer les risques liés aux opérations. La gestion du risque opérationnel est devenue le sujet de réflexion profond pour les institutions bancaires et les autorités de surveillance.

### **2.1 La politique de gestion des risques opérationnels**

Elle consiste pour les dirigeants à la mise en place d'une politique de gestion de risques opérationnels adéquate, des processus et des procédés adaptés.

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

Selon JIMENEZ & al (2008 : 271)<sup>9</sup>, les objectifs poursuivis par la politique de gestion des risques opérationnels sont au nombre de quatre :

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

---

<sup>9</sup> CHELLY Dan, MERLIER Patrick, JIMENEZ Christian (2008), Risques opérationnels : la mise en place du dispositif à son audit, Revue Banque, P. 271

- répondre aux exigences réglementaires.

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

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

## **2.2 Les acteurs et organes de pilotage du dispositif**

Plusieurs acteurs interviennent dans le pilotage du dispositif

### **2.2.1 Les actionnaires et le Conseil d'Administration**

Selon SARDI (2002 : 312)<sup>10</sup>, l'organe délibérant doit être conscient que le risque opérationnel est une catégorie de risque à part entière, distincte et contrôlable. Il doit approuver et revoir périodiquement la stratégie de la banque dans ce domaine.

Il doit également approuver la structure dédiée à la gestion de ce risque et s'assurer que l'organe exécutif assume ses responsabilités dans ce domaine.

### **2.2.2 La Direction générale**

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

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

---

<sup>10</sup>SARDI Antoine (2002), Audit et Contrôle internes bancaires, AFFGE édition, P. 312

### **2.2.3 Le comité des risques opérationnels**

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

Il doit traiter en particulier :

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

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

- de faire évoluer le dispositif de suivi, de surveillance et de contrôle des risques opérationnels ;
- de décider l'engagement de plans d'actions ;
- de réduire certaines expositions aux risques opérationnels en fixant ou proposant des normes de gestion et des limites.
- 

### **2.2.4 Les responsables risques opérationnels**

Selon JIMENEZ & al, (2008 :115), l'organe exécutant à la responsabilité de mettre en œuvre la stratégie approuvée par l'organe délibérant. Il a aussi la responsabilité de développer les processus et les procédures pour gérer ce risque dans toutes les activités de la banque. Le responsable risque opérationnel est rattaché au directeur des risques. Il est en charge de :

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

périodique des bases d'incidents, de la résolution des incidents, de l'état d'avancement des plans d'actions ; de documenter le dispositif de gestion ( procédures, contrôles ....).

## **2.3 Dispositif de maîtrise des risques opérationnels liés aux moyens de paiement scripturaux**

Le dispositif de maîtrise de risque opérationnel nous permet d'avoir une bonne compréhension de ces risques, un dispositif de détection, de contrôle et de suivi des activités de banque.

### **2.3.1 Objectif du dispositif de maîtrise des risques opérationnels**

La finalité d'un dispositif de maîtrise des risques opérationnels est de pouvoir agir sur les différents éléments identifiés et quantifiés afin de modifier le profil de risque de banque ou tout de moins sa sensibilité en cas de survenance d'évènements non souhaités.

### **2.3.2 La prise de connaissance du processus de gestion des moyens de paiement scripturaux**

L'objectif de la prise de connaissance est d'identifier les principales procédures et d'apprécier la fiabilité d'ensemble du contrôle interne.

Pour RENARD (2010 :469)<sup>11</sup>, il n'y a pas de méthode d'audit qui ne commence pas par la prise de connaissance des processus ou des activités que l'on veut auditer. L'auditeur doit en avoir au moins la culture pour être en mesure de comprendre les explications qu'il va chercher et solliciter et, plus généralement pour se faire admettre aisément.

---

<sup>11</sup> RENARD Jacques (2010), Théorie et pratique de l'audit interne, 7<sup>ième</sup> édition, groupe Eyrolles P.469

## **2.4 Identification, évaluation et suivi des risques opérationnels liés au processus de règlement des moyens de paiements scripturaux.**

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

### **2.4.1 Identification des risques opérationnels liés aux moyens de paiement scripturaux**

Les risques opérationnels sont inhérents à tous les types d'activités, de produits, de processus et systèmes. Une identification efficace doit comprendre les facteurs. L'identification des risques nous permettra d'évaluer l'impact des risques opérationnels. Elle passe nécessairement par une description précise du processus. Le processus d'identification des risques devrait également comprendre la détermination des risques qui sont contrôlables par la banque et ceux qui ne le sont pas. Il n'existe pas de méthodes d'identification plus fiable que d'autres ; l'essentiel pour COOPERS & al (2000 : 378)<sup>12</sup>, est que les dirigeants tiennent compte de certains facteurs qui peuvent contribuer à l'apparition d'un risque, voire à son aggravation. Ces facteurs peuvent être :

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

Ils existent plusieurs techniques d'identifications des risques.

#### **2.4.1.1 Identification basée sur l'atteinte des objectifs**

Très souvent le risque est défini comme un événement qui empêche l'atteinte des objectifs de l'organisation. Ainsi suivant cette approche, on identifie d'abord les objectifs de l'activité ou de l'organisation, pour ensuite leur adjoindre les menaces qui pèsent sur eux. L'efficacité de cette approche repose sur une identification claire et partagée des objectifs en amont. Quant à sa réussite, elle est fonction d'un langage

---

<sup>12</sup> COOPERS et LYBRAND (2000), la nouvelle pratique du contrôle interne, 5<sup>ème</sup> tirage, Editions d'organisation, Paris P. 378

commun, partagé par les acteurs pour ce qui est des objectifs poursuivis par l'organisation.

- identification basée sur les check-lists ;
- identifications basée sur l'analyse de l'environnement ;
- identification basée sur les scenarii ;
- identification par analyse historique ;
- identification par taches élémentaires.

Des différentes techniques citées ci-dessus notre étude sera basée sur les deux (2) dernières

#### **2.4.1.2 Identification par analyse historique**

Cette approche consiste à identifier les risques opérationnels en se basant sur ceux déjà survenus au sein de l'organisation.

#### **2.4.1.3 Identification par taches élémentaires**

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

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

## 2.4.2 Evaluation des risques opérationnels liés au processus de moyens de paiement scripturaux

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

Ainsi, pour BARTHELEMY et COURREGES (2004 : 33)<sup>13</sup> évaluer un risque c'est l'apprécier à travers sa probabilité d'occurrence, ou fréquence, et par ses effets, ou sa gravité. L'exposition d'un établissement financier au risque opérationnel est mesurée à l'aide d'une variété d'approche. Les banques ont la possibilité de choisir celles qui leur paraissent correspondre le mieux à la spécificité de leur activités, mais aussi à leur capacité globale d'action. Elles doivent en effet s'assurer qu'elles disposent de l'ensemble des moyens nécessaires à la mise en œuvre de la solution retenue. Le comité de Bâle propose trois approches par ordres croissants de complexité et de sensibilité au risque :

- L'approche de l'indicateur de base :

Selon l'approche de l'indicateur de base (basic indicator approach ou BIA), le capital réglementaire en couverture de risque opérationnel est égal à 15% du revenu annuel brut moyen de l'établissement sur les trois dernières années.

- L'approche standard:

Elle est en fait un prolongement plus fin de la BIA. Le capital réglementaire est ici fonction d'un pourcentage du produit brut, il est établi à 12%, 15%, ou 18% selon le niveau du risque opérationnel estimé de chaque activité. L'approche standardisée prend en compte la nature de l'activité de l'institution.

- Les approches de mesures avancées :

Il ne s'agit plus d'une approche unique, définie par le régulateur, mais d'un ensemble de modèles internes réunies sous le vocable « d'approches de mesures complexes (AMC) » ou AMA (Advanced Measurement Approach) approuvé par les autorités de contrôle sur la base d'une série de critères. Les accords de Bâle2 n'imposent aucune méthode particulière de calcul pour les banques adoptant l'approche de mesures complexes (AMA). Ce choix est laissé à la discrétion des banques, pourvu qu'elles satisfassent aux critères qualitatifs et quantitatifs énoncés dans l'accord.

---

<sup>13</sup> BARTHELEMY Bernard & COURREGES Philippe (2004), Gestion des risques, Méthode d'optimisation globale, Edition d'organisation 2<sup>ème</sup> édition, Paris, P. 33

### **2.4.3 Suivi des risques opérationnels liés aux processus de moyens de paiement scripturaux**

Un système de suivi de l'exposition au risque opérationnel et des événements de pertes par grands secteurs d'activités doit être mis en œuvre sur une base continue. Le suivi est plus efficace lorsque le système de contrôle interne est inclut dans les procédures et produits des rapports réguliers qui sont intégrés dans le système de reporting destinés aux organes dirigeants (SARDI, 2002 : 315)<sup>14</sup>

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

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

Les étapes de la démarche de cartographie sont la suivantes :

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

### **2.4.4 Les composants du dispositif de maîtrise des risques opérationnels liés aux moyens de paiements scripturaux**

Pour le cabinet PricewaterhouseCoopers (2005 : 32-33)<sup>15</sup>, le dispositif de contrôle des risques opérationnels comprend huit éléments qui résultent de la façon dont l'organisation est gérée et s'intègrent au processus de management :

- l'environnement interne ;
- la fixation des objectifs ;

---

<sup>14</sup> SARDI Antoine (2002), Audit et contrôle interne bancaires, Edition AFGES Paris, P. 315

<sup>15</sup> Pricewaterhousecoopers (2005), la pratique du contrôle interne, Edition d'organisation, P. 32-33

- l'identification des risques ;
- l'évaluation des risques ;
- le traitement des risques ;
- les activités de contrôles ;
- l'information et la communication ;
- le pilotage.

## **2.5 Le contrôle interne du processus de gestion des moyens de paiement scripturaux**

Le contrôle interne concerne la banque dans toutes ces activités. Il s'applique aux biens, aux individus, et aux informations, quelles que soient les circonstances ou l'époque de l'année.

Toutefois, on ne peut contrôler que ce qui est organisé. L'ensemble des activités de la banque doit, au préalable être structuré : définition des niveaux de contrôle, organisation rigoureuse de la fonction (BERTIN, 2007 : 96)<sup>16</sup>

Le COSO 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 quant à la réalisation des objectifs suivants :

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

Pour SIRUGUET (2001 : 460-462)<sup>17</sup>, les fondamentaux du contrôle interne sont les suivants :

- définition des habilitations, délégations, autorisations ;
- limitation des accès ;
- surveillance des conditions de conservation ;
- contrôle de la sécurité des actifs ;

---

<sup>16</sup> BERTIN Elisabeth (2007), Audit interne : enjeux et pratiques à l'international, EYROLLES, P. 96

<sup>17</sup> SIRUGUET Jean Luc (2001), le contrôle comptable bancaire tome II, pratique du contrôle comptable des opérations de banques classiques, revue banque, éditeur 18, Rue la Fayette, Paris, P. 460-362

- manuels de procédures ;
- réalité des informations ;
- séparation des fonctions.

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

Selon SARDI (2002 : 952-960)<sup>18</sup>, les objectifs du système de contrôle interne des risques opérationnels liés aux moyens de paiement sont les suivants :

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

### **2.5.1 Les dix (10) Principes de bonne pratique en matière de gestion des risques opérationnels**

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

---

<sup>18</sup> SARDI Antoine (2002), Audit et contrôle interne bancaires, Edition AFGES, Paris, P. 952-960

## **Elaboration d'un environnement adéquat pour la gestion de risque opérationnel**

- Principe 1

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

- Principe 2

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

- Principe 3

La Direction Générale devrait avoir pour mission de mettre en œuvre le dispositif de gestion des risques opérationnels approuvé par le conseil d'administration. Ce dispositif devrait être appliqué de façon cohérente dans l'ensemble de l'organisation bancaire, et les membres du personnel à tous les niveaux, devraient bien comprendre leur responsabilité dans la gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants.

### **Gestion des risques : identification, évaluation, suivi et maîtrise/atténuation du risque opérationnel.**

- Principe 4

Les banques devraient identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles devraient aussi, avant de

lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent.

- Principe 5

Les banques devraient mettre en œuvre un processus de suivi régulier des profils de risques opérationnels et des expositions importantes à des pertes. Les informations utiles à une gestion dynamique du risque opérationnel devraient être régulièrement communiquées à la Direction Générale et au Conseil d'Administration.

- Principe 6

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

- Principe 7

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

## **Rôle des superviseurs**

- Principe 8

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

- Principe 9

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

### **Rôle de la communication financière**

- Principe 10

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

A travers ce chapitre nous avons abordé les dispositifs de maîtrise des risques opérationnels liés aux moyens de paiement scripturaux ainsi que les dix (10) principes de bonnes pratiques en matière de gestion des dits risques. Nous allons maintenant passer à la méthodologie de recherche de notre travail.

#### **2.5.2 Les objectifs de l'évaluation du dispositif de contrôle interne des risques opérationnels**

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

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

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

### **2.5.3 Les étapes d'évaluation du contrôle interne des risques opérationnels liés au processus des moyens de paiement scripturaux**

Pour OGIEN (2008 :466-467)<sup>19</sup>, le contrôle interne doit être approché par processus (et dont de manière transverse sur les différents services), Son analyse devant porter en priorité sur ceux qui sont susceptibles de soulever des difficultés. L'identification des dysfonctionnements peut être réalisée à l'aide de la revue du niveau des suspens comptables, des réclamations de la clientèle ou en s'appuyant sur les travaux réalisés par les différents corps de contrôle (audit interne, inspection)

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

- La sécurité et l'efficacité des systèmes d'informations, en s'appuyant sur la revue des cartographies applicatives ;
- Le niveau des procédures opérationnelles et leurs applications effectives dans les back-offices et les centres de techniques ;
- La compréhension détaillée des schémas comptables ;
- L'analyse du contrôle comptable.

---

<sup>19</sup> OGIEN Dov (2008), comptabilité et audit bancaire, 2<sup>e</sup> édition, DUNOD, P. 466-467

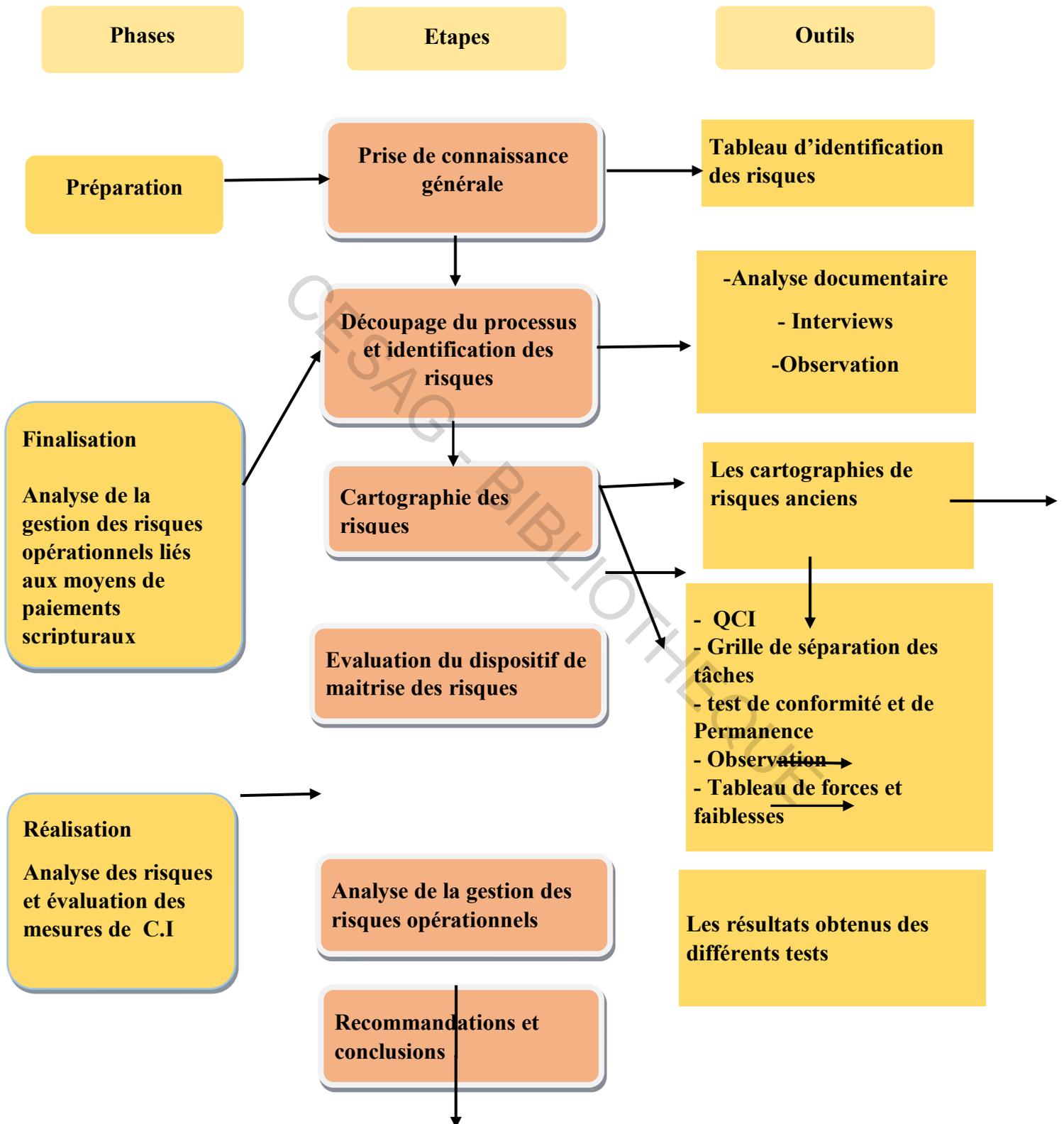
## **CHAPITRE 3 : METHODOLOGIE DE LA RECHERCHE**

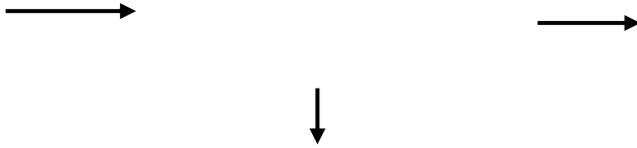
Pour réaliser cette étude, la méthodologie de recherche consiste à la mise en œuvre de notre démarche théorique du processus de gestion des moyens de paiement scripturaux. Ce chapitre présente dans un premier temps, un modèle d'analyse, et dans un second temps, les outils de collecte et d'analyse des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

### **3.1 Modèle d'analyse**

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

Figure 1 : Modèle d'analyse





Source : nous même

### **3.2 Outils de collecte et d'analyse des données**

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

#### **3.2.1 L'analyse documentaire**

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

#### **3.2.2 L'observation physique**

Une observation physique est la constatation de la réalité instantanée de l'existence et du fonctionnement d'un processus, d'un bien, d'une transaction ou d'une valeur. Elle consiste essentiellement à la description détaillée et visuelle d'un dispositif donné. Elle doit permettre de porter un avis sur l'état physique et/ou du fonctionnement apparent du bien à l'instant de l'observation (LEMANT, 1995 : 181-203)<sup>20</sup>

---

<sup>20</sup> LEMANT Olivier (1995), la conduite d'une mission d'audit interne, DUNOD, P.181-203

### **3.2.3 L'interview**

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

Ainsi, nous allons nous entretenir avec les personnes suivantes :

- l'agent chargé de la clientèle ;
- les responsables des opérations ;
- les responsables de la direction du contrôle interne ;

### **3.2.4 La grille de séparation des tâches**

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

Elle va véritablement relier l'organigramme fonctionnel à l'organigramme hiérarchique et justifier les analyses de postes. Sa lecture va permettre de déceler sans erreur possible les manquements à la séparation de tâches et donc d'y porter remède.

Elle décrit la répartition du travail et décèle les éventuels cumuls de fonctions incompatibles afin d'y remédier.

### **3.2.5 Les tests de conformité et de permanence**

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

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

### **3.2.6 Le tableau des forces et faiblesses apparentes**

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

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

## **Conclusion Première partie**

La gestion des moyens de paiement scripturaux est une activité très importante de la banque. Leur sécurité est essentielle au maintien de la confiance dans la monnaie et entre les différents partenaires. Les établissements de crédit doivent alors assurer une gestion adéquate des risques opérationnels liés à cette activité.

La revue de littérature ainsi présentée nous a permis de cerner les variables que sont l'activité bancaire, les différents moyens de paiement scripturaux et la gestion des risques opérationnels associés. Ainsi nous avons pu aborder la notion de risque opérationnel, le dispositif de contrôle de ce risque, l'analyse de la gestion des risques. Tous ces points importants nous aiderons à répondre aux questions ci-dessous qui feront l'objet de la deuxième partie de notre travail.

Quels sont les risques liés au traitement des moyens de paiements scripturaux traités via le système SICA-UEMOA et le STAR-UEMOA ?, comment ces risques sont-ils gérés à VERSUS BANK ?

CESAG - BIBLIOTHEQUE

## **DEUXIEME PARTIE : CADRE PRATIQUE**

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

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

- Le chapitre 4 consacré à la présentation de VERSUS BANK ;
- Le chapitre 5 axé sur la description des procédures de gestion des moyens de paiement par la télé compensation « aller » et par RTGS, ainsi que la gestion des risques opérationnels associés ;
- Le chapitre 6 consacré à la mise en œuvre de notre modèle d'analyse.

## **Chapitre 4 : Présentation de VERSUS BANK**

VERSUS BANK est l'entreprise qui nous a accueillis pour ce stage de fin de cycle. Etablissement bancaire, son insertion sur le marché ne fut pas aisée étant donné la rude concurrence qui caractérise ce secteur.

La présentation de cette entreprise, basée sur les informations fournies par le Département des Ressources Humaines sera axée sur les points suivants :

- ✓ L'histoire de sa création
- ✓ Son mode de fonctionnement

### **4.1 Présentation Générale de l'Entreprise**

#### **4.1.1 Historique, Objectifs et Statut juridique**

#### **4.1.1.1 Historique**

VERSUS BANK a été créée en 2003 par le groupe AIGLON SA. Ce groupe, dont le siège se trouvait à Genève en SUISSE, était présent dans une dizaine de pays d'Afrique (Côte d'Ivoire, Benin, Togo, Cameroun, Burkina Faso, Niger, Guinée-Bissau, République Centrafricaine et Guinée Conakry). Bien qu'étant créée depuis 2003, c'est en 2004 que la banque commence ses activités.

#### **4.1.1.2 Objectifs**

VERSUS BANK est un établissement financier dont les missions principales sont de gérer les dépôts, collecter les épargnes des clients, accorder des prêts et offrir des services financiers. En clair, il s'agit de faire la banque. Toutes ces activités, la banque les mène à travers son réseau d'agences et de sous agences, sur le territoire de la ville d'Abidjan. La Banque appartient au secteur économique qui regroupe les activités de conception, de production et de commercialisation des services offerts dans le marché bancaire.

#### **4.1.1.3 Statut juridique**

VERSUS BANK est une société anonyme de droit ivoirien, avec Conseil d'Administration, constituée en mars 2003 et agréée en qualité de banque par arrêté ministériel n°425 du 1er décembre 2003 du Ministre de l'Economie et des Finances. Versus Bank a effectivement démarré ses activités en mars 2004.

Banque à capitaux privés à l'origine, Versus Bank a été reprise par l'Etat de Côte d'Ivoire, comme actionnaire unique depuis janvier 2009.

Après des débuts prometteurs, la banque a traversé des difficultés qui ont conduit les autorités à la placer sous administration provisoire, à compter du 02 août 2006.

Cette administration provisoire s'est achevée le 31 décembre 2008, avec la reprise totale de la banque par l'Etat de Côte d'Ivoire.

Aujourd'hui banque nationale, avec son Directeur Général, Monsieur Guy KOIZAN, nommé en Avril 2011 à la tête de l'institution, VERSUS BANK a amorcé une dynamique novatrice et compte participer pleinement au développement de l'économie ivoirienne.

## **4.2 Organisation, Fonctionnement et Organigramme**

### **4.2.1 Organisation**

Depuis avril 2011, VERSUS BANK a à sa tête monsieur Guy KOIZAN, son Directeur Général. Celui-ci est aidé dans ses fonctions d'administration par un Directeur Général Adjoint. Le Directeur Général et son adjoint travaillent sous la supervision d'un Conseil D'Administration composé de Six (6) membres. La banque est organisée en Cinq (5) Directions qui sont:

#### **➤ La Direction Générale (DG) :**

La Direction générale a pour attributions de définir les missions et objectifs des directions sous sa responsabilité. Par ailleurs, elle anime, coordonne et oriente les activités des directions en vue de leur permettre d'atteindre les objectifs qui sont les leurs. En elle s'applique à définir les choix stratégiques de la banque et veille à sa mise en œuvre. Enfin, elle appuie les autres directions dans la gestion de leurs activités.

#### **➤ La Direction des Finances-Opérations et Technologies (DFOT) :**

Cette Direction a en charge la gestion des finances, des opérations et de la technologie de la banque. Elle assure les relations avec les partenaires de la banque et les autorités de contrôle. Elle anime et coordonne les activités des entités sous sa responsabilité.

➤ **La Direction de l'Exploitation (DEX) :**

Sous la conduite de la Direction Générale, elle a pour mission principale d'animer, de coordonner les activités des départements opérationnels sous sa responsabilité. En effet, elle doit s'investir à développer l'activité bancaire, notamment les ressources, les emplois de sorte à engager des revenus substantiels pour la banque.

➤ **La Direction du Contrôle Interne (DCI) :**

Cette Direction met en place l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. Elle a pour but d'assurer la protection, la sauvegarde du patrimoine et la qualité de l'information, de l'autre l'application des instructions de la Direction et de favoriser l'amélioration des performances. Afin d'atteindre cet objectif, la direction de contrôle veillera à mettre en place une organisation de la banque, les méthodes et les procédures de chacune des activités de la banque en vue de maintenir sa pérennité. Enfin, elle animera et coordonnera les activités des services sous sa responsabilité.

➤ **La Direction des Engagements**

Cette direction est composée du service juridique, du service crédit, du service de recouvrement, du service de l'Administration du Crédit, et du secrétariat général

## 4.2.2 Fonctionnement

L'organe exécutif est la Direction Générale, qui dirige la banque afin de la faire émerger du lot de toutes les banques concurrentes. Le fonctionnement de VERSUS BANK est illustré dans l'organigramme simplifié suivant: (voir annexes 1)

## **Chapitre 5 : Description des procédures de gestion des moyens de paiement scripturaux traités via le SICA-UEMOA, le STAR- UEMOA et la gestion des risques opérationnels associés**

A travers ce chapitre nous allons décrire les différentes procédures concernant la gestion des moyens de paiement scripturaux traités via le SICA- UEMOA et le STAR UEMOA, plus précisément les procédures de traitement concernant les chèques sur confrères, les effets escomptés, les virements et transferts émis qui ont été décrites dans le manuel de procédures.

### **5.1 Description de la procédure de traitement des chèques sur confrères.**

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

La procédure intégrale est décrite dans un logigramme en annexe 2(Page 91)

## **5.2 Description de la procédure de Traitement des effets escomptés**

L'effet à l'escompte est en effet une opération de cession à une banque d'un effet de commerce détenu par un tiers (le créancier, le fournisseur, le bénéficiaire, le tireur) sur un de ses clients (le débiteur, le client, le tiré) en échange d'une avance de trésorerie. La procédure pour le traitement des effets à VERSUS BANK est décrite dans un logigramme en annexe 3 (page 92)

## **5.3 Description des procédures de traitement des virements et transferts émis**

Nous allons d'abord voir la description de la procédure de traitement des virements et ensuite aborder celui des transferts.

### **5.3.1 Procédures de traitement des virements interbancaires**

Cela concerne les virements qui se font dans la même zone francs (Zone UEMOA) pour tout montant inférieur ou égal à cinquante millions (50 000 000) FCFA. Le donneur d'ordre donne l'ordre à sa banque (VERSUS BANK) de virer une certaine somme à une autre banque de la zone franc au profit d'un bénéficiaire si cette somme n'excède pas cinquante millions (50 000 000) Francs CFA, après vérification de la conformité de la signature du client et des autres mentions sur l'ordre de virement, l'agent de la banque chargé des opérations débite le compte client et crédite le compte du bénéficiaire via la banque indiquée mais les fonds seront disponible à la banque du bénéficiaire que le lendemain de l'opération ; c'est-à-dire jour j+1. La procédure intégrale de traitement des virements interbancaires est décrite dans un logigramme en annexe 4(page 93)

### **5.3.2 Procédures de traitement des transferts émis**

Le real Time Gross Settlement (RTGS) est un système conçu pour les transferts interbancaires de gros montants supérieurs à cinquante millions de francs CFA (50 000 000 FCFA). C'est un système dans lequel chaque transaction est réglée sur une base brute et en temps réel. Le règlement ayant lieu en même temps.

Dans ce système, les paiements transitent par la banque centrale en passant par un réseau « swift ». Cependant le système RTGS accepte les virements inférieurs à cinquante millions (50 000 000) FCFA pour gérer certains circuits qui ne peuvent pas passer par la compensation.

La procédure de traitement des transferts par RTGS de VERSUS BANK est décrite dans un logigramme en annexe 5 (page 94)

#### **5.4 La gestion des risques liés aux moyens de paiement scripturaux à VERSUS BANK**

La gestion des risques opérationnel est défini par VERSUS BANK, et s'applique à l'ensemble des institutions de la banque.

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

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

Elle consiste aussi à contrôler l'éventualité et la gravité potentielle d'un incident défavorable, et il comprend trois mécanismes inter- liés.

- **Le dispositif de contrôle interne**

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

- **Audit interne**

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

- **Audit externe**

Une évaluation externe des contrôles de l'institution.

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

## **5.5 Identification et évaluation des risques opérationnels liés au processus des moyens de paiement scripturaux**

Nous verrons ici les éléments constituant le dispositif d'évaluation des risques opérationnels liés aux moyens de paiement scripturaux et comment suivre ces risques au quotidien

### **5.5.1 Identification des risques opérationnels liés au processus des moyens de paiement scripturaux au niveau de VERSUS BANK**

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

- L'auto-évaluation des risques, qui a pour but d'évaluer les opérations et activités de la banque. Ce processus est une dynamique interne qui intègre souvent des listes de contrôle et/ou des ateliers pour identifier les forces et les faiblesses de l'environnement du risque opérationnel ;
- Cartographie des risques : le processus de gestion des moyens de paiement est cartographié. Cet exercice peut révéler des zones de faiblesse et aider à prioriser les mesures de gestion ultérieures
- Les indicateurs clé de risque ou (KRI : Key Risk indicators) les indicateurs de risques sont des statistiques et/ou mesures, souvent d'ordre financier, qui peuvent donner un aperçu des risques. Ces indicateurs devraient être examinés sur une base périodique (souvent mensuelle ou trimestrielle) pour alerter la banque sur les changements potentiels qui peuvent être source de risques ;
- Tableaux de bord : Ceux-ci fournissent un moyen de traduire des évaluations qualitatives en paramètres quantitatifs qui peuvent être utilisées pour répartir le capital économique aux secteurs d'activité par rapport à la performance dans la région et le contrôle des divers aspects du risque opérationnel.

### **5.5.2 Le suivi des risques opérationnels liés au processus de moyens de paiement scripturaux au niveau de VERSUS BANK**

Le suivi des risques opérationnels consiste à :

- Une évaluation périodique des contrôles mis en place sous la supervision des responsables de risques opérationnels (la direction du contrôle et du contrôle interne) en s'appuyant sur les procédures de contrôles interne

- Mesurer l'exposition de la banque au risque ;
- Procéder aux analyses de scénarii pertinentes ;
- Définir les actions nécessaires pour maintenir ou ramener les risques à un niveau acceptable et s'assurer de leur suivi.

Les principales catégories de risques opérationnels sont liées à des défaillances dans la gestion des risques et celles-ci entraînent souvent des pertes financières par suite d'erreur ou fraude.

Dans ce chapitre nous avons décrit les différentes procédures concernant la gestion des moyens de paiement scripturaux traités via le SICA-UEMOA et le STAR-UEMOA. Ensuite nous avons présenté la gestion des risques opérationnels liés aux moyens de paiement au niveau de VERSUS BANK. Le chapitre suivant sera consacré à l'analyse du dispositif de maîtrise des risques opérationnels liés à la gestion des moyens de paiement scripturaux traités via le SICA-UEMOA et le STAR-UEMOA ensuite nous apporterons quelques recommandations pour remédier aux insuffisances constatées.

## **Chapitre 6 : Analyse du dispositif de maîtrise des risques opérationnels liés aux moyens de paiement scripturaux.**

L'activité de gestion des moyens de paiement est une activité rigoureuse qui exige la mise en œuvre de moyen de protections fiables, puissantes et performantes. Leur sécurité est essentielle.

Cette activité peut être exposée au risque de fraude, de dégradation des ressources et du système, ou de pertes. Ces risques peuvent être issus des procédures, du personnel, et/ou des systèmes internes ou de certains événements extérieurs tels que les catastrophes naturelles, les lois et réglementations, etc. les établissements de crédit doivent assurer une gestion adéquate des risques opérationnels liés à cette activité. La gestion des risques opérationnels aide les entités à réaliser des objectifs de rentabilité et de performance et constitue une prévention contre la perte de ressources.

Ainsi, la maîtrise des risques opérationnels d'une entité peut être perçue comme l'ensemble des initiatives souhaitables qu'elle devrait adopter pour faire face aux principaux risques inhérents à ses activités. (FAUTRAT Michel 2000 :24)<sup>21</sup>

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

### **6.1 Identification et évaluation des risques opérationnels liés aux moyens de**

---

<sup>21</sup> FAUTRAT Michel (2000), De l'audit au management de la maîtrise des risques, Audit 2000, n°148, P.24-25

## paiement scripturaux traités via le SICA-UEMOA et le STAR-UEMOA.

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

Nous allons essayer d'identifier les différents risques opérationnels liés à la gestion des moyens de paiement scripturaux traités via la télé compensation et le STAR-UEMOA en découpant le processus en sous processus, les sous-processus en activité. Les tableaux comprennent cinq (05) éléments qui sont : la sous activité, l'objectif de contrôle interne, le risque opérationnel, la conséquence opérationnelle et enfin le dispositif de maîtrise de risque.

**Tableau 2 : Identification des risques opérationnels liés à la gestion des remises chèques sur confrères**

| Sous-activité  | Objectif de C.I   | Risques encourus   | Conséquence opérationnelle                | Dispositifs de maîtrise  |
|--|---|--|---|--|
| Réception du chèque et du bordereau de remise par le chargé de clientèle | S'assurer de la conformité du chèque et du bordereau de remise                                | Erreur sur le montant du chèque ou sur le bordereau de remise                | Perte financière                          | Vérifier la conformité du chèque et le correct remplissage du bordereau de remise  |
| Réception du chèque et du bordereau de remise par la banque              | S'assurer que tous les chèques sont correctement endossés                                     | Paiement non autorisé par le client<br>Acceptation de chèque volé ou ramassé | Perte financière<br>Litige avec le client | Vérifier que le chèque comporte le numéro de compte, la signature du bénéficiaire, le cachet de celui-ci si c'est une personne morale. |
| Scanning du chèque et du bordereau de remise                             | S'assurer que les chèques et les bordereaux sont bien scannés et apparaissent dans le système | Valeur non prise en compte par le système                                    | Perte financière<br>Litige avec le client | Image de tous les chèques et bordereaux de remise apparaissent bien dans le système  |

|   |   |  |  |  |
|---|---|--|--|--|
| Règlement par le système de télé compensation ou par RTGS | S'assurer que les réseaux et systèmes informatiques permettent l'échange des fichiers entre les établissements participants à la compensation et aux transferts | Détournement du moyen de paiement au profit d'un bénéficiaire illégitime.<br><br>Mauvais fonctionnement du réseau et du dispositif de systèmes informatiques | Perte financière                                     | Assurer un niveau de sécurité élevé aux moyens de paiements<br><br>Evaluation régulière du niveau de sécurité du dispositif technique et organisationnel de compensation et de transfert   |
| Saisie des références du chèque dans le système           | S'assurer que les références du chèque sont bien saisies par l'agent opération dans le système  | Erreur dans la saisie du compte dans le système  | Perte financière                                     | Procéder au pointage des valeurs saisies   |
| Intégration du chèque dans le système                     | S'assurer de la bonne intégration des ordres dans le système.   | Non prise en compte de certains ordre pas le système   | Conflit entre les banques<br><br>Perte de ressources | Contrôler dans le système, le montant total et le nombre de chèques intégrés   |
| Transmission des ordres à la BCEAO                        | S'assurer que les ordres sont bien reçus par la BCEAO   | Retard dans la transmission des ordres<br><br>transmission de données erronées   | Litige entre banques                                 | Vérification du code état qui doit passer de 050 à 130   |
| Aller des Chèques physiques à la compensation             | S'assurer que les chèques sont prêts pour la compensation   | Vol de chèques<br><br>Perte de chèques   | Perte de ressources                                  | Faire imprimer le rapport détaillé des chèques traités par banques tirées et Procède à un pointage entre ledit état et les valeurs<br><br>-Insérer les chèques et exemplaire de toutes les décharges de valeurs transmises aux confrères |

**Source : nous même**

**Tableau 3 : Identification des risques opérationnels liés à la gestion des virements et transferts émis.**

| Sous-activité                                   | Objectif de C.I  | Risques encourus  | Conséquence opérationnelle                           | Dispositifs de maitrise  |
|---|--|---|--|--|
| Réception des ordres de virement ou prélèvement | <p>S'assurer de l'autorisation préalable du client</p> <p>S'assurer de la conformité de la signature du client</p> | <p>Opérations non autorisée par le client</p> <p>Usurpation d'identité</p>                              | <p>perte financière</p> <p>Litige avec le client</p> | <p>Vérifier que le formulaire d'ordre de virement ou la lettre d'ordre est bien renseigné.</p> <p>Vérifier l'authenticité et la régularité de la signature du client portée sur l'ordre.</p> |
| Autorisation de l'ordre de virement             | S'assurer que l'ordre est autorisé par les autorités hiérarchiques bancaires habilitées.                           | <p>Paiement non autorisé</p> <p>Non-respect de la limite autorisée</p> <p>Insuffisance de provision</p> | Perte financière                                     | L'ordre doit être visé par les autorités hiérarchiques habilitées qui vérifient l'existence d'une provision sur le compte.   |
|   |  |   |  |  |

|   |   |   |   |  |
|---|---|---|---|--|
| Saisie des autorisations de virements ou de transferts        | S'assurer de l'enregistrement correct des ordres de virement ou de transfert dans le système  | Erreur dans la saisie du compte à débiter ou à créditer | Perte financière<br>Litige avec le client                         | Visa de l'agent opérations et apposition du cachet transaction vérifiée sur l'ordre                |
| Validation de la saisie de l'ordre par le chef des opérations | S'assurer du contrôle et de la validation des instructions de l'ordre dans le système avant la transmission à la banque intermédiaire | Transmission d'ordre erroné à une banque intermédiaire  | Perte financière<br>Litige entre banques<br>Litige avec le client | L'ordre de virement ou de transfert doit être paraphé par une autorité hiérarchique des opérations |

**Source : nous même**

**Tableau 4 : Identification des risques opérationnels liés à la gestion des effets escomptés**

| Sous-activité  | Objectif de C.I   | Risques encourus  | Conséquence opérationnelle                | Dispositifs de maîtrise   |
|--|---|---|---|---|
| Validation de l'ordre de l'effet par le comité de crédit | S'assurer de l'authenticité de l'instrument de paiement | Règlement d'un ordre de paiement falsifié<br>Usurpation d'identité<br>Client fictif   | Litige avec le client<br>Perte financière | vérifier que tous les signataires ont bien approuvé la demande  |
| Saisie de l'effet dans le système                        | S'assurer de la bonne Saisie de l'effet dans le système | Omission volontaire ou involontaire de données dans le système<br><br>Erreur dans la saisie de compte à créditer ou à débiter | Perte financière<br>Litige entre banques  | vérifier que l'effet comporte toutes les diligences nécessaires avant la saisie.<br><br>Noter la référence de la transaction et apposer son visa sur l'ordre. |
| Validation de la   | S'assurer que la saisie de l'effet                      |   |   | Validation du chef opération des informations dans  |

|   |  |   |  |   |
|---|--|---|--|---|
| saisie par un responsable hiérarchique de l'opération                     | dans le système a été validée par un responsable hiérarchique de l'opération             | Transmission d'ordres erronés                   | Perte financière                                       | le système, et apposer son visa<br><br>Apposer le cachet « escompte » sur les effets et les classer par échéance                                    |
| Intégration dans le Système de tous les effets échus pour la compensation | S'assurer que les effets ont été correctement intégrés, le lendemain, dans le progiciel. | Aucune transmission d'effets aux autres banques | Perte financière<br><br>Litige avec les autres banques | Comparer le nombre des effets physiques à ceux du système corriger les erreurs constatées, en cas de différence<br><br>Envoie des ordres à la BCEAO |
| Aller des effets physiques à la compensation                              | S'assurer que les effets sont prêts pour la compensation                                 | Perte ou vol des effets escomptés               | Perte de ressources<br><br>Litige avec le client       | Faire imprimer le rapport détaillé des valeurs traitées par banques tirées et Procède à un pointage entre ledit état et les valeurs                 |

**Source :** nous même

## 6.2 Evaluation du dispositif de contrôle interne

Cette étape vise à évaluer la qualité des dispositifs mis en place par VERSUS BANK pour maîtriser les risques opérationnels liés à son processus de gestion des moyens de paiement par télé compensation et STAR-UEMOA

Nous allons utiliser nos outils de collecte de donnée et d'information précédemment définis dans la méthodologie de recherche.

### 6.2.1 Test de conformité et de permanence.

Nous avons effectué notre test sur un échantillon d'opérations effectués en notre présence au cours du mois de Mars 2015. Nous avons sélectionnés dix opérations sur les chèques, cinq sur les virements interbancaire, cinq sur les transferts internationaux et cinq sur les effets escomptés.

**Tableau 5 : Test de conformité et de permanence sur les chèques et remises chèques sur confrères**

|           | conformité des références du chèque et le bordereau de remise | chèque correctement endossés | concordance des montants en chiffres et en lettres | Scanning et bonne saisie des références du chèque dans le système de télé compensation « aller » | bonne intégration de l'ordre dans le système | ordre bien reçus par la BCEAO | chèque prêt pour aller à la compense du jour |
|-----------|---|------------------------------|--|--|--|-------------------------------|--|
| N°1       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°2       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°3       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°4       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°5       | Oui   | <b>Non</b>                   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°6       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°7       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°8       | <b>Non</b>  | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°9       | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°10      | Oui   | Oui                          | Oui  | Oui  | Oui  | Oui                           | Oui  |
| Rslte n % | <b>90%</b>  | <b>90%</b>                   | <b>100%</b>  | <b>100%</b>  | <b>100%</b>                                  | <b>100%</b>                   | <b>100%</b>                                  |

**Source : nous même**

**Tableau 6 : Test de conformité et de permanence sur les virements interbancaires**

|           | le formulaire d'ordre de virement ou la lettre d'ordre est bien renseigné | l'authenticité et la régularité de la signature portée sur l'ordre a été vérifié. | Ok des autorités hiérarchiques sur l'ordre de virement ou de transfert | correct enregistrement comptable et auto contrôle Matérialisé par un paraphe | Paraphe du chef opération pour le contrôle de L'écriture comptable | Ordre bien reçu par la BCEAO. | Inscription de la mention MT950 sur l'ordre de transfert |
|-----------|---|---|--|--|--|-------------------------------|--|
| N°1       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°2       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°3       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°4       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°5       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | Oui  |
| N°6       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | X  |
| N°7       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | X  |
| N°8       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | X  |
| N°9       | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | X  |
| N°10      | Oui   | Oui   | Oui  | Oui  | Oui  | Oui                           | X  |
| Rslt en % | <b>100%</b>   | <b>100%</b>   | <b>100%</b>  | <b>100%</b>  | <b>100%</b>  | <b>100%</b>                   | <b>100%</b>  |

**Source : nous même**

**X : Nous n'avons sélectionnés que 5 ordres de Transferts internationaux.**

**Tableau 7 : Test de conformité et de permanence sur les effets escomptés**

|           | Le client à établir une demande d'escompte pour l'effet | Le comité de crédit a bien approuvé la demande | l'effet comporte toutes les diligences nécessaires avant la saisie dans le système. | la référence de la transaction a été notée sur l'ordre et le visa apposé | Validation du chef opération des informations dans le système, et a apposé son visa | Apposition du cachet « escompte » sur l'effet | Envoie des ordres à la BCEAO Lorsque l'effet arrive à échéance. |
|-----------|---|--|---|--|---|---|---|
| N°1       | Oui   | Oui  | Oui   | Oui  | Oui   | Oui   | Oui   |
| N°2       | Oui   | Oui  | Non   | Oui  | Oui   | Oui   | Oui   |
| N°3       | Oui   | Oui  | Oui   | Oui  | Oui   | Oui   | Oui   |
| N°4       | Oui   | Oui  | Non   | Oui  | Oui   | Oui   | Oui   |
| N°5       | Oui   | Oui  | Oui   | Oui  | Oui   | Oui   | Oui   |
| Rslt en % | <b>100%</b>   | <b>100%</b>                                    | <b>100%</b>   | <b>100%</b>  | <b>100%</b>   | <b>100%</b>                                   | <b>100%</b>   |

**Source : nous même**

Ce test a été effectué sur des opérations passées à la banque. Le tableau ci-dessus nous a permis de nous assurer que les procédures concernant les opérations sur les effets sont

bien appliquées et permanente. Nous avons vu qu'un effet ne comportait pas la signature et que sur un autre manquait le timbre que doit apposer le bénéficiaire.

### 6.2.2 Grille de séparation des tâches.

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

**EX : exécution**

**A : autorisation**

**C : contrôle**

**Tableau 8 : grille de séparation des tâches sur les chèques et remises chèques**

| Chèques sur confrères  | Fonctions | Chargé Clientèle | Agent Opérations | Agent compensateur |
|--|-----------|------------------|------------------|--------------------|
| Réception du chèque et du bordereau de remise par le chargé de clientèle | Ex        | X                |                  |                    |
| Vérification des mentions obligatoires                                   | C         | X                | X                |                    |
| Scanning du chèque et du bordereau de remise                             | Ex        | X                | X                |                    |
| Saisie des références du chèque dans le système                          | Ex        |                  | X                |                    |
| Intégration du chèque dans le système                                    | Ex        |                  | X                |                    |
| Envoi des ordres à la BCEAO  | Ex        |                  | X                |                    |
| Aller des Chèques physiques à la compensation                            | Ex        |                  |                  | X                  |

**Source : nous même**

**Tableau 9 : grille de séparation des taches sur virements et transferts émis**

| <b>Virements et transferts émis</b>                              | <b>Fonctions</b> | <b>Chargé Clientèle</b> | <b>Gestionnaire de compte</b> | <b>Middle office</b> | <b>Agent Trésorerie</b> | <b>Agent opérations</b> |
|--|------------------|-------------------------|-------------------------------|----------------------|-------------------------|-------------------------|
| Réception des ordres de virements ou de transferts               | Ex               | X                       |                               |                      |                         |                         |
| Vérification des mentions obligatoires                           | c                | X                       | X                             |                      |                         |                         |
| Donne son accord pour le virement ou le transfert                | A                |                         | X                             |                      |                         |                         |
| Recueille les approbations de ses responsables hiérarchiques     | Ex               |                         |                               | X                    |                         |                         |
| S'assure de la disponibilité des fonds sur le compte de la BCEAO | C                |                         |                               |                      | X                       |                         |
| Vérification du visa des autorités hiérarchiques                 | C                |                         |                               |                      |                         | X                       |

| habilités  |    |  |  |  |  |   |
|--|----|--|--|--|--|---|
| Saisie des autorisations de virements ou de prélèvements | Ex |  |  |  |  | X |
| Intégration dans le système                              | Ex |  |  |  |  | X |

**Source : nous même**

**Tableau 10 : grille de séparation des tâches sur les effets escomptés émis**

| Virements et transferts émis  | Fonctions | Chargé Clientèle | Gestionnaire de compte/Middle office | CAD | Agent opérations | Chef Opérations | Agent compensateur |
|---|-----------|------------------|--------------------------------------|-----|------------------|-----------------|--------------------|
| Réception de l'effet et le bordereau de remise du client                          | Ex        | x                |                                      |     |                  |                 |                    |
| Initiation de l'opération d'escompte par une fiche d'approbation                  | C         |                  | x                                    |     |                  |                 |                    |
| Validation des informations contenues dans le dossier d'escompte                  | A         |                  |                                      | x   |                  |                 |                    |
| Saisie dans le système des effets   | C         |                  |                                      |     | x                |                 |                    |
| Validation des effets dans le système   | C         |                  |                                      |     |                  | x               |                    |
| Faire sortir la veille, les effets échus qui iront à la compensation le lendemain | Ex        |                  |                                      |     | x                |                 |                    |

|  |    |  |  |  |   |  |   |
|--|----|--|--|--|---|--|---|
| S'assurer que les effets ont été correctement intégrés | C  |  |  |  | x |  |   |
| Envoie des effets à la BCEAO                           | EX |  |  |  | x |  |   |
| Aller des effets physiques à la compensation           | EX |  |  |  |   |  | x |

**Source : nous même**

Les fonctions d'exécution, de contrôle et d'autorisation sont bien séparées. Nous pouvons dire que le système de contrôle interne permet d'assurer une bonne séparation des tâches. Cependant dans certains départements qui disposent d'un personnel restreint certaines fonctions soient cumulées.

### 6.2.3 Forces et faiblesses apparentes

**Tableau 11 : forces et faiblesses apparentes sur les chèques sur confrères**

| Opérations   | Objet de contrôle  | Indicateurs   | Risques   | conséquences                              | Test à effectuer  | Observations F/f  | Risques maîtrisés |
|--|--|---|---|---|---|---|-------------------|
| Réception du chèque et du bordereau de remise par le chargé de clientèle | S'assurer de la conformité du chèque et du bordereau de remise   | Réception du chèque et bordereau de remise par le chargé de clientèle           | Erreur sur le montant du chèque ou sur le bordereau de remise                       | Perte financière                          | Sélectionner un échantillon de 10 chèques et vérifier que les mentions sur le chèque et le bordereau concordent | f<br>Tous les chèques sélectionnés et leur bordereaux de remise ne sont pas tous conformes    | non               |
| Réception du chèque et du bordereau de remise par le chargé de clientèle | S'assurer que tous les chèques sont correctement endossés        | L'endos du chèque possède toutes les mentions obligatoires                      | Paiement non autorisé par le client<br><br>Acceptation de chèques volés ou ramassés | Perte financière<br>Litige avec le client | Vérifier que les chèques sont bien endossés   | f<br>Nous avons 2 chèques nombre parmi les chèques sélectionnés qui ne sont pas bien endossés | non               |
| Scanning du tous les chèques et des bordereaux de remise                 | S'assurer que tous les chèques et bordereaux de remise sont bien | Le nombre d'ordres dans le système et le nombre de chèques physiques concordent | Valeur non prise en compte par le système   | Perte financière                          | Vérifier le nombre d'ordres dans le système et le nombre d'ordres physiques                                     | F<br>tous les chèques et bordereaux apparaissent bien dans le système                         | oui               |

Analyse de la gestion des risques opérationnels liés aux moyens de paiement scripturaux par le SICA-UEMOA  
et le STAR-UEMOA : cas de VERSUS BANK

|  |   |                                       |   |   |   |  |     |
|--|---|---------------------------------------|---|---|---|--|-----|
|  | scannés   |                                       |   |   |   |  |     |
| Saisie et intégration des références du chèque dans le système | S'assurer que les références du chèque sont bien saisies et intégré dans le système |                                       | Erreur dans la saisie des chèques<br><br>Erreur de compte lors de la saisie       | Perte financière<br><br>Litige avec le client | Procédé avec l'agent opérations aux pointages des valeurs saisies | F<br>Toutes les références du chèque ont bien saisie dans le système | oui |
| Envoi des ordres à la BCEAO                                    | S'assurer que les ordres sont bien reçus par la BCEAO                               | Le code état doit passer de 050 à 130 | Retard dans la transmission de données<br><br>Transmission de données incorrectes | Perte financière                              | Vérifier dans le système que le code état est passé de 050 à 130  | F<br>Tous les ordres sont bien reçus par la BCEAO                    | oui |

**Source : nous-même**

**Tableau 12 : forces et faiblesses apparentes sur la gestion des virements et Transferts émis**

| Opérations   | Objet de contrôle   | Indicateurs   | Risques   | conséquences                                  | Test effectuer à  | Observations F/f  | Risques maîtrisés |
|--|---|---|---|---|---|---|-------------------|
| Réception des ordres de virement ou transfert émis<br>Par le chargé de clientèle | S'assurer de l'autorisation préalable du client   | L'ordre est bien renseigné par le client                      | Opérations non autorisée par le client  | Perte financière<br><br>Litige avec le client | Sélectionner un échantillon de 5 opérations sur les virements émis et 5 opérations sur les transferts émis vérifié que les formulaires sont bien renseignés | F<br><br>Les ordres de virement ou de transfert sont bien autorisés par le client           | oui               |
| Autorisation de l'ordre par les autorités de la banque                           | S'assurer que l'ordre est autorisé par les autorités bancaires hiérarchiques habilitées | Le ok des autorités bancaires habilitées apparaît sur l'ordre | Paiement non autorisé<br>Non-respect de la limite autorisée<br>Insuffisance de provision pour le client | Perte financière                              | Vérifier que les ordres sont bien visés par les autorités hiérarchiques bancaires habilitées  | F<br>Les ordres comportent tous l'autorisation préalable des autorités bancaires habilitées | oui               |
| Saisie des autorisations de virements ou de transferts                           | S'assurer de la correcte saisie dans le système de l'ordre                              | Le paraphe de l'agent chargé de la saisie                     | Erreur dans la saisie.<br>Erreur de compte à  | Perte financière                              | Vérifier que le paraphe de l'argent chargé de la saisie apparaît bien sur   | F<br>tous les ordres sont bien saisis   | oui               |

Analyse de la gestion des risques opérationnels liés aux moyens de paiement scripturaux par le SICA-UEMOA  
et le STAR-UEMOA : cas de VERSUS BANK

|   |  |   |  |                                     |  |  |     |
|---|--|---|--|-------------------------------------|--|--|-----|
|   | donnée par le client   |   | créditer ou à débiter  |                                     | l'ordre  | dans le système  |     |
| Validation de la saisie de l'ordre par le chef des opérations | S'assurer que la saisie des ordres a été correcte  | Le paraphe du chef des opérations sur l'ordre               | Règlement d'un ordre de paiement falsifié<br>Erreur de compte lors de la saisie                          | Perte financière<br>clients fictifs | Vérifier que le paraphe du chef des opérations apparaît bien sur l'ordre   | f<br>Tous les ordres sont bien saisis dans le système  | oui |
| Envoi des ordres aux structures bancaires intermédiaires      | S'assurer que les ordres sont bien reçus par les structures bancaires intermédiaires pour les virements ou transferts. | Le code état doit passer de 050 à 130<br>Pour les virements | Retard dans la transmission des ordres de transferts ou virements.<br>Transmission de données incorrecte | Perte financière                    | Vérifier que le code état passe de 050 à 130 pour la télécompensation et pour le RTGS aussi que sur le relevé MT950du correspondant le montant du transfert a été débité | F<br>Tous les ordres sont bien reçus<br>Soit par la BCEAO ou par la banque intermédiaire pour le transfert | oui |

**Source : nous même**

**Tableau 13 : forces et faiblesses apparentes sur la gestion des effets escomptés**

| Opérations                                    | Objet de contrôle  | Indicateurs   | Risques   | conséquences                                  | Test à effectuer  | Observations F/f   | Risques maîtrisés               |
|---|--|---|---|---|---|--|---------------------------------|
| Réception de la demande d'escompte du client  | S'assurer que le client à établir une demande d'escompte et vérifier que l'ordre et l'effet sont bien renseignés | L'ordre est bien renseigné par le client et le gestionnaire de compte   | Autorisation non accordée<br><br>Erreur sur la demande ou sur l'effet | Perte financière<br><br>Litige avec le client | Sélectionner un échantillon de 5 dossiers effets escomptés et vérifier qu'ils sont bien renseignés et possède toutes les diligences nécessaires | f<br>Certains ne contiennent pas soit la signature du bénéficiaire ou soit le timbre | Non<br>Insuffisamment maîtrisés |
| Validation de l'effet par le comité de crédit | S'assurer de l'autorisation préalable de tous les membres du comité de crédit pour escompter l'effet             | Le ok de tous les membres du comité de crédit sur le dossier d'escompte | Règlement d'un effet falsifié<br><br>Client fictif                    | Perte financière<br><br>Litige avec le client | vérifier toutes les ordres contient toutes les signatures des membres du comité de crédit   | F<br>Tous les dossiers effets à l'escompte sont validés par le comité de crédit      | oui                             |
| Validation de la saisie de l'ordre            | S'assurer que la saisie des effets a été correcte  | Le paraphe du chef des opérations                                       | Erreur dans la saisie<br>Erreur de compte lors                        | Perte financière<br><br>Litige avec           | Vérifier que le paraphe du chef des opérations  | F<br>La saisie des effets est bien   | oui                             |

|   |   |  |   |   |  |   |     |
|---|---|--|---|---|--|---|-----|
| par le chef des opérations  | avant envoie à la BCEAO   | sur l'ordre  | de la saisie des ordres   | la banque Litige avec le client                                   | apparaît bien sur les effets   | validée dans le système.                                |     |
| Intégration dans le système de tous les effets échus pour la compensation | S'assurer que les effets escomptés sont correctement intégrés, le lendemain dans le système | Le compte du bénéficiaire peut ne pas être impacté par l'opération | Retard dans la réception par le bénéficiaire de l'effet pas de réception de fond pour le bénéficiaire<br><br>Pas de transmission d'ordres | Perte financière<br><br>Litige avec le client et avec les banques | faire imprimer le rapport détaillé des valeurs traitées par banques tirées et procéder à un pointage entre ledit état et les effets physiques. | F<br>Tous les effets sont bien intégrés dans le système | oui |

**Source : nous même**

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

L'étape d'évaluation des dispositifs de contrôle interne et de maîtrise est une étape particulièrement importante dans la démarche d'évaluation des risques opérationnels. En effet c'est par définition des écarts entre le référentiel-cible et les dispositifs existant que seront cotés les systèmes de contrôle interne afin de mettre en place les plans d'actions destinés à sécuriser les processus et diminuer les risques. Notre évaluation sera faite par rapport à la probabilité de survenance et à l'impact des risques identifiés en tenant compte des résultats du test d'existence et de permanence.

#### 6.3.1 Evaluation de la probabilité de survenance

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

**Tableau 14 : échelle de mesure de la probabilité de survenance**

| Niveau | Probabilité | Description |
|--------|-------------|-------------|
|--------|-------------|-------------|

|   |             |   |
|---|-------------|---|
| 5 | Très forte  | Il est presque certain que le risque se réalise   |
| 4 | Forte       | Il ya de forte chance que le risque se réalise    |
| 3 | Moyenne     | Il est possible que le risque se réalise          |
| 2 | Faible      | Il ya peu de chance que le risque se réalise      |
| 1 | Très faible | Il Ya très peu de chance que le risque se réalise |

**Source :** nous même

**Tableau 15 : Tableau d'évaluation de la probabilité de survenance des risques identifiés**

| Risques opérationnels  | Probabilité de survenance |
|--|---------------------------|
| 1) Erreur sur le montant du chèque ou sur le bordereau de remise | 3                         |
| 2) Paiement non autorisé par le client                           | 1                         |
| 3) Acceptation de chèques volés ou ramassé                       | 2                         |
| 4) Valeur non prise en compte par le système                     | 3                         |
| 5) Erreur dans la saisie des chèques                             | 3                         |
| 6) Règlement d'un chèque falsifié                                | 3                         |
| 7) Erreur de compte lors de la saisie des chèques                | 3                         |
| 8) Transmission de données incorrectes                           | 3                         |
| 9) Opérations non autorisées par le client                       | 2                         |
| 10) Paiement non autorisé par la banque                          | 2                         |
| 11) Non-respect de la limite autorisée                           | 2                         |
| 12) Insuffisance de provision pour le client                     | 2                         |
| 13) Erreur de compte à créditer ou à débiter                     | 3                         |

|  |   |
|--|---|
| 14) Retard dans la transmission des données                            | 3 |
| 15) Erreur sur l'ordre ou sur l'effet escompté                         | 2 |
| 16) Opération non autorisée par la banque                              | 3 |
| 17) Défaillance du système informatique                                | 2 |
| 18) Retard dans la réception des fonds par le bénéficiaire de l'effet  | 2 |
| 19) pas de réception de fonds des effets escomptés par le bénéficiaire | 2 |
| 20) Pas de transmission d'ordres d'effets escomptés à la BCEAO         | 1 |

**Source : nous même**

### 6.3.2 Evaluation de l'impact des risques identifiés

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

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

| Niveau | impacts        | Description               |
|--------|----------------|---------------------------|
| 5      | Catastrophique | Conséquences très élevées |
| 4      | Elevé          | Conséquences élevées      |
| 3      | Modéré         | Conséquences Moyennes     |
| 2      | Mineur         | Conséquences Faibles      |

|   |              |                           |
|---|--------------|---------------------------|
| 1 | Insignifiant | Conséquences négligeables |
|---|--------------|---------------------------|

Source : nous même

**Tableau 17 : Evaluation de l'impact des risques identifiés**

| Risques opérationnels  | Impacts |
|--|---------|
| 1) Erreur sur le montant du chèque ou sur le bordereau de remise | 4       |
| 2) Paiement non autorisé par le client                           | 5       |
| 3) Acceptation de chèque volé ou ramassé                         | 5       |
| 4) Valeur non prise en compte par le système                     | 5       |
| 5) Erreur dans la saisie des chèques                             | 4       |
| 6) Règlement d'un chèque falsifié                                | 4       |
| 7) Erreur de compte lors de la saisie des chèques                | 5       |
| 8) Transmission de données incorrecte                            | 5       |
| 9) Opérations non autorisées par le client                       | 4       |
| 10) Paiement non autorisé par la banque                          | 5       |
| 11) Non-respect de la limite autorisée                           | 4       |
| 12) Insuffisance de provision pour le client                     | 3       |

|  |   |
|--|---|
| 13) Erreur de compte à créditer ou à débiter                           | 5 |
| 14) Retard dans la transmission des données                            | 3 |
| 15) Erreur sur l'ordre ou sur l'effet escompté                         | 3 |
| 16) Opération non autorisée par la banque                              | 5 |
| 17) Défaillance du système informatique                                | 5 |
| 18) Retard dans la réception des fonds par le bénéficiaire de l'effet  | 3 |
| 19) pas de réception de fonds des effets escomptés par le bénéficiaire | 5 |
| 20) Pas de transmission d'ordres d'effets escomptés à la BCEAO         | 5 |

**Source : nous même**

## 6.4 Evaluation des risques opérationnels liés aux moyens de paiement

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

### 6.4.1 Tableau de cotation des risques

Criticité = Probabilité de survenance x Impact

**Tableau 18 : Tableau de cotation des risques**

| Risques opérationnels  | Probabilité de survenance | Impact | criticité |
|--|---------------------------|--------|-----------|
| 1) Erreur sur le montant du chèque ou sur le bordereau de remise | 4                         | 4      | 16        |
| 2) Paiement non autorisé par le client                           | 1                         | 5      | 5         |
| 3) Acceptation de chèque volé ou ramassé                         | 2                         | 5      | 10        |
| 4) Valeur non prise en compte par le système                     | 3                         | 5      | 15        |
| 5) Erreur dans la saisie des chèques                             | 3                         | 4      | 12        |
| 6) Règlement d'un chèque falsifié                                | 3                         | 4      | 12        |
| 7) Erreur de compte lors de la saisie des chèques                | 3                         | 5      | 15        |

|   |   |   |    |
|---|---|---|----|
| 8) Transmission de données incorrectes                                | 3 | 5 | 15 |
| 9) Opérations non autorisées par le client                            | 2 | 4 | 8  |
| 10) Paiement non autorisé par la banque                               | 2 | 5 | 10 |
| 11) Non-respect de la limite autorisée                                | 2 | 4 | 8  |
| 12) Insuffisance de provision pour le client                          | 2 | 3 | 6  |
| 13) Erreur de compte à créditer ou à débiter                          | 3 | 5 | 15 |
| 14) Retard dans la transmission des données                           | 3 | 3 | 9  |
| 15) Erreur sur l'ordre ou sur l'effet escompté                        | 2 | 3 | 6  |
| 16) Opération non autorisée par la banque                             | 3 | 5 | 15 |
| 17) Défaillance du système informatique                               | 2 | 5 | 10 |
| 18) Retard dans la réception des fonds par le bénéficiaire de l'effet | 2 | 3 | 6  |
| 19) pas de réception de fond des effets escomptés par le bénéficiaire | 2 | 5 | 10 |
| 20) Pas de transmission d'ordres d'effets à la BCEAO                  | 1 | 5 | 5  |

**Source :** nous même

#### 6.4.2 Hiérarchisation des risques opérationnels selon leur criticité

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

**Tableau 19 : Tableau de Hiérarchisation des risques**

| Risques opérationnels  | Probabilité de survenance | Impact | criticité |
|--|---------------------------|--------|-----------|
| 1) Erreur sur le montant du chèque ou sur le bordereau de remise | 4                         | 4      | 16        |
| 5) Erreur dans la saisie du chèque                               | 3                         | 5      | 15        |
| 7) Erreur de compte lors de la saisie du chèque                  | 3                         | 5      | 15        |
| 8) Transmission de données incorrectes                           | 3                         | 5      | 15        |
| 13) Erreur de compte à créditer ou à débiter                     | 3                         | 5      | 15        |
| 16) Opération non autorisée par la banque                        | 3                         | 5      | 15        |
| 4) Valeur non prise en compte par le système                     | 3                         | 5      | 15        |
| 6) Règlement d'un chèque falsifié                                | 3                         | 4      | 12        |
| 10) Paiement non autorisé par la banque                          | 2                         | 5      | 10        |
| 3) Acceptation de chèque volé ou ramassé                         | 2                         | 5      | 10        |

|  |   |   |    |
|--|---|---|----|
| 17) Défaillance du système informatique                                | 2 | 5 | 10 |
| 19) pas de réception de fonds des effets escomptés par le bénéficiaire | 2 | 5 | 10 |
| 14) Retard dans la transmission des données                            | 3 | 3 | 9  |
| 9) Opérations non autorisées par le client                             | 2 | 4 | 8  |
| 11) Non-respect de la limite autorisée                                 | 2 | 4 | 8  |
| 12) Insuffisance de provision pour le client                           | 2 | 3 | 6  |
| 15) Erreur sur l'ordre ou sur l'effet escompté                         | 2 | 3 | 6  |
| 18) Retard dans la réception des fonds par le bénéficiaire de l'effet  | 2 | 3 | 6  |
| 2) Paiement non autorisé par le client                                 | 1 | 5 | 5  |
| 20) Pas de transmission d'ordres d'effets à la BCEAO                   | 1 | 5 | 5  |

**Source : nous même**

### 6.4.3 La matrice des risques opérationnels

**Figure 2 : Matrice des risques**

|                       |  |  |  |  |  |
|-----------------------|--|--|--|--|--|
| <i>catastrophique</i> | 2) Paiement non autorisé par le client<br>20) Pas de transmission d'ordres d'effets à la BCEAO | 10) Paiement non autorisé par la banque<br>3) Acceptation de chèque volé ou ramassé<br>17) Défaillance du système informatique<br>19) pas de réception de fonds des effets escomptés par le bénéficiaire | 5) Erreur dans la saisie du chèque<br>7) Erreur de compte lors de la saisie du chèque<br>8) Transmission de données incorrectes<br>13) Erreur de compte à créditer ou à débiter<br>16) Opération non autorisée par la banque<br>4) Valeurs non prise en compte par le système<br>16) Opération non autorisée par la banque |  |  |
| <i>élevé</i>          |  | 9) Opérations non autorisées par le client<br>11) Non-respect de la limite autorisée   | 6) Règlement d'un chèque falsifié  | 1) Erreur sur le montant du chèque ou sur le bordereau de remise |  |

|                     |                    |   |   |              |                   |
|---------------------|--------------------|---|---|--------------|-------------------|
| <i>Modéré</i>       |                    | 12) Insuffisance de provision pour le client<br>15) Erreur sur l'ordre ou sur l'effet escompté<br>18) Retard dans la réception des fonds par le bénéficiaire de l'effet | 14) Retard dans la transmission des données |              |                   |
| <i>Mineur</i>       |                    |   |   |              |                   |
| <i>Insignifiant</i> |                    |   |   |              |                   |
|                     | <i>Très faible</i> | <i>Faible</i>   | <i>Moyenne</i>                              | <i>Forte</i> | <i>Très forte</i> |



|        |        |        |        |        |
|--------|--------|--------|--------|--------|
| ZONE 1 | ZONE 2 | ZONE 3 | ZONE 4 | ZONE 5 |
|--------|--------|--------|--------|--------|

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

**Tableau 20 : Synthèse du dispositif de contrôle interne**

|                                   | <b>Dispositif de contrôle interne</b>  | <b>Constat</b>                                     |
|-----------------------------------|--|--|
| Traitement des moyens de paiement | <ul style="list-style-type: none"> <li>- Procédure de traitement des chèques sur confrères</li> <li>- procédure de traitement des virements extérieurs et transferts</li> <li>- Procédure de traitement des effets escomptés</li> <li>- Procédure de traitement de la télé compensation</li> </ul> | <p>Oui</p> <p>Oui</p> <p>Oui</p> <p>Oui</p>        |
| Définition des habilitations      | <ul style="list-style-type: none"> <li>- Vérification du traitement des opérations</li> <li>- Procédure de contrôle des opérations</li> <li>- Séparation des tâches</li> <li>- Respect total du manuel de procédure</li> </ul>   | <p>Oui</p> <p>Oui</p> <p>Oui</p> <p><b>Non</b></p> |
| Limitations des accès             | <ul style="list-style-type: none"> <li>- Procédure de limitation de l'accès aux moyens de paiement</li> <li>- Procédure de limitation de l'accès aux comptes des clients</li> <li>- Respect total du manuel de procédure</li> </ul>  | <p>Oui</p> <p>Oui</p> <p>Oui</p>                   |

|   |  |  |
|---|--|--|
| Surveillance des conditions de conservation | - Procédure de surveillance par une personne habilitée<br>- Procédure d'endossement des valeurs  | Oui<br>Oui                             |
| Contrôle des risques                        | - Service de gestion des risques opérationnels<br>- Surveillance permanente des risques opérationnels<br>- Suivi périodique des risques opérationnels<br>- Service d'audit interne | <b>Non</b><br>Oui<br>Oui<br><b>Non</b> |
| Contrôle de la Sécurité des actifs          | - Procédure de rapprochement<br>- Procédure de contrôle<br>- Procédure d'information<br>- Respect des procédures   | Oui<br>Oui<br>Oui<br>Oui               |

**Source : nous même**

Certaines tâches dans le traitement des chèques et remises chèques sur confrères ne sont pas souvent appliquées par tous les acteurs désignés à cet effet dans le manuel de procédure.

Le dispositif de contrôle interne joue un rôle clé dans la conduite et pilotage de ses différentes activités. Toutefois, le contrôle interne ne peut pas fournir une garantie absolue que les objectifs de la banque seront atteints, aussi bien conçu et appliqués soit-il.

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

Au terme de notre analyse, nous pouvons dire que le dispositif de maîtrise des risques opérationnels liés aux moyens de paiement de VERSUS BANK présente quelques petites insuffisances quant à sa mise en œuvre. Ainsi nous allons faire des recommandations qui dans le but de réduire encore plus les risques opérationnels dans le processus des moyens de paiement.

## 6.5 Analyse et recommandations

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

### 6.5.1 Analyse de la matrice des risques opérationnels liés aux moyens de paiement

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

- La première zone ou zone I est la plus critique car elle regroupe les risques qui ont une forte probabilité de survenance et des conséquences catastrophiques sur la banque. Ce sont les risques à éviter à tout prix et pour lesquels il faut des actions immédiates. Et une surveillance permanente à travers un dispositif de maîtrise adapté.
- Les zones 2 et 3 ont un niveau de risques moins élevés car elles sont constituées des risques dont la probabilité de survenance et l'impact sur les affaires de l'organisation sont moyennes. Ce sont des risques pour lesquels un suivi, de manière périodique, constituerait un gage de leur maîtrise.
- Les zones 4 et 5 ne contiennent pas de risques majeurs

### 6.5.2 Recommandations

Après avoir menés tous les travaux nécessaires pour l'analyse des risques opérationnels liés à la gestion des moyens de paiement scripturaux traités via le SICA-UEMOA et STAR-UEMOA à VERSUS BANK, nous avons formulé les recommandations suivantes qui sont adressées aux différents acteurs de la banque pour une amélioration des dispositifs de maîtrise des différents risques opérationnels liés à ce processus.

- **A la direction générale :**

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

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

- La création d'un service d'audit interne dont le rôle serait de développer les procédures adéquates pour détecter et gérer le risque opérationnel dans toutes les activités de la banque serait très judicieuse ;
- L'instauration au sein de la banque d'une culture qui souligne et démontre à tous les niveaux du personnel, l'importance des contrôles internes. Tous les niveaux du personnel de l'organisation doivent comprendre leur rôle dans le contrôle interne et s'impliquer activement dans ce processus ;
- Améliorer la politique de communication.

- **A la direction des opérations :**

- Une bonne maîtrise des risques passe par une bonne application des procédures mises en place. La direction des opérations doit alors prendre des mesures nécessaires pour une application des procédures par le personnel.
- L'exhaustivité dans le traitement de toutes les demandes de paiements et dans le traitement des ordres à la compensation aller

- **Aux chefs d'agences**

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

Ils pourraient s'assurer que les agents sous sa direction suivent correctement les procédures concernant les chèques et remises chèques, les ordres de virement et de transferts.

## **Conclusion de la deuxième partie**

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

Notre étude pourrait être utile à VERSUS BANK dans la mesure où elle constitue une synthèse de quelques difficultés rencontrées dans le processus de gestion des moyens de paiement par le SICA- UEMOA et STAR-UEMOA. Ainsi donc dans le but de réduire les risques opérationnels liés à ces processus nous avons formulé des recommandations pour renforcer le dispositif de contrôle interne existant.

## CONCLUSION GENERALE

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

Au cours de nos travaux nous avons rencontré quelques difficultés, parmi lesquelles les difficultés d'évaluation des risques, le fait que les opérations sur les moyens de paiement soient trop volumineuses, La difficulté de pouvoir collecter toutes les données

du faites de la confidentialité et de la grande importance de certaines données. Nous avons donc dû opérer des choix grâce à la revue de littérature pour aboutir à un modèle d'analyse dans la première partie et sa mise en œuvre effective dans la deuxième partie de notre étude.

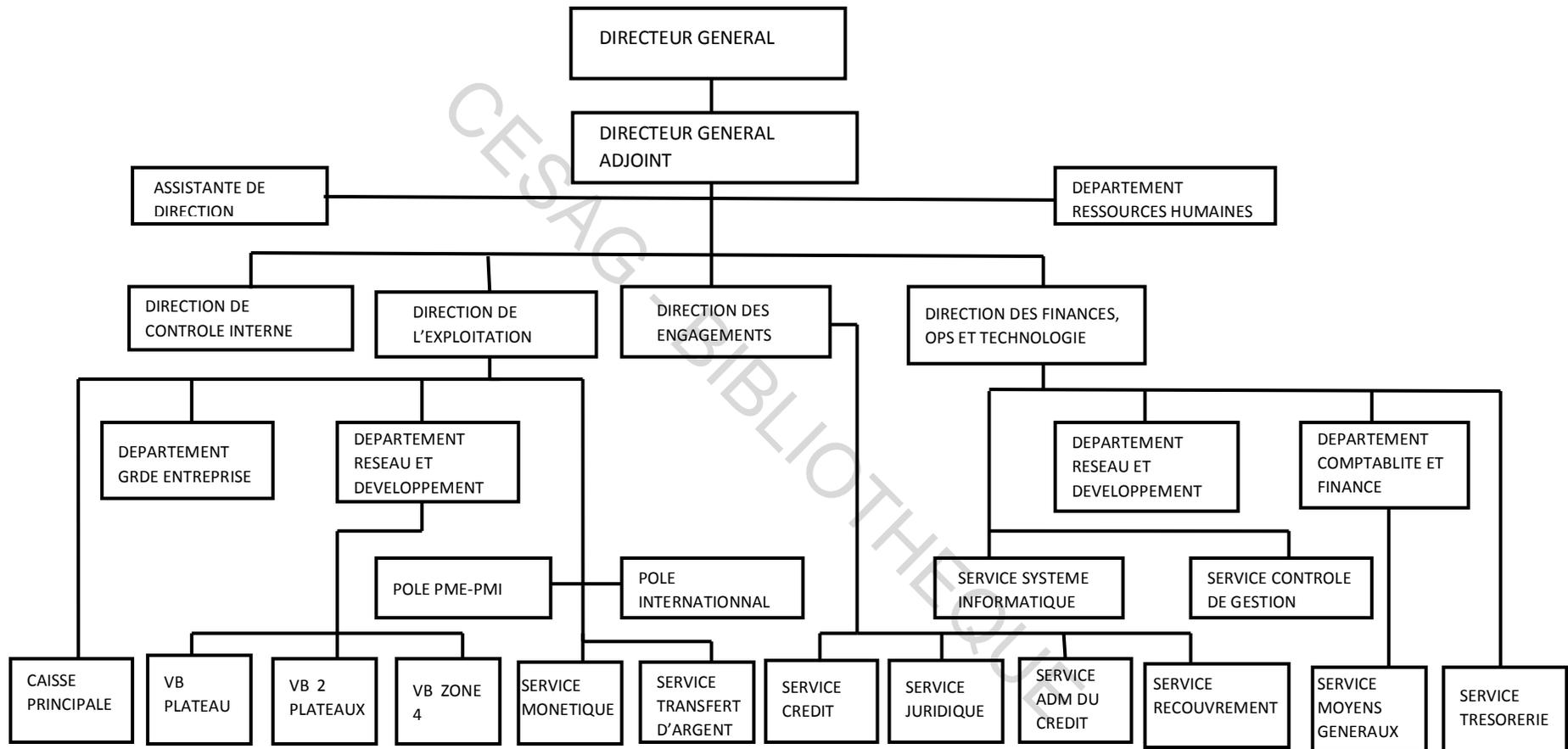
Cette analyse nous a permis de montrer comment les risques opérationnels liés à ce processus sont gérés, mais aussi de déceler les forces et les faiblesses du système de contrôle interne. Au bout de notre analyse, nous avons formulé des recommandations. Cependant comme toute œuvre humaine présente des insuffisances, il appartient aux dirigeants de la banque de prendre les dispositions nécessaires pour enrichir notre étude. L'idéal pour nous serait de contribuer un tant soit peu à la gestion efficace des risques opérationnels liés aux moyens de paiement scripturaux traités via le système de télé compensation et le STAR- UEMOA.

CESAG - BIBLIOTHEQUE

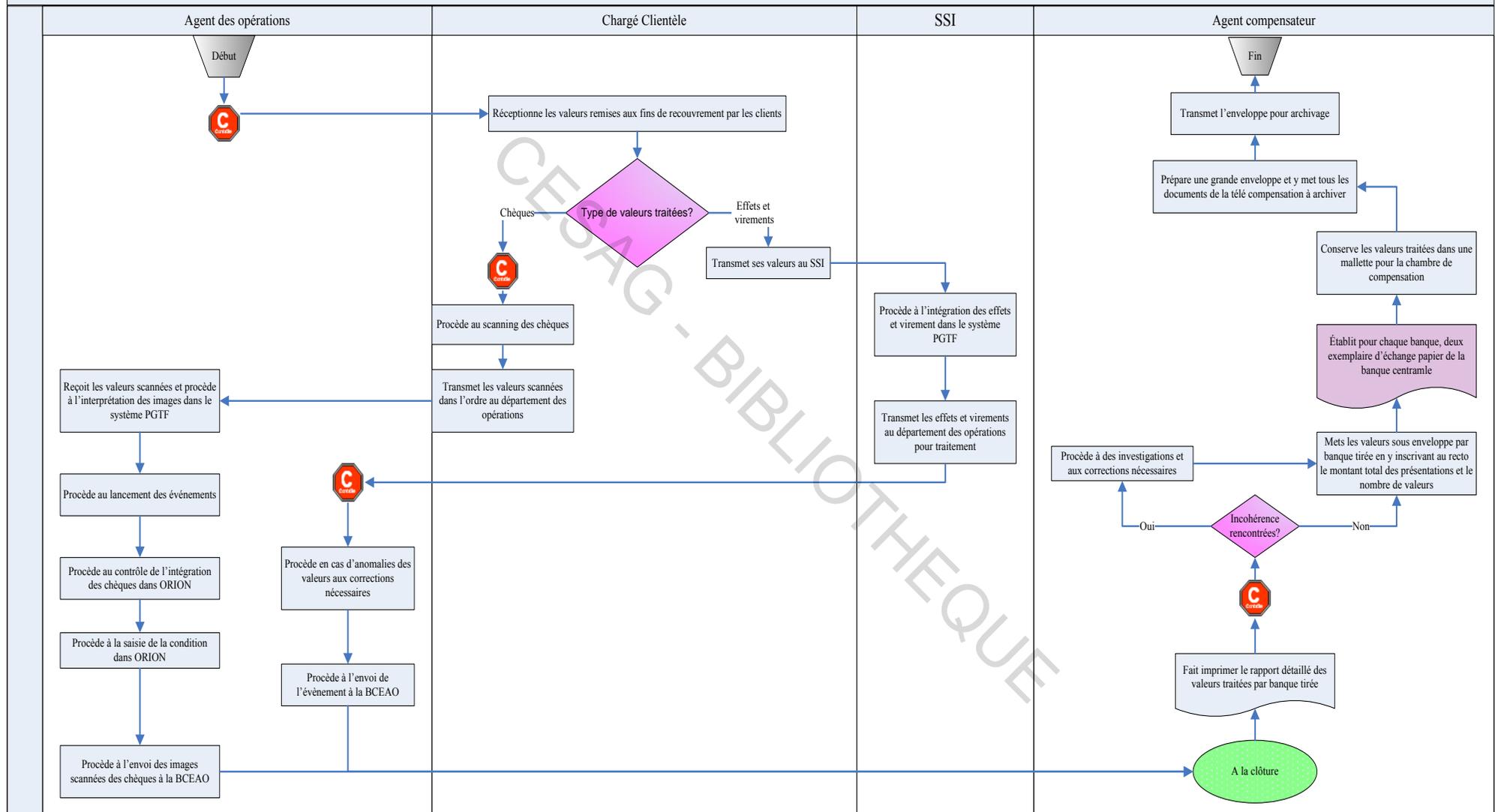
ANNEXES

CESAG - BIBLIOTHEQUE

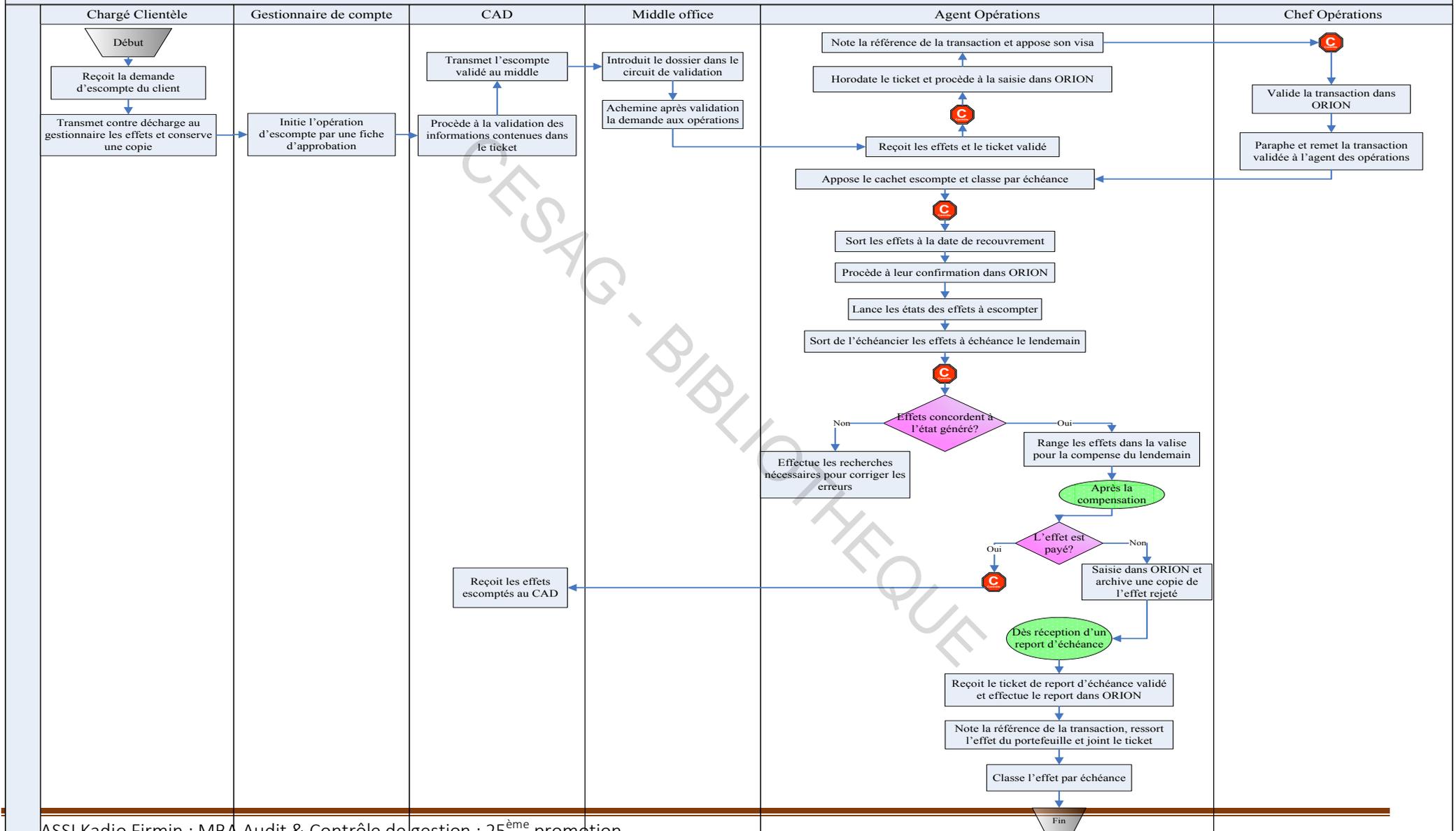
Annexe 1 : Organigramme VERSUS BANK



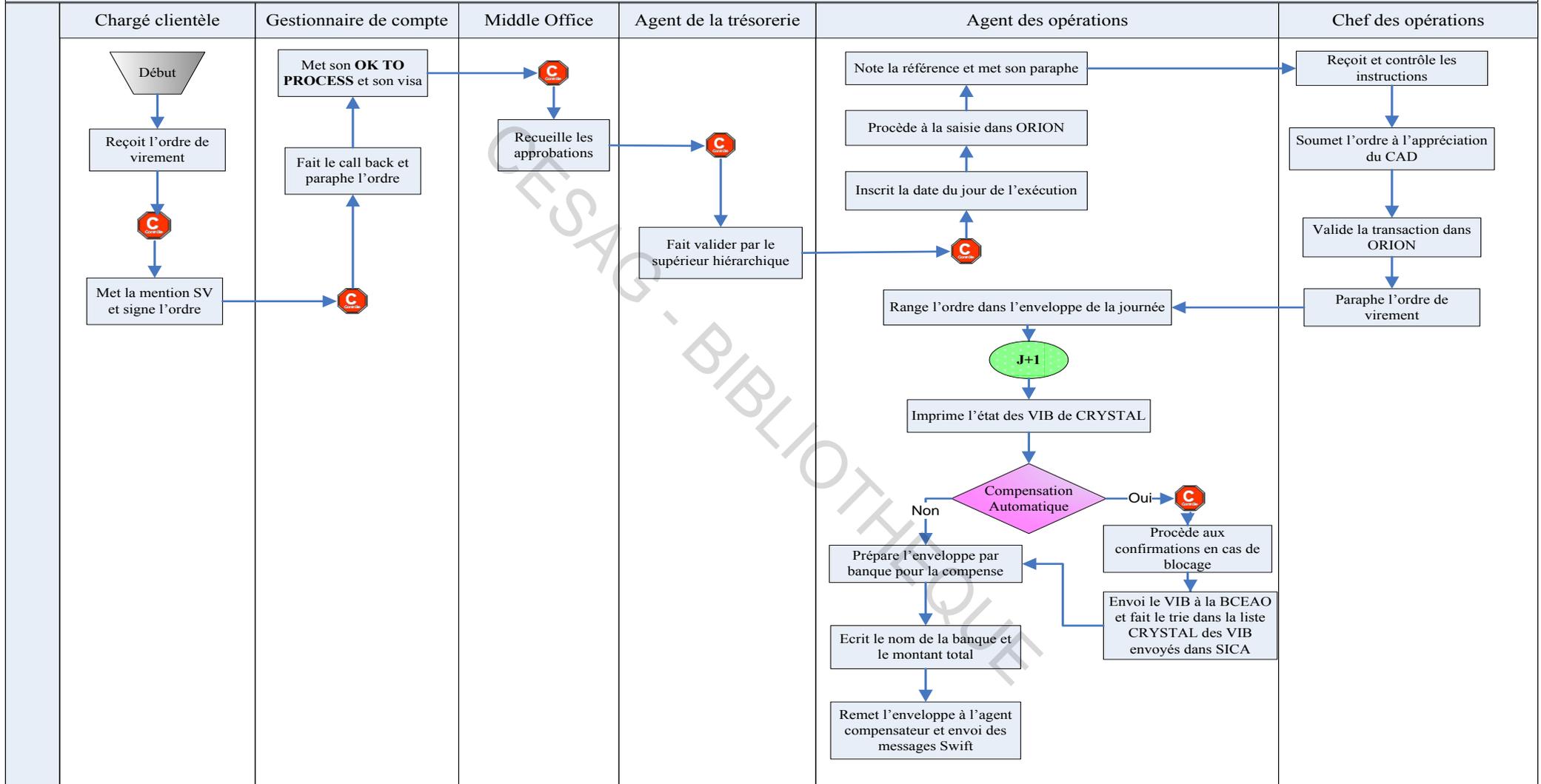
2. LOGIGRAMME DU PROCESSUS DE TRAITEMENT DES TELE COMPENSATIONS ALLER



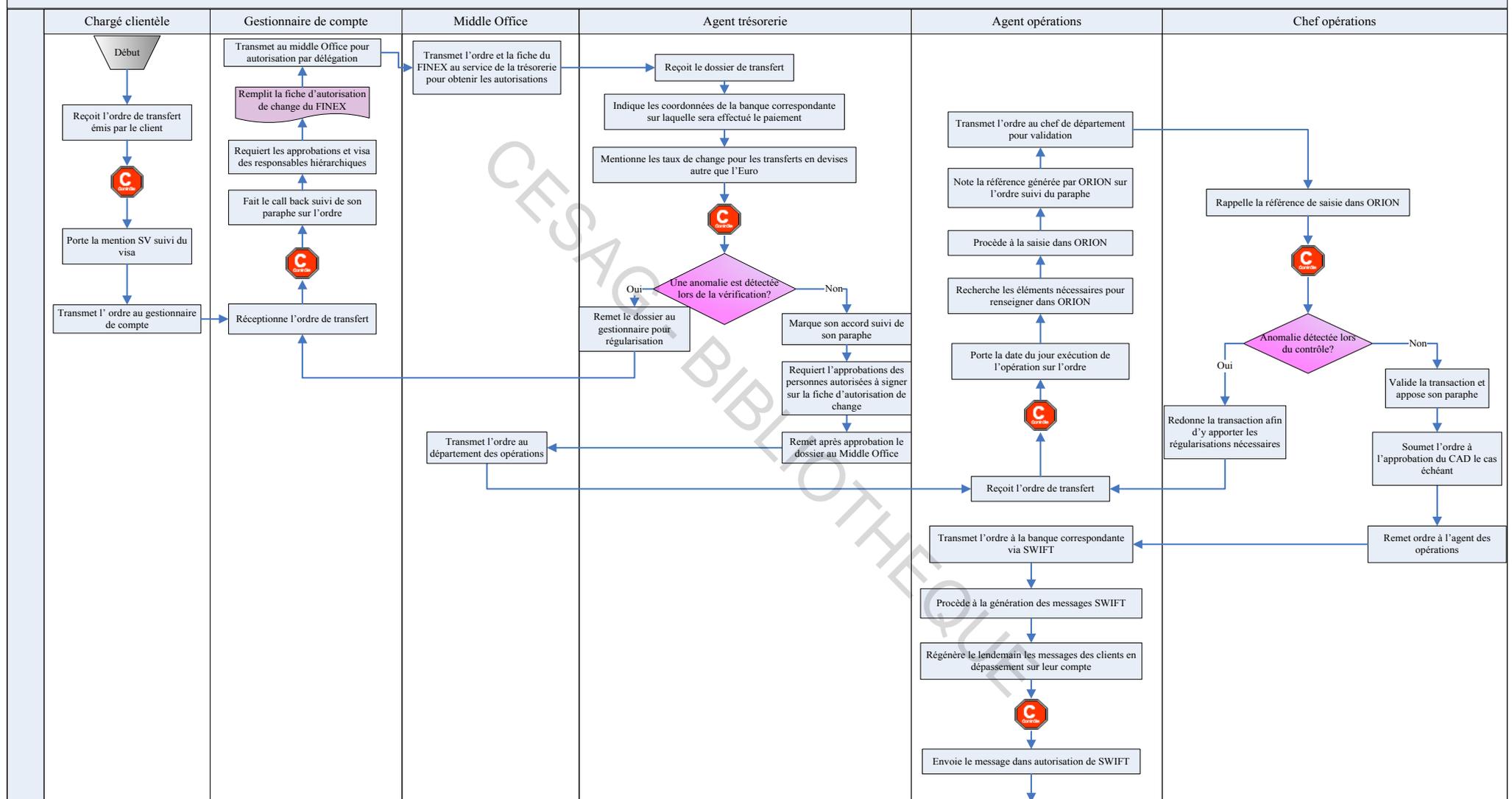
2. LOGIGRAMME DU PROCESSUS DE TRAITEMENT DES EFFETS A L'ESCOMPTE



## 2. LOGIGRAMME DU PROCESSUS DE TRAITEMENT DES VIREMENTS INTERBANCAIRES (VIB)



2. LOGIGRAMME DU PROCESSUS DE TRAITEMENT DES TRANSFERTS EMIS



### Symbole

|   |                                  |  |                       |
|---|----------------------------------|--|-----------------------|
|  | Contrôle à effectuer             |   | Début ou Fin          |
|  | Tâche                            |  | Document produit      |
|  | Liaison entre tâche et une autre |   | Vérification au choix |
|  | Moment de la procédure           |  |                       |

## BIBLIOGRAPHIE ET WEBOGRAPHIE

CESAG - BIBLIOTHEQUE

## BIBLIOGRAPHIE

1. ANDRIES MARC & CARLOS MARTIN (2004), *la surveillance des moyens de paiement scripturaux : objectifs et modalités de mise en œuvre*, Banque de France, Revue de la stabilité financière N°5, Novembre, P.92
2. BARTHELEMY Bernard & COURREGES Philippe (2004), *Gestion des risques, Méthode d'optimisation globale*, Edition d'organisation 2ème édition, Paris, P. 33
3. BERTIN Elisabeth (2007), *Audit interne : enjeux et pratiques à l'international*, EYROLLES, P. 96
4. CHELLY Dan, MERLIER Patrick, JIMENEZ Christian (2008), *Risques opérationnels : la mise en place du dispositif à son audit*, Revue Banque, P. 271
5. COOPERS et LYBRAND (2000), *la nouvelle pratique du contrôle interne, 5ème tirage*, Editions d'organisation, Paris P. 378
6. DESMITCH François (2007), *la pratique de l'activité bancaire*, 2e édition Dunod, Paris P354
7. Frédéric MISHKIN (2010), *Monnaie banque et Marchés financiers*, 9ème édition, Pearson éducation, Paris, P. 439
8. GREUNING Van Henri & al (2004), *analyse et gestion du risque bancaire : un cadre de référence pour l'évaluation de la gouvernance d'entreprise et du risque*, éditions ESKA, P 386
9. Hennie Van GREUNING & Sonja BRAJOVICBRATANOVIC(2004), *analyse de la gestion du risque bancaire* P.120
10. KAUFFMAN Pascal (2008), *l'union monétaire européenne*, Presse universitaire de bordeaux Pesac, P. 124

11. LEMANT Olivier (1995), *la conduite d'une mission d'audit interne*, DUNOD, P.181-203
12. Manuel de Procédures Opérationnelles de VERSUS BANK
13. NICOLET Marie-Agnès (2000), Risques opérationnels : de la définition à la gestion, banque magazine n°615 P. 44
14. OGIEN Dov (2008), comptabilité et audit bancaire, 2e édition, DUNOD, P. 466-467
15. PricewaterhouseCoopers (2005), *la pratique du contrôle interne*, Edition d'organisation, P. 32-33
16. RENARD Jacques (2010), *Théorie et pratique de l'audit interne*, 7ième édition, groupe Eyrolles P.469
17. RENARD Jacques (2010), *Théorie et pratique de l'audit interne*, 7ième édition, groupe Eyrolles P.469
18. SARDI Antoine (2002), *Pratique de la comptabilité bancaire*, Edition AFGES Paris, P. 315
19. SARDI Antoine (2005), *Audit et contrôle interne bancaires*, Edition AFGES Paris, P. 405
20. SIRUGUET Jean Luc (2001), *le contrôle comptable bancaire tome II, pratique du contrôle comptable des opérations de banques classiques*, revue banque, éditeur 18, Rue la Fayette, Paris, P. 460-362
21. VALLET Elisabeth (2003), *les correspondants du trésor*, Edition l'Harmattan, 5-7, rue de l'école-polytechnique, 75005 Paris, France, P.31

## SITE INTERNET

IFACI (2009), Normes professionnelle de l'Audit interne

[http://www.journaldunet.com/solutions/0403/040319\\_chro\\_bpms.shtml](http://www.journaldunet.com/solutions/0403/040319_chro_bpms.shtml)

BCEAO (2015), Système interbancaire de compensation automatisée

<http://www.bceao.int/SICA-UEMOA.html>.

## BIBLIOTHEQUE CESAG

[bibliotheque.cesag.sn/](http://bibliotheque.cesag.sn/) consulté le 08 février 2015

WIKIPEDIA (Mars 2008), le risque opérationnel (établissement financier)

[http://fr.wikipedia.org/wiki/Risque\\_op%C3%A9rationnel\\_\(%C3%A9tablissement  
financier\)](http://fr.wikipedia.org/wiki/Risque_op%C3%A9rationnel_(%C3%A9tablissement_financier)) consulté le 03 mars 2015

PIRUS Jean-Luc (2004), l'analyse des risques opérationnels : un enjeu qui dépasse le  
secteur bancaire

[http://www.journaldunet.com/solutions/0403/040319\\_chro\\_bpms.shtml](http://www.journaldunet.com/solutions/0403/040319_chro_bpms.shtml)