Centre Africain d'Études Supérieures en Gestion

CESAG EXCECUTIVE EDUCATION

MBA – AUDIT ET CONTRÔLE DE GESTION

29ème Promotion
2017/2018

MEMOIRE DE FIN D'ETUDES

ÉVALUATION DU PROCESSUS DE GESTION DES RISQUES OPÉRATIONNELS D'UNE BANQUE PAR LE CABINET PRICEWATERHOUSECOOPERS, CÔTE D'IVOIRE.

Présenté par :	Dirigé par : Maty Laye SAMB
ZADRE Christiane Loïs Siacoh	Associée gérante chez Mea Lux Consulting SARL et Enseignante au CESAG

Mai 2019

DÉDICACE

Ce mémoire est dédié :

- au Seigneur Jésus-Christ, pour la force, l'intelligence et la sagesse qu'il m'a accordée durant tout mon parcours scolaire et lors de la rédaction de ce mémoire ;
- à mes parents, pour l'amour, les conseils et le soutien infaillible qu'ils m'ont apportés durant mon parcours scolaire et lors de la rédaction de ce mémoire.

REMERCIEMENTS

Cette étude n'aurait pas été faite n'eut été l'aide incessante, la compréhension et le dévouement d'un certain nombre de personnes qui, par leurs conseils et leur disponibilité m'ont apporté tout leur soutien. Nous leur exprimons nos sincères remerciements :

- A Dieu pour m'avoir accompagnée et guidée tout au long de ma formation, pour la force qu'il m'a donnée dans les moments de faiblesses, pour les expériences et surtout les moments de joie ;
- A monsieur Jean-Marcel KOUASSI, coach et maître de stage, Manager Assurance chez PricewaterhouseCoopers, Côte d'Ivoire pour ses conseils et le temps qu'il a bien voulu m'accorder afin de me guider dans mes recherches et à la réalisation de ce mémoire de fin d'études ;
- A madame Maty SAMB, Directeur de mémoire, Associée gérante chez Mea Lux Consulting SARL, consultante et formatrice en services financiers et Enseignante au Centre Africain d'Etudes Supérieures en Gestion pour sa son aide qu'elle a bien voulu m'accorder pour la rédaction du mémoire de fin d'études ;
- Au docteur Rouba KANE, Responsable du Département CESAG EXECUTIVE EDUCATION et Enseignante chercheur au Centre Africain d'Etudes Supérieures en Gestion pour, l'encadrement, mais aussi pour sa disponibilité et ses qualités humaines.
- A monsieur Souleymane Soro COULIBALY, Associé, Assurance leader chez PricewaterhouseCoopers, Côte d'Ivoire et à Monsieur Didier N'GUESSAN, Associé Assurance chez PricewaterhouseCoopers, Côte d'Ivoire ; pour m'avoir donné l'opportunité d'effectuer un stage au sein de leurs effectifs dans le but de rédiger mon mémoire de fin d'études.
- A tout le corps professoral du programme de MBA en Audit et Contrôle de Gestion pour la contribution à notre formation.
- A la famille MBA ACG ; promotion 2017/2018 pour la solidarité démontrée, les échanges d'idées et les encouragements durant l'année académique.

LISTE DES TABLEAUX

SIGLES ET ABBREVIATIONS

IIA : The Internal Institute of Auditors
KRI : Key risks indicators
MIFID : Market in Financial Instruments Directive
UMOA : Union Monétaire Ouest Africaine
SOA : Sarbanes Oxley Act
S.I : Systèmes d'Informations
BAS : Business Advisory Services
COSO : Committee of Sponsoring Organizations of the Treadway Commission
BÂLE II et III : constituent un dispositif prudentiel destiné à mieux appréhender les risques bancaires.
AZF : Azote Fertilisants
UBS : Union Bank of Switzerland

LISTE DES ANNEXES

SOMMAIRE

INTRODUCTION GENERALE

Le risque opérationnel est défini par CHURCHILL et COSTER, (2001) comme étant la vulnérabilité à laquelle sont confrontées les institutions financières dans leur gestion quotidienne pouvant provoquer la destruction de leurs actifs. Lorsque le risque opérationnel constitue le risque principal, il entraîne la perte financière à travers les crédits défaillants, les fraudes ainsi que les vols.

La circulaire n°04-2017/cb/c relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA définit également le risque opérationnel comme étant le risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes. Il s'agit ici d'erreurs humaines, de fraudes et malveillances, de défaillances des systèmes d'information, des problèmes liés à la gestion du personnel, de litiges commerciaux, d'accidents, incendies, inondations, etc.

Prenons l'exemple de la banque Barings en 1995. Elle constituait l'une des plus anciennes et des plus prestigieuses banques du Royaume-Uni et a fait faillite après 233 ans d'existence. Un dysfonctionnement du système de contrôle interne, notamment dans la filiale de Singapour a conduit la Banque à sa perte. En effet, un jeune trader Nick Leeson, à cette époque, responsable du marché des produits dérivés à la Bourse de Singapour, était chargé d'organiser l'ensemble des transactions pour le compte des clients de la banque, mais également du back-office et du trading du marché. Il avait l'habitude de spéculer à la Bourse japonaise en vendant des contrats à termes sur l'indice Nikkei afin de profiter au maximum de l'effet levier. Alors, sans réel contrôle, il va investir les fonds des clients dans des opérations spéculatives non autorisées, mais connues des dirigeants de la Barings. Il devint rapidement, aux yeux de la profession, un opérateur renommé. Cependant, après le tremblement de terre de Kobéen janvier 1995, ne considérant pas l'ampleur des pertes financières et voulant contrôler l'indice Nikkei, Nick Lesson était convaincu que le marché allait repartir à la hausse et continua d'acheter de nouveaux contrats pour couvrir ses premières pertes. Néanmoins, l'indice japonais continua sa chute et entraîna avec lui Nick Lesson et la Barings. Les pertes cumulées étaient estimées à 860 millions de livres sterling faisant environ 860 milliards de FCFA, soit plus de deux fois le montant des capitaux propres de la banque. La cause première de cette chute était dû à un dysfonctionnement du système, plus spécifiquement dans l'absence de maîtrise ou de l'insuffisante de maîtrise d'un risque opérationnel, d'une absence de contrôle, dans l'accomplissement d'opérations spéculatives non autorisées, mais connues des dirigeants.

Le COSO définit le contrôle interne comme un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants :

- réalisation et optimisation des opérations ;
- fiabilité des informations financières ;
- conformité aux lois et aux réglementations en vigueur.

Tout ceci contribue aux sécurités participant à la maîtrise des opérations de l'entreprise. Le contrôle interne a donc pour but d'un côté 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. 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.

La Banque des Règlements Internationaux (BRI) de son côté, considère qu'un contrôle interne efficace constitue le fondement d'un fonctionnement sûr et prudent d'une organisation bancaire et en aval du système bancaire de l'économie concernée.

Ainsi, le contrôle interne étant un système destiné à s'assurer qu'une entreprise fonctionne correctement, il comprend des mesures visant à prévenir les erreurs, la perte financière que représentent les excès de frais de déplacements etc. ainsi que le vol. Il joue également un rôle prépondérant dans la gestion des risques des banques. En effet, un contrôle interne efficace permet à la banque de mieux contrôler son activité et donc de mieux gérer les risques auxquels elle doit faire face et de faire face aux exigences réglementaires, notamment les exigences des circulaires relatives à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA ainsi que les réglementations Bâloises.

On distingue plusieurs risques bancaires notamment ; les risques opérationnels, de crédit, les risques de marché et le risque de non-conformité.

OverBlog, dans « Quels sont les risques du crédit bancaire ? » (2017 :45), indique que le risque de crédit représente la configuration la plus vieille du risque sur les marchés financiers. Le risque de crédit est défini comme étant : « Le risque résultant de l'incertitude ou la volonté des clients de ne pas remplir leurs obligations ». En d'autres termes, le risque de crédit constitue la possibilité pour le client de ne pas honorer ses engagements de manière volontaire ou non. Il existe donc un risque pour la banque dès lors qu'elle se met en situation d'attendre une entrée de fonds de la part d'un client ou d'une contrepartie de marché.

Selon Bâle II, la non-conformité équivaut au risque de sanction judiciaire, administrative ou disciplinaire, de perte financière, d'atteinte à la réputation, occasionnée par le non-respect des dispositions législatives et réglementaires, des normes et usages professionnels et déontologiques, propres aux activités bancaires. Parmi ces risques, sont notamment incluses les dispositions concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme. Les principaux risques de non-conformité résultent de la non-observance de règles relevant pour la plupart de l'ordre public.

Le risque de marché est le risque de perte qui peut résulter des fluctuations des prix des instruments financiers qui composent un portefeuille. Le risque peut porter sur le cours des actions, les taux d'intérêts, les taux de change, les cours de matières premières, etc. Par extension, c'est le risque des activités économiques directement ou indirectement liées à un tel marché, par exemple un exportateur est soumis aux taux de change, un constructeur automobile au prix de l'acier, etc. Il est dû à l'évolution de la totalité de l'économie, de la fiscalité, des taux d'intérêts, de l'inflation, et aussi du sentiment des investisseurs vis-à-vis des évolutions futures. Il affecte plus ou moins l'ensemble des titres financiers.

Cependant, notre étude sera basée principalement sur la gestion des risques opérationnels.

Les risques opérationnels ont pris une importance considérable dans le contexte bancaire né de l'insuffisance de la réglementation, de l'imbrication croissante des acteurs du monde financier, de l'augmentation des capitaux manipulés et de la sophistication des produits comme l'ont montré les affaires Barings et Société Générale. De plus, la notion de risque opérationnel apparaît de prime abord comme peu novatrice, dans la mesure où les banques n'ont pas attendu le comité de Bâle pour organiser leurs activités sous forme de procédures, et pour se doter elles-mêmes de départements d'audit interne chargés de vérifier la bonne application de ces procédures.

Toutefois, des défaillances spectaculaires, comme celle de la Barings, ont attiré l'attention des autorités de tutelle sur la nécessité de doter les banques de mécanismes de prévention et de couverture (via la constitution de fonds propres dédiés) contre les risques opérationnels.

Ainsi, pour réduire la vulnérabilité des institutions financières aux risques opérationnels, les banques élaborent des politiques et procédures qui servent de socle au dispositif de contrôle interne à l'organisation. Ces mesures de contrôles sont préventives et détectrices. Les contrôles préventifs empêchent les résultats indésirables de se produire. Une évaluation de ces contrôles internes est

alors plus que nécessaire pour s'assurer de l'efficacité de ces procédures opérationnelles ainsi que la prévention des risques liés à ces opérations.

Toute entreprise financière est confrontée à une multitude de risques de natures différentes. La gestion des risques, repose alors sur un processus séquentiel et itératif de même structure et consiste à réaliser successivement l'analyse, le traitement et le suivi de ces risques. Ainsi notre étude aura pour objectif d'évaluer le processus de gestion des risques opérationnels de la Banque afin de mieux les mitiger.

En effet, nous pouvons noter quelques problèmes que rencontre la banque dans le cadre de la gestion de ses risques opérationnels. Ce sont principalement :

- le renforcement des contraintes réglementaires ainsi que l'augmentation des attentes des directions générales et du conseil d'administration ;
- les audits approfondis réclament des évidences de plus en plus complexes à fournir ;
- les analyses mises en œuvre sont souvent globales et ne permettent pas de déduire et de traiter directement les risques opérationnels bruts.

Ces difficultés témoignent d'une certaine fragilité par rapport aux risques qui peuvent entraver le déroulement des activités opérationnelles de la banque.

La garantie d'une gestion efficace du dispositif de gestion des risques opérationnels repose sur la mise en pratique des normes conformes à la réglementation bancaire au niveau international et de l'UMOA. Ceci doit être effectué de façon permanente de sorte que le processus de gestion des risques mis en place soit en mesure d'éviter l'occurrence des risques ou de minimiser l'incidence de ces risques remettant en cause la bonne réalisation des objectifs de l'entreprise.

Nous nous posons alors une question fondamentale qui porterait une réponse à notre étude. C'est la suivante : « Le processus de gestion des risques opérationnels mis en place par la Banque lui permet-il d'identifier et maîtriser ses risques opérationnels ? » En d'autres termes :

1. Quelle est la démarche du cabinet PricewaterhouseCoopers, Côte d'Ivoire dans sa mission d'évaluation du processus de gestion des risques opérationnels de la banque ?
2. Quel est le processus de gestion des risques opérationnels dans la banque ?
3. Quels sont les forces et les faiblesses de ce processus de gestion des risques opérationnels ?
4. Quelles mesures la banque peut-elle mettre en place pour gérer au mieux ses risques opérationnels ?

Afin de trouver une réponse à toutes ces questions, notre étude sera portée sur le thème suivant : « Evaluation du processus de gestion des risques opérationnels d'une banque par le cabinet PricewaterhouseCoopers, Côte d'Ivoire ».

Notre objectif principal est d'évaluer le processus de gestion des risques opérationnels de la banque ; ce qui nous mènera aux objectifs spécifiques suivants :

1. Identifier la démarche du cabinet PricewaterhouseCoopers, Côte d'Ivoire dans sa mission d'évaluation du processus de gestion des risques opérationnels de la banque.
2. Prendre connaissance du processus de gestion des risques opérationnels de la banque.
3. Identifier les forces ainsi que des faiblesses de ce processus de gestion des risques.
4. Recommander quelques mesures à mettre en place par la banque dans le but de mieux gérer ses risques opérationnels.

Les intérêts pour ce sujet se trouvent à trois niveaux :

- Premièrement pour la banque soumise à notre étude ;

A travers cette étude, la banque pourra connaître les forces et les faiblesses de son processus de gestion des risques et si elle met en application les différentes recommandations apportées lors de l'évaluation, ceci lui permettra d'améliorer la qualité de son processus de gestion et de la conduire à l'efficacité de ses activités.

- Deuxièmement, pour le lecteur,

Notre étude sera une aide à la connaissance des méthodes d'évaluation ainsi que des bonnes pratiques en matière de gestion des risques opérationnels dans les institutions financières de façon générale.

- Enfin, pour nous même,

Car cette étude sera l'occasion pour nous d'appliquer les connaissances théoriques acquises durant nos années de formation, d'approfondir nos connaissances en matière de gestion des risques et d'avoir une idée beaucoup plus claire et approfondie sur les différents risques opérationnels qui pourraient exister au sein d'une institution bancaire de façon générale.

Dans le but d'atteindre les objectifs visés, notre travail s'articulera en deux parties :

- La première partie va comporter le cadre théorique de l'étude qui porte sur le thème de l'Evaluation du processus de gestion des risques opérationnels d'une banque par le cabinet PricewaterhouseCoopers, la méthodologie de recherche ainsi que la présentation du cadre de notre étude. Elle sera axée sur le cadre conceptuel, la revue de la littérature, sur

l'évaluation du processus de gestion des risques opérationnels, sur la méthodologie de recherche qui sera adoptée ainsi que du cadre qui nous a permis d'effectuer nos recherches.

- La deuxième partie va porter sur le cadre pratique de notre étude ; elle prend en compte la description de la banque soumise à notre étude, le dispositif de gestion des risques opérationnels de la banque soumise à notre étude, les forces et les faiblesses du processus de gestion des risques opérationnels de la Banque ainsi que les différentes recommandations apportées à la suite de notre analyse.

PREMIERE PARTIE : CADRE THEORIQUE, METHODOLOGIQUE DE LA DEMARCHE D'EVALUATION DU PROCESSUS DE GESTION DES RISQUES OPERATIONNELS D'UNE BANQUE ET PRESENTATION DE LA BANQUE SOUMISE A NOTRE ETUDE

CHAPITRE 1 : PROCESSUS DE GESTION DES RISQUES OPERATIONNELS

Section I : Cadre conceptuel de l'étude

BENOÎT (2007), indique que le risque opérationnel jusqu'à maintenant n'a pas une définition unanime permettant d'adopter une approche commune et une méthodologie unique de gestion par toutes les entreprises financières, notamment chez les banques. Le débat sur la définition a donc commencé avec le comité de Bâle qui définit les risques opérationnels comme les risques de pertes directes et indirectes résultant de l'inadéquation ou de la défaillance de procédures, de personnes et des systèmes ou résultant d'événements extérieurs. Cette définition ayant été critiquée ; notamment au regard de la difficulté de quantification de certaines pertes indirectes, le comité de Bâle pour la surveillance bancaire (1998) a donc proposé une autre définition qui soutient que : « les risques opérationnels se définissent comme le risque de pertes dues à une inadéquation ou à une défaillance des procédures, des personnels, des systèmes internes ou à des événements extérieurs ».

Cette définition inclut certes le risque juridique, mais ne prend pas forcément en compte les risques stratégiques et de réputation. Ce qui emmène VANINI (2004 : 76) à critiquer la définition de Bâle parce que selon lui, l'utilisation de cette définition sans aucune extension amènerait à des difficultés d'application dans les banques. Le risque opérationnel représentant seulement une possibilité de perte, le potentiel de gain serait négligé. La définition indique que le personnel et les systèmes sont les causes de pertes, mais elle ne prend pas en compte le fait qu'ils soient les mieux placés pour détecter les sources de pertes potentielles et lancer des avertissements.

VANINI (2004 : 77) ajoute également que cette définition sous-entend que les pertes résultant des risques opérationnels sont seulement directes alors qu'en réalité, les pertes indirectes sont comparativement plus importantes. Il apporte donc une définition plus appropriée selon lui aux risques opérationnels en indiquant que le risque opérationnel représente le risque de déviation entre le profit associé à la production d'un service et les attentes de la planification managériale. Le risque opérationnel correspond alors à l'écart enregistré, positif ou négatif, par rapport au profit attendu. La gestion du risque opérationnel doit être basée sur trois facteurs : le gain, les coûts et le risque de production des services.

A la recherche d'une relation causale entre les différents risques bancaires et une représentation plus significative des pertes, les gestionnaires ont défini le risque opérationnel selon leurs propres points de vue. JEZZINI (2005 : 2) par exemple, défini le risque opérationnel comme étant tous risques autres que les risques de crédit et de marché. Le risque opérationnel présente un caractère distinct du risque de crédit et du risque de marché ; ce qui indique que l'exposition au risque opérationnel n'est pas la contrepartie d'un gain potentiel.

KING (2001 : 54) également définit le risque opérationnel comme le risque qui « ne dépend pas de la façon de financer une entreprise, mais plutôt de la façon d'opérer son métier », et « le risque opérationnel est le lien entre l'activité du travail d'une entreprise et la variation de résultat du travail ».

Une autre approche de la définition du risque opérationnel s'appuie sur la décomposition des risques bancaires en deux grandes catégories : financiers et non financiers.

Ici, c'est WHARTON (2002 :85) qui définit le risque opérationnel comme un risque non financier ayant 3 sources :

- le risque interne ; résultant de causes internes à l'entreprise par exemple le risque de divulgation de données personnelles des clients ;
- le risque externe ; résultant de tout événement extérieur incontrôlable (ex : une attaque terroriste) ;
- et le risque stratégique (ex : un affrontement dans une guerre de prix) qui constitue selon Kuritzkes, le risque le plus important. Il est cependant ignoré par l'accord de Bâle.

1. La gestion du risque opérationnel

La gestion du risque opérationnel est un sous-ensemble de la gestion des risques que l'on pourrait identifier dans une entreprise. Elle représente une discipline qui fournit aux professionnels des risques des cadres et outils pour identifier, évaluer, surveiller et contrôler les risques opérationnels.

Le risque opérationnel est défini comme des pertes dues aux lacunes du processus, du système ou aux défaillances humaines, à des événements inattendus ou au caractère inexécutable des contrats. Cette catégorie de risques comporte des effets pervers illimités et peut exposer une institution à des pertes financières et de réputation considérable. Tel est notamment le cas des échecs enregistrés récemment par de grandes entités dans le monde.

Au même titre que les autres institutions financières, la banque s'expose à divers types de risques opérationnels. Parmi ces risques, nous pouvons citer ; les pertes opérationnelles potentielles liées aux activités internes ou les événements externes causés par les interruptions des systèmes d'information, de communication, de sécurité matérielle, de continuité des activités, de supervision, de traitement des transactions, des systèmes et procédures de règlement et l'exécution de responsabilités fiduciaires légales et de fonctions d'agence.

En vue de la bonne gestion des risques opérationnels, il est important que la banque comprenne les évènements entraînant les pertes opérationnelles et collecte l'historique de ces pertes-là afin de mettre en œuvre des mesures de gestion des risques opérationnels efficace et accord avec les réalités auxquelles la banque est confrontée.

1.1. Les événements de pertes opérationnelles

Aussi appelés incidents opérationnels, les événements de pertes opérationnelles doivent être classés dans l'une des sept catégories ci-après définies afin d'assurer la cohérence au niveau de l'identification, de l'évaluation et de la fixation des objectifs de gestion des risques opérationnels à l'échelle de l'établissement.

1.1.1. La fraude interne

Ce risque de pertes est dû à des actes intentionnels impliquant au moins une partie interne à l'établissement, visant à duper, détourner des biens appartenant à l'établissement ou à sa clientèle, manipuler des informations, contourner les règlements, la législation ou la politique de l'établissement. Nous pouvons citer comme exemple ; les détournements d'actifs, la vente fictive, etc...

1.1.2. La fraude externe

Ce risque de pertes résulte d'actes de la part d'un tiers visant à dérober des fonds ou des marchandises. Nous avons comme exemples de fraude externe :

- l'usurpation d'identité
- l'interception et falsification de factures
- l'interception et falsification de commandes, à la suite de quoi les biens ne sont pas livrés

à la bonne destination

- la falsification de voix, de signature, de courriels en vue d'usurper l'identité d'une personne et de commettre un détournement financier, etc…

1.1.3. Les risques liés aux pratiques en matière d'emploi et de sécurité sur le lieu de travail

Ces risques de pertes découlent de démarches non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, y compris les litiges ou différends entre l'établissement et ses employés.

1.1.4. Les risques liés aux pratiques concernant les clients, les produits et l'activité commerciale

Ces risques de pertes résultent d'un manquement non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients ou d'un manquement imputable à la nature ou à la conception d'un produit donné.

1.1.5. Les dommages occasionnés aux actifs physiques

Ils constituent des risques de pertes occasionnés par des destructions résultant d'une catastrophe naturelle ou provenant de causes externes.

1.1.6. Les interruptions d'activités et défaillances des systèmes

Ces risques de pertes proviennent de la non-continuité d'exploitation ou du dysfonctionnement des systèmes technologiques.

1.1.7. La mauvaise exécution des opérations, livraison et gestion des processus

Ces risques de pertes constituent un risque de pertes lié à une défaillance dans le traitement d'une transaction ou dans la gestion des processus et les pertes subies dans le cadre des relations avec les contreparties commerciales et les fournisseurs.

1.1.8. Collecte des données de pertes opérationnelles

L'établissement doit collecter les données relatives aux événements de pertes opérationnelles. Le processus relatif à ces pertes opérationnelles doit être documenté et mis à jour périodiquement. Les données de pertes collectées doivent répondre à certains critères minimaux, afin d'uniformiser le processus de collecte à l'échelle de l'établissement ainsi qu'à travers l'industrie bancaire et faciliter les analyses comparatives. Les pertes doivent être directes, intègres, intégrales et rétractables.

- La perte est directe

On dit que la perte est directe lorsque l'événement a eu une incidence négative directe reconnue sur les résultats de l'établissement et par conséquent comptabilisée. Il s'agit ici de l'ensemble des frais/dépenses internes et externes encourus par l'établissement mais qui ne l'auraient pas été sans l'événement.

Cependant, les coûts d'opportunité et les revenus manqués liés à l'événement, les coûts relatifs aux modifications apportées à un processus ou à l'ajout de contrôles post-événementiels, les coûts des programmes d'investissement réactifs ou proactifs à l'événement ne sont pas considérés comme directs.

Les éléments ci-dessous peuvent entraîner la perte directe.

- L'intégrité des données

Lorsque les données manquent d'intégrité, cela signifie que celles-ci représentent bien des pertes opérationnelles telles que définies dans la circulaire relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA.

- L'intégralité des données

Lorsque les données ne sont pas dans leur intégralité, cela veut dire que celles-ci n'incluent pas l'ensemble des pertes opérationnelles subies par l'établissement, y compris celles qui sont liées aux risques de crédit et de marché, dans la limite du seuil minimal de collecte approuvé par l'organe délibérant.

- La traçabilité

Chaque événement à l'origine des pertes doit être documenté et conservé dans une base de données, dans le respect des politiques définies par l'établissement en matière de conservation de données. La documentation doit comprendre ainsi entre autres, la référence interne du dossier, la catégorie d'événements de pertes opérationnelles, le type de risque, la description de l'incident, le montant brut de la perte, le montant recouvré, les dates de l'incident, de comptabilisation de la perte et du recouvrement ainsi que les entités ou les lignes de métiers concernées, le cas échéant.

2. Le processus de gestion des risques opérationnels

Ces dernières années, de nombreuses affaires liées aux risques opérationnels telles que la catastrophe de l'usine chimique Azote Fertilisants (AZF) de Toulouse (causant la mort de 31 personnes, faisant 2 500 blessés et de lourds dégâts matériels) ou la très récente affaire de l'Union Bank of Switzerland (UBS) (qui selon les estimations pourrait avoisiner 1,8 Milliards d'€) ont attiré l'attention des décideurs sur la nécessité de doter leurs entreprises de dispositifs préventifs.

Toutes ces crises qui, par contagion ont affecté tout le reste de l'économie, ont permis de mettre en évidence la fragilité des différents dispositifs de maîtrise des risques en vigueur dans les établissements financiers, les agences de notation et les autorités de surveillance des marchés financiers. Toutes ces crises ont conduit au renforcement de la réglementation sur la gestion des risques ces dernières années avec les accords du comité de Bâle II, MIFiD, Sarbanes - Oxley act ; la loi sur la Sécurité Financière, la lutte contre le blanchiment de capitaux et le financement du terrorisme.

En effet, il est intéressant de constater que le rythme de pilotage des risques s'est fortement accéléré ces dernières années et il devient désormais courant de voir des entreprises piloter leurs risques à des fréquences hebdomadaires voir quotidienne là où quelques années en arrière la norme était trimestrielle ou mensuelle.

Mais au-delà des bonnes intentions, Guillaume DURUPT dans « Décision Performance Conseil », (2018 :67) indique que la mise en œuvre d'une stratégie de gestion du risque se heurte souvent à des freins d'ordre psychologique. Ils représentent un champ d'application très vaste et difficilement mesurable et/ou d'ordre organisationnel qui reste un sujet généralement déjà couvert partiellement par plusieurs départements tels que l'audit interne, les équipes incidents, les secrétariats généraux.

Cependant, l'avènement et la transposition de nouvelles réglementations ne permettent pas aux entreprises d'être complètement exonérés des facteurs de risques à l'origine de ces pertes financières.

En effet, de récentes mesures prises par les Autorités américaines pour renforcer le secteur financier avec l'extension des pouvoirs de la Federal Reserve Bank ainsi que les réflexions et initiatives européennes ne pourront être efficaces que si les différents acteurs s'approprient pleinement leur système de gestion des risques.

S'approprier son dispositif de gestion des risques opérationnels reviendrait à mettre en place une démarche structurée jalonnée par un certain nombre d'étapes indispensables notamment.

2.1. Etablir une cartographie des processus métier

La première étape et sans doute la plus importante consiste à établir une cartographie des processus métiers. Qu'ils soient endogènes ou exogènes, les risques s'expriment au travers des processus ; c'est pourquoi il est indispensable de les cartographier.

En effet, réaliser une cartographie des processus consiste à représenter l'entreprise sous la forme de logigrammes cohérents (niveau des processus) intégrant l'ensemble des activités réalisées par l'entreprise ainsi que leur interdépendance.

2.2. Positionner sur chaque activité les acteurs et les systèmes d'information qui y contribuent

Dans un objectif de pilotage des risques, il est fondamental d'enrichir cette cartographie en positionnant sur chaque activité les acteurs ainsi que les systèmes qui y contribuent. Cela permettra par la suite d'identifier aisément les défaillances relatives au personnel ou aux systèmes (2 composantes majeures du risque opérationnel).

Ce travail de cartographie réalisé, l'entreprise dispose désormais d'une vision exhaustive des activités ainsi que des acteurs et des systèmes d'informations concernés.

Il s'agit maintenant d'identifier les risques opérationnels potentiellement encourus par l'organisation.

2.3. Définir la typologie des risques en fonction du profil de l'entreprise

La notion de risque opérationnel recouvrant un champ d'application très vaste, chaque entreprise doit mener sa propre réflexion afin d'identifier la typologie de risques qui correspond à son profil. Cette étape est généralement confiée à un département transverse de type Risk Management ou Audit Interne. Cela s'explique par les deux dimensions de la démarche à entreprendre :

1. La dimension interne qui consiste à identifier sur l'ensemble des processus modélisés, les risques qu'ils pourraient faire encourir à l'entreprise.
2. La dimension externe qui consiste, par l'intermédiaire d'un benchmark sectoriel (recensement des incidents ayant eu lieu sur des activités similaires aux nôtres) à compléter et ou à valider l'approche interne.

   Le travail de benchmark, bien que long et fastidieux, se doit d'être mené. En effet, celui-ci permet d'une part de garantir l'exhaustivité des risques identifiés mais il permettra ultérieurement d'enrichir considérablement la base historique des incidents avec l'ensemble des incidents qui ont eu lieu au sein d'entreprises qui encourent les mêmes risques.

2.4. Positionnement sur chaque activité les risques opérationnels associés

Pour chaque activité identifiée dans la cartographie des processus, il faut maintenant y associer les risques correspondants. Il conviendra par exemple d'associer à une activité de paiement, un risque de fraude ainsi qu'un risque de non-paiement. Ce travail collaboratif associe d'une part les responsables opérationnels qui deviennent ainsi des « process-owner » et d'autre part les correspondants risques locaux, garants de la bonne utilisation de la typologie de risque.

La cartographie des processus est désormais enrichie de l'ensemble des risques potentiels générés par les activités que l'entreprise exerce.

2.5. Recenser les incidents, évaluer les risques et définir le niveau de risque "acceptable"

Cette étape consiste à recenser les incidents survenus par le passé au sein de l'entreprise. Cela nécessite la mise en place d'une base de données de gestion des incidents qui sera renseignée de manière déclarative par les correspondants risques locaux. Cette base de données sera ensuite

enrichie par l'équipe centrale (Risk Management ou Audit Interne) qui aura mené en amont le benchmark sectoriel évoqué précédemment. Pour étayer l'importance de ce benchmark, prenons le tragique exemple de la centrale de Fukushima ; il apparaît évident que chaque centrale en bordure de mer se doit d'en tirer les leçons et d'intégrer le risque de Tsunami dans son référentiel de risque opérationnel. Pour être pleinement exploitable cette base de recensement des incidents doit s'aligner sur la cartographie des processus. Chaque incident devra donc être renseigné en précisant l'activité et le risque concerné.

L'analyse de cette base des incidents, associée à la connaissance des responsables opérationnels, doit permettre d'évaluer les risques. Cette évaluation passe notamment par la définition des Key Risk Indicators (KRI) : éléments quantitatifs susceptibles d'augmenter la probabilité de réalisation d'un risque.

Enfin, au regard de ces informations, l'entreprise doit déterminer le niveau de risque qu'elle juge 'acceptable', permettant ainsi de dimensionner les mesures de contrôles à mettre en place.

2.6. Définir et mettre en œuvre le plan de contrôle au regard du niveau de risque défini comme "acceptable"

Une fois le niveau d'acceptabilité du risque défini, la phase suivante consiste à déployer sur l'ensemble des activités de l'entreprise un plan de contrôle permettant de maîtriser ces risques.

Afin d'en garantir une parfaite couverture, chaque binôme 'activité – risque' modélisé devra faire l'objet d'un ou plusieurs contrôles. Ces contrôles seront ensuite intégrés au sein de la cartographie.

2.7. Piloter le plan de contrôle

Le plan de contrôle (ensemble des contrôles précédemment identifiés) doit être piloté par les opérationnels en charge des activités. La fréquence des contrôles est définie en fonction du niveau de risque et de la fréquence même de l'activité.

Ce pilotage peut être formalisé à travers différents dispositifs :

- Reporting a posteriori (du contrôle). Cela permet de s'assurer de la bonne réalisation du contrôle sans toutefois rendre possible le lancement des procédures d'urgences permettant d'éviter l'incident.

- Alerte temps réel (pendant le contrôle). Ce dispositif d'alerte permet d'agir au moment auquel survient la défaillance et permet donc potentiellement d'éviter que celle-ci se transforme en incident.

Le dispositif d'alerte temps réel paraît être la solution idéale de prime abord ; toutefois sa mise en œuvre s'avère souvent très lourde et très coûteuse (ex : automatisation des contrôles au sein des systèmes de production et couplage avec un système de reporting en temps réel pour une remontée automatique des alertes).

A l'échelle d'une entreprise, il n'est pas rare de voir les deux systèmes coexister. Un compromis intéressant consiste à piloter les activités très risquées et fortement automatisées via un dispositif d'alerte temps réel ; le reste des activités étant piloté via un reporting de contrôles a posteriori.

Section II : Les forces et les faiblesses potentielles d'un processus de gestion des risques opérationnels

L'identification et l'analyse des forces et faiblesses d'un processus de gestion est une méthode de planification stratégique utilisée pour évaluer les opportunités internes de l'institution. En effet, elle permet de développer un contrôle et un suivi viable du processus.

L'évaluation du processus de gestion des risques opérationnels dans notre étude consistera au rapprochement entre l'existant (le processus de gestion des risques opérationnels de la banque soumise à notre évaluation) et les saines pratiques en matière de gestion des risques opérationnels. Cela nous a permis de mettre en évidence les principales forces et faiblesses du système.

1. Les notions de forces et faiblesses du processus de gestion des risques opérationnels

L'efficacité d'un système de contrôle de façon générale suppose d'abord l'efficacité des acteurs participants à ce dispositif. Ainsi, nous pouvons distinguer deux grandes catégories d'acteurs notamment ; les collaborateurs internes de l'entreprise sous la responsabilité de la direction générale qui doit proposer une organisation respectant les grands principes de cette fonction ainsi que les acteurs externes à l'entreprise exerçant pour la plupart une mission réglementaire de

surveillance des établissements financiers. Un diagnostic est donc obligatoire afin d'obtenir un état des lieux précis à un moment donné. Il tourne autour de deux questions majeures :

- La première concerne l'environnement de l'entreprise qui relève du diagnostic externe ;
- La deuxième concerne ses propres capacités à affronter cet environnement et relève du diagnostic interne ; c'est-à-dire les forces et les faiblesses qui représentent le facteur sur lequel nous allons orienter notre analyse.

En vue de la bonne gestion des risques de façon générale liés aux activités bancaires, la Circulaire n°01-2017/CB/C relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA fixe les règles minimales en matière de gouvernance. Cette régulation doit être observée par les établissements financiers à caractère bancaire en activité dans l'UMOA, tel que cela est défini dans l'article 2 de la circulaire.

Ainsi, le cas soumis à notre étude étant une institution bancaire, se doit de respecter les règles établies par la circulaire. L'application donc des règles établies par la circulaire constitueront des forces du processus de gestion des risques de la banque et le non-respect de ces règles cependant formeront des faiblesses au processus de gestion des risques opérationnels.

2. Les forces du processus de gestion des risques opérationnels

Un dispositif de gouvernance efficace repose sur des principes qui lui permettent de gérer au mieux ses risques opérationnels en vue de les mitiger.

2.1. Le principe de proportionnalité

Ce principe indique que l'établissement bancaire doit d'une part, mettre en place un dispositif de gouvernance conforme aux saines pratiques et adapté à sa taille, sa structure, la nature et la complexité de ses activités ainsi qu'à son profil de risque et, le cas échéant, à celui du groupe auquel il appartient. En effet, le dispositif de gestion des risques opérationnels de la banque doit correspondre exactement aux activités ainsi qu'à l'environnement interne de l'entreprise au risque de ne pas pouvoir répondre de façon adéquate aux besoins de l'institution.

Un établissement bancaire d'importance systémique régionale ou nationale doit disposer d'autre part, d'un cadre de gouvernance adapté à son envergure et aux conséquences de sa défaillance éventuelle sur la stabilité du système financier de l'UMOA ou de son Etat d'implantation.

Il est important pour la banque de pouvoir identifier sa position sur le marché ainsi que son niveau d'instabilité potentielle dans le but de la mise en place d'un dispositif de gouvernance qui permettra de palier à ces défaillances.

2.2.Les principes généraux de gouvernance

2.2.1. La sécurité des systèmes d'information

Un dispositif de gouvernance efficace qui permet la bonne maîtrise du processus de gestion des risques opérationnels doit être élaboré et mis en œuvre en tenant compte notamment de la sécurité des systèmes d'information mis en place par la banque, la couverture de l'ensemble des risques encourus par l'établissement financier et des éventuels conflits d'intérêts au sein de la structure financière.

2.2.2. La formalisation des stratégies, politiques et procédures

La banque doit établir et formaliser ses stratégies, politiques et procédures à mettre en place au sein de l'entité dans le but de définir et organiser les divers moyens nécessaires à l'atteinte d'une saine gouvernance.

2.2.3. La définition des rôles et obligations des intervenants

La banque doit définir les rôles et les obligations de chaque employé et dirigeant intervenant dans les processus opérationnels de l'institution afin de promouvoir la séparation des tâches et que ces différents intervenants sachent exactement leurs missions au sein des processus de la banque.

2.2.4. Réponse aux besoins de l'établissement

Le dispositif de gouvernance mis en place par la banque doit pouvoir répondre aux besoins de la structure financière dans son ensemble ainsi que de chacune de ses unités organisationnelles et opérationnelles.

2.2.5. Intégration de mécanismes en cas de discontinuité

La banque doit prévoir dans son dispositif de gouvernance des méthodes que l'institution mettra en place en vue de maintenir et/ou de rétablir son fonctionnement en cas de discontinuité d'exploitation.

2.2.6. Refléter les changements

La structure bancaire doit refléter, au fil du temps, les changements qui découlent de ses caractéristiques et de son environnement externe ainsi que des évolutions relatives aux meilleures pratiques en matière de gouvernance afin d'adapter son processus de gestion des risques opérationnels en vue de mieux gérer ses activités.

2.2.7. L'intégrité et de l'engagement des intervenants

L'entité doit prévoir des mécanismes permettant de s'assurer de l'intégrité et de l'engagement des employés et dirigeants de la banque, intervenants dans la gestion du dispositif de gouvernance. Ceux-ci doivent être en nombre suffisant, compétents et avoir une bonne connaissance des activités de l'établissement, de ses risques ainsi que de ses obligations juridiques. Tout ceci dans le but de travailler dans l'atteinte les objectifs fixés par la banque en matière de gestion de ses risques opérationnels.

3. Les faiblesses du processus de gestion des risques opérationnels

Le non-respect des principes de bonne gouvernance des établissements financiers et de crédit, tel qu'indiqué dans la circulaire n°01-2017/CB/C relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA pourrait engendrer des faiblesses dans le processus de gestion des risques opérationnels de la banque.

Parmi ces faiblesses, nous pouvons noter à titre d'exemple ;

- la non-conformité du processus de gestion des risques opérationnels aux saines pratiques en matière de gestion des risques opérationnels en banque.
- le dispositif de gestion des risques opérationnels est non-adapté à la taille, la structure, la nature, à la complexité de des activités et au profil de risque de la banque.
- Le non-respect de l'envergure et des conséquences de la défaillance éventuelle de la banque.

- Un cadre de gouvernance non-adapté à la stabilité du système financier de l'UMOA ou de son Etat d'implantation
- des systèmes d'information non-sécurisés ;
- les procédures, stratégies et la politique de l'entreprise ne sont pas formalisés ;
- les rôles et obligations des intervenants ne sont pas clairement définis ;
- le dispositif de gouvernance ne répondant pas aux besoins de l'entreprise ;
- la banque n'a prévu aucune mesure qui permette de rétablir son activité ou son fonctionnement en cas de discontinuité d'exploitation ;
- le changement dans l'environnement interne et / ou externe de l'entreprise n'es pas intégré dans les activités de l'entreprise ;
- l'intégrité et l'engagement des employés et dirigeants intervenant dans la gestion du dispositif de gouvernance de l'entité sont douteux.

Pour faciliter le suivi et l'évolution des activités de l'entreprise pour la minimisation des risques opérationnels probables, il est primordial pour toute entreprise financière de mettre en place un processus de gestion de ces risques.

En effet, la banque se doit de respecter les règlementations bancaires mises en place en vue de la bonne gestion et maîtrise de ses processus de façon générale et plus précisément, de son processus de gestion des risques opérationnels.

Dans le chapitre suivant, qui constitue le second chapitre de notre étude, nous allons d'abord présenter la démarche méthodologique de l'évaluation du processus de gestion des risques opérationnels dans la Banque. Ensuite, nous allons présenter la démarche mise en œuvre dans le cadre de notre mission d'évaluation du processus de gestion des risques opérationnels.

CHAPITRE II : DEMARCHE METHODOLOGIQUE ET CADRE DE L'ETUDE

Après avoir présenté les forces et les faiblesses du processus de gestion des risques opérationnels, l'objectif de ce chapitre est de définir dans un premier temps les différentes analyses que nous effectuerons dans le cadre de l'évaluation du processus de gestion des risques opérationnels. Nous présenterons dans un deuxième temps les outils de collecte et d'analyse des données. Enfin, nous exposerons le cadre de notre étude.

SECTION I : Démarche méthodologique de l'étude

1. Le modèle d'analyse

Le modèle d'analyse adopté se déroule en trois (3) niveaux sur la base des outils sélectionnés de notre choix en vue d'une démarche d'évaluation analytique et de la présentation de recommandations pertinentes. Ces différents modèles décrivent ainsi notre étude méthodologique pour le traitement de cette thématique.

Ce sont : l'évaluation de la gouvernance, l'évaluation de la fonction de gestion des risques et l'évaluation du dispositif de gestion des risques.

1.1. L'évaluation de la gouvernance

1.1.1. Principes de bonne gouvernance des comités mis en place

La circulaire n°01-2017/cb/c relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA indique que l'organe délibérant fixe, par écrit, le mandat et la composition des comités spécialisés. Il veille à ce que lesdits comités interagissent et lui rendent compte au moins deux fois par an.

Ces comités doivent être composés exclusivement d'administrateurs non-exécutifs et majoritairement d'administrateurs indépendants. Un administrateur ne peut appartenir à plus de deux comités spécialisés à la fois.

Le Président de chaque comité spécialisé est choisi parmi les membres dudit comité. Il ne peut être le Président de l'organe délibérant ou d'un autre comité. Il doit disposer de connaissances approfondies dans le domaine d'activité du comité qu'il préside.

Chaque comité spécialisé doit disposer d'une charte ou d'un document équivalent retraçant son mandat, l'étendue de ses travaux et les modalités de son fonctionnement. Les comités spécialisés se réunissent, au moins deux fois par an, et en tant que de besoin. Les délibérations, décisions et recommandations des réunions ainsi que les opinions divergentes exprimées sont consignées dans un procès-verbal ou compte-rendu signé du Président du Comité. L'établissement doit adopter un système de rotation périodique des sièges et de la présidence de ces comités.

1.1.2. Description, composition et fonctionnement des comités

1.1.2.1. Le comité d'audit

Selon la circulaire n°1, le comité d'audit est chargé d'assister l'organe délibérant dans les domaines de l'information financière, du contrôle interne, y compris l'audit interne. Le secrétariat du comité d'audit est assuré par le responsable de la fonction audit.

Le comité d'audit doit notamment :

- être composé de membres disposant collectivement d'une expérience avérée dans le domaine de l'audit, de l'information financière et de la comptabilité ;
- procéder à l'examen des comptes et s'assurer de la pertinence et de la permanence des méthodes comptables adoptées par l'établissement ;
- surveiller le processus d'élaboration de l'information financière ;
- examiner les performances périodiques, notamment les états périodiques d'exécution du budget et du plan d'affaires, analyser les écarts et proposer des ajustements, le cas échéant ;
- approuver les procédures de contrôle interne et assurer le suivi de leur efficacité ;
- superviser, examiner et approuver les programmes d'audit interne et externe de l'établissement ;
- proposer ou recommander à l'organe délibérant ou aux actionnaires, pour approbation, la nomination, la rémunération et la révocation des commissaires aux comptes selon les voies appropriées ;

- réexaminer et approuver le périmètre et la fréquence des audits interne et externe ;
- être destinataire des rapports d'audit ainsi que de ceux des commissaires aux comptes et de la Commission Bancaire. Il doit s'assurer que l'organe exécutif prend sans délai des mesures pour remédier aux déficiences de contrôle interne relevées, sanctionne le non-respect des politiques et textes juridiques en vigueur et résout tout autre problème identifié ;
- tenir au moins deux réunions par an sur la base d'un rapport préparé par la structure chargée de l'audit interne, intégrant les activités des fonctions audit interne et conformité. Les réunions sont sanctionnées par un procès-verbal ou un compte rendu soumis à l'organe délibérant. Ce procès-verbal ou compte rendu doit faire ressortir les principales anomalies relevées et les recommandations du comité d'audit assorties d'échéances de mise en œuvre.

1.1.2.2. Le comité des risques

La circulaire n°1 indique également que le comité des risques est chargé d'assister l'organe délibérant dans sa mission de surveillance de la mise en œuvre du dispositif de gestion des risques de l'établissement. Pour l'exercice de ses attributions, le comité des risques doit être composé de membres disposant d'une expérience avérée en matière de gestion des risques. Le secrétariat du comité des risques est assuré par le responsable de la fonction risque.

Le comité des risques doit notamment :

- participer à l'élaboration des stratégies de gestion des risques de l'établissement et procéder annuellement à leur examen, à la fois sur une base agrégée, et par type de risques ;
- veiller à ce que l'organe exécutif mette en place des procédures visant à promouvoir la mise en œuvre effective des stratégies et politiques par les unités concernées de l'établissement ;
- réviser, au moins une fois par an, les politiques et procédures de risques de l'établissement au regard des évolutions enregistrées dans ses activités et s'assurer qu'elles sont adaptées aux stratégies et au degré d'appétence pour le risque approuvés par l'organe délibérant ;
- veiller à ce que l'organe exécutif prenne les mesures nécessaires pour contrôler et maîtriser tous les risques significatifs conformément aux stratégies et degré d'appétence pour le risque qui ont été approuvés ;
- s'assurer de la mise en place d'une saine culture de la gestion des risques à l'échelle de l'établissement ;

- avoir une bonne connaissance de la nature et de l'ampleur des risques encourus par l'établissement, les interrelations qui existent entre ces différents risques ainsi que les niveaux de fonds propres et de liquidité requis pour couvrir ces expositions ;
- exiger de l'organe exécutif un rapport, au moins semestriel, sur les risques significatifs auxquels l'établissement est exposé, l'état actuel de la culture du risque, le degré d'utilisation de l'appétence pour le risque, à savoir la gestion des limites de risque, les dépassements de ces limites et les mesures d'atténuation mises en place.
- s'assurer de la mise en place, au sein de l'établissement, d'un dispositif de gestion intégrée des risques conforme aux exigences énoncées dans la Circulaire relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA ;
- soumettre à l'organe délibérant, pour approbation, des propositions relatives au degré d'appétence pour le risque actuel et futur à l'échelle de l'établissement ainsi que les limites en matière, notamment, d'octroi de crédits, d'investissements et de concentration ;

1.1.2.3. Le comité de rémunération

La circulaire n°1 indique que le comité de rémunération est chargé d'assister l'organe délibérant dans sa mission relative à la rémunération du directeur général, des administrateurs, des autres membres de l'organe exécutif et des cadres supérieurs de l'établissement.

Le comité de rémunération doit au minimum :

- élaborer la politique de rémunération des administrateurs, des membres de l'organe exécutif et des cadres supérieurs de l'établissement ;
- surveiller l'élaboration et la mise en œuvre du système de rémunération de l'établissement ;
- veiller à ce que ce système soit approprié et cohérent avec la culture et l'appétence pour le risque de l'établissement, ses activités à long terme, sa stratégie de gestion des risques à long terme, sa performance ainsi que son système de contrôle interne ;
- s'assurer que ce système est en conformité avec toutes les exigences légales et réglementaires ;
- examiner, analyser et suivre, au moins une fois par an, les plans, les procédures et les résultats du système de rémunération à l'échelle de l'établissement afin de déterminer s'il crée les incitations permettant une bonne gestion des risques, des fonds propres et de la

liquidité ;

- travailler en étroite collaboration avec le comité des risques qui doit également déterminer si les incitations générées par le système de rémunération tiennent dûment compte du profil de risque de l'établissement, de ses besoins de fonds propres et de liquidité ainsi que la prévision de ses revenus.

1.1.2.4. Le comité de nomination

Le comité de nomination est chargé d'assister l'organe délibérant dans le processus de sélection de nouveaux administrateurs et de nomination des membres de l'organe exécutif.

- s'assurer, en permanence, du bon fonctionnement des dispositifs de contrôle interne et de gestion des risques et prendre des mesures nécessaires pour remédier, en temps opportun, à toute carence ou insuffisance relevée ;
- s'assurer que les rôles et les obligations des différentes fonctions au sein de l'organe exécutif, y compris ceux du Directeur Général, sont clairement délimités ;
- œuvrer pour l'adhésion de l'ensemble du personnel aux principes d'éthique et de professionnalisme ainsi qu'aux saines pratiques en matière de gouvernance ;
- entretenir des relations régulières avec la Commission Bancaire et les autres superviseurs.

Dans l'évaluation de la gouvernance de la Banque, nous avons procédé à des entretiens, à l'observation des pratiques de la banque ainsi qu'à une analyse documentaire à travers le rapprochement de pièces justificatives avec les éléments observés ou entendus lors des entretiens. Tout ceci dans le but de nous assurer que l'institution financière soumise à notre étude est en accord avec les règles établies par la circulaire n°1-2017/cb/c relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA citées ci-dessus.

1.2. L'évaluation de la fonction de gestion des risques

Pour une excellente gestion des risques opérationnels, la mise en œuvre d'une étude particulière s'avère indispensable. Le respect de ces quelques étapes permet donc à l'entité d'assurer sa gestion des risques de sorte qu'ils ne puissent pas constituer de barrières pour les projets de la structure.

En effet, dans le cadre de notre analyse, nous procèderons à l'évaluation de la fonction de gestion de risques de la Banque après avoir évalué la gouvernance de l'entreprise.
Nous nous assurerons à travers des entretiens, l'observation des pratiques de la banque, ainsi qu'à travers l'analyse documentaire que les étapes citées ci-dessous sont effectivement prises en compte par la fonction de gestion des risques de la Banque.

1.2.1. L'identification des risques opérationnels

Dans cette première étape de gestion des risques opérationnels, la banque procède au recensement de toutes les fonctions de l'institution exposées au risque. Dans cette optique, l'entreprise établit une liste contenant tous les risques potentiels et distingue ensuite les risques les plus importants d'un côté et les moins importants de l'autre côté. Elle pourra donc analyser leur corrélation.

1.2.2. L'évaluation, la hiérarchisation et la cartographie des risques opérationnels

L'évaluation, La seconde étape consiste pour la banque à l'évaluation de ses risques identifiés dans la première étape en fonction de leur gravité afin d'identifier leur impact potentiel et l'étendue des préjudices y afférents. En effet, ces risques sont évalués selon leur probabilité de survenance, leur impact potentiel et éventuellement selon le niveau de maitrise actuel. Cette évaluation sert alors de base à leur présentation synthétique sous une forme hiérarchisée appelée la cartographie des risques.

À part cela, elle permet de mesurer les coûts associés aux risques identifiés. Pour la réaliser, l'institution devra procéder à une collecte de données et à des analyses statistiques.

1.2.3. Définition des solutions

Après avoir évalué, hiérarchisé et cartographié ses risques opérationnels potentiels, la banque dans cette troisième étape va déterminer plusieurs solutions envisageables afin d'identifier la plus adaptée.
Elle pourra soit définir la solution en fonction du risque lui-même ; en étudiant la possibilité d'une élimination ou d'une limitation de ses effets ou tenir compte des caractéristiques du projet et y appliquer quelques modifications afin de réduire ou esquiver ces risques opérationnels potentiels.

1.2.4. La mise en œuvre des solutions

Après avoir déterminé la solution la plus adaptée, la Banque doit procéder dans cette quatrième étape à sa mise en application. Il s'avère important de définir le coût de mise en œuvre de la solution en fonction des moyens dont dispose la banque.

1.2.5. Le contrôle

La gestion des risques nécessite un suivi régulier. Ce suivi vise à garantir la fiabilité de chaque étape. Cela permet de mettre en place des solutions à moyen et à long terme.

1.3. L'évaluation du dispositif de contrôle interne

Le référentiel COSO définit le contrôle interne comme un processus mis en œuvre par les dirigeants à tous les niveaux de l'entreprise et destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants :

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

Selon le COSO, un dispositif de contrôle interne efficace est basé sur cinq (5) composantes que la Banque devrait respecter dans le but d'atteindre ses objectifs de performance. Dans le cadre de notre mission d'évaluation, nous allons d'une part nous assurer que la banque a effectivement mis en place un dispositif de contrôle interne qui est en accord avec ce qu'indique le référentiel COSO.

Ces cinq composantes sont les suivantes :

- **l'environnement de contrôle**

Plusieurs éléments sont indispensables à la banque afin de s'assurer qu'elle dispose d'un environnement de contrôle efficace.

Premièrement, la banque doit démontrer son engagement en faveur de l'intégrité et des valeurs éthiques. Ensuite, le conseil d'administration doit faire preuve d'indépendance vis-à-vis du management dans sa mission de surveillance de la mise en place et du bon fonctionnement du système de contrôle interne. La direction de la Banque, agissant sous la surveillance du conseil

d'administration, troisièmement doit définir les structures, les rattachements, ainsi que les pouvoirs et les responsabilités appropriés pour permettre à la banque d'atteindre ses objectifs.

L'organisation bancaire démontre ainsi son engagement à attirer, former et fidéliser des collaborateurs compétents conformément aux objectifs, instaurant également pour chacun de ses employés et dirigeants un devoir de rendre compte de leurs responsabilités en matière de contrôle interne.

- **l'évaluation des risques**

- l'organisation spécifie les objectifs de façon suffisamment claire pour permettre l'identification et l'évaluation des risques associés aux objectifs.

- l'organisation identifie les risques associés à la réalisation de ses objectifs dans l'ensemble de son périmètre de responsabilité et elle procède à leur analyse de façon à déterminer les modalités de gestion des risques appropriées.

- l'organisation intègre le risque de fraude dans son évaluation des risques susceptibles de compromettre la réalisation des objectifs.

- l'organisation identifie et évalue les changements qui pourraient avoir un impact significatif sur le système de contrôle

- **les activités de contrôle**

- l'organisation sélectionne et développe les activités de contrôle qui contribuent à ramener à des niveaux acceptables les risques associés à la réalisation des objectifs.

- l'organisation sélectionne et développe des activités de contrôle général en matière de système d'information pour faciliter la réalisation des objectifs.

- l'organisation met en place les activités de contrôle par le biais de directives qui précisent les objectifs poursuivis, et de procédures qui mettent en œuvre ces directives.

- **l'information et la communication**

- l'organisation obtient ou génère puis utilise des informations pertinentes et de qualité pour faciliter le fonctionnement des autres composantes du contrôle interne.

- l'organisation communique en interne les informations nécessaires au bon fonctionnement des autres composantes du contrôle interne, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne.

- l'organisation communique avec les tiers au sujet des facteurs qui affectent le bon fonctionnement des autres composantes du contrôle interne.

- **le pilotage**

- l'organisation sélectionne, met au point et réalise des évaluations continues et/ou ponctuelles afin de vérifier si les composantes du contrôle interne sont bien mises en place et fonctionnent.

- l'organisation évalue et communique les faiblesses de contrôle interne en temps voulu aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration.

Dans un deuxième temps, nous aurons trois (3) étapes tel que définies dans la figure 3 ci-dessous qui nous permettront la bonne évaluation du contrôle interne de la banque.

Tableau 1 : modèle d'analyse du dispositif de contrôle interne

PHASES	**ETAPES**	**OUTILS**
Préparation	Prise de connaissance générale et description des processus	1. Entretien 2. Observation 3. Analyse documentaire
Planification	Analyse du processus	1. Narration 2. QCI 3. Grille d'analyse des tâches
	Identification des forces du processus	1. Tests de permanence 2. Tests d'études qualitatives et quantitatives de la Criticité
	Identification des faiblesses du processus	
	Evaluation et matrice des forces et faiblesses liées au processus de gestion des risques opérationnels	
Plan d'actions	Actions à mener face aux forces et faiblesses du processus	**1.** Recommandations pour la maîtrise du processus

Source : nous-mêmes

Aussi, une bonne gestion d'un dispositif de contrôle interne permettant d'atteindre des objectifs de performance repose sur la mise en place de processus métiers et d'un système d'information efficace. Dans notre évaluation, nous allons nous assurer que la Banque a effectivement mis en place ses processus métier et un système d'information adapté aux activités de la banque qu'elle gère efficacement.

La gestion des processus métiers consiste à concevoir, maîtriser, faire évoluer et améliorer les processus, dans une perspective d'alignement stratégique. L'objectif recherché est qu'ils apportent de la valeur à l'entreprise, tout en contribuant à traduire concrètement ses orientations stratégiques. C'est ce que vise notamment le courant de la re-configuration des processus. De son côté, le courant de la maturité des processus recherche un meilleur contrôle des processus. Différents référentiels ont ainsi été proposés, en particulier pour les processus liés aux métiers des systèmes d'information (développement de logiciel, fourniture de services informatiques, management des S.I.). Un des moyens de mieux maîtriser le système d'information global de l'entreprise consiste à le restructurer de façon urbanisée, ce qui implique une cartographie des processus.

1.3.1. Les processus métier

La gouvernance des processus correspond à une volonté de placer sous contrôle la mise en œuvre et le fonctionnement des processus. Elle s'inscrit généralement dans une perspective d'amélioration continue. En effet, depuis la fin du XXe siècle, toute Organisation est poussée à s'adapter aux fluctuations de ses environnements. La banque doit non seulement définir et mettre en place les processus, mais également les faire évoluer au gré des nouvelles orientations stratégiques et organisationnelles. Les normes (ISO 9000, ISO 10006) préconisent que la performance de ces processus métiers doivent être évalués régulièrement en vue de les améliorer. Ainsi, le but de notre évaluation sera de s'assurer que la Banque, dans son objectif d'amélioration continue a mis en place ses processus métiers qu'elle gère et évalue régulièrement. Le cycle d'amélioration est divisé en quatre phases : Planifier (Plan) – Faire (Do) – Vérifier (Check) – Agir (Act).

- **Planification (Plan)** : La banque commence par planifier une action d'amélioration. Cela peut demander de recueillir des informations ou des mesures concernant le processus. Il faut alors déterminer de façon précise les buts de l'amélioration, ainsi que les méthodes pour les atteindre.

- **Exécution (Do) :** Elle met en œuvre ensuite, un plan d'amélioration. Cela se traduit souvent par des actions participatives : rechercher des solutions d'amélioration, implémenter un changement, communiquer, former, définir des métriques pour mesurer l'atteinte des buts.
- **Vérification (Check) :** La banque vérifie l'effet du changement, en utilisant les métriques précédemment définies, et on analyse les résultats. Si les buts n'ont pas été atteints, on revient sur la phase de planification, puis sur la phase d'exécution.
- **Action (Act) :** Dans cette étape, la Banque fait le nécessaire pour assurer la pérennité de l'amélioration ou bien initier une nouvelle amélioration basée sur les contrôles de la phase précédente. Cela conduit à des actions de communication officielle permettant d'institutionnaliser le changement ou à des orientations pour un nouveau tour de roue.

1.3.2. Les systèmes d'informations

Le système d'information (SI) est un élément central d'une entreprise ou d'une organisation. Il permet aux différents acteurs de véhiculer des informations et de communiquer grâce à un ensemble de ressources matérielles, humaines et logicielles. Un SI permet de créer, collecter, stocker, traiter, modifier des informations sous divers formats. L'objectif d'un SI est de restituer une information à la bonne personne et au bon moment sous le format approprié. En entreprise, la bonne gestion du système d'information permet à l'entité d'assurer la sécurité physique et logique des biens et des personnes. Elle permet également de gérer les changements qui surviennent au cours de l'activité.

Ainsi, dans notre mission d'évaluation du processus de gestion des risques opérationnels, nous allons nous assurer par le biais de certains membres de notre équipe, spécialisés dans ce domaine (l'équipe du BAS) que la Banque a effectivement mis en place un système d'information efficace qui permet la gestion effective des activités de l'entité.

2. Outils de collecte et d'analyse des données

C'est l'ensemble des outils que nous avons utilisé pour collecter et analyser les données relatives au processus de gestion des risques opérationnels de la Banque tels qu'identifiés dans la figure ci-dessous.

Un outil étant un moyen ou une technique servant à la réalisation d'un processus ou d'une tâche. Les outils tels que décrits plus bas nous paraissent mieux appropriés pour recueillir et analyser les données.

2.1. Les outils de collecte des données

Lors de notre évaluation, nous avons utilisé les différents outils de collecte des données ci-dessous.

2.1.1. Interviews (guide d'entretien)

« Une interview est un entretien avec une personne en vue de l'interroger sur ses actes, ses idées et de divulguer la teneur de l'entretien », SCHICK (2008 : 181). Le guide d'entretien est soit directif, soit non directif. Dans le cadre de cette étude, nos répondants sont le Directeur du Département d'Audit Interne et nous utiliserons tour à tour les deux techniques ci-dessus évoquées.

Par un questionnaire composé d'une question principale et des questions spécifiques que nous avons élaboré, nous avons procédé au face à face avec nos répondants pour effectuer l'entretien selon un rendez-vous pris à une période convenue avec nos interlocuteurs. Les réponses obtenues nous ont permis de comprendre et d'organiser notre domaine d'études et de préparer aussi l'élaboration du Questionnaire de Contrôle Interne (QCI).

2.1.2. Observation

Au cours de la mission d'évaluation du processus de gestion des risques opérationnels, nous avons eu l'opportunité d'être présents sur les lieux pendant deux (2) semaines. En effet, notre présence physique au sein de la banque nous a permis d'observer de nous-même ce qui nous avait été dit durant l'entretien afin d'en tirer des conclusions. L'observation nous a donc permis de valider les entretiens.

2.2. Les outils d'analyse des données

En vue de mener à bien l'analyse des données collectées, nous avons utilisé des outils d'analyse, notamment :

2.2.1. Narration

C'est la description simple des fonctions de l'activité par une technique d'investigation, par un « face à face », une écoute attentive avec les principaux acteurs ou interlocuteurs et une validation des informations collectées avec ces derniers.

2.2.1.1. Questionnaire de contrôle interne

Cet outil nous permet d'apprécier le dispositif de contrôle interne mis en place, de constater les forces et faiblesses du dispositif, de confirmer ou d'infirmer les tests de conformité et de permanence liés au processus.

Cet outil composé de questions- types nous permettra de relever les forces et les faiblesses des dispositifs du Contrôle interne à travers les réponses « oui » et « non » données par nos interlocuteurs. Le « face à face » sera utilisé pour collecter les réponses de nos répondants et relatives aux questions dans le QCI que nous avons élaborées.

2.2.1.2. Grille d'analyse et de séparation des tâches

Elle décrit la répartition du travail et décèle les éventuels cumuls de fonctions incompatibles afin d'y remédier OBERT, (2004 : 77). Cet outil aura pour particularité de nous permettre de déterminer l'incompatibilité des tâches du processus, et complètera les autres précédemment décrits pour nous permettre d'atteindre nos objectifs prédéfinis. Par ailleurs, la narration et le guide d'entretien serviront à établir la grille de séparation des tâches. Pour réaliser notre grille, nous aurons à mettre en relation toutes les activités du processus étudiés avec les personnes concernées, ensuite préciser les tâches des uns et des autres afin de déceler les éventuelles accumulations de tâches sources de risques.

2.2.1.3. Test de conformité

Ils permettent de s'assurer de l'application du dispositif décrit lors de l'entretien et de sa conformité à la réalité d'une part et d'autre part du fonctionnent des points forts théoriques de façon permanente tel que prévu dans le manuel de procédures HAMZAOUI, (2008 : 196).

2.2.1.4. Test d'efficacité

Il est constitué des tests de survenance et de fréquence. Ils ont pour objectif de s'assurer de l'efficacité du dispositif de contrôle interne. Ils permettent de garantir ou d'infirmer le degré de confiance accordé au dispositif de contrôle interne à travers la survenance des événements à risques et la fréquence avec laquelle ils sont survenus.

2.2.1.5. Tableau d'identification des risques

Il permet d'identifier les risques opérationnels à travers un découpage du processus en des tâches ou étapes élémentaires selon RENARD (2008 : 220- 222). Il nous facilitera l'élaboration du QCI.

Tableau 2 : Modèle d'analyse des travaux d'évaluation du processus de gestion des risques opérationnels d'une banque par le cabinet PricewaterhouseCoopers, Côte d'Ivoire.

Phases	Etapes	Outils d'analyses et/ou de collecte de données
Phase de préparation	Prise de connaissance de la banque soumise à notre étude	- Questionnaires -Analyse documentaire -Entretien -Observations
	Evaluation du dispositif de gouvernance de la banque soumise à notre étude	
	Evaluation du dispositif de gestion des risques de la banque soumise à notre étude	
	Evaluation du dispositif de contrôle interne de la banque soumise à notre étude	
Phase d'analyse	Identification des forces et des faiblesses du processus de gestion des risques opérationnels de la banque soumise à notre étude	Analyse documentaire
Phase de finalisation	Recommandations pour une meilleure gestion du processus de gestion des risques opérationnels de la banque	-Analyse des forces et faiblesses -Commentaires personnels

Source : Nous-mêmes

Section II : Cadre de l'étude

Notre mémoire s'inscrit dans le cadre de notre stage de fin de MBA (Master of Business Administration) en Audit et Contrôle de Gestion du Centre Africain d'Etudes Supérieures en Gestion. Il a été réalisé à l'issue d'un stage de six (6) mois au sein du Cabinet PricewaterhouseCoopers SA (PwC), Côte d'Ivoire au cours duquel nous avons eu l'opportunité d'intervenir dans le cadre d'une mission d'évaluation du processus de gestion des risques opérationnels dans un établissement financier qui représente le cas pratique de notre mémoire de fin d'études universitaires.

Durant notre cadre d'étude, nous avons effectué une mission d'environ un (1) mois dont un séjour permanent de deux (2) semaines dans l'institution.

1. Présentation de la structure d'accueil

PricewaterhouseCoopers (PwC), est le résultat de la fusion des cabinets d'audit et de conseil Price Waterhouse et Coopers & Lybrand, intervenue le 1er juillet 1998.

En effet, la nouvelle entité ainsi formée représente l'un des plus grands prestataires de services intellectuels à travers le monde avec près de 180 000 personnes travaillant en réseau dans 158 pays. Les différentes étapes de la constitution de PwC sont notamment :

- 1849 : fondation à Londres du cabinet Price par Samuel Lowell Price ;
- 1854 : fondation à Londres du cabinet Cooper Brothers ;
- 1865 : Edwin Waterhouse rejoint le cabinet Price qui devient Price Waterhouse ;
- 1929 : ouverture du bureau de Coopers & Lybrand à Paris ;
- 1957 : Coopers & Lybrand International est créé par l'association de Cooper Brothers & Co (Royaume-Uni) avec Lybrand, Ross Bros & Montgomery (États-Unis) et McDonald, Currie & Co (Canada) ;
- Septembre 1997 : Coopers & Lybrand et Price Waterhouse annoncent leur projet de rapprochement ;
- Novembre 1997 : les associés des différentes activités membres de Coopers & Lybrand et de Price Waterhouse votent le principe de rapprochement dans les différents pays ;
- 1998 : lancement de PricewaterhouseCoopers après autorisation du rapprochement par la Commission européenne.

Cette fusion s'est traduite par la mise en place, entre autres, de systèmes d'informations performants afin d'exploiter la puissance du réseau ainsi constitué. Les clients de la firme peuvent alors bénéficier des services du réseau mondial, quelles que soient la taille et la nature de leurs activités ou encore le domaine et le pays dans lesquels ils sont implantés.

PricewaterhouseCoopers, exerçant sous la raison sociale de PwC développe des missions d'audit, d'expertise comptable et de conseil créatrices de valeur pour ses clients, privilégiant des approches sectorielles.

PwC fait référence au réseau PwC et/ou à une ou plusieurs de ses entités membres, dont chacune constitue une entité juridique distincte.

De manière pratique, le bureau d'Abidjan est divisé en 2 lignes de services :

- celle de l'Assurance and Advisory (A&A) en charge de l'audit et du conseil en organisation, comprenant également le Service BAS (Business Advisory Services) pour l'assistance comptable et de gestion ;
- ainsi que celle du Tax and Legal Services (TLS) en ce qui concerne le volet juridique et fiscal.

PricewaterhouseCoopers, est également l'auteur de nombreuses publications à travers le monde. Il s'agit le plus souvent de guides, de nouvelles d'informations, de rapports sur le développement de certaines activités et de revues sur les principaux problèmes qui affectent le monde des affaires. La plus connue de ces publications en Côte d'Ivoire est la revue juridique et fiscale Fidafrica.

Tout au long de ce stage, nous avons participé à de nombreuses missions, différentes les unes des autres par l'organisation, l'activité ou le référentiel dont il fallait tenir compte.

C'est dans le cadre de ce stage que nous avons eu la chance de travailler dans une banque, filiale d'un grand groupe et de cerner ainsi la problématique liée à la maitrise de la gestion des risques opérationnels.

2. Présentation de la mission

Cette étude s'inscrit dans le cadre d'une mission spéciale d'évaluation du processus de gestion des risques d'une banque. Cette mission a été contractée dans le but d'identifier les forces ainsi que les faiblesses de ce dispositif de gestion afin d'apporter des recommandations visant à l'amélioration dudit dispositif.

3. Exécution de la mission

La mission s'est déroulée en quatre (5) grandes étapes que sont :

Phase 1 : La phase de cadrage de la mission

Cette première phase constitue l'étape de préparation de la mission. L'objectif de cette phase est d'appréhender le sujet à auditer (entité, processus, thématique, …) et de se fixer des objectifs d'audit précis. En effet, c'est au cours de cette phase que les enjeux, les objectifs, les intervenants, la période d'intervention ainsi que l'organisation de façon générale de la mission est définie.

Tout ceci est effectué par le manager sur la mission ainsi que le chef de mission en accord avec le client.

Phase 2 : La phase de réalisation de la mission

Les auditeurs, dans cette seconde étape prennent d'abord connaissance de la documentation applicable aux procédures de travail ; notamment, les politiques, les procédures, le budget, ainsi que de l'environnement de contrôle relatif au thème de la mission.

Les auditeurs dans un deuxième temps effectueront un gap analysis que représente une comparaison entre la situation actuelle et la situation projetée afin de repérer les leviers et tâches à mener dans le but de supprimer cet écart.

A la suite du gap analysis, une évaluation sera faite par l'équipe d'audit dans le but d'identifier les points forts et les points faibles du processus de gestion des risques opérationnels de la Banque.

Les points faibles feront l'objet de recommandations de façon automatique, cependant, des tests seront effectués pour confirmer les points forts.

Phase 3 : La phase de conclusion

Dans cette troisième étape, l'équipe d'auditeurs va organiser les résultats de leurs tests de manière structurée dans un rapport et va émettre une opinion à l'attention du management quant au degré de maîtrise des opérations auditées et élaborer des recommandations afin d'optimiser les processus.

Phase 4 : La phase de suivi

L'équipe d'auditeurs après avoir apporté des recommandations dans la dernière étape assure un suivi de la mise en œuvre des actions élaborées sur base des recommandations de l'audit.

Les modèles d'analyse, à travers le troisième chapitre constituent le plan schématique de l'évaluation du processus de gestion des risques opérationnels de la Banque. Nous avons spécifié et défini la méthode et les outils de collecte des données pour répondre aux objectifs d'évaluation du processus de gestion des risques au sein de la banque soumise à notre étude. Le modèle a été élaboré en tenant compte de la complexité du processus de gestion des risques opérationnels liés aux entreprises financières notamment les banques.

CONCLUSION DE LA PREMIERE PARTIE

L'évaluation du processus de gestion des risques opérationnels montre que les risques sont de divers ordres et existent de manière permanente. Il faudrait pour cela renforcer les pratiques de contrôle interne par la mise en place d'outils de suivi des risques ainsi que de la réduction pour assurer la viabilité et la pérennité de l'institution en le mettant dans un cadre réglementaire souple et adapté à leur situation.

En effet, la recherche de solutions performantes afin de mieux maîtriser le risque opérationnel s'apparente à la quête du Graal pour la plupart des institutions bancaires. Le risque opérationnel a largement dépassé le cadre restreint de la banque et concerne désormais le secteur financier dans sa globalité. Ce changement d'échelle s'accompagne inévitablement d'une montée en puissance des risques opérationnels, notamment ceux liés à l'erreur humaine, à la fraude, ou à l'environnement légal et réglementaire. Corrélativement, la nécessité d'adopter des mesures plus strictes de surveillance et de contrôle du risque fait l'objet d'une attention croissante de la part des autorités de régulation, entraînant de fait une exigence accrue vis-à-vis des banques.

L'action simultanée de ces différentes sources de pression devrait contraindre les banques à adopter dans les prochaines années une stratégie globale de gestion du risque opérationnel. Les défis à relever sont nombreux et, comme souvent, les solutions sont loin d'être triviales.

Dans la deuxième partie de notre travail, nous nous attellerons à découvrir de manière pratique le processus de gestion des risques de l'entreprise soumise à notre étude afin de détecter les forces et faiblesses associées à ce processus et apporter de recommandations en vue de minimiser ces faiblesses, voire les mitiger.

DEUXIEME PARTIE : CADRE PRATIQUE DE L'ETUDE

CHAPITRE III : DESCRIPTION DES PRATIQUES GENERALES DE GESTION DES RISQUES OPERATIONNELS DE LA BANQUE SOUMISE A NOTRE ETUDE

Section I : Présentation de la banque

Le secteur bancaire ivoirien a connu une croissance soutenue ces dernières années, portée par la montée en puissance des filiales de groupes bancaires ouest-africains ou marocains. Le total bilan a progressé de 75% entre 2012 et 2018, pour se situer à 12,5 Mds €, et se traduit par une progression soutenue des crédits et des placements dans les titres de dette publics émis sur le marché régional. Ceux-ci absorbent désormais 38% de la liquidité bancaire. La concurrence s'est renforcée, mais le secteur reste concentré puisqu'un tiers des établissements détient près de 80% du marché des crédits. Les banques financent essentiellement les grandes entreprises, en large partie sur des crédits à court terme. La forte réduction du coût du risque en 2018 a contribué à renforcer la rentabilité du secteur. Celui-ci souffre de fragilités qui nécessitent un renforcement et un suivi strict de la réglementation bancaire. La filiale ivoirienne de la Société générale, la SGBCI, demeure le leader du secteur.

Selon le rapport de la BCEAO du 4^{e} trimestre de l'année 2018, page 13, le réseau bancaire de l'UMOA au 31/12/2017 comptait 44 établissements de crédits agréés dont 126 banques et 18 établissements financiers à caractère bancaire. Le décompte n'inclut pas Stanbic qui n'est pas encore membre de l'APBEF-CI ainsi que la Banque d'Abidjan (filiale de Banque De Dakar) qui vient de recevoir un avis conforme de la commission bancaire. Selon l'association professionnelle, 536 milliards FCFA ont été accordés au titre de crédit aux petites et moyennes entreprises ivoiriennes en 2016, soit 13% des concours des banques à l'économie.

1. Les missions et les valeurs de la Banque

Par la diversification de son offre de produits et services bancaires financiers, la Banque se présente comme un portail financier capable de répondre à l'ensemble des besoins des clients ; d'où la mission de la banque qui est : « Répondre aux attentes de nos clients ».

La Banque s'efforce également au quotidien de demeurer dans le respect sans faille de ses 5 valeurs fondamentales partagées par le Groupe que sont le Travail, l'Intégrité, la Transparence, la Responsabilité et l'Esprit d'équipe, et dans la manière dont elles sont véhiculées.

Cette culture d'entreprise lui sert aussi de guide dans l'accomplissement de sa mission contribuant ainsi à la performance de la banque.

2. Les domaines d'activités et les produits de la Banque

2.1. Les domaines d'activités de la banque

La Banque, dans la poursuite de ses objectifs de performances à plusieurs domaines d'activité notamment ; les financements structurés, les marchés de capitaux d'actions et de dettes, l'étude et la recherche, l'octroi de crédit aux entreprises, aux particuliers ainsi qu'aux PMI/PME. Elle est également une banque privée de détail qui exerce majoritairement dans le secteur agricole et industriel.

2.2. Les produits de la banque

2.2.1. Les financements structurés

En plus de faire des évaluations d'entreprise, la Banque accompagne ses clients dans leurs opérations de financement de projets en s'appuyant sur des instruments de dette, de quasi-fonds propres et fonds propres où le Capital de la banque agirait.

2.2.2. Les marchés de Capitaux d'actions

La banque conseille et accompagne ses clients également sur des opérations d'introduction en bourse ou d'augmentation de capital par émission d'actions en nous appuyant sur nos compétences d'analyse de marché et nos compétences de marketing.

2.2.3. Les marchés de Capitaux dette

La Banque est également impliquée dans le conseille des entreprises et des Etats sur l'élaboration de stratégies d'acquisition ou de désinvestissement et plus précisément sur des opérations de fusions, acquisitions ou de cessions.

2.2.4. Les recherches et études

La Banque fait recours à l'étude et la recherche afin d'orienter la vision globale du Groupe, sa volonté sans cesse renouvelée d'excellence, à tous les niveaux et dans chaque activité, ayant pour ambition de devenir un acteur international de première place ainsi que dans la poursuite de leurs engagements sociétaux.

2.2.5. Les autres produits de la Banque

La Banque propose une offre étendue de services bancaires et financiers. L'objectif pour la banque étant de s'adapter en permanence, avec souplesse et réactivité, aux caractéristiques socio-économiques des zones géographiques où la structure bancaire est présente et de développer une stratégie marketing différenciée en fonction des segments de marché auxquels s'adressent chacune de ses filiales.

Ces dernières sont actives dans les métiers suivants :

- Dépôts à vue ; pour les comptes courants ;
- Dépôts à termes ; pour les comptes d'épargne ;

La banque met aussi à la disposition de ses clients ;

- des cartes bancaires ;
- des cartes bancaires magnétiques ;
- la Banque online ;
- la numérisation des chèques ;
- les comptes d'épargne spéciale.

3. La structure organisationnelle de la banque

L'organe délibérant de la Banque est organisé autour d'un Conseil d'Administration et de trois (3) Comités Spécialisés que sont :

- Le Comité d'Audit
- Le Comité des Risques
- Le Comité de Gouvernement, des Ressources Humaines et des Rémunérations

Ces différents comités ont pour but de préparer et de faciliter le travail du Conseil d'administration sur des points spécifiques qui seront ensuite débattus en séance. Leurs attributions sont clairement définies dans une charte ou dans le règlement du Conseil.

En plus de ces comités, nous avons le département d'audit interne qui aide l'organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gestion des risques, de contrôle, et de gouvernance ainsi que trois (3) pôles sous la direction de la Direction générale qui sont :

- le pôle de gestion globale des risques qui comprend les départements suivants :
    - de crédit et d'engagement ;
    - juridique et de recouvrement ;
    - de risques et de contrôles permanents ;
    - de conformité ;
    - de sécurité des systèmes d'information.
- le pôle commercial qui est composé des départements ci-dessous :
    - commercial ;
    - d'entreprises ;
    - de banque privée ;
    - de communication et de marketing
    - d'un réseau d'agences bancaires d'affaires.
- le pôle fonction support qui inclut les départements suivant :
    - de finances et d'administration ;
    - d'opération et de trésorerie ;
    - de systèmes d'informations et monétiques ;
    - de ressources humaines
    - et de qualité ainsi que de services clients.

Cette nouvelle structure organisationnelle doit permettre l'accélération de la transformation afin d'améliorer la performance sur tous ses indicateurs tout en garantissant la pérennité de la Banque.

Section II : Le dispositif de gestion des risques de la banque soumise à notre étude

1. Le dispositif de gouvernance de la banque

La circulaire relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA fixe les règles minimales en matière de gouvernance devant être observées par les établissements en activité dans l'UMOA.

1.1. Le principe de proportionnalité

En effet, après analyse du dispositif de gouvernance de l'entité soumise à notre étude ; la Banque, nous avons pu noter que celle-ci a mis en place un dispositif de gouvernance conforme aux saines pratiques et adapté à sa taille, sa structure, la nature et la complexité de ses activités ainsi qu'à son profil de risque. La Banque dispose également d'un cadre de gouvernance adapté à son envergure et aux conséquences de sa défaillance éventuelle sur la stabilité du système financier de l'UMOA ou de son Etat d'implantation.

1.2. Les principes généraux de gouvernance

Le dispositif de gouvernance de la Banque :

- est élaboré et mis en œuvre en tenant compte de la sécurité des systèmes d'information de la banque, de la couverture de l'ensemble des risques encourus par l'établissement et des éventuels conflits d'intérêts ;
- établit et formalise les stratégies, politiques et procédures à mettre en place, pour définir et organiser les divers moyens nécessaires à l'atteinte d'une saine gouvernance de la banque;
- définit les rôles et obligations des intervenants ;

- permet de répondre aux besoins de l'établissement dans son ensemble et de chacune de ses unités organisationnelles et opérationnelles à travers son système de gestion des procédures qui est bien fournit et mis à jour régulièrement.
- à intégré dans ses activités quotidiennes des mécanismes visant à maintenir et à rétablir son fonctionnement en cas de discontinuité ;
- reflète au fil du temps, les changements découlant des caractéristiques de l'établissement et de son environnement externe ainsi que des évolutions relatives aux meilleures pratiques en matière de gouvernance. En effet, après les reformes de Bâle II et Bâle III, la banque a dû réadapter ses activités en créant une direction à part entière chargée de la gestion des risques encourus par la Banque qui n'existait pas avant les reformes de Bâle.
- à prévu des mécanismes permettant de s'assurer de l'intégrité et de l'engagement des intervenants à travers le code de déontologie de la banque, qui doivent être en nombre suffisant, compétents et avoir une bonne connaissance des activités de l'établissement, de ses risques ainsi que de ses obligations juridiques.

2. Les organes de gouvernance de la banque dans la gestion des risques opérationnels

Les organes de gouvernance de la banque soumise à notre étude, selon les règles établies par la circulaire n°04-2017/cb/c relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA ont veillé effectivement à ce que la banque :

- dispose d'un dispositif de gestion de ses risques opérationnels;
- mette en place une fonction gestion des risques couvrant tous ses risques opérationnels significatifs, à l'échelle de la banque et disposant d'attributions distinctes de celles des unités opérationnelles ;
- soit dotée d'une fonction gestion des risques indépendante et munie de ressources nécessaires ainsi que d'une autorité suffisante pour mener à bien ses missions dans la gestion des risques opérationnels de l'institution ;
- exerce pleinement les responsabilités qui lui ont été dévolues en matière de risque opérationnel, conformément aux dispositions énoncées dans la circulaire relative à la gouvernance des établissements de crédit et des compagnies financières de l'UMOA.

En plus des éléments identifiés plus haut, les organes de management de la banque ont mis en place :

Tableau 3 : Tableau de certains éléments du dispositif de gestion des risques opérationnels

Eléments du dispositif de gestion des risques opérationnels	Explications
La culture du risque	En effet, la banque soumise à notre étude encourage le développement de la culture du risque à tous les niveaux de son organisation à travers notamment des formations et des actions de sensibilisation. Ceci est fait de sorte que tous les membres du personnel comprennent l'approche des risques opérationnels de l'établissement et du groupe.
L'appétence au risque	La banque soumise à notre étude a effectivement mis en place un dispositif d'appétence au risque approuvé, supervisé et révisé annuellement par l'organe délibérant et mis en œuvre par l'organe exécutif (la Direction des risques de la banque).
La gestion des limites	La banque s'est fixée des limites globales et des limites opérationnelles au niveau du siège ainsi que de ses filiales. Elle a également mis en place un dispositif d'identification et de gestion des dépassements de limites.
Des systèmes d'information	L'institution bancaire soumise à notre étude s'est dotée d'un dispositif de gouvernance des données sur ses risques opérationnels ainsi que d'une architecture de données relatives ces risques opérationnels et d'une infrastructure informatique.
Reporting à l'organe délibérant	Un rapport sur la nature et le niveau d'exposition aux risques opérationnels encourus par la banque soumise à notre étude est effectivement soumis à l'organe délibérant une fois par semestre.
La simulation de crise	Des programmes de simulations de crises aux fins de la gestion des risques opérationnels ont été mis en place par la banque. Ces programmes lui permettent d'évaluer l'impact potentiel de scénarios adverses sévères mais plausibles sur sa solidité financière, conformément à la Circulaire relative à la simulation de crise. Ils incluent tous les risques opérationnels importants auxquels l'établissement est exposé.

Source : Nous-même.

3. Implications de l'audit interne et la direction des risques dans la gestion des risques opérationnels

3.1. L'audit interne dans la gestion des risques opérationnels

La direction de l'audit interne de la banque soumise à notre étude exerce en toute indépendance dans sa mission de vérification du processus de gestion des risques opérationnels de l'entité. Elle vérifie en se référant aux des normes applicables en matière de gestion des risques opérationnels ; notamment les circulaires relatives à la bonne gouvernance des établissements de crédit et des compagnies financières de l'UMOA.

3.2. La direction des risques dans la gestion des risques opérationnels

L'établissement financier soumis à notre étude s'est doté d'une direction des risques qui est chargée de la gestion des risques opérationnels de l'entité selon ce qui est indiqué dans la circulaire n°04-2017/cb/c relative à la gestion des risques dans les établissements de crédit et les compagnies financières de l'UMOA.
Cette direction est adaptée à sa taille, à la structure de la banque, la nature et la complexité des activités ainsi qu'au profil de risque de l'entité.

3.2.1. Les stratégies, politiques et procédures de la direction des risques

La direction des risques de la banque soumise à notre étude met en place des stratégies, politiques et des procédures dynamiques, de manière à refléter l'évolution du degré d'appétence au risque de l'institution, au profil de risque de la banque ainsi qu'aux conditions de marché et l'environnement macroéconomique. Parmi ces stratégies, on peut citer ;

La cartographie des risques opérationnels	La direction des risques de la banque recense, évalue et hiérarchise l'ensemble de ses risques opérationnels à travers une cartographie qui est validée par l'organe délibérant. Cet outil de pilotage lui permet de s'assurer une bonne gestion et un suivi adéquat de ses risques opérationnels.
Le contrôle interne	La direction des risques de la banque soumise à notre étude a intégré dans son dispositif de gestion des risques opérationnels de l'établissement des contrôles internes rigoureux. Ces contrôles sont adaptés à l'ampleur, à la nature et à la complexité de ses expositions conformément aux dispositions définies dans la Circulaire relative au contrôle interne.

Source : Nous-même.

4. Les étapes du processus de gestion des risques opérationnels

4.1. Etablir une cartographie des processus métier

La Banque dans la gestion de ses risques opérationnels à travers sa Direction des risques a mis en place une cartographie de ses processus métier afin de représenter l'entreprise sous la forme de logigrammes cohérents (niveau des processus) intégrant l'ensemble des activités réalisées par l'entreprise ainsi que leurs interdépendances.

La cartographie du processus permet à la banque de comprendre comment ses différents processus d'activité fonctionnent et de vérifier si ceux-ci lui permettent d'atteindre ses objectifs à travers l'image fidèle de l'état du processus que la cartographie lui procure.

4.2. Positionnement sur chaque activité les acteurs et les systèmes d'information qui y contribuent

Après avoir établi une cartographie de leur processus métier, la direction des risques de la Banque dans son objectif de pilotage des risques enrichit cette cartographie en positionnant sur chaque activité de la banque, les acteurs ainsi que les systèmes qui y contribuent. Ceci lui permet ensuite d'identifier aisément les défaillances relatives au personnel ou aux systèmes impliqués dans le processus. Cette étape réalisée, la Banque dispose alors d'une vision quasi

exhaustive des activités ainsi que des acteurs et des systèmes d'informations concernés, elle peut désormais définir la typologie des risques en fonction du profil de l'entreprise.

4.3. Définir la typologie des risques en fonction du profil de l'entreprise

Comme indiqué plus haut, la Banque dans la gestion de ses risques s'est dotée d'une direction des risques qui est chargée de l'identification des risques, de l'évaluation de ces risques en général qui doivent être traités et la mise en œuvre de stratégies pour faire face à ces risques. La Banque ayant identifié ces risques, définit la typologie de ceux-ci en fonction du profil de l'entité ; ce qui permet à la banque d'être mieux préparée et de les traiter une façon plus rentable.

Nous avons deux dimensions par lesquels la banque peut procéder à la typologie de ses risques :

4.3.1. La dimension interne

Elle consiste à identifier sur l'ensemble des processus modélisés en interne, les risques qu'ils pourraient faire encourir à la banque.

4.3.2. La dimension externe

Cette dimension consiste à compléter et valider l'approche interne par l'intermédiaire d'un benchmark sectoriel en procédant au recensement des incidents ayant eu lieu sur des activités similaires à ceux de la banque dans le but d'enrichir la base historique des incidents avec l'ensemble des incidents qui ont eu lieu au sein d'institutions financières qui encourent les mêmes risques.

Cette étape réalisée, la Banque dispose alors d'une vision quasi exhaustive des activités ainsi que des acteurs et des systèmes d'informations concernés, elle peut désormais définir la typologie des risques en fonction du profil de l'entreprise.

4.4. Positionner sur chaque activité les risques opérationnels associés

Après la typologie des risques, la banque pourra déterminer exactement ses risques opérationnels. Cette étape permet à l'institution financière soumise à notre étude ensuite pour chaque activité identifiée dans la cartographie des processus d'y associer les risques opérationnels correspondants.

Ceci permet à la Banque par exemple d'associer à une activité de paiement, un risque de fraude ainsi qu'un risque de non-paiement. A travers ce travail collaboratif, la banque peut associer d'une part les responsables opérationnels qui deviennent ainsi des process-owner et d'autre part les correspondants risques locaux, garants de la bonne utilisation de la typologie de risque.

La cartographie de processus de la Banque étant enrichie de l'ensemble de ses risques opérationnels potentiels générés par les activités que l'entité exerce, la banque peut alors procéder au recensement des incidents, à l'appréciation des risques et à la définition du niveau de risque acceptable.

4.5. Recenser les incidents, évaluer les risques et définir le niveau de risque "acceptable"

La Banque recense les incidents survenus par le passé au sein de l'entreprise conservée dans une base de données de gestion des incidents qui sera renseignée de manière déclarative par sa direction des risques. Cette base de données bien que pas conséquente tel qu'indiqué précédemment est alignée sur la cartographie des processus. Chaque incident est donc renseigné en précisant l'activité et le risque brut concerné. L'analyse de la petite base des incidents de la banque, associée à la connaissance des responsables opérationnels permet d'évaluer les risques et cette évaluation passe notamment par la définition des Key Risk Indicators (KRI) qui représentent des éléments qualitatifs pour la banque soumise à notre analyse puisque ne disposant pas de base de données d'incidents conséquents.

Au regard donc de ces informations, l'entité détermine le niveau de risque qu'elle juge 'acceptable'. Cela lui permet ainsi de mesurer les mesures de contrôles à mettre en place.

4.6. Définir et mettre en œuvre le plan de contrôle au regard du niveau de risque défini comme "acceptable"

Une fois le niveau d'acceptabilité du risque défini, la direction des risques de la banque déploie sur l'ensemble des activités de la banque un plan de contrôle intégré au sein de la cartographie permettant lui de maîtriser ses risques opérationnels.

4.7. Piloter le plan de contrôle

La banque à travers sa direction de l'audit interne pilote cet ensemble de contrôles dans le plan de contrôle intégré au sein de la cartographie des risques. La fréquence de ces contrôles est définie en fonction du niveau de risque et de la fréquence même de l'activité.

Ils effectuent un pilotage semestriel ; c'est-à-dire avant chaque conseil qui a lieu trois (3) fois dans l'année ; en mars, juillet et en Novembre.

Une bonne compréhension du risque opérationnel permet donc d'améliorer la prise de décision au moyen de l'observation et de l'analyse des incidents opérationnels passés et des tendances observées dans les comportements au sein des institutions financières. De plus, la mise en place d'un dispositif de gestion du risque opérationnel fiable crée un mécanisme de discussion et de signalement des problèmes aux échelons supérieurs, ce qui conduit, à terme, à une meilleure gestion du risque ainsi qu'à une plus grande résilience institutionnelle.

Cette étape de notre étude nous a permis de prendre connaissance de l'entreprise soumise à notre analyse à travers l'historique, les ressources, les domaines d'activités de l'entreprise ainsi que sa mission, son statut juridique et sa structure. Tout ceci va permettre de mener à bien notre travail.

CHAPITRE IV : ANALYSES ET RECOMMANDATIONS

Toute bonne stratégie de gestion des risques est prospective et contribue à faciliter la prise de décisions opérationnelles. Elle ne contribue pas seulement à éviter ou à minimiser les pertes mais elle contribue également à identifier et à saisir les opportunités. Une bonne gestion des risques est fondée sur une stratégie planifiée, pertinente, complète et bien étayée. Cette stratégie va normalement déboucher sur des orientations, des plans et des procédures de type général qui pourront être utilisés dans le cadre des activités quotidiennes de la banque en matière de gestion des risques opérationnels. Chaque structure financière telle que la Banque aura à déterminer sa propre politique de gestion des risques, qui tiendra compte de ses objectifs stratégiques et des plans y afférents.

L'objectif de ce chapitre est de faire une description et une analyse du processus de gestion des risques opérationnels de la Banque. Cette analyse nous permettra d'identifier les forces et les faiblesses de ce processus afin d'apporter des recommandations.

Section I : Identification des forces et faiblesses du processus de gestion des risques opérationnels de la banque soumise à notre étude

Après avoir décrit le processus de gestion des risques opérationnels ainsi que les principes généraux de gouvernance de la Banque, nous allons identifier dans ce chapitre, les forces et les faiblesses de ce dispositif en vue de proposer des solutions.

1. Les forces du processus de gestion des risques opérationnels de la Banque

La bonne gestion du processus de gestion des risques opérationnels peut grandement augmenter la performance de toute entreprise financière. En effet, les mentalités et les outils informatiques évoluant, les entreprises doivent sans cesse se remettre en cause afin d'optimiser ses modes de fonctionnements (processus). Cette gestion des processus doit être dynamique afin de permettre d'identifier les dysfonctionnements ainsi que les menaces potentielles.

Lors de notre analyse du processus de gestion des risques opérationnels de la Banque, nous avons pu constater que celui-ci était doté de plusieurs forces qui guidaient la banque dans l'atteinte de ses objectifs de performance et de pérennité.

En effet, la Banque a mis en place un modèle de gestion de ses risques opérationnels ayant cinq (5) principes dans le but de respecter les normes réglementaires. Ce modèle de gestion lui permet d'effectuer un suivi de ses risques opérationnels en développant la cartographie de ces risques qui lui permet de procéder au recensement des risques opérationnels auxquels est exposée la banque et à les synthétiser tout en tenant compte de l'impact en cas de survenance du risque et de la fréquence de réalisation de ce risque.

1.1. La responsabilisation des différents niveaux de management

L'intégration des différents niveaux de management dans la gestion des risques opérationnels peut être exécutée afin d'identifier et d'analyser les intérêts, les préoccupations, l'influence et les réactions attendues des parties prenantes. La gestion des risques comprend alors encore une dimension organisationnelle et participative, incluant un ensemble des différents niveaux de management. La direction des risques et de conformité de la Banque participe à l'évolution de la banque, elle analyse et gère le risque, non pas en tant que fonction déconnectée de l'entreprise, mais en tant qu'activité transverse liée à toutes les branches d'activités de l'entreprise. Le risque n'est pas géré en tant que tel, mais ce sont les activités qui sont gérées et de ce fait le risque qui en découle. De plus, les autres niveaux de management de la Banque sont ensuite jumelés à différents types d'implication au moyen de stratégies d'implication correspondantes. Ainsi, la communication efficace au sein des différentes directions de la banque permet de contribuer à améliorer la transparence, à éviter les malentendus et à attirer les parties prenantes. Les avantages concrets de l'investissement dans les connaissances de gestion des risques sont quantifiés et harmonisés avec le cadre décisionnel traditionnel de l'organisation pour la comparaison et la sélection des projets. La validation est importante pour accroître la crédibilité de l'analyse relative à la gestion des risques. L'objectif à long terme consiste à instaurer une culture du risque saine. L'analyse de l'écart entre la culture actuelle et la culture du risque cible aide à concevoir des plans d'intervention visant à améliorer les attitudes et les comportements en matière de gestion des risques.

1.2. L'indépendance de la fonction en charge du contrôle du risque

Avant les reformes de Bâle II et Bâle III, la Banque ne disposait pas de fonction à part entière en charge de la gestion de ses risques de façon générale et plus particulièrement de ses risques opérationnels. Cependant, avec les nouvelles réformes sur le contrôle bancaire visant au renforcement de la réglementation, le contrôle et la gestion des risques bancaires, la Banque a créé une Direction des risques et de conformité qui est directement rattachée à la Direction générale comme toutes les autres directions de la Banque. Cette direction est chargée d'identifier, d'évaluer et de prioriser les risques relatifs aux activités de la banque, quelles que soient la nature ou l'origine de ces risques, pour les traiter méthodiquement de manière coordonnée et économique, de manière à réduire et contrôler la probabilité des événements redoutés, et réduire l'impact éventuel de ces événements.

Après l'indépendance de la fonction en charge du contrôle du risque, la banque doit s'assurer que la communication interne et externe du risque opérationnel est effectuée efficacement.

Aussi, dans notre étude, nous nous sommes basés sur la mise en œuvre des 5 pratiques suivantes pour vérifier l'efficacité du dispositif de gestion des risques opérationnels chez la Banque.

Un dispositif de gouvernance efficace repose sur des principes qui lui permettent de gérer au mieux ses risques opérationnels en vue de les mitiger.

1.3. Le principe de proportionnalité

Ce principe indique que l'établissement doit d'une part, mettre en place un dispositif de gouvernance conforme aux saines pratiques et adapté à sa taille, sa structure, la nature et la complexité de ses activités ainsi qu'à son profil de risque et, le cas échéant, à celui du groupe auquel il appartient.
Le dispositif de gestion des risques opérationnels de la Banque correspond effectivement à sa taille, sa structure, la nature et la complexité de ses activités ainsi qu'au profil de risques lié à l'environnement interne de l'entité.

1.4. Les principes généraux de gouvernance

1.4.1. La sécurité des systèmes d'information

La Banque a mis en place un dispositif de gouvernance efficace qui lui permet de maîtriser de manière efficace son processus de gestion des risques opérationnels. Celui-ci lui permet ainsi de couvrir l'ensemble des risques encourus par l'établissement financier et des éventuels conflits d'intérêts au sein de la structure financière.

1.4.2. La formalisation des stratégies, politiques et procédures

Les différentes stratégies, politiques et procédures établies par le management de la Banque sont formalisées et elles permettent de définir et d'organiser les divers moyens nécessaires à l'atteinte d'une saine gouvernance de la banque.

1.4.3. La définition des rôles et obligations des intervenants

La Banque, à travers ses fiches de postes a défini les rôles et les obligations de ses employés et dirigeants intervenant dans les processus opérationnels de l'institution afin de leur permettre d'avoir connaissance de leurs différentes missions et tâches au sein des processus de la banque.

1.4.4. Réponse aux besoins de l'établissement

Tous ces éléments du dispositif de gouvernance cités ci-dessous permettent à la Banque de répondre aux besoins de l'institution dans son ensemble ainsi que de chacune de ses unités organisationnelles et opérationnelles.

1.4.5. Intégration de mécanismes en cas de discontinuité

La Banque a prévu dans son dispositif de gouvernance des méthodes que la structure mettra en place en cas de discontinuité dans le but de maintenir et/ou de rétablir le fonctionnement de la banque.

1.4.6. Refléter les changements

La Banque reflète au fil du temps les changements qui provenant de ses caractéristiques et de son environnement externe ainsi que des évolutions relatives aux meilleures pratiques en matière de gouvernance afin d'adapter son processus de gestion des risques opérationnels en vue de mieux ses activités. La preuve est que la banque qui autrefois ne disposait pas de direction chargée de la gestion de ses risques a créé une direction après les reformes de Bâle II

et des circulaires relatives à la gouvernance des institutions financières.

1.4.7. L'intégrité et de l'engagement des intervenants

Un code de déontologie a été formalisé par la Banque et mis à la disposition du personnel de la banque qui lui permet d'avoir une bonne connaissance des activités de l'établissement, de ses risques ainsi que de ses obligations juridiques. Un casier judiciaire est aussi requis lors du recrutement du personnel de la structure ; ce qui permet à la banque de s'assurer de l'intégrité et de l'engagement des employés et dirigeants de la banque, intervenants dans la gestion du dispositif de gouvernance. Tout ceci dans le but de travailler dans l'optique d'atteindre les objectifs fixés par la banque en matière de gestion de ses risques opérationnels.

1.5. Politique et stratégie

- L'appétence aux risques est définie par le conseil ;

Le Baromètre de l'appétence au risque de Deloitte Tunisie, (2017 :15) défini l'appétence au Risque comme étant le niveau et les types de risques qu'une institution financière est capable et prête à assumer dans le cadre de la réalisation de ses objectifs stratégiques et son Business Plan.

Ainsi, le conseil d'administration de la Banque ayant pour vocation de gérer les grandes orientations de la banque et de déterminer ses choix stratégiques, cet organe gère effectivement toute question nécessaire au bon fonctionnement de l'entreprise. Dans sa mission de gestion, il définit l'appétence pour le risque de la banque ; ce qui lui permet de surveiller efficacement tous les points qu'il estime devoir surveiller.

- Les responsabilités en matière de gestion des risques ainsi que les problématiques de délégation sont clairement définies et diffusées au sein de l'entité ;

En effet, pour la bonne gestion de ses risques opérationnels, la Banque a mis en place une direction des risques et de conformité ainsi qu'une direction de l'audit interne qui s'assurent que le dispositif de gestion des risques opérationnels fonctionne correctement et qu'il permet de réduire ou d'éradiquer les risques opérationnels auxquels la banque est confrontée.

1.6. L'analyse de l'exposition aux risques

La Banque à travers sa direction des risques et de conformité procède effectivement au recensement des événements potentiels susceptibles d'avoir un impact sur les objectifs de l'entité. Ceci est réalisé de manière exhaustive et l'univers des risques est régulièrement mis à jour.

1.7. Evaluation des risques

La Banque possède un tableau de suivi de ses risques opérationnels qui met en évidence les différents risques liés aux opérations bancaires, les incidences potentielles que peuvent causer ces risques, les mesures de gestion de ces incidents ainsi que les risques résiduels. Ce tableau de suivi permet à la banque d'évaluer efficacement les risques opérationnels auxquels la banque est confrontée et de définir le niveau de risque acceptable tel que défini par le conseil.

1.8. Activités de contrôle

Le management de la Banque s'assure également que des activités de contrôle sont mises en œuvre dans chaque processus de l'organisation. Ces activités de contrôle font l'objet d'une évaluation ou auto-évaluation qui est supervisée par des fonctions de surveillance que représente la direction des risques et de conformité qui elle aussi fait l'objet de revue indépendante effectuée par la direction de l'audit interne de la Banque.

1.9. Le Pilotage

La Banque définit ses indicateurs-clés de performance relatifs à son dispositif de gestion des risques ce qui lui permettent de mesurer la santé de l'entreprise qui constitue un outil efficace d'aide à la décision**.** Ensuite, les plans de remédiation des risques opérationnels identifiés font l'objet d'un suivi documenté, les incidents avérés sont recensés et analysés enfin, les objectifs et la stratégie du dispositif sont régulièrement mis à jour.

In fine, suivre l'efficacité d'un système revient à suivre le niveau de réalisation de ses objectifs. Cela suppose qu'il en existe une mesure, une évaluation.

2. Les faiblesses du processus de gestion des risques opérationnels de la Banque

La bonne gestion du dispositif de gestion des risques opérationnels dans les entreprises financières, notamment les banques permet d'éviter de nombreux risques que pourraient engendrer les faiblesses dues à la mauvaise gestion du processus ou l'inefficacité du dispositif de gestion des risques opérationnels.

Un système est dit efficace dès lors qu'il répond aux objectifs pour lesquels il a été conçu et mis en œuvre, dans le cas contraire, il contient des faiblesses.

Ainsi, après avoir identifié plus haut dans notre analyse les différentes forces du dispositif de gestion des risques opérationnels de la Banque, nous pourront décerner les objectifs de performances auxquels le dispositif ne répond pas forcément qui constituent les faiblesses du processus de gestion des risques opérationnels de la banque.

2.1. L'absence de communication interne et externe du risque opérationnel

Les informations sur le risque opérationnel fournies par le système d'information provenant de la Direction des risques de la Banque doivent être adaptées aux besoins de l'organisation afin d'identifier, d'évaluer et de répondre aux risques.

Cependant, la Banque ne communique pas efficacement sa politique de gestion des risques opérationnels au personnel de la banque. Cette communication devrait être établie dans la banque de manière que chacun ait conscience de ses responsabilités et de ce qui est attendu de lui.

2.2. L'absence de base de données conséquente pour la réduction de l'exposition aux risques opérationnels

Du fait de la mise en place récente de la Direction des risques et de conformité de la Banque, la banque ne possède pas encore de base de données contenant des événements négatifs externes pouvant générer des risques opérationnels, cependant elle dispose d'une base interne qui n'est pas suffisamment fournie pour permettre à la banque de mesurer son exposition aux risques opérationnels.

2.3. Une vieille cartographie des risques

La direction de la banque a défini dans ses stratégies que la cartographie des risques de la banque devrait être renouvelée chaque année ; c'est-à-dire en début d'année financière. Cependant, lors de notre évaluation, nous avons pu noter que la cartographie de la Banque était vieille de deux (2) ans ; ce qui constitue une faiblesse du processus de gestion des risques opérationnels de l'entité.

2.4. Non-respect des limites dans les encaisses

Dans le but de se préserver de la fraude interne, telle que les détournements d'actifs, la Banque avait prévu dans sa politique de gestion de sa caisse ne pas avoir de montants supérieurs à 500.000 FCFA dans sa caisse. Cependant, après notre analyse, il se trouve que cela n'est pas forcément respecté dans certaines agences. Ce qui constitue une faiblesse du processus de gestion des risques opérationnels de la Banque.

Section II : Recommandations

Après l'analyse du processus de gestion des risques opérationnels de la banque et identification des faiblesses associés au processus, nous avons proposé à la structure quelques recommandations qui pourraient lui permettre de réduire, voire d'éradiquer ses faiblesses.

Tableau 3 : Tableau récapitulatif des faiblesses du processus de gestion des risques opérationnels de la banque soumise à notre étude ainsi que des recommandations

Les faiblesses du dispositif de gestion des risques opérationnels de la banque	**Proposition de recommandations**
Non-respect des limites dans les encaisses	La Banque devrait veiller à ce que chaque agence respecte de façon systématique l'instruction de ne pas excéder la somme de 500.000 FCFA dans sa caisse de sorte à éviter les fraude interne qui est le résultat de cette faiblesse.
Une vieille cartographie des risques	La direction des risques de la Banque doit s'assurer que la cartographie de ses risques opérationnels est bien effectuée en début de chaque année financière au risque de ne pas pouvoir atteindre ses objectifs de mitigation des risques opérationnels.
L'absence de base de données conséquente pour la réduction de l'exposition aux risques opérationnels	La Banque à travers sa Direction des risques et de conformité doit fournir sa base de données d'événements négatifs externes de sorte que la banque puisse se baser sur les faits qui se sont précédemment passés dans d'autres entreprises dans des circonstances similaires de mesurer au mieux son exposition aux risques opérationnels.
L'absence de communication interne et externe du risque opérationnel	Le management de la Banque doit s'assurer que les informations sur le risque opérationnel de la Banque sont correctement communiquées au personnel de l'entité. Cela s'applique, bien entendu, aux employés agissant au niveau individuel ou comme membre d'un groupe de travail. Tout cela doit faire partie de la communication interne mais aussi de la communication externe à double sens entre l'entreprise, ses clients, ses fournisseurs et l'ensemble des acteurs pouvant avoir un rôle à jouer dans l'atteinte des objectifs de la Banque.

Source : Nous-même.

CONCLUSION GENERALE

Au terme de notre étude qui avait comme thématique ; la démarche d'évaluation du processus de gestion des risques opérationnels d'une banque par le cabinet PricewaterhouseCoopers, nous avons pu noter que la gestion du risque opérationnel constitue l'une des préoccupations majeures des dirigeants des institutions financières ces dernières années.

En effet, plusieurs champs de sa gestion sont encore à explorer et à découvrir alors que les autorités règlementaires mettent de la pression pour une quantification rigoureuse de capital du risque opérationnel.

Nous avons essayé dans le cadre de notre mémoire d'évaluer le dispositif de gestion des risques opérationnels de la Banque. Pour ce faire, nous avons identifié dans un premier temps le processus de gestion des risques opérationnels de la Banque, ce qui nous a permis de nous imprégner des étapes par lesquelles l'entreprise gère ses risques opérationnels. Dans un second temps, nous avons identifié les forces et les faiblesses dudit dispositif afin de proposer des recommandations afin d'une meilleure maîtrise des opérations de la banque.

A la suite de notre évaluation, nous pouvons dire que la bonne gestion du dispositif de gestion des risques opérationnels relève de la responsabilité des dirigeants de l'entreprise. L'objectif étant de donner une assurance raisonnable que les objectifs de l'entreprise seront atteints. Les directions opérationnelles évaluent et gèrent donc les risques tout en mettant en œuvre les activités de contrôle.

BIBLIOGRAPHIE

1) AHOUANGANSI EVARISTE (2006), Audit Révision des comptes, éditions mondexperts, 729 pages.
2) Athmane BOUAZABIA et Samir BOUDJEDRA, 2007 Analyse et gestion des risques, Edition, Université Lumière Lyon, 201 Pages.
3) BENOÎT COUGNAUD (2007), L'univers des risques en finance - le risque opérationnel, Chapitre, (pages 103 à 114).
4) BILOGO OYONO NSEGUE Noemi (2011), Evaluation de la gestion de risques operationnels lies au processus comptable, 1ère Edition, Archives ouvertes, 27 pages.
5) CIA LEARNING SYSTEM DE L'IIA, vol. 1, 2 et 3 (2014), 296 Pages.
6) CRAIG CHURCHILL ET DAN COSTER (2001), Manuel de gestion des risques en microfinance, 20ème Edition, 120 Pages.
7) EUSTACHE EBONDO WA MANDZILA ET DANIEL ZEGHAL (2009), Management des risques de l'entreprise : Ne prenez pas le risque de ne pas le faire, Edition, Revue des Sciences de Gestion (n° 237-238), pages 258.
8) ÉRIC LAMARQUE ET FRANTZ MAURER LAVOISIER (2009), le risque opérationnel bancaire dispositif d'évaluation et système de pilotage, 6ème Edition, Revue française de gestion, 108 Pages.
9) FRANTZ MAURER (2006), Quelles données pour le risque opérationnel ? Edition, Banque Stratégie, 242 pages.
10) GUILLAUME DURUPT (2018), Mieux gérer les risques opérationnels : une approche par les processus, 1ère Edition Fimarkets, 41 Pages.
11) HIMINO R (2004), Bale ou définition d'un langage commun, Edition, Rapport trimestriel de la Banque des Règlements Internationaux, 7 Pages.
12) IACOLARE VINCENT (2009), Les risques dans l'approche processus - Démarches Maîtriser les risques de stratégie et d'organisation, 2ème Edition, 81 Pages.
13) IFACI (2012), Méthodologie de conduite d'une mission d'audit interne, 1ère Edition, Fiches méthodologiques, 107 Pages.

14) KURT F. READING & Al. (2015), Manuel d'audit interne (Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques), 4ème Edition, IFACI, EYROLLES, The IIA Research Foundation, 95 Pages.

15) KAWTAR TANTAN (2007), Le processus de gestion et de mesure du risque opérationnel selon les exigences de comité de Bâle – Edition, Université TIME, Tunisie, 145 pages.

16) La circulaire n°10/MPMB (18décembre2014), les règles de gouvernance, Edition BCEAO, 15 Pages.

17) M. MOR BADIANE TINE (2013), Méthodologie et outils d'élaboration de la cartographie des risques et du plan d'audit basé sur les risques, 2ème Edition, Système Intégré de Maîtrise des Risques, 200 Pages.

18) Nitza Marjorie M'BOUROU PAMBOLT (2007), La gestion du risque opérationnel dans l'activité bancaire : Cas des banques tunisiennes, 1ère Edition, Université Libre de Tunis, 120 pages.

19) OKBA BOULI (23 décembre 2014) La gestion du risque opérationnel (cas de la Trust Bank Alge).

20) PRICEWATERHOUSECOOPERS, LANDWELL &ASSOCIÉS, COSO II REPORT (2005), Le management des risques de l'entreprise, IFACI, Editions d'Organisation, p. 340.

21) Pierre Veyrat (2018), 11 étapes pour apprendre à réaliser une cartographie des processus métiers, 2ème Edition, Modélisation des processus, 6 Pages.

22) SÉNOUSSI EPAYE (2009), Le risque opérationnel au sein des Banques : Quelle stratégie pour une meilleure maitrise, 1ère Edition, ESG Business School Paris – ESGF, 110 Pages.

ANNEXES

Annexe 1 : Questionnaire de recherche

I. HISTORIQUE

1. Dans quelle année a été créée la banque ?
2. Quel était l'objectif et mission de la banque ?
3. Quel est la structure organisationnelle de la banque ?
4. Combien d'employés constitue la banque ?
5. La banque est constituée de combien d'agences ?

II. ENVIRONNEMENT DE L'ENTREPRISE

6. Quelle sont vos produits mis à part l'octroi de crédit ?
7. Quel est le positionnement de votre département au sein de l'organisation ?

DG Comité d'audit Autre :

III. ORGANISATION ET FONCTIONNEMENT

Questions	Oui	Non	Pourquoi	Comment
La banque a-t-elle mis en place un dispositif de gouvernance conforme aux saines pratiques et qui est adapté à sa taille, structure, nature et complexité de ses opérations				
Les stratégies, politiques et procédures de la banque sont-elles formalisées ?				
Les différents rôles des personnes impliquées dans les procédures sont-ils définis et formalisés ?				
La banque a-t-elle mis en place et responsabilisé une unité de gestion du Risque Opérationnel ?				
Une Politique de Gestion des Risques Opérationnels a-t-elle été élaborée et communiquée au personnel de la banque ?				

La banque établit-elle une Cartographie de ses Risques Opérationnels ?				
Est-ce que la banque procède à des mises à jour des procédures opérationnelles après l'établissement de la cartographie des risques ?				
Est-ce que la banque dispose d'une base de données des incidents de risques opérationnels qu'elle documente régulièrement ?				
Est-ce qu'un plan de secours et de continuité de l'activité a été mis en place par la banque en cas d'incidents de risques opérationnels grave ?				
Les différents rôles des personnes impliquées dans les procédures sont-ils définis et formalisés ?				
Est-ce que vous avez des mécanismes qui permettent de maintenir ou rétablir le fonctionnement du dispositif en cas de défaillance de gouvernance ?				
Est-ce que des méthodes de vérification de l'intégrité et de l'engagement des intervenants sont mis en place ou prévus ?				
Est-ce qu'un plan de secours et de continuité de l'activité a été mis en place par la banque en cas d'incidents de risques opérationnels grave ?				
En cas de changement interne et / ou de l'environnement externe, est-ce que ces changements sont reflétés dans le dispositif de gouvernance ?				
La banque évalue-t-elle périodiquement le dispositif de gestion des risques opérationnels ?				

Autres questions de l'organisation et du fonctionnement de la banque :

1) Qui est chargé des évaluations permanentes du dispositif de gestion des risques opérationnels ?
   - les managers
   - les fonctions de gestion des risques

- l'audit interne

Autres personnes impliquées :

2) L'Audit interne évalue-t-il le dispositif de gestion des risques opérationnels ?

Oui Non

A quelle fréquence ?

- Quotidienne - Mensuelle - Semestrielle - Annuelle

3) Comment qualifieriez-vous votre dispositif de gestion des risques opérationnels ?

Sommeil Eveil Croissance Maturité

Pourquoi ?

IV. APPORT DE LA GESTION DES RISQUES OPERATIONNELS AU SEIN DE L'ORGANISATION

1) Selon vous, le dispositif de gestion des risques opérationnels mis en place par votre établissement a-t-il des faiblesses ?

Oui Non

2) Si oui, ces faiblesses constituent-elles un obstacle majeur dans les objectifs de performance de l'entreprise ?

Oui Non Pourquoi ?

3) Quels sont les risques opérationnels auxquels la banque est plus exposée ?

Les risques opérationnels auxquels la banque est exposée	Très fréquent	Fréquent	Moins fréquent
La fraude interne (*par exemple, informations inexactes sur les positions, vol commis par un employé et délit d'initié d'un employé opérant pour son propre compte)*			
La fraude externe (*par exemple, hold-up, faux en écriture, chèques de cavalerie et dommages dus au piratage informatique)*			

Les risques liés aux pratiques en matière d'emploi et de 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 pratiques concernant les clients, les produits et l'activité commerciale (*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)*			
Dommages aux biens physiques (*Par exemple, actes de terrorisme, vandalisme, séismes, incendies et inondations)*			
Interruption d'activité et pannes de systèmes (*par exemple, pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité)*			
Exécution des opérations, livraisons et processus (*par exemple, des erreurs de saisie, erreurs comptables, le non-respect des délais, etc…)*			

V. OUTILS DE GESTION DU RISQUE OPERATIONNEL

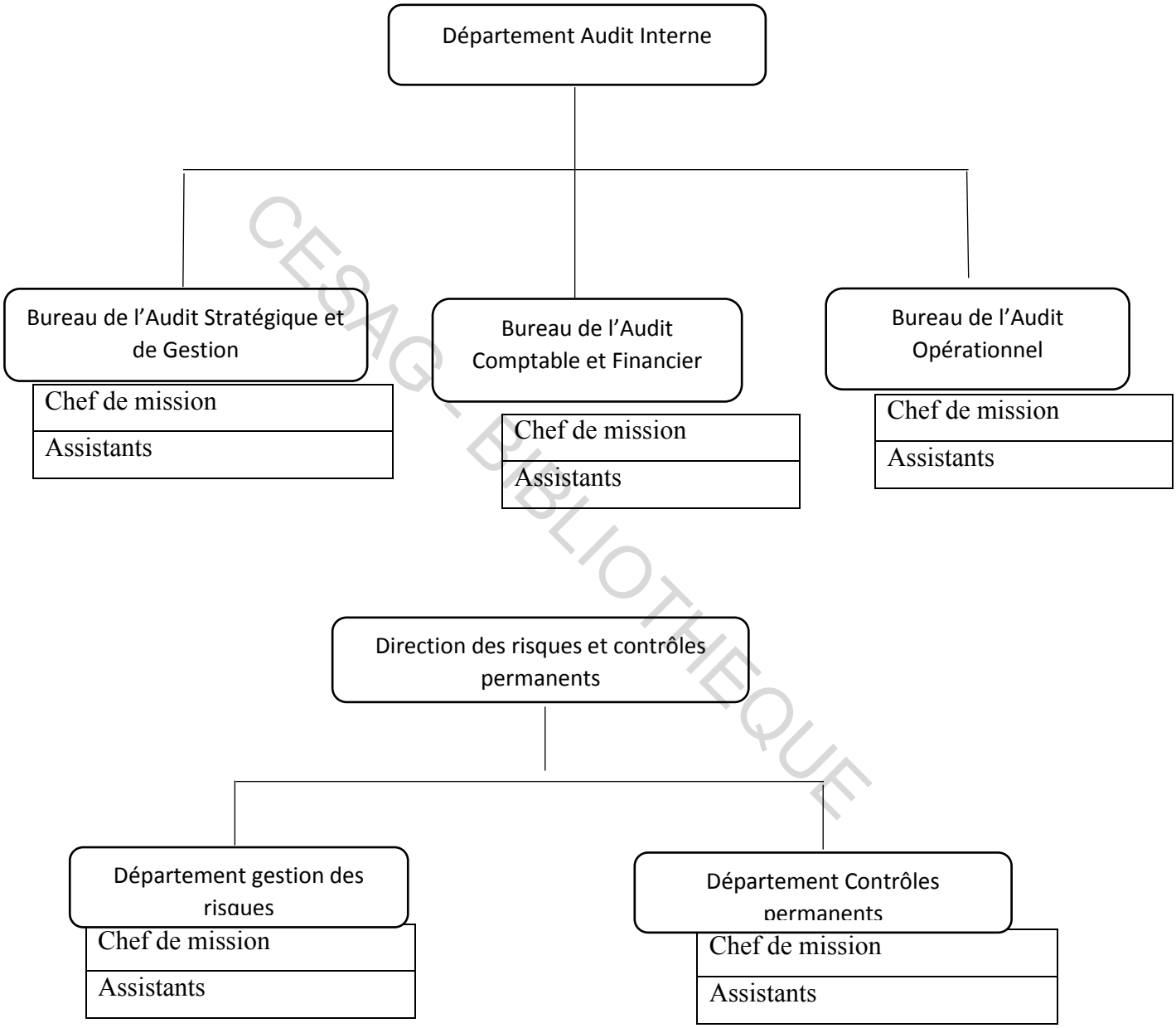
Comment identifiez et évaluez-vous le risque opérationnel ?

A travers ;

- Les autoévaluations du risque opérationnel
- La cartographie des processus opérationnels
- Les indicateurs de risque et de performance en matière de surveillance du risque opérationnel et les indicateurs d'efficacité du système de contrôle interne
- Les analyses des évènements de pertes opérationnelles tant à l'intérieur qu'à l'extérieur de l'établissement
- Les analyses de risques spécifiques à chaque produit, processus et système en place

- Les analyses de scénarios

Annexe 2 : Organigrammes des directions en charge de la gestion du risque opérationnel



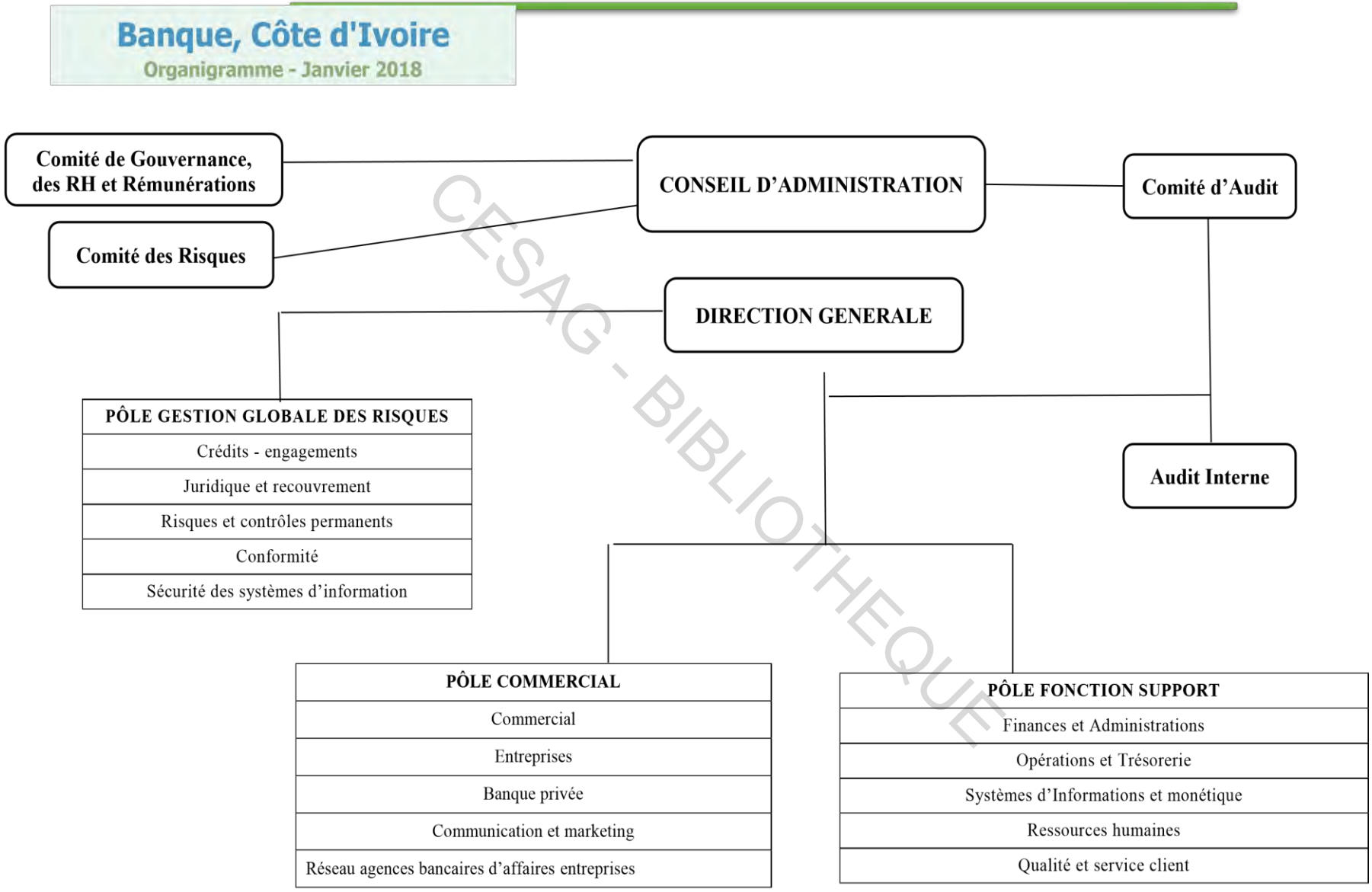


TABLE DES MATIERES