CENTRE AFRICAIN D'ETUDES SUPERIEURES
EN GESTION
MASTER EN BANQUE ET FINANCE

CESAG

OPTION GESTION BANCAIRE ET MAITRISE DES RISQUES
ANNEE ACADEMIQUE 2004-2005

MEMOIRE DE FIN DE CYCLE

MBF
MBA in Banking and Finance
Mastère en Banque et Finance
CESAG

CONTROLE INTERNE ET MAITRISE DES RISQUES OPERATIONNELS DANS UNE BANQUE COMMERCIALE : LE CAS D'ECOBANK COTE D'IVOIRE

ECOBANK

STAGIAIRE :
HERMANN
BOSSE
MBF 4

DIRECTEUR DE MEMOIRE :
CAMARA LUCIEN
MAITRE DE CONFERENCE ITB

Remerciements

A mes Parents qui ont permis que tout soit possible,

Aux formateurs et à l'équipe du master en banque et Finance

A mon Directeur de Mémoire pour sa disponibilité

A M Djabia Edgard et à tous mes collègues d'Ecobank Côte d'Ivoire

Acronymes

A.M.F : Autorité des marchés financiers

A.M.A. : Advanced Measurement Approach

B.I.A. : Basic Indicator Approach

C.O.S.O. : Committee of Sponsoring Organization of The Treadway Commission

E.R.P. : Enterprise Resource Planning

I.I.A. : Institute of Internal Auditors

P.N.B. : Produit Net Bancaire

SYSCOA : Système Comptable Ouest Africain

U.E.M.O.A. : Union Economique et Monétaire Ouest Africaine

TABLE DES MATIERES

INTRODUCTION GENERALE 6

PREMIERE PARTIE : CONTROLE INTERNE ET RISQUE OPERATIONNEL DANS LA BANQUE

CHAPITRE I : DEFINITION DES CONCEPTS 11

A : LE CONTROLE INTERNE DES ETABLISSEMENTS DE CREDIT 11
I : AMELIORATION DU CONTROLE PAR L'AUDIT INTERNE 13

B : LE RISQUE OPERATIONNEL 14
I : TYPOLOGIE DES RISQUES OPERATIONNELS 14
I.1 Définition des Risques Opérationnels 14
I.2 Facteurs de risques 16

CHAPITRE II : EVALUATION DU RISQUE OPERATIONNEL 23

A : METHODES D'EVALUATION 23
I : LE TOP DOWN 23
II : LE BOTTOM UP 23
III : LE RAM 24

B : EXIGENCES REGLEMENTAIRES 25
I : L'INDICATEUR DE BASE 25
II L'APPROCHE STANDARD 26
III LA METHODE DES MESURES AVANCEES 26

DEUXIEME PARTIE : LA MAITRISE DU RISQUE OPERATIONNEL DANS L'ORGANISATION ET LES ACTIVITES DE ECOBANK COTE D'IVOIRE

CHAPITRE I : PRESENTATION GENERALE DE ECOBANK COTE D'IVOIRE (ECI) 29

A : HISTORIQUE DE ECOBANK 29

B : ORGANISATION GENERALE ET FONCTIONNEMENT DE LA BANQUE 30

CHAPITRE II : IMPACT DU SUIVI DES RISQUES OPERATIONNELS SUR L'ORGANISATION ET LES METHODES 36

A : LA REVUE PERIODIQUE DES PROCEDURES PAR L'AUDIT INTERNE 36

B : LE RAPPROCHEMENT ET LA JUSTIFICATION DES COMPTES 38
I : FORCES CONSTATEES 41
I.1 Suivi Des Comptes Internes 41
I.2 Constitution d'une Base de Données Fiable 42
I.3 Détection et Régularisation des Dysfonctionnements et des Erreurs 43

C : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DE CREDIT 43

D : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DE DEPOT 44

E : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DES MOYENS DE PAIEMENT 45

F : LA PREVENTION ET LA COUVERTURE DU RISQUE INFORMATIQUE 45
I : LES NORMES DE SECURITE DU SYSTEME D'INFORMATION 45
II LE PLAN DE CONTINGENCE INFORMATIQUE 47

D : LE REPORTING 49

CHAPITRE III : RECOMMANDATIONS ET PERSPECTIVES 54

CONCLUSION 56

INTRODUCTION GENERALE

Le présent mémoire vise à mettre en relief la nature du contrôle interne et le rôle de celui-ci dans la maîtrise du risque opérationnel des banques.

Qu'est ce que le risque opérationnel ? Comment se manifeste t il ? Peut ont le prévenir ou le maîtriser ?

Il s'agit pour nous d'attirer l'attention sur la nature et l'importance des risques opérationnels puis de faire l'état des lieux, c'est-à-dire rappeler les exigences présentes et à venir des autorités de contrôle en la matière et le mode de gestion de ceux-ci dans notre structure d'accueil. S'appuyant sur le fait qu'un risque ne peut être maîtrisé que s'il est correctement identifié puis évalué, nous nous proposons donc de passer en revue et d'évaluer ses composantes.

Pour le recueil des données et informations, nous avons procédé par des entretiens, l'analyse des documents internes de la structure (Procédures, manuels, notes de service et d'instruction) et la revue de la littérature sur le sujet.

Intermédiaire entre les agents économiques à capacité de financement et ceux à besoin de financement, la banque est un lieu ou subsistent de nombreux risques, inhérents à son activité. Ces risques sont de divers ordres et leur maîtrise conditionne la pérennité de l'entreprise bancaire.

Les risques majeurs de l'activité bancaire sont les suivants :

- Le risque de contrepartie
- Le risque de marché (taux, change, règlement)
- Le risque opérationnel
- Le risque de liquidité
- Le risque de taux
- Le risque systémique

Les risques de crédit et de marché peuvent être évalués par des outils bien connus et maîtrisés (notation du crédit, notation de la contrepartie), le risque opérationnel par contre fait rarement l'objet d'un recensement et d'une évaluation.

Les risques opérationnels peuvent être définis sous deux angles, une définition par défaut et une définition positive plus récente.

Dans le premier cas, on les considère comme étant tous les risques non compris comme étant ceux de crédit ou de marché. Ces derniers sont couverts à priori par la mise en place d'une série de critères pour discriminer la contrepartie, l'utilisation de techniques financières (couverture à terme), la prise de garanties et à posteriori par la réalisation des dites garanties, le monitoring d'indicateurs, la collecte et l'exploitation d'informations sur l'économie etc.... .

Le dispositif de gestion des risques de crédit et de marché, résulte de l'expérience acquise et de l'existence et de la disponibilité d'informations historiques pouvant permettre la prise de décision.

Contrairement à la première catégorie, les risques opérationnels, qui n'étaient pas suivis distinctement, n'ont pas fait l'objet de collecte de données suffisamment longue pour affiner le dispositif les éludant. Le challenge est donc entier et consiste à construire les systèmes d'information, en déterminant la nature, la source et enfin la forme qu'ils doivent avoir.

Dans le second cas : les risques opérationnels sont définis comme étant « des risques de pertes directes ou indirectes résultant d'une inadéquation ou d'une défaillance attribuable aux procédures, au facteur humain et aux systèmes, ou à des causes externes». Cette définition issue des réflexions du comité de Bâle sur la réforme du ratio Cook, dans le second document consultatif publié en janvier 2001[1], permet d'uniformiser les conceptions parfois variables que les différents protagonistes se faisaient de cette acception. Dans cette définition, sont inclus

[1] Revue banque magazine n°624 Avril 2001. p82

les risques juridiques et informatiques.

L'une des difficultés majeures de l'appréciation des risques opérationnels est la quantification de leur impact. En effet, quand la perte maximale subie avec le risque de crédit est l'encours à la date de réalisation du risque, celle concernant le risque opérationnel est plus difficile à prévoir, parce que les conséquences sont indirectes et se soldent par une perte plus étendue.

Comment le contrôle Interne d'ECOBANK Côte d'Ivoire peut il permettre de maîtriser le risque opérationnel ? C'est à cette question que nous nous emploierons à répondre au terme de notre exposé.

Dans la perspective d'une évolution de la réglementation vers l'application de différentes approches de mesure des risques opérationnels, chaque établissement bancaire devra être capable d'opter pour le mode d'évaluation le plus adapté à ses besoins. Parmi les méthodes préconisées, celle des mesures avancées ; Advanced Measurement Approach (AMA) impose de disposer de données historiques susceptibles d'être validées par les autorités de contrôle. Des modèles internes doivent être construits afin que la collecte de données permette de proposer une évaluation dont la fiabilité va dépendre de la méthode de collecte des données et des éléments à prendre en compte dans la conception de ces bases de données.
L'importance de l'analyse des risques opérationnels vient du fait que pour la structure, ceux-ci représentent une part significative dans les pertes totales.

L'introduction récente sur trois places boursières du groupe Ecobank, lui impose d'adopter les meilleurs standards internationaux en matière de gestion des risques bancaires.
De plus, c'est un risque transversal, qui est diffus à tous les niveaux de

l'organisation, qui est mal maîtrisé et qui fait l'objet de la littérature la moins abondante.

Le risque opérationnel comme on peut le constater n'est pas nouveau en soi, mais son importance grandissante dans le profil de pertes des établissements bancaires à entraîné une évolution de la réglementation bancaire qui lui donne une importance nouvelle à travers le ratio Mac Donough (Bâle II).

La suite de notre exposé s'articulera comme suit :
Dans une première partie, nous passerons en revue les concepts à travers la rubrique « contrôle interne et risque opérationnel dans la banque », puis dans la seconde, nous allons aborder la gestion proprement dite de ce risque opérationnel dans la structure d'accueil.

PREMIERE PARTIE : CONTROLE INTERNE ET RISQUE OPERATIONNEL DANS LA BANQUE

CHAPITRE I : DEFINITION DES CONCEPTS

La maitrise des risques en général et des risques opérationnels en particulier impose l'utilisation d'un outil performant qu'est le contrôle interne . Ce concept est défini dans ce chapitre, avant d'aborder son utilisation par l'audit interne. Un large aperçu des risques opérationnels est ensuite donné dans une seconde partie du chapitre.

A : LE CONTROLE INTERNE DES ETABLISSEMENTS DE CREDIT

Le contrôle interne est il un dispositif, une entité ou un état, plusieurs définitions ont été élaborées sur le sujet.

Selon l'OECCC en France, «Le Contrôle Interne est l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. Il a pour but d'assurer d'un coté, la protection, la sauvegarde du patrimoine et la qualité de l'information et de l'autre l'application des instructions de la Direction en favorisant l'amélioration des performances. Il se manifeste par l'organisation, les méthodes et les procédures de chacune des activités de l'entreprise, pour maintenir la pérennité de celle-ci »

Celle du groupe de place mandaté par l'AMF introduit la responsabilité en matière de contrôle interne, en stipulant que,

« Le contrôle interne est un dispositif de la société, défini et mis en œuvre sous sa responsabilité. Il comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques propres de chaque société qui contribue à la maîtrise de ses activités, à l'efficacité de ses opérations et à l'utilisation efficiente de ses ressources, et doit lui permettre de prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité[2]» .Suite aux différents scandales et aux crises financières survenues ces dernières années (Enron,.... Et à la conséquence qui s'en est suivie, en termes d'évolution des lois et de la

[2] P. Schick- « Mémento d'Audit Interne »- Editions Dunod, p20

réglementation, il est apparu nécessaire de repréciser les attributions et objectifs du contrôle interne.

La structuration du contrôle interne est alors appréhendée à travers ses composantes ci après :

- L'environnement de contrôle
- L'évaluation des risques
- Les activités de contrôle
- L'information et la communication
- Le pilotage

Les établissements de crédits soumis à une réglementation particulière sont régis par un référentiel spécifique en matière de d'activités de contrôle. Le cadre en est donné par la note circulaire du N° 10-2000/CB/UEMOA du 23 JUIN 2000 portant réorganisation du contrôle interne des établissements de crédit.

Le contrôle interne est perçu comme une finalité de l'Audit Interne, il se définit selon plusieurs approches :

Approche de la profession comptable :

La définition la plus récente nous est donnée par le COSO (Committee of sponsoring Organizations of the Treadway Commission) : « Le contrôle Interne est le processus mis en œuvre par le Conseil d'Administration, les dirigeants et le personnel d'une organisation, destiné à fournir l'assurance raisonnable quand aux objectifs suivants : la réalisation et l'optimisation des opérations, la fiabilité des opérations financières, la conformité aux lois et aux réglementations en vigueur ».

Approche des autorités de contrôle bancaire de l'UEMOA :

Le cadre est fourni par la circulaire N° 10-2000/CB/UEMOA du 23 JUIN 2000 relative à la réorganisation du contrôle interne des établissements de crédit. Cette circulaire définit le contrôle interne des établissements de crédit par son objet :

-Vérifier que les opérations réalisées, l'organisation et les procédures internes sont conformes aux dispositions législatives et réglementaires en vigueur, aux normes et usages professionnels et déontologiques ainsi qu'aux orientations de l'organe exécutif (Direction générale) ;

-vérifier que les limites fixées par l'organe délibérant (Conseil d'Administration) en matière de risques, notamment de signature, de change et de taux d'intérêt, sont strictement respectées ;

-veiller à la qualité de l'information comptable et financière, en particulier aux conditions d'enregistrement, de conservation et de disponibilité de cette information.

I : AMELIORATION DU CONTROLE PAR L'AUDIT INTERNE

Diverses appellations sont attribuées aux départements et/ou services qui ont pour objet de conseiller la direction générale sur le fonctionnement de l'activité, on parle pèle mêle d'audit interne, de contrôle interne, d'inspection générale, de contrôle général etc.... . Quelles différences se cachent derrière ces termes, y a-t-il des attributions différentes ou des pouvoirs différents ?

L'Audit interne, comme le contrôle interne comporte plusieurs définitions. Ces définitions permettent de cerner le champ très vaste, qui constitue leurs domaines d'application.

L'audit interne comporte plusieurs définitions dont nous verrons quelques unes[3] :

L'Audit Interne est un dispositif interne à l'entreprise qui vise à :

-Apprécier l'exactitude et la sincérité des informations, notamment comptables

-Assurer la sécurité physique et comptable des opérations

[3] J. Renard –« Théorie et Pratique de l'Audit Interne »-Editions d'organisation

-Juger de l'efficacité des systèmes d'information »

Cette définition quelque peu restrictive, parce qu'elle ne tient pas compte du positionnement de la fonction a été complétée par la définition également restrictive de l'APEC :

« Réalisé par un service de l'entreprise, l'Audit interne consiste à vérifier si les règles édictées par la société elle-même sont respectées » ; ici on se limite à un audit de conformité, on va seulement comparer les pratiques aux normes internes en éludant la comparaison à des normes extérieures à l'entreprise, pourtant susceptibles d'apporter une amélioration.

Nous leur préférons la définition de l'IIA[4]

« L'Audit Interne est une activité **indépendante** et **objective** qui donne à une Organisation une **assurance** sur le degré de **maîtrise** de ses opérations, lui apporte ses **conseils** pour les améliorer, et contribue à créer de la **valeur ajoutée**.

Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de **management des risques**, de contrôle et de **gouvernement d'entreprise**, et en faisant des propositions pour renforcer leur efficacité.

B : LE RISQUE OPERATIONNEL

I : TYPOLOGIE DES RISQUES OPERATIONNELS

Qu'est ce que le risque opérationnel, comment se manifeste t il et qu'elles sont les différentes catégories de risque opérationnels ?

I.1 Définition des Risques Opérationnels

[4] Institute of Internal Auditors /www.theiia.org

Définition du risque :

Le risque se définit comme une exposition à un danger potentiel, inhérent à une situation ou une activité. Ce danger potentiel s'apprécie alors comme un évènement adverse qui vient contrarier la réalisation du projet ou de l'entreprise, il est généralement caractérisé par son impact et sa fréquence.

Le risque doit être identifié et évaluer afin de lui appliquer les mesures appropriées pour le neutraliser, le transférer ou réduire son impact.

Définition par défaut du risque opérationnel:

Tous les risques non compris comme étant des risques de crédit ou de marché

Exemple :

L'effondrement de Barings a constitué la faillite la plus spectaculaire au monde, c'était la disparition de l'institution bancaire la plus ancienne du Royaume Uni. La maison Barings s'est effondrée parce qu'elle ne pouvait pas assumer les énormes engagements financiers, que son trader Nicolas Leeson avait pris sur les marchés financiers au nom de la banque.

Ce trader, du fait des importantes positions qu'il prit à découvert sur l'indice NIKKEI, causa la faillite de son employeur.

Au fur et à mesure qu'il subissait des pertes, il s'est obstiné à cacher ses positions débitrices en les compensant.

Pour arriver à ses fins, il a utilisé un compte de transit qui lui a servi à cacher les pertes qu'il a causées.

L'analyse de cet incident permet de tirer de nombreuses leçons :

- Le trader a agi au delà de ses limites ;
- Il n'y avait pas une réelle séparation de tâches (engagement et enregistrement) qui lui ont permis de cacher les pertes subies dès qu'elles ont eu lieu ;
- Il n'y avait manifestement pas de supervision efficace de ses activités (suivi de ses transactions, liquidation de ses positions, surveillance des

limites de dealing).

Des incidents de ce type sont nombreux dans l'histoire de la finance et ont contraint les autorités de contrôle à prendre des mesures qui ont abouti aux accords de BÂLE.

Définition du comité de Bâle :

«Le risque opérationnel se définit comme le risque de pertes résultant de carences ou de défauts attribuables à des procédures, personnels et systèmes internes ou à des événements extérieurs. La définition inclut le risque juridique, mais exclut les risques stratégique et de réputation[5]».

I.2 Facteurs de risques

Procédures internes : (Inexistence, non respect de l'existant, contrôles inefficaces ou inexistants…)

L'existence et l'efficacité du contrôle interne se mesure par l'ensemble des procédures couvrant l'ensemble des activités de l'organisation. Ces procédures peuvent être écrites ou non. Les procédures internes lorsqu'elles ne couvrent pas l'ensemble de l'organisation, fragilisent sa continuité d'exploitation.

Les risques induits par les carences de procédures internes, découlent de ce que ces dernières, même si elles existent ne sont pas toujours formalisées, ne couvrent pas l'ensemble des activités ou, sont libellées de telle façon qu'elles ne permettent pas de couvrir l'ensemble des risques de l'organisation.

En la matière, l'existence de l'écrit permet d'assurer une certaine homogénéité et continuité dans le traitement des activités. Les procédures qui comportent des insuffisances non décelées laissent planer un risque sur l'organisation, ce risque peut alors se réaliser à n'importe quel moment, mettant à nu les faiblesses du

[5] Convergence internationale de la mesure et des normes de fonds propres : Dispositif révisé/ 10 Juin 2004/www.bis.org

système.

Les risques identifiés sous la rubrique des procédures dans les risques opérationnels sont qualifiés de risques administratifs.

Les risques administratifs : Ces risques se manifestent par des insuffisances dans le traitement des transactions ; par exemple, un client, victime d'un vol de son chéquier le déclare à son gestionnaire. Par la suite, un des chèques tirés de son chéquier est émis par une personne mal intentionnée, et payé par la banque du fait de la non transmission de l'ordre d'opposition du client au Service Clientèle de la banque. La perte subie par le client est entièrement imputable à cette dernière. Les procédures internes n'ont pas été appliquées, causant ainsi un préjudice au premier cité.

La faille ou le dysfonctionnement réside dans les faits suivants :

- La procédure ou l'une de ses étapes n'a pas été prévue par l'entreprise ;
- La procédure a été prévue mais a été mal formulée ou insuffisamment explicitée ;
- La procédure regroupe au niveau d'un agent ou d'un responsable des tâches incompatibles (celui qui exécute l'opération procède à son enregistrement) ;
- La procédure est mal appliquée ou n'est pas pratiquée.

Les agents auteurs des malversations connaissent, par la pratique quotidienne, ces failles et dysfonctionnements et bâtissent toute leur stratégie de fraude sur ces insuffisances.

Personnes : (Fraude, Incompétence, Indiscipline, mauvaise organisation, tâches mal définies ...)

Le risque humain constitue un aspect important des risques opérationnels. En effet, l'homme est à juste titre au centre de toute organisation ou de tout outil de production. Les théories récentes du management font de la satisfaction des

besoins de celui-ci, la clef du succès de l'entreprise. Ce grand espoir placé en lui (exigences de compétences, d'honnêteté, de loyauté, de disponibilité et d'efficacité) peut ne pas être satisfait. Dès lors, quelle que soit la technologie ou l'intensité capitalistique, l'œuvre est vouée à l'échec.

Les causes de la survenance de ce risque sont multiples et sont résumées dans la fraude, l'incompétence, l'indiscipline, la mauvaise organisation, la mauvaise définition des tâches ou tout simplement le manque de formation. Ces causes peuvent ensuite être classées en actes volontaires ou involontaires, la malveillance créant la différence.

Dans le lot des actes involontaires (incompétence indiscipline, défaut de formation…), ont peut considérer la cas de cet employé qui par étourdissement ou par méconnaissance des règles de comptabilité crédite le compte d'un client devant faire l'objet d'un gage espèce, cette erreur va alors se manifester par un solde non justifié ou anormal (Compte de gage d'espèces créditeur par nature qui se retrouve débiteur du fait de l'écriture erronée). L'erreur ainsi créé ne sera découverte que trop tard, (le client a utilisé les fonds) du fait des défaillances de l'agent dans l'analyse des comptes qu'il utilise.

L'acte volontaire par nature est la fraude[6] «Tromperies ou tentatives de tromperies commises dans le cadre de conventions ayant pour objet la fourniture de biens ou de prestations de service… ».

La norme 280 de l'IIA distingue deux cas de fraude :

- Les fraudes qui profitent à une personne physique mais aussi à l'organisation.
- Les fraudes qui profitent à une personne physique mais nuisent à l'organisation.

Dans le premier cas, l'on retrouve les évaluations erronées d'actifs faites dans le cadre de l'introduction en bourse d'une entreprise fraîchement côtée « window dressing », ou le paiement de pots de vins à des personnes clefs dans le but de

[6] J. Siruguet, « Formation sur la Fraude », Finabanque Conseil, Novembre 2006

bénéficier d'avantages concurrentiels ou de marchés publics.
Dans le second cas, il s'agit par exemple de l'employé qui détourne à son profit des valeurs de l'entreprise en exploitant des insuffisances du contrôle interne (cumul de fonctions incompatibles ou défaut de supervision) , utilisation pour son propre compte d'informations obtenues dans le cadre professionnel au détriment des clients.

Matériel (Systèmes) : (Informatique : perte de données, mauvaise protection, documentation des informations et systèmes…).
L'informatique est un outil de production à part entière pour la banque ; le risque informatique découle de la non maîtrise du système d'information.
La généralisation des ERP (Enterprise ressource Planning) ou logiciels de gestion intégrés ne s'est pas faite sans survenance de risques de types nouveaux demandant des mesures de prévention spécifiques.

Juridique et fiscal : (Absence de personne ressource, mauvaise conception et/ou documentation des contrats, application d'une réglementation et/ou législation obsolète…).

Le risque juridique est le risque de pertes encouru du fait de l'inadaptation de contrats, de leur non mise à jour ou de la mauvaise documentation de transactions. Il se réalise par l'inadaptation ou l'inapplicabilité des contrats. Ce fait se matérialise de diverses manières :
Pour exemple, prenons le cas d'un client qui bénéficie d'une convention avec sa banque pour faire exécuter des ordres de paiement sur son compte sur des formulaires non normalisés et authentifiés. Le client de mauvaise moralité peut utiliser les failles d'un tel contrat et faire exécuter une transaction qu'il ne reconnaîtra pas par la suite. Ce type de convention qui fait l'objet d'un contrat peut se retourner contre la banque si elle ne comporte pas des clauses de déni de

responsabilité.

De même, l'évolution de la réglementation doit pouvoir être prise en compte en permanence et dans l'ensemble des domaines d'activité de la banque ou elle s'applique.

Le risque fiscal quand à lui découle d'une mauvaise interprétation de la loi fiscale ou d'une insuffisance dans la déclaration de certains impôts.

Le risque juridique et fiscal est généralement du à l'absence de personne ressource pour l'analyse ou la conception des contrats ou à des procédures permissives qui ne prévoient pas de recueillir l'avis d'un juriste alors que c'est nécessaire.

Blanchiment d'argent : (Dispositif non-conforme à la réglementation en vigueur, non détection de cas, non déclaration…).

« Le blanchiment est le fait de faciliter par tout moyen la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré a celui-ci un profit direct ou indirect. Constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect du crime ou du délit.»[7]

Le blanchiment implique généralement une multiplicité de transactions ayant pour but de dissimuler l'origine de gains financiers afin qu'ils puissent être utilisés en toute impunité par leurs détenteurs.

Il comprend en général trois phases :

1) le placement ou dépôt des fonds illégitimes dans des institutions financières

2) l'empilement, qui consiste à éloigner de sa source le produit d'activités criminelles grâce à toute une série de transactions financières complexes, et

3) l'intégration, c'est-à-dire l'utilisation d'une transaction en apparence légitime

[7] Art 324-1 du code pénal

pour dissimuler des avoirs illicites[8].

Le développement de la criminalité financière a un impact sur l'économie en général. Les activités des banques sont soumises à une réglementation stricte, qui leur impose d'adapter leur système d'information afin de déceler toute activité susceptible de tomber sous le coup de la loi. L'inefficacité de l'organisation mise en place peut aboutir à la rupture des transactions avec certaines banques correspondantes ou au retrait de l'agrément d'exercice par les autorités de tutelle.

Le Comité Bâle II a mené une analyse quantitative de ces risques sur près d'une centaine d'établissements : les résultats démontrent la fréquence et le coût global élevés des incidents opérationnels : ils génèrent en moyenne près de 90 millions d'euros de perte. Une analyse plus fine démontre que si les sinistres les plus élevés sont aussi les mieux couverts (incendie, dégâts des eaux), c'est finalement la diversité des risques non couverts qui explique l'importance du coût final.

Les exigences de maîtrise du risque opérationnel suivent la démarche suivante : définition d'une politique générale appuyée par la direction, identification et quantification de ces risques, mise en place de mesures préventives et de mesures correctives en cas de sinistre et enfin surveillance permanente et reporting[9].

I-3 Catégories d'évènements

Selon les travaux du comité de Bâle, sept catégories d'évènements peuvent

[8] FMI-Afritac de l'Ouest : Atelier sur la lutte contre le blanchiment d'argent et la criminalité financière- Dakar Mai 2004

[9] L'analyse des risques opérationnels un enjeu qui dépasse le secteur bancaire, par JF Pirus (BPMS_info).htm

permettre d'analyser le risque opérationnel :

a) Fraude interne : par exemple, informations inexactes sur les positions, falsifications, vol commis par un employé et délit d'initié d'un employé opérant pour son propre compte.

b) Fraude externe : par exemple, hold-up, faux en écriture et dommages dus au piratage informatique.

c) Clients, produits et pratiques commerciales : par exemple, violation de l'obligation fiduciaire, utilisation frauduleuse d'informations confidentielles sur la clientèle, opérations boursières malhonnêtes pour le compte de la banque, blanchiment d'argent et vente de produits non autorisés.

d) Dommages aux actifs corporels : par exemple, actes de terrorisme, vandalisme, séismes, incendies et inondations.

e) Dysfonctionnement de l'activité et des systèmes : par exemple, pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité.

f) Exécution, livraison et gestion des processus : par exemple, erreur d'enregistrement des données, défaillances dans la gestion des sûretés, lacunes dans la documentation juridique, erreur d'accès aux comptes de la clientèle et défaillances des fournisseurs ou conflits avec eux.

g) Pratiques en matière d'emploi et sécurité sur le lieu de travail : par exemple, demandes d'indemnisation de travailleurs, violation des règles de santé et de sécurité des employés, activités syndicales, plaintes pour discrimination et responsabilité civile en général.

Les banques doivent évaluer leur exposition à chacun de ces types de risques pour chacune des 8 lignes de métier.

CHAPITRE II : EVALUATION DU RISQUE OPERATIONNEL

A : METHODES D'EVALUATION[10]

I : LE TOP DOWN

Le processus part de la vision stratégique du top management, sur la base de la rentabilité globale des opérations, une allocation de capital réglementaire aux différentes activités sera décidée par les organes exécutifs en fonction de leurs risques opérationnels. Dans ce contexte, les décisions prises aux niveaux supérieurs de la hiérarchie seront répercutées et traduites en plans d'actions suivis et maîtrisés par les managers au moyen d'indicateurs adéquats.

Cette approche propose une estimation du risque opérationnel sur la base des variations historiques des résultats, corrigées par la prise en compte de l'évolution de l'activité, en postulant que les pertes historiques sont une bonne mesure des risques opérationnels.

II : LE BOTTOM UP

Selon cette approche, les indicateurs clés des risques opérationnels sont définis et mesurés aux niveaux inférieurs, là où l'appréciation individuelle des managers exercera un levier maximum sur le suivi des risques opérationnels, pour être ensuite consolidés progressivement jusqu'à un niveau central. L'analyse est effectuée en distinguant l'impact des personnes, des processus et de la technologie.

L'approche de la cartographie peut être utilisée (Sites, ligne métier, activité…).

[10] Institut de l'Audit Interne/Price Waterhouse Coopers : « Le management des Risques de l'entreprise » Editions d'organisation, 2009

III : LE RAM

Consiste à élaborer une notice d'évaluation des risques de la banque, répartie sur l'ensemble des activités, ses unités structurelles et ses entités légales.

Cinq niveaux de risques pondérés ont été déterminés dans ce but :

Le risque haut est pondéré à 5 ;

Le risque moyen / haut est pondéré à 4 ;

Le risque moyen est pondéré à 3 ;

Le risque moyen /bas est pondéré à 2 ;

Le risque bas est pondéré à 1.

A chaque type de risques est attribué un indice de risque qui constitue une mesure de la probabilité qu'une perte survienne et de sa valeur.

L'indice de risque peut être calculé également par implantation selon la pondération pré définie.

Un indice de coût représentant les frais opérationnels pour gérer ces risques est déterminé.

Un ratio coût / risque (ratio de coût du risk – management) est calculé en faisant le rapport de l'indice du coût par l'indice du risque.

Exemple : Impact potentiel du risque de rejet de matériaux dangereux[11] :

Objectif : Gérer les matériaux dangereux en conformité avec les lois des états et les lois communautaires		
Risque		Unités de mesure
Rejet non planifié de matériaux dangereux		Perte de production (heures non travaillées) Coût des conteneurs Accidents Rémunérations et coûts connexes
Niveau	Impact	Critères
1	Insignifiant	Pas d'incident signalé Pertes de production minimes Aucun accident corporel
2	Mineur	1-2 Accidents signalés

[11] Institut de l'Audit Interne/Price Waterhouse Coopers : « Le management des Risques de l'entreprise » Editions d'organisation, p 209

Objectif : Gérer les matériaux dangereux en conformité avec les lois des états et les lois communautaires		
Risque		Unités de mesure
Rejet non planifié de matériaux dangereux		Perte de production (heures non travaillées) Coût des conteneurs Accidents Rémunérations et coûts connexes
Niveau	Impact	Critères
		Les matériaux sont gardés sur site par le personnel Effet inférieur à 5% des heures de production du jour Accident corporel minime ou absent
3	Modéré	Plusieurs incidents signalés Les matériaux sont gardés sur site grâce à une assistance externe Perte de production entre 5% et 20% des heures non travaillées dans la journée. Traitement médical nécessaire (sans hospitalisation)
4	Majeur	Evénement majeur signalé Matériaux rejetés dans l'environnement, mais sans effet réel ou perçu préjudiciable Perte significative de production(entre 20% et 100% des heures non travaillées dans la journée. Hospitalisation légère requise
5	Catastrophique	Plusieurs évènements majeurs ou un évènement catastrophique signalés Rejet dans l'environnement avec préjudice significatif, rendant nécessaire le concours de tiers Perte substantielle de la capacité de production, perte de production correspondant à plus de deux jours Accidents corporels significatifs

Cette évaluation est déclinée par activité et par unité organisationnelle.

B : EXIGENCES REGLEMENTAIRES

Le dispositif de Bâle II propose trois méthodes de calcul des exigences de Fonds propres au titre du risque opérationnel[12] :

I : L'INDICATEUR DE BASE

Une méthode simple , « Basic Indicator Approach ou BIA », consistant en un calcul forfaitaire (alpha = 15 %) des exigences (KBIA) sur la base du produit net bancaire moyen sur les trois derniers exercices de la banque : KBIA = 15%

[12] Convergence internationale de la mesure et des normes de fonds propres - Dispositif révisé 10 juin 2004 ;www.bis.org

*PNB ;

Cette méthode n'intègre aucun indicateur de perte, mais consiste essentiellement à constituer des fonds propres contre les risques opérationnels.

Le pourcentage forfaitaire à retenir devrait se situer entre 15 et 20%.

II L'APPROCHE STANDARD

Une méthode standard (The Standardised Approach ou TSA), consistant pour chaque ligne de métiers de la banque en un calcul forfaitaire (bêta = 12 % à 18 % selon les huit lignes définies) des exigences (KTSA) sur la base du produit net bancaire moyen enregistré sur cette ligne sur les trois derniers exercices :

KTSA = □(PNB1 - 8 x □1 - 8) ;

Les huit lignes de métier définies par le comité de Bâle sont les suivantes :

- Financement d'entreprise
- Négociation et vente
- Banque de détail
- Banque commerciale
- Paiements et règlements
- Services d'agence
- Courtage de détail
- Gestion d'actifs

Pour chaque ligne d'activité, un facteur de pondération reflétant le risque lié à l'activité vient corriger l'indicateur unique défini dans l'approche de base.

III LA METHODE DES MESURES AVANCEES

La méthode des mesures avancées (Advanced Measurement Approaches ou AMA), consistant en un calcul des exigences (K_{AMA}) par le modèle interne de mesure développé par la banque et validé par l'autorité de contrôle.

La mise en œuvre de cette méthode suppose l'existence de procédures de

contrôle du risque opérationnel et de données fiables sur l'historique des pertes.

Elle se décline en plusieurs sous méthodes :

-L'approche mesures internes ou IMA (Internal Measurement Approach) :

Elle reprend l'approche standard en combinant aux huit lignes de métier sept types d'évènements identifiés comme représentatifs de l'ensemble des cas possibles de pertes :

- Fraudes internes
- Fraudes externes
- Sécurité de l'environnement de travail et tous problèmes liés au recrutement.
- Pratiques liées à la clientèle, aux produits, aux activités.
- Actifs endommagés
- Arrêt accidentel de l'activité.
- Problèmes liés à l'exécution à la livraison ou à la gestion des procédés.

Les évènements devront être examinés pour en déterminer les causes, et le contrôle interne devra porter sur ces causes, soit pour réduire leur probabilité de survenance, soit pour en réduire les effets en termes de gravité des pertes. Rôle attribué à la charge en fonds propres.

DEUXIEME PARTIE : LA MAITRISE DU RISQUE OPERATIONNEL DANS L'ORGANISATION ET LES ACTIVITES DE ECOBANK COTE D'IVOIRE

CHAPITRE I : PRESENTATION GENERALE DE ECOBANK COTE D'IVOIRE (ECI)

A : HISTORIQUE DE ECOBANK

Le groupe ECOBANK est une institution bancaire régionale présente dans 14 pays de l'Afrique de l'Ouest et du Centre (Bénin, Burkina Faso, Côte d'Ivoire, Cameroun, Ghana, Guinée Bissau, Guinée Conakry, Libéria, Mali, Niger, Nigéria, Sénégal, Togo) dont la création remonte au début des années 1980. C'est à l'initiative de la Fédération des Chambres de Commerce de l'Afrique de l'Ouest dans son projet de création d'une banque régionale du secteur privé en Afrique de l'Ouest que les bases de cette institution ont été formulées. Il a fallu attendre en août 1984 pour que les actionnaires fondateurs aient apporté le capital initial devant servir au financement des études de faisabilité, du travail d'évaluation et des activités de promotion en vue de la création du groupe ECOBANK.

En 1985, Ecobank Transnational Incorporated (ETI) fut créée avec l'accord des Etats membres de la Communauté des Etats de l'Afrique de l'Ouest (CDEAO) comme une société de holding de banque. 1200 actionnaires originaires de 14 pays ont souscrit à son capital. ETI a démarré ses activités effectivement avec sa première filiale au Togo en mars 1988.

La filiale Ivoirienne, Ecobank Côte d'Ivoire a débuté ses activités en 1989 suite à la reprise des actifs de La Chase Manhattan Bank.

Sa mission est de fournir des produits bancaires et des services financiers aux personnes physiques, entreprises, institutions et aux gouvernements en Afrique de l'Ouest et Centrale. Sa clientèle est composée d'institutions

étatiques, d'organisations non gouvernementales (ONG), d'institutions multilatérales, bilatérales et régionales, de sociétés multinationales, nationales et de particuliers.

Elle offre une gamme complète de produits et services de banque commerciale et d'investissement dont :

- Les comptes courants ;
- Les comptes de dépôts ;
- Les comptes d'épargne ;
- Les prêts et découverts ;
- Le financement du commerce ;
- Les Transferts
- La gestion de portefeuille ;
- La gestion de trésorerie ;
- Western Union
- ECOBANK CI dispose d'un capital social de FCFA 4 276 600 000.

Après avoir passé en revue l'historique de ECI, nous allons étudier son organisation et son fonctionnement.

B : ORGANISATION GENERALE ET FONCTIONNEMENT DE LA BANQUE

Suite à une récente réorientation stratégique (vision de banque de détail), le groupe Ecobank dont la nouvelle vocation est de devenir une banque dominante en Afrique au sud du sahara a subi une profonde refonte de son organisation.

La nouvelle structure organisationnelle de ECOBANK fait apparaître outre le Conseil d'Administration et la Direction Générale, les départements suivants (cf. annexe 1 pour l'organigramme):

le Département de la Clientèle Privée, des petites entreprises et de la Microfinance (Retail Bank)

Le Département des Grandes Entreprises (Wholesale Bank)

Le Département de la Trésorerie et des Institutions

Le Département des Opérations et de la Technologie

Le Département du Risque

Le Département des Ressources Humaines (Human Resources)

Le Département du Contrôle Financier (FCU)

Le Département Audit & Respect des Normes (ARN)

Le Département Juridique et du Secrétariat Général

Les attributions des départements

- ✓ ***Le Département de la Clientèle Privée, des petites entreprises et de la Microfinance (Retail Bank)***

Ce département est chargé du marketing de la banque. Il joue le rôle d'interface entre les clients et les services opérationnels. Il s'occupe des ouvertures et fermetures de comptes, d'informer les clients sur leur position et des produits offerts par la banque. Le département a en charge les sept (7) agences (agence principale du Plateau et les agences des Deux Plateaux, de Treichville, d'Adjamé, de San Pedro, de Yopougon et celle de Bouaké, non fonctionnelle pour l'instant du fait de la crise). Il s'occupe en outre du portefeuille d'une partie de l'Ex-département du Commercial Banking, qui avait à charge, le développement de la clientèle des petites entreprises.

✓ ***Le Département des grandes entreprises (Wholesale Banking WSB)***

Le WSB comprenant le CBG est chargé de gérer les comptes des Grandes Entreprises privées. Il a pour mission de suivre le portefeuille de ses clients et de prospecter le marché pour attirer de nouveaux clients. Le WSB est également chargé de proposer de nouveaux produits et services aux clients afin de les fidéliser.

✓ ***Le Département du Contrôle Financier (Financial Control)***

Le département du contrôle financier est chargé d'établir le budget de la banque, les états financiers, les déclarations fiscales et les rapports d'activité destinés à la Direction Générale, au Groupe et aux Autorités Monétaires. Il réalise l'étude des gros investissements, fait le suivi des immobilisations et est responsable de la comptabilisation des écritures d'opérations diverses et de régularisations.

✓ ***Le Département des Ressources Humaines (Human Resources)***

Le département des ressources humaines est le département chargé du recrutement, de la formation, de la paie et de la gestion prévisionnelle du personnel de la Banque.

✓ ***Le Département Juridique***

Le Département Juridique est chargé du Secrétariat Général des différents conseils et comités de la banque : Il a une mission générale d'assistance des départements en matière juridique, de gestion des contrats, des dossiers litigieux et du contentieux, en collaboration avec les avocats de la banque.

✓ ***Le Département du Risque***

Ce département est chargé de la mise en œuvre de la politique du groupe Ecobank en matière de risques. Il s'occupe de l'ensemble des moyens mis en

œuvre pour gérer les risques pris par la banque particulièrement le risque de contrepartie (la gestion des prêts et découverts).

Service de l'Administration du crédit

Il est chargé entre autres tâches de la conservation et du suivi des garanties, et de la documentation des dossiers de crédit et de la collecte des approbations nécessaires aux différents engagements consentis. Il veille également à la correcte documentatiou des dossiers.

Service du Recouvrement

Ce service assure la prise en charge du suivi des créances compromises de la banque, le suivi de cette activité est assuré en collaboration avec les avocats de la banque.

✓ ***Le Département des Opérations et de la Technologie***

Le Département des Opérations et de la technologie est issu de la fusion de l'ex-Département des Opérations et de ce lui de l'Informatique, il a en charge toutes les opérations de la banque, notamment :

La Division des Opérations

- Les opérations de transfert : c'est un envoi de fonds d'une banque à une autre en faveur d'un bénéficiaire à l'initiative d'un client ou d'une banque.
- Les opérations du commerce extérieur (TRADE) : elles concernent les remises documentaires à l'importation et à l'exportation, les « bills negociated », les lettres de crédit à l'importation et à l'exportation, les cautions et garanties, les crédits documentaires
- Les opérations du portefeuille local : elles concernent l'encaissement et le paiement des valeurs sur place par l'intermédiaire de la " Chambre de Compensation " de la BCEAO.
- Les opérations du money market : il s'agit des dépôts à terme, des chèques et

effets à l'encaissement, des effets à l'escompte.

De plus, le Département des Opérations se charge de l'approvisionnement et de la tenue de stocks de fourniture de bureau.

La Division Informatique et Technologie (I.T)

Il joue un rôle de premier plan dans la banque. Il étudie et propose des solutions aux problèmes que rencontre la banque en vue d'améliorer la qualité de ses services. Il comprend deux services : le service réseau et le service développement.

✓ ***Le Département de la Trésorerie***

Ce département se compose de deux services : le service marché monétaire et le service des opérations de change.

Le service marché monétaire est chargé de :

- déterminer les taux du jour à appliquer pour toutes les opérations à partir du Reuters ;
- renseigner la situation des réserves obligatoires ;
- établir l'état du solde des comptes des filiales afin d'éviter que la banque ne subisse des pénalités ;
- faire le point des avoirs en caisse et en coffre des agences.

Le service des opérations de change se charge de :

- la vente et l'achat des devises ;
- la détermination des taux à appliquer aux clients et aux correspondants pour toutes les opérations de transfert.

✓ ***Le Département de l'Audit et Respect des Normes***

Le Département de l'Audit & Respect des Normes (A. R.N) est un département rattaché hiérarchiquement à la Direction Générale et fonctionnellement à l'Audit du groupe E.T.I. Il est chargé d'assurer la mise en œuvre du contrôle interne au sein de la banque.

Le département est divisé en deux services :

Audit et investigations : Chargé de la mise en œuvre du planning d'audit, du traitement des réclamations et confirmations de solde et de l'accomplissement des missions ponctuelles d'Inspection.

Contrôle interne : Ce service est chargé quant à lui d'animer les contrôles de premier et second niveau, et de conduire des missions de contrôle ponctuel sur place.

Les missions et responsabilités de l'Audit Interne sont précisées dans la charte d'audit Interne, et conformes à la circulaire n° 10-2000/CB du 23 Juin 2000, relative à l'organisation du contrôle interne des établissements de crédit, y sont également précisées les missions et responsabilités de l'organe délibérant (Conseil d'Administration/comité d'audit) et exécutif (DG/DGA) en matière de contrôle interne. Les activités du département font l'objet de reportings réguliers au Management, aux autorités de contrôle et à l'Audit du groupe, afin que les différents acteurs puissent exercer leurs prérogatives réglementaires.

CHAPITRE II : IMPACT DU SUIVI DES RISQUES OPERATIONNELS SUR L'ORGANISATION ET LES METHODES

A : LA REVUE PERIODIQUE DES PROCEDURES PAR L'AUDIT INTERNE

Une procédure se définit comme un ensemble de règles qu'il faut appliquer strictement, de formalités auxquelles il faut se soumettre, dans une situation déterminée[13]

Pour en revenir à la définition des risques opérationnels (Procédures internes ; P13) les causes de risque liés aux procédures sont les suivants :

- la procédure ou l'une de ses étapes n'a pas été prévue par l'entreprise,
- la procédure a été prévue mais a été mal formulée ou insuffisamment explicitée ;
- la procédure regroupe au niveau d'un agent ou d'un responsable des tâches incompatibles, (celui qui initie l'opération procède à sa validation) ;
- la procédure est mal appliquée ou n'est pas pratiquée ;
- la procédure existe mais n'est pas formalisée.

Comme suite aux éléments précités, l'audit interne procède à une revue des procédures de la banque en utilisant la démarche suivante :

Découpage de l'institution selon les départements, services, activités et produits (Arborescence).

Exemple :

DEPARTEMENT	SERVICE	PRODUITS
OPERATIONS	PORTEFEUILLE LOCAL	COMPENSE ALLER
		COMPENSE RETOUR
		GESTION DES IMPAYES

[13] Dictionnaire hachette Multimédia 1998

		CHEQUES DE BANQUE
	CONTRÔLE DES OPERATIONS	RAPPROCHEMENT BANCAIRE
		SUIVI DES OPERATIONS WU.
		INCIDENTS DE PAIEMENT
RETAIL BANKING	SERVICE CLIENTELE	GESTION DES CHEQUIERS
CONTRÔLE FINANCIER		PRODUCTION, CONTRÔLE, TRANSMISSION DES ÉTATS DE SYNTHÈSE ET RÉGLEMENTAIRES
GESTION DES RISQUES	CAD(Administration du crédit)	GESTIONS DES GARANTIES
INFORMATIQUE	INFRASTRUCTURES COMMUNES	GESTION DES EQUIPEMENTS RESEAUX
		MODIFICATION DE LA STRUCTURE DU RESEAU
RESSOURCES HUMAINES		ASSURANCE PERSONNEL

Les opérationnels sont ensuite conviés à décrire le processus de réalisation des différents produits, sur des fiches comportant les rubriques suivantes :

- **Intervenant**

L'opérationnel précise son poste dans la rubrique concernée.

- **Délai**

Le temps mis par l'opérationnel pour l'accomplissement de la tâche, qui sera rapproché des délais standards institutionnels, ou de ceux de la concurrence afin de tirer des conclusions quand à la performance de nos services par rapport aux normes internes ou concurrentielles.

- **Description technique des tâches à effectuer**

Permet de répondre aux questions :

Quoi faire ?

Comment le faire ?

Décrivant le mode opératoire, et permettant de décliner le processus en tâches élémentaires.

- **Observation :**

Cette rubrique, permet au réviseur de faire des suggestions sur les anomalies constatées : imprécisions, cumul de tâches incompatibles, absence de contrôle permettant de couvrir un risque particulier etc.... .

Les procédures ainsi recensées et consolidées permettent de renforcer le contrôle interne et de servir de base fiable et à jour pour les auditeurs internes et externes.

B : LE RAPPROCHEMENT ET LA JUSTIFICATION DES COMPTES

Les spécificités de l'activité bancaire ne sont pas sans conséquences sur son organisation interne, en effet « tout acte de banque est un acte financier qui se traduit in fine par un acte comptable[14]… ».

Les risques liés à l'utilisation des comptes se retrouvent amplifiés du fait de cette décentralisation poussée de l'acte comptable.

L'une des missions du contrôle interne est d'appuyer le département des opérations, dans le but d'atteindre un haut degré de perfection dans le processus des transactions.

Le dispositif de contrôle des comptes de la banque, pour être efficace, nécessite de situer chaque compte de la balance dans une catégorie particulière afin de lui appliquer le traitement adéquat.

L'objectif poursuivi en effectuant de tels contrôles est d'abord la prévention, par l'existence d'un contrôle de premier niveau, ensuite, d'éviter les pertes par fraude ou par erreur de traitement, en les décelant précocement.

La démarche de l'auditeur interne dans l'accomplissemeut de cette mission est de déterminer les causes des risques qui peuvent être qualifiés d'opérationnels, afin d'apporter des solutions en terme d'amélioration ou de formalisation de procédures et de dispositifs propres à rendre ces évènements improbables.

La normalisation et l'uniformisation de l'information comptable à l'échelle de l'union, permettront une comparabilité des états financiers bancaires ; et une évolution de l'information financière vers les meilleurs standards internationaux.

[14] A. Sardi, « L'Audit Interne des banques-puf- juin 1990 p 8

Le cadre comptable est défini par le plan comptable bancaire PCB, institué par la Banque Centrale et la Commission Bancaire et est organisé comme suit :

Les classes de comptes de la balance d'une banque :

Classe 1 : Comptes de trésorerie et d'opérations interbancaires

Classe 2 : Comptes des opérations avec la clientèle

Classe 3 : Comptes des opérations sur titres et opérations diverses

Classe 4 : Comptes de valeurs immobilisées

Classe 5 : Comptes de provisions, fonds propres et assimilés

Classe 6 : Comptes de charges

Classe 7 : Comptes de produits

Classe 9 : Comptes d'engagements hors bilan.

Spécificités de fonctionnement :

Exemple de la classe 1

Classe 1 : Les comptes de trésorerie sont débiteurs par nature, ils enregistrent les actifs détenus au débit et toutes les sorties de compte au crédit. Ces comptes font l'objet d'un inventaire exhaustif et inopiné. Le résultat de cet inventaire est rapproché au brouillard de caisse à la date d'arrêté.

Risques liés : Les risques que le contrôle de ces comptes peut permettre d'éviter sont principalement les risques opérationnels dont les conséquences sont les suivants :

Vol : dépassement des limites imposées par les procédures au solde du compte.

Les comptes peuvent être organisés en quatre groupes :

Comptes à solde débiteur.

Comptes à solde créditeur.

Comptes à solde nul.

Autres comptes.

Une anomalie sur les comptes des trois premières catégories se traduit généralement par un solde anormal, conséquence :

D'une double imputation.

D'une opération constatée tardivement.

D'une imputation erronée.

D'un prélèvement frauduleux

Ces catégories de comptes font l'objet d'un traitement qui est fonction de la nature du compte:

Comptes à suivre quotidiennement :

Ce sont des comptes présentant un risque particulier du fait qu'ils sont semi automatiques ou non analysés.

Méthode de contrôle :

Les suspens éventuels sur ces comptes doivent être détaillés et justifiés par les agents initiateurs des écritures.

Comptes faisant l'objet d'une analyse mensuelle :

Ces comptes sont analysés et appuyés des pièces justificatives, sur la base d'une demande inopinée du département d'audit et de contrôle.

Autres comptes :

-Faisant déjà l'objet d'un contrôle (ex des opérations de trésorerie rapprochées quotidiennement par un agent du contrôle, des comptes de caisse, faisant l'objet d'un inventaire inopiné).

-Enregistrant des écritures automatiques uniquement.

etc....

I : FORCES CONSTATEES

La banque dispose d'un dispositif dénommé « Proofing System » instituant un recensement périodique pour justification de tous ses comptes internes :

I.1 Suivi Des Comptes Internes

Dans ses relations avec les tiers, (prêteurs et emprunteurs de fonds), la banque enregistre des mouvements sur des comptes dits internes.

Du fait de la multitude des comptes de tiers existant à son passif et dont le contrôle ne peut se faire que par des réclamations, l'institution bancaire est contrainte de suivre et de contrôler le contenu de ses comptes internes.

En effet, vu le nombre important des comptes de la clientèle, la procédure la plus efficace pour s'assurer de la conformité de leur solde est l'examen des réclamations qui sont adressées à l'institution, par les clients, quand ils reçoivent leurs relevés de compte.

Le contrôle met en œuvre les diligences suivantes :

A travers le suivi de ces comptes, l'on s'assure que les écritures passées sont conformes aux ordres reçus (internes comme externes) avec des documents sources à l'appui (documents signés ou approuvés), dans le respect des délais de traitement.

S'assurer de la liquidation des opérations sur le compte dans les délais correspondants au sort du produit comptabilisé, quand un suspens demeure selon un délai anormalement long, des investigations plus poussées doivent être menées afin de procéder aux régularisations nécessaires.

S'assurer de la correcte identification de tous les montants en suspens dans un solde de compte, les écritures non justifiées sur les comptes internes devront être évitées .Toutes les transactions se manifestent par la constatation ou le débouclement d'une opération sous tendue par un engagement lié à l'activité.

Les erreurs et les dysfonctionnements des comptes mais aussi des cas de fraudes sont mis en évidence par le suivi de ces comptes. Le suivi est globalement effectué à ECOBANK COTE D'IVOIRE, et fonctionne malgré certains incidents survenus, en cours d'exercice 2006, et dont les causes ont été identifiées (absence de supervision d'un agent, usurpation d'un mot de passe pour dénouer une transaction, mauvaise maîtrise de l'applicatif bancaire, suivie d'une insuffisance dans la justification d'un compte ayant abouti à un double emploi non détecté. Etc…)

Cette procédure de contrôle permet d'accorder du crédit à la fiabilité des comptes et aussi de s'assurer du respect du principe d'image fidèle que préconise le SYSCOA .

I.2 Constitution d'une Base de Données Fiable

L'analyse des comptes internes permet de :

- justifier toute information par une pièce d'origine ;
- expliquer les évolutions des soldes d'un arrêté comptable à un autre et de l'initiation de la transaction au solde du compte (piste d'audit) ;
- reconstituer les opérations dans un ordre chronologique.

La procédure d'établissement des Justificatifs de solde permet d'obtenir les pièces justificatives des éléments en suspens sur les comptes. Les éléments se trouvent donc justifiés sur les comptes par des pièces comptables et autres documents. Elle constitue donc une base de données des éléments ayant transité par les comptes internes.

Cette base de données répond aux besoins de recherche ; l'audit interne dispose dans ses locaux des analyses de solde avec les copies des pièces justificatives sur un horizon de deux ans.

Cette mesure oblige les opérationnels et leur hiérarchie à vérifier régulièrement le contenu des comptes et permet un gain de temps dans la procédure de demande des pièces comptables une fois que celles-ci sont arrivées aux « archives ».

Le gain de temps est encore plus appréciable pour les commissaires aux comptes et les inspecteurs de la commission bancaire qui peuvent ainsi s'assurer de la maîtrise des transactions de la banque.

Les analyses de comptes permettent donc d'avoir une base de données fiable pour toutes recherches et vérifications ultérieures.

I.3 Détection et Régularisation des Dysfonctionnements et des Erreurs

L'un des objectifs essentiels de la procédure de contrôle des comptes internes est de permettre un suivi régulier de leur fonctionnement. Ce suivi se résume à veiller au respect des procédures en vigueur pour la réalisation des opérations et à la bonne application des règles du Plan Comptable.

Cette surveillance améliore la fiabilité de l'information financière et par conséquent la maîtrise des risques opérationnels.

Lorsque des irrégularités sont constatées, des recherches sont entreprises afin de trouver leurs causes et prendre dans un premier temps des mesures de régularisation, puis dans un second temps des mesures correctives afin de s'assurer que ces erreurs ne se répètent plus.

C : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DE CREDIT

En dehors du risque de crédit, qui est le risque de non remboursement d'un concours octroyé à un client, les risques opérationnels surviennent également dans ce pan majeur de l'activité de la banque.

Parmi ces facteurs de risques, on peut relever :

- découvert non autorisé ;

- méconnaissance des règles juridiques s'appliquant au statut des clients (possibilité de contracter, validité des garanties) ;
- absence de séparation des tâches lors de la mise en place des lignes de crédit ;
- mauvaise conservation des garanties ;

Exemple : des activités de contrôle mises en place pour couvrir les risques opérationnels de l'activité de crédit.

- rapprochement entre les autorisations et les lignes de crédit en cours ;
- revue des autorisations de crédit par le contrôle interne ;
- utilisation de formulaires standard et visa du département juridique requis avant les mises en place de crédits ;
- double validation nécessaire pour la mise en place des lignes de crédit ;
- normes de conservation des garanties dans des armoires ignifuges ;
- suivi extra comptable et inventaire périodique des garanties.

D : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DE DEPOT

Facteurs de risques de l'activité de dépôt :

- absence de séparation de tâches lors de la mise en place ou de la liquidation des comptes de dépôts ;
- mauvais paramétrage des taux sur les dépôts à terme ;
- non respect de la limite maximale sur les comptes ;
- non respect du montant minimum imposé sur les comptes ;
- absence de contrôle des comptes dormants (comptes sans mouvement à l'initiative du titulaire) et des comptes ne donnant pas lieu à édition de relevés.

Exemple des activités de contrôle mises en place pour couvrir les risques opérationnels de l'activité de dépôt :

- double validation requise pour la mise en place ou la liquidation des

dépôts ;

- revue périodique des comptes ne respectant pas les limites par le contrôle interne ;
- blocage automatique des comptes dormants, avec autorisation préalable de tout retrait par un cadre supérieur de la banque.

E : SUIVI DES RISQUES OPERATIONNELS DES ACTIVITES DES MOYENS DE PAIEMENT

- doublons générés lors du transfert des données du logiciel de traitement des effets, vers le logiciel comptable ;
- Limites de validation des effets et chèques, inadéquates ;
- Logiciel de communication Swift (protocole sécurisé de règlement de banque à banque) non interfacé au logiciel bancaire ;

Exemple des activités de contrôle mises en place pour couvrir les risques opérationnels de l'activité des moyens de paiements :

- rapprochement journalier entre les fichiers comptables et les extractions du logiciel de traitement ;
- Vérification régulières des limites de validation par l'audit informatique ;
- Interfaçage du logiciel de communication Swift avec le logiciel bancaire.

F : LA PREVENTION ET LA COUVERTURE DU RISQUE INFORMATIQUE

I : LES NORMES DE SECURITE DU SYSTEME D'INFORMATION

L'informatique qui se définit comme le traitement automatisé de l'information, est un outil essentiel dans la banque. La fonction informatique comprend plusieurs composantes nécessaires à son fonctionnement :

- Les ressources humaines : personnel technique comprenant des ingénieurs systèmes et réseaux (gestion des utilisateurs, sécurité informatique, gestion et

maintenance du matériel…), des ingénieurs logiciel (développement d'applications, paramétrage du software, études diverses…) ;

- Les Infrastructures et équipements ;
- Les bâtiments abritant les équipements informatiques et leurs périphériques, les équipements de protection contre les incendies, les installations de protection contre les fluctuations ou la rupture de courant électrique, les liaisons de communication (lignes téléphoniques, commutateurs, modems, routeurs).

La prévention et la détection du risque informatique comportent les mesures suivantes :

✓ Un plan stratégique informatique

Ce plan détermine sur un horizon donné, les objectifs, les ressources et les résultats attendus de la fonction système d'information.

✓ Un système de gestion des profils et habilitations :

Il permet :

- d'adapter les profils utilisateurs à leur description de tâches ;
- de désactiver les profils des agents absents de peur qu'ils ne soient utilisés par des malveillants (Il est d'ailleurs recommandé lors du recrutement de faire signer une décharge aux agents, leur rappelant la responsabilité à laquelle ils sont engagés par la violation de la confidentialité de leur mot de passe).

En effet, du fait de la séparation des niveaux d'habilitation pour les imputations et les autorisations, l'utilisation par une même personne de deux profils de niveaux différents peut lui permettre d'effectuer une opération hors de tout contrôle.

✓ L'existence de limites individuelles de traitement et de validation :

Elles sont fonction des niveaux de responsabilité et de la politique générale de l'institution. Les limites approuvées doivent faire l'objet d'un paramétrage, mis à jour en fonction des modifications de l'organisation et des procédures.

✓ Une procédure de sauvegarde des données :

Afin de limiter les risques de perte de données suite à des sinistres ou des dysfonctionnements, il convient de mettre en place une procédure journalière de sauvegarde et de conservation prévoyant que des copies des bandes de sauvegarde soient stockées sur des sites distants.

Les cycles de sauvegarde des bandes doivent être précisés afin de connaître l'horizon de sécurité, en s'assurant également que les sauvegardes de fin de période ne soient pas recyclées (réutilisation des bandes).

✓ La documentation des logiciels et applicatifs :

S'assurer que les logiciels sont correctement documentés afin de permettre l'optimisation de leur utilisation et assurer la continuité du service.

II LE PLAN DE CONTINGENCE INFORMATIQUE

Il énonce toutes les mesures préventives et préparatoires destinées à éliminer les risques potentiels d'incidents ainsi que les différentes mesures de reprise à prendre afin de réduire au minimum les effets d'un éventuel incident ou désastre.

Ses objectifs sont entre autres :

- Minimiser l'impact d'un éventuel désastre sur le système d'information,
- Assurer un niveau de fonctionnement acceptable du système en cas de désastre/incident, avant le rétablissement total des services dans les meilleurs délais.

Les causes possibles d'incidents :

✓ Les catastrophes naturelles : Dans cette rubrique on retrouve généralement les inondations (dégâts des eaux), les tremblements de terre, la foudre, la sécheresse etc… . Ces évènements peuvent aussi bien avoir un impact direct (destruction) qu'indirect (conséquences sur l'économie).

Cette évaluation permet de prendre des mesures de protection en fonction de l'exposition potentielle (Isolation des bâtiments abritant les équipements, dispositif de protection contre la foudre, aménagement d'un site de secours, en cas de catastrophe naturelle…).

✓ Les causes matérielles : sont les plus probables et les moins catastrophiques :

- Fluctuations électriques qui engendrent la corruption ou la perte de données sur les ordinateurs ;
- Défaillance du réseau de transmission de données ;
- Arrêt système pour cause de défaillance matérielle ;
- Arrêt système pour cause de défaillance logicielle ;
- Destruction des différents câblages par les rongeurs et autres bestiaux pouvant entraîner des courts circuits sur le réseau électrique ;
- Dégâts des eaux ;
- Incendies ;
- Explosions ;
- Malveillance et négligence du personnel.

Elles sont en général provoquées par un défaut de maintenance des installations et des équipements.

✓ Les autres causes :

- L'espionnage
- La guerre

Le plan de contingence informatique prévoit la description quantitative et qualitative du matériel, des logiciels et des liaisons.

Ledit matériel y est scindé en deux entités :

Les équipements critiques et les équipements non critiques.

Est qualifié d'équipement critique, le matériel support constitué des serveurs hébergeant les bases de données du système d'information, tandis que l'équipement non critique est constitué des terminaux des utilisateurs.

Les liaisons réseaux et leurs caractéristiques y sont également décrites.

Le plan de contingence informatique comprend également les caractéristiques des logiciels et applicatifs bancaires.

Les procédures de reconstitution des données et de fonctionnement minimal en cas d'indisponibilité ou de crash de la base de données.

Ce plan a montré sa viabilité lors de tests menées par l'auditeur informatique, et donne l'assurance d'une correcte couverture en cas d'incident.

D : LE REPORTING

Le suivi et le reporting des risques opérationnels s'inscrit dans le cadre de l'Approche des Mesures Avancées (AMA) qui exige la constitution d'une base de données fiable des pertes opérationnelles subies par l'institution.

Les procédures d'ECOBANK prennent en compte un suivi journalier à des fins de reporting, des comptes de pertes et profit.

Cette tâche journalière consiste à extraire les données d'un rapport spécifique édité par l'informatique, reprenant les différents postes de charges et produits définis par le groupe comme constituant des rubriques de perte opérationnelle.

Les comptes à suivre sont agrégés en deux lignes dans le rapport de gestion :

LIGNE	DESCRIPTION
10	INTEREST REVENUES
20	INTEREST EXPENSES
30	NET REVENUE FROM FUNDS
40	FX
50	FEES COMMISSIONS
60	OTHER REVENUES
65	DOTATION AUX PROVISIONS
68	REPRISES PROVISIONS
70	GROSS WRITE OFFS

LIGNE	DESCRIPTION
80	LESS RECOVERIES
90	NET REVENUES
100	STAFF EXPENSES
110	ALLOCATED EXPENSES
120	CONTRACTUAL EXPENSES
130	OTHER EXPENSES
140	FIDELITY LOSSES
141	PL ADJUSTMENT
150	OTHER OPERATING EXPENSES
160	E B I T
170	INCOME TAX
180	NET INCOME
190	INTEREST SHADOW RECORDS
200	UNASSIGNED

Les lignes 140 et 141 font l'objet du rapport sur les pertes et profits. Leur détail est donné ci après :

LIGNE	RUBRIQUE	COMPTES	INTITULE
140	FIDELITY LOSSES	667000003	PERTE OPERATIONNELLE
		669110000	AUTRES PERTES
		672100001	PERTES D'EXPLOITAT BCAIRE/EXO ANTERIEURS
141	PROFIT AND LOSS ADJUSTMENT	609920001	PERTES BILTS SS CRS LEGAL
		651000000	DOT.FDS PR RIS BCRES GX
		666000001	PROV AUT.ELEMENTS ACTIF
		667000000	DOT.PROV.PR RISQUE & CHAR
		671200000	AMENDES ET PENALITES FISC
		671200001	AMENDES
		671400000	RAPPELS D'IMPOT SAUF BIC
		671500000	PERTES DE CHANGEMT METHOD
		671610000	PERTES EXCEPTIONNELLES
		672100000	PERTES D'EXPLOITAT BCAIRE
		672110000	PERTES/ EXERCICE EN COURS
		672120000	PERTE D'EXPLOITATION
		672210000	AJUST P&L AVT DEPENSE ANN
		672220000	PERTES/EXERC. ANTERIEURS
		672230000	RESULTATS EXERCICE ANT.
		751000000	REPRISE DU FRBG
		767000000	REPRISE DE PROVISIONS POUR RISQUES ET CH.
		771100000	PRODUITS EXCEPTIONNELS
		771700001	PRODUITS EXCEPTIONNELS
		772110000	PROFITS D'EXPLOITATION BANCAIRES/EXO ANTERIEURS

L'exploitation des rapports s'effectue en allant du général au particulier, les montants identifiés dans le rapport consolidé sont ensuite détaillés par ligne de compte de charge.

Les transactions enregistrées dans chacun des comptes identifiés sont analysées conformément à la grille du rapport de pertes et profits :

- Erreur de traitement

(L'erreur n'est pas intentionnelle)

- Réajustement volontaire

(Du fait d'une réclamation fondée d'un client)

- Erreur de facturation

(Ecritures au débit représentant l'annulation de montants précédemment constatés comme revenu (commissions, intérêts…))

- Fraude interne/Vol

Perte résultant de la malversation d'un employé.

- Fraude externe/Vol

Perte résultant de la malversation d'un tiers.

- Perte due au rapprochement

Perte résultant d'un rapprochement erroné ou tardif des comptes nostri, interbranches ou à recevoir des autres filiales.

- Pertes dues au règlement de litiges
- Amendes et pénalités

Pertes causées par des pénalités pour violation des obligations légales et réglementaires.

- Pertes due à une défaillance matérielle.
- Autres pertes non précisées.

Recouvrement de montants précédemment constatés en perte opérationnelle.

(Par compensation, recouvrement, assurance etc.…)

- Pertes dues à une erreur de tarification.

(Mauvaise évaluation d'actif ou application d'un mauvais taux de change dans

une transaction).

Exemple : (Cf page suivante)

PERTES ET PROFITS MOIS DE												
	1	2	3	4	5	6	7	8	9	10	11	12
N° CPTE	Process,Error	Goodwill Loss	Erreur de tarification	Fraude interne	Fraude externe	Erreur de rapprochement	Perte judiciaire	Amendes et pénalités	Défaillances système	Autres pertes non précisées	Recouvrement de perte opérationnelle	Erreur de tarification
667000003				-5 050 025	Règlement du préjudice sur fraude agent							
672100001	-16 390	Pertes due aux clôtures de comptes										
672100001	-12 437	Pertes due aux clôtures de comptes										
672100001	-11 045	Pertes due aux clôtures de comptes										
672100001	-3 800	Pertes due aux clôtures de comptes										
672100001	-5 730	Pertes due aux clôtures de comptes										
672100001	-15 806	Pertes due aux clôtures de comptes										
672220000	-500	Perte exercice antérieur sur règlement facture faveur X										
672220000	-1	Perte exercice antérieur sur règlement pose télésurveillance										
672220000	-29 000	Perte exercice antérieur sur règlement fourniture espace Privilège										
672220000	-40 000	Perte exercice antérieur confection meuble de rangement faveur espace privilège										
672220000	-1	Perte exercice antérieur achat cafetière faveur Espace privilège										
672220000	-21 500	Perte exercice antérieur confection grille et porte blindée de rangement faveur Agence 5										
TOTAL	**-156 210**	**0**		-5 050 025	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

CHAPITRE III : RECOMMANDATIONS ET PERSPECTIVES

Nous avons constaté dans l'organisation en place d'ECOBANK l'existence d'une organisation du contrôle Interne conforme aux exigences minimales de la réglementation bancaire. Dans une optique de maîtrise accrue des opérations d'une part et de respect des politiques institutionnelles et de la réglementation d'autre part, des réformes restent néanmoins à mettre en œuvre si l'on veut opter pour une meilleure approche d'évaluation spécifique des risques opérationnels, et se donner les moyens d'être prêts .

Réformes organisationnelles :

1-La création d'un comité ou d'une cellule de gestion des risques Opérationnels : cette structure permettrait d'appréhender ce risque dans son aspect pluridisciplinaire. A l'image des comités existant déjà dans la banque (comité de technologie, comité des archives etc…..), il permettrait de trouver une réponse adaptée et servirait de cellule de réflexion impliquant tous les acteurs.

2- La formation du personnel et le renforcement de l'automatisation des traitements, suivi et contrôlé par un auditeur informaticien.

3- La mise en place d'un contrôle de gestion, pour le suivi des encours moyens, qui permettrait de valider le bon paramétrage des intérêts débiteurs et créditeurs.

Réforme du reporting et du système d'information :

1-Mettre en œuvre un projet de cartographie des risques qui permettra d'identifier les éléments clefs, inducteurs des incidents qualifiés

d'opérationnels et susceptible de servir de données pour la base.

Les données devront être collectées et renseignées au fur et à mesure sous un format exploitable statistiquement, lors de la mise en œuvre de l'approche choisie.

2-Mettre en place des fiches de déclaration d'incidents qui seraient remontées à la cellule de suivi et qui feraient l'objet de traitement sous deux aspects : compréhension de la cause de l'anomalie et suivi de la régularisation.

3-Acquisition d'un logiciel de gestion des risques opérationnels qui permettrait d'identifier toutes les réformes à effectuer au niveau des procédures, et d'évaluer le niveau d'exposition dans chaque métier.

4- Mettre en place un reporting des données de risque opérationnel au comité afin qu'il évalue l'efficacité du dispositif.

5- Adresser un rapport sur les activités et évaluations du comité de pilotage des risques opérationnels aux organes délibérants et exécutifs afin de leur permettre d'exercer pleinement leurs responsabilités.

CONCLUSION

Au terme de notre étude, il est important de souligner qu'au nombre des risques auxquels est exposée ECOBANK COTE d'IVOIRE, ceux faisant partie de la catégorie des risques opérationnels ne font pas encore l'objet d'un traitement distinct, en termes d'organisation. Toutefois, un reporting des pertes liées à ces risques est effectif, mais n'est pas adapté aux exigences à venir de la réglementation (Bâle II).

Une remise à plat du profil de risque de l'institution s'impose donc, par la confection d'une cartographie des risques s'appuyant sur une évaluation constante de l'efficacité du contrôle interne , afin de permettre de bâtir un système d'information prenant en compte toutes les variables influant sur les pertes opérationnelles.

BIBLIOGRAPHIE

A. Sardi, « L'Audit Interne des banques »-puf- juin 1990

Code pénal Dalloz

Convergence internationale de la mesure et des normes de fonds propres - Dispositif révisé 10 juin 2004 ;www.bis.org

Dictionnaire hachette Multimédia 1998

FMI-Afritac de l'Ouest : Atelier sur la lutte contre le blanchiment d'argent et la criminalité financière- Dakar Mai 2004

H. GBEASOR-« Cours de Réglementation Bancaire »-CESAG/PMBF 2005

Institut de l'Audit Interne « Le Management des risques de l'entreprise », Editions d'organisation

Institute of Internal Auditors www.theiia.org

Revue banque magazine n°624 Avril 2001.

P. Schick- « Mémento d'Audit Interne »- Editions Dunod

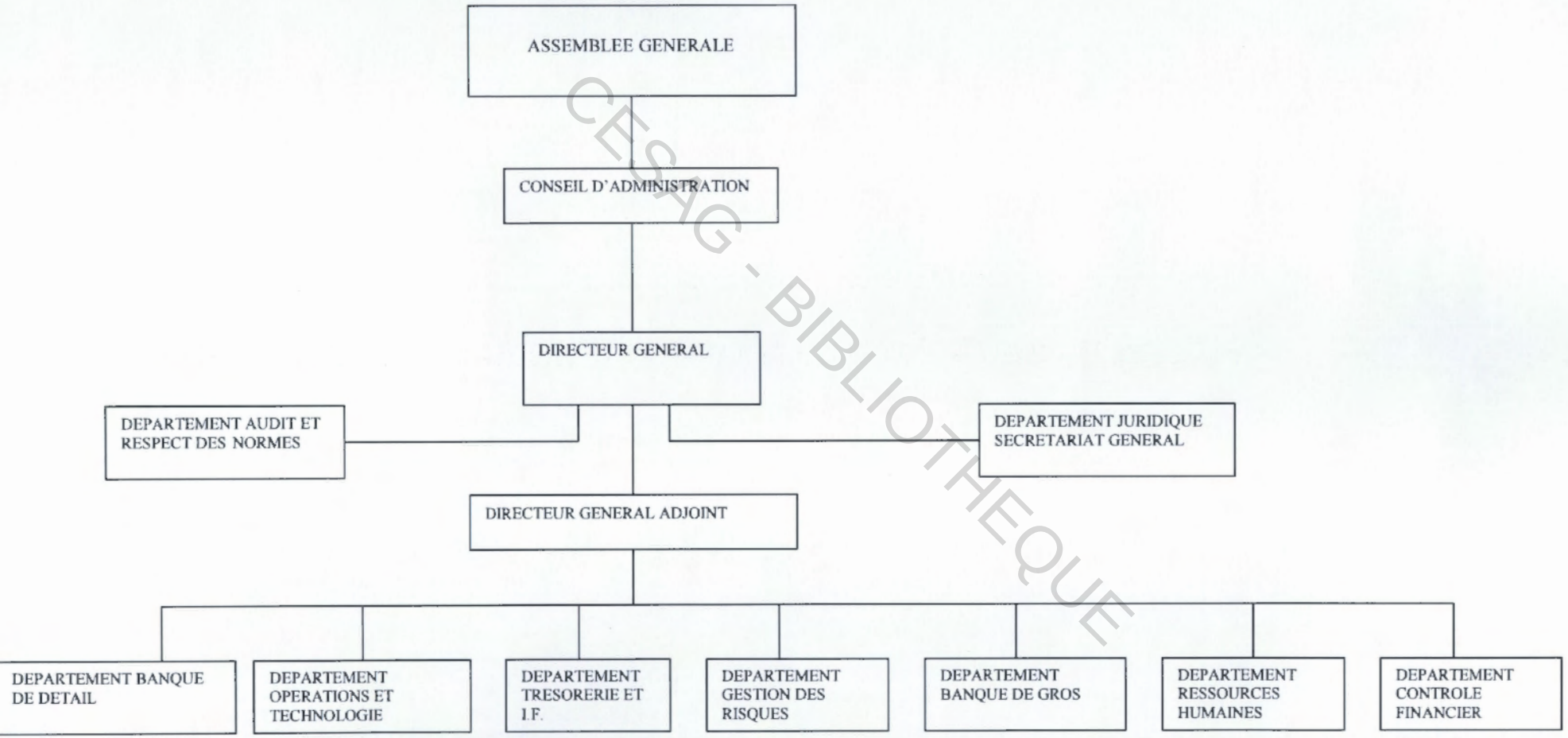
J. Renard –« Théorie et Pratique de l'Audit Interne »-Editions d'organisation

J. Siruguet, « Formation sur la Fraude », Finabanque Conseil, Novembre 2006

JF Pirus L'analyse des risques opérationnels un enjeu qui dépasse le secteur bancaire (BPMS_info).htm

ANNEXES

ANNEXE 1 : ORGANIGRAMME D'ECOBANK COTE D'IVOIRE AU 31/01/2007



ANNEXE 2

MATRICE DE CONTRÔLE DES COMPTES DE LA BALANCE[15]

N	Libellé	Technique de contrôle	Périodicité	Responsable	Sens	Risque lié	Contrôle	Observation
	1)Comptes de trésorerie et op. Int.							
10	Caisse	Inventaire/Justification	J	CAISSE	Débiteur ou nul	Imputation erronée Blanchiment Dépassement de limite d'encaisse	Inventaires périodiques	
12	Autres comptes de dépôts chez Ets de crédit.	Rapprochement	M	Contrôle financier	Débiteur ou créditeur	Risque de contrepartie Erreur d'identification du type d'ets (attribut)	Régularisation et apurement des suspens Vérification des dates de valeur des suspens	Proof
13	Prêts au j. le j.	Rapprochement/confirmation	M	Contrôle financier	Débiteur			
	Prêts à terme	Justification	M	OPS	Débiteur			
17	Emprunts au jour le jour	Justification	M	OPS	Créditeur			
	Emprunts à terme	Justification	M	OPS	Créditeur			
	Créances douteuses	Justification	M	OPS	Débiteur			
	Provisions sur créances douteuses	Justification	M	CAD	Créditeur			Proof
	2)Opérations avec la clientèle							
20	Crédits à la clientèle	Justification	M	OPS	Débiteur ou nul	Imputation erronée (mt et/ou sens) Risque financier Risque commercial		

[15] Source : Le Contrôle Comptable Bancaire

MATRICE DE CONTRÔLE DES COMPTES DE LA BALANCE[15]

N	Libellé	Technique de contrôle	Périodicité	Responsable	Sens	Risque lié	Contrôle	Observation
25	Comptes de la clientèle	Justification/Inventaire	M	Retail	Débiteur ou créditeur	Imputation erronée (mt et/ou sens) Risque de contrepartie Risque commercial		
27	Emprunts et autres sommes dues à la clientèle	Confirmation	M	Retail	Créditeur	Non exhaustivité et sous évaluation des charges liées		Proof
	Créances douteuses			CAD	Débiteur	Mauvaise évaluation Risque fiscal		
	3)Opérations sur titres et diverses							
30	Titres de placement		M	Trésorerie				Proof
33	Débiteurs divers créditeurs divers		M	Contrôle financier				Proof
37	Comptes transitoires et d'attente	Rapprochement	J	OPS				Proof
371	Comptes d'encaissement	Justification	J	OPS	Créditeur	Perte liée au non enregistrement d'une valeur Double imputation d'un client Non imputation sur un compte client		
372	Comptes de recouvrement	Justification	J	OPS	Débiteur			
38	Comptes de régularisation	Justification	J	OPS				Proof
381	Actif	Justification	J	OPS	Débiteur			
382	Passif	Justification	J	OPS	Créditeur			
39	Comptes de liaison Interbranche Interfiliales	Rapprochement Rapprochement	Quotidien Mensuel	Back Office opérations Contrôle Financier				
	4)Valeurs immobilisées							

MATRICE DE CONTRÔLE DES COMPTES DE LA BALANCE[15]

N	Libellé	Technique de contrôle	Périodicité	Responsable	Sens	Risque lié	Contrôle	Observation
41	Immobilisations financières	Inventaire	ANNUEL				Inventaire	
42	Dépôts et cautionnements	Inventaire	ANNUEL				Inventaire	
44	Immobilisations d'exploitation	Inventaire	ANNUEL				Inventaire	