Agrément/Habilitation

N° HA-2022 19MESRI/ANAQ-SUP/SE/DIPriv/nmf

DEPARTEMENT : Institut Mercure

SPECIALITE : Gestion

MEMOIRE

Présenté par :

Marième MBODJ

Master of Science in Management
(Option : Audit & Contrôle de Gestion)

Thème :

Etude sur la gestion des risques opérationnels dans une banque

Cas de la Banque Islamique du Sénégal

Président du jury : Dr Mor Talla Diallo	**Professeur titulaire des Universités**	**SUPDECO**
Encadreur : M. Fernand DAGOUDO	**Professeur d'Audit**	**SUPDECO**
Membre du jury 1 : M. Mouhamadou DIA	**Docteur en Sciences de Gestion**	**SUPDECO**
Membre du jury 2 : M. Pape Touty Diouf	**Doctorant en Sciences Economiques**	**SUPDECO**

Année académique : 2021-2022

DEDICACES

Après avoir rendu grâce au Tout Puissant et son Prophète Muhammad (PSL), nous dédions ce présent travail à nos parents en particulier notre très chère mère qui depuis toute petite veille à la réussite de nos études, à nos chers frères et sœurs et à notre mentor de toujours, notre très cher oncle Cheikh Ahmed Tidiane Mbaye.

Ce mémoire est aussi dédié à tous ceux qui ont participé de près ou de loin à la réussite de la modeste personne que nous sommes.

REMERCIEMENTS

Comme disait un adage, « Rendons à César ce qui appartient à César » cela dit que nous ne saurions terminer sans honorer l'ensemble du corps professoral et administratif de notre école qui nous a inculqué les connaissances acquises au cours de nos deux ans de formation et spécialement à M. Fernand Ezola DAGOUDO pour son encadreur de qualité, ses conseils et son soutien moral.

J'exprime une profonde gratitude à tous ceux qui d'une manière ou d'une autre ont œuvré à la réalisation de ce mémoire. A savoir :

-Le Directeur Général de la BIS M. Madana KANE qui nous a fait honneur d'exercer dans sa prestigieuse institution en qualité de contrôleur à la cellule de contrôle des agences.

-La Directrice du Capital Humain Mme Khar NIANG qui nous a autorisés à prendre la BIS comme exemple de notre étude.

-Le Directeur des Risques et Suivi des Engagements M. Abdourahmane SOW pour sa collaboration et son accord sur le sujet de notre étude.

-Le Responsable du Service Risques Opérationnels M. Oumar Bambo CISSOKHO pour sa collaboration sans faille, sa disponibilité et son support considérable

-Le Conseiller du DG M. Sidy Alpha BEYE pour son soutien, ses encouragement et conseils

-Mme Mame Diarra Bousso Ndiaye notre chère collègue pour sa serviabilité et son soutien

-Tous nos amis et familles proches pour leur inconditionnel soutien moral et leur prière.

SIGLES ET ABREVIATIONS

BIS : Banque Islamique du Sénégal

RO : Risque Opérationnel

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

UEMOA : Union Economique Monétaire Ouest Africaine

COSO : Commitee Of Sponsoring Organisations of the Treadway

IIA : Institute of Internal Auditors

ISO 31000 : Norme de gestion des risques

CB : Commission Bancaire

FERMA : Federation Of European Risk Management Association

ERM : Entreprise Risque Management

AAOIFI : Accounting and Auditing Organisation Of Islamic Financial Institutions

AMA : Advanced Measurement Approach

LDA : Loss Distribution Approach

TAH : Tamweel Africa Holding

BID : Banque Islamique de Développement

PCA : Plan de Continuité d'Activité

LAB/FT : Lutte Anti Blanchiment et Financement du Terrorisme

GAB : Guichet Automatique de Banque

FIQH : Droit musulman regroupant tous les aspects de la vie, religieux, socio politiques et privés.

GIM : Groupement Interbancaire Monétique

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

SOMMAIRE

Introduction Générale

Les institutions financières sont au cœur de l'économie mondiale en générale et occupent particulièrement une place de renom dans l'émergence et l'expansion économique des pays de la zone UEMOA.

Ainsi, leur ancrage économique permet à certains agents (État, ménage, entreprise…) de financer leurs activités d'où leur rôle d'intermédiaire financier. Mais malgré ce rôle capital que jouent ces institutions notamment les banques ; elles ne sont pas à l'abri des risques. Elles font face à de multiples risques qui entravent la croissance de leurs résultats.

Aussi, l'entrée dans le XXIe siècle a mis en exergue l'importance des risques à travers plusieurs facteurs tels que le terrorisme, la faillite de la gouvernance d'entreprise, le développement du risque informationnel avec l'essor des nouvelles technologies de l'information ; à cela s'ajoute le blanchiment des capitaux, la corruption et le manque d'éthique qui de nos jours connaissent une évolution fulgurante. Le listing de ces facteurs de risques est loin d'être exhaustif et oblige les entreprises particulièrement les banques à s'investir ou se réinvestir sur la gestion des risques.

Jusqu'aux années 1930, la gestion de risque proprement dit n'existait pas. Afin de se protéger des risques d'accident ou de pertes financières, les entreprises faisaient appel à des compagnies d'assurance. Seulement, tous les risques et toutes les entreprises ne pouvaient être assurés, soit à cause de la nature de l'activité industrielle ou commerciale particulièrement risquée, soit par manque de solvabilité pour certaines sociétés. Les entreprises concernées ont alors commencé à pratiquer l'auto assurance dans les années 1950 afin de gérer elles-mêmes leurs risques. Dans le même temps, les premières publications de recherche fondamentale sur la gestion des risques apparaissent grâce à des chercheurs comme Markowitz, Lintner, Treynor, Sharpe, et Mossin. Les risques sont avant tout considérés sous leur aspect financier et des publications spécialisées, tel que le « Journal of Risk and Insurance », mettent en avant les théories modernes de choix de portefeuille comme le « Capital Asset Pricing Model ».

Ces études sur la réduction des risques financiers atteignent leur pleine maturité dans les années 1970, avec la parution de nombreux journaux spécialisés et l'apparition d'outils boursiers de partage des risques, comme le « Chicago Board Options Exchange » en 1973 à la bourse des matières premières et agricoles de Chicago. Ces outils sont rendus nécessaires à cette époque par la mathématisation de la finance et l'apparition des ordinateurs personnels qui diminuent la part d'instinct entrepreneurial dans la finance pour augmenter la rationalité des investissements. En 1975, est créée la « Risk and Insurance Management Society » qui

rassemble 4500 membres, dont des sociétés et des organisations publiques. Le risque est alors envisagé comme une problématique sérieuse, et à part entière par les décideurs économiques occidentaux, en particulier aux Etats-Unis.

La gestion de risque contemporaine naît, quant à elle, au milieu des années 1980. Alors que débute l'ère de la mondialisation moderne et que les économies occidentales connaissent une dynamique néolibérale, les grandes banques mondiales et les multinationales créent des départements de prévention des risques en leur sein. Ceux-ci sont souvent en lien direct avec le comité directeur, et sont chargés non seulement d'anticiper les risques, mais également de connaître et d'utiliser les outils de réduction des risques financiers, de plus en plus nombreux et disponibles.

En 1988, « l'accord de Bâle » oblige les banques des pays membres à détenir un minimum de capital requis pour se protéger des différents risques. Dans une économie où les capitaux peuvent désormais se déplacer presque instantanément, les 10 pays les plus industrialisés comprennent la menace qu'un retrait soudain de capitaux d'une banque peut faire peser sur les économies interdépendantes.

Enfin, les années 1990 achèvent de créer la gestion contemporaine des risques financiers.

C'est à cette même époque que le poste de directeur de gestion des risques (Corporate Risk Officer, CRO) est créé. Les grandes décisions stratégiques du conseil d'administration sont désormais validées au préalable par le directeur de gestion des risques. Il a acquis une certaine indépendance vis-à-vis du conseil d'administration après « l'accord de Bâle 2 » en 2004, dont le but était de responsabiliser les entreprises et d'éviter les crises économiques mondialisées.

La gestion des risques devient ainsi un des principaux cœurs de métiers d'une banque. Car selon COSO, il est un processus mis en œuvre par les dirigeants et personnel d'une entreprise afin d'assurer la réalisation des objectifs ; et visant à limiter les tentatives de fraude dans les rapports financiers des entreprises.

Sur ce, nous pouvons classifier les risques bancaires en plusieurs typologies notamment celles prises en charge par les accords de Bâle : les risques financiers (risque de crédit, de liquidité et de taux), le risque de marché et le risque opérationnel.

De cette classification découle les risques opérationnels à qui leur survenance est l'une des raisons majeures de pertes que subissent les banques.

C'est dans ce sillage que l'on se pose la question de savoir comment avoir une gestion optimale des risques opérationnels dans une banque ?

Pour tenter de répondre à cette question, nous avons pris l'exemple de la gestion des risques opérationnels à la Banque Islamique du Sénégal (BIS).

Afin de mener à bien ce travail, nous allons user de plusieurs outils de collecte et d'analyse de données tels que des entretiens, des observations, une analyse documentaire entre autres.

Cette étude va spécifiquement s'articuler sur les questions suivantes :

- En quoi la gestion des risques est-elle nécessaire dans une banque
- Quel est le dispositif de contrôle mis en place par la BIS pour gérer ses risques opérationnels?
- L'efficacité du contrôle interne contribue-t-elle à une bonne gestion des risques opérationnels ?

L'objectif principal de cette étude est d'apprécier le dispositif de gestion des risques opérationnels au sein de la Banque Islamique du Sénégal et d'analyser son impact sur l'activité de la banque.

Les objectifs spécifiques de ce travail sont les suivants :

- Cette étude nous permettra de mettre en évidence nos connaissances théoriques et pratiques acquises au cours de notre formation et en entreprise ;
- Mais aussi d'approfondir nos connaissances dans le domaine bancaire et de nous approprier les spécificités d'une maitrise des risques opérationnels ;
- Elle sera également une source de commodité pour optimiser la gestion des risques opérationnels de la BIS à travers sa direction générale.

Dans le cadre du traitement de notre problématique, nous aborderons dans la première partie le cadre théorique et conceptuel de la gestion des risques opérationnels à la BIS et ensuite du cadre méthodologique portant sur la démarche de notre travail et la présentation de la BIS mais aussi du cadre analytique dans la seconde partie.

PREMIÉRE PARTIE : Cadre Théorique & Conceptuel

CHAPITRE 1 : CADRE THÉORIQUE

Section I : Clarification des concepts

1.) Le risque opérationnel et ses composants :

Dans le cadre général, le risque est défini comme un danger potentiel inhérent à une situation ou une activité. Autrement dit, le risque est une possibilité qu'un événement survienne et ait un impact défavorable sur la réalisation des objectifs.

Il désigne un danger bien identifié et associé à un événement ou une série d'évènements parfaitement descriptibles dont on ignore s'ils se produiront ou non mais dont on sait qu'ils sont susceptibles de se produire dans une situation exposante.

De cette notion de risque découle la nécessité d'anticiper de potentielles réalisations de risques en mettant en place un système de surveillance et de collecte systématique des données pour déclencher les alertes dès que des événements inhabituels se produisent.

Le risque a de multiples définitions selon différentes organisations et normes internationales :

- **Le COSO définit le risque** comme « la possibilité qu'un événement survienne et nuise à l'atteinte des objectifs ».
- **L'IIA définit le risque** comme « la possibilité qu'il se produise un événement susceptible d'avoir un impact sur la réalisation des objectifs. Le risque se mesure en termes de conséquences et de probabilité ».
- **La norme ISO 31000 définit le risque** comme « l'effet de l'incertitude sur l'atteinte des objectifs ».

En outre, nous tenterons de donner la définition de quelques types de risques ainsi que celle de certains concepts :

❖ **Exemples de quelques types de risques**

_ Le risque inhérent

C'est un risque d'anomalie significative qui correspond à la possibilité que sans tenir compte du contrôle interne qui pourrait exister dans l'entité, une anomalie significative se produise. Il

désigne le risque auquel l'entité est exposée en l'absence de mesures prises par le management pour modifier la probabilité d'occurrence ou l'impact de ce risque.

_ Le risque lié au contrôle

Il correspond au risque qu'une anomalie significative ne soit ni prévue ni détectée par le contrôle interne et donc non corrigée.

_ Le risque de non détection

Le risque de non détection qui est le risque que le professionnel ne détecte pas une anomalie matérielle qui existe.

_ Le risque résiduel

Le risque résiduel reflète le risque auquel l'organisation reste exposée une fois que les mesures sont prises par le management pour limiter le risque inhérent. C'est un risque qui subsiste après la réponse au risque ou après l'application de mesures d'atténuation du risque. On distingue, en pratique, deux cas de risque résiduel : le risque résiduel prévisionnel qui tient compte de l'efficacité escomptée des mesures d'atténuation et le risque résiduel après la mise en œuvre effective des mesures d'atténuation.

- **L'appétence aux risques**

« L'appétence pour le risque désigne le niveau de risque qu'une organisation juge acceptable dans le cadre de sa mission ou de ses activités ». Certaines organisations considèrent l'appétence pour le risque d'un point de vue qualitatif, en fonction de critères tels que « élevé », «moyen » et faible, tandis que d'autres adoptent une approche quantitative qui reflète et met en balance leurs objectifs de croissance et de rendements pondérés par les risques. En terme simple, l'**appétence au risque** est le niveau de **risque** global qu'une organisation est disposée à assumer dans la poursuite de ses objectifs stratégiques**. Le seuil d'appétence** est donc le niveau de risque jugé acceptable au niveau de l'entreprise.

Cependant, face aux fluctuations de la sphère monétaire et à plusieurs aspects économiques, les banques sont de plus en plus exposées à une diversité de risques qui peut porter atteinte à la croissance de leurs résultats. Nous allons ainsi développer dans la partie qui suit la typologie des risques bancaires.

1. a.) <u>Typologie de risques bancaires</u> :

Le métier de banque comme toute activité à but lucratif implique la prise de positions risquées. L'inventaire des risques associés à l'activité bancaire fait état d'une variété de risques considérables.

Des divergences existent néanmoins sur leur nature et leur étendue. Toutefois, au-delà des diversités d'appréciation, du périmètre restreint ou étendu que l'on entend donner à chaque type de risque, une tendance se dégage.

Nous pouvons alors classifier les risques bancaires en plusieurs typologies de risques et parmi ces risques nous pouvons citer :

- **Le risque de crédit**

Le risque de crédit est définit comme étant : « la perte potentielle consécutive à l'incapacité par un débiteur d'honorer ses engagements. Cet engagement peut être de rembourser des fonds empruntés, cas le plus classique et le plus courant; risque enregistré dans le bilan.

Cet engagement peut être aussi de livrer des fonds ou des titres à l'occasion d'une opération à terme ou d'une caution ou garantie donnée; risque enregistré dans le hors bilan17».

Le risque de crédit classique reste toujours la cause principale de problèmes bancaires. Les pertes consécutives défaillances des clients sont malheureusement inévitables et inhérentes au métier du banquier.

Le dispositif de contrôle du risque de crédit doit permettre de s'assurer que les risques auxquels peut s'exposer l'établissement de crédit, du fait de la défaillance de la clientèle, sont correctement évalués et régulièrement suivis.

C'est ainsi qu'avant l'octroi de tout crédit, les organes compétents doivent procéder à l'évaluation du risque de crédit en prenant en considération, notamment, la nature des activités exercées par le demandeur, sa situation financière, la surface patrimoniale des principaux actionnaires ou associés, sa capacité de remboursement et, le cas échéant, les garanties proposées.

Elle prend également en compte toutes autres informations permettant une appréciation plus complète des risques tels que la compétence des dirigeants et l'environnement économique dans lequel le demandeur de crédit exerce son activité. Cette évaluation donne lieu à l'attribution, à chaque client, d'une note par référence à une échelle de notation interne.

Les encours des créances en souffrance ainsi que les résultats des démarches, amiables ou judiciaires, entreprises pour leur recouvrement doivent être régulièrement, et à tout le moins deux fois par an, porté à la connaissance de l'organe d'administration. Celui-ci doit également

être tenu informé des encours des créances restructurées et de l'évolution de leur remboursement.

- **Le risque de marché**

On entend par risque de marché, les risques de pertes qui peuvent résulter des fluctuations des prix des instruments financiers qui composent le portefeuille de négociation ou des positions susceptibles d'engendrer un risque de change, notamment les opérations de change à terme et au comptant. C'est donc un risque de perte sur les positions de bilan et hors bilan liées à la variation des prix du marché. Les risques répondant à cette définition sont les risques de taux d'intérêt, le risque de position sur titre de propriété, le risque de change et le risque sur produits de base.

- **Le risque opérationnel**

La masse et la diversité des opérations traitées quotidiennement par une banque sont toujours considérables. Des erreurs, négligences, retards et fraudes se produisent inévitablement. Ils engagent, non seulement la responsabilité pécuniaire de l'établissement, mais également contribuent à détériorer son image de marque.

L'inefficacité est aussi un risque important, qui se traduit par un coût excessif des services qui obère la rentabilité. A cette inefficacité, s'ajoute en générale une mauvaise qualité des services, qui là encore est un facteur de détérioration de l'image de marque de l'établissement. Or, autant les pertes consécutives à des risques mesurés, et consciemment assumés et contrôlés, sont normales car inhérentes au métier de banquier, autant les pertes par négligences, par inadvertance, par inconscience ou par l'insuffisance d'organisation sont intolérables. Elles sont toujours la conséquence d'une carence dans le système de contrôle interne.
Ce sont là quelques aspects du risque opérationnel sans que cette liste soit exhaustive ou limitative.

Le risque opérationnel précédemment cité est l'objet de notre étude et nous tenterons de le développer dans tous ses aspects.

1. b.) <u>Définition et spécificités du risque opérationnel</u> :

Le risque opérationnel peut se définir comme une probabilité de perte résultant de la défaillance du système interne, des procédures ou des personnes ; ou alors « un risque de perte résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à

des évènements extérieurs. Cette définition inclut le risque juridique mais exclut les risques stratégiques et d'atteinte à la réputation.

Dans la pratique, on peut considérer comme réalisation d'un risque opérationnel tout évènement qui perturbe le déroulement des processus et qui génère des pertes financières ou une dégradation de l'image de la banque.

Nous pouvons donc en déduire que les risques opérationnels sont réalisés essentiellement par les employés (fraudes, dommages, sabotages, etc…), le processus interne de gestion (risque sur opérations, de liquidité,…), le système (risques liés à l'investissement technologique, violation, etc…) et par des évènements externes (aspects juridiques, catastrophes naturelles,…).

Le risque opérationnel fait également face à certains enjeux car la mise en place d'un dispositif de maîtrise des risques opérationnels met la banque en conformité avec la réglementation bancaire afin d'optimiser ses fonds propres (non liés à des activités rémunératrices) à allouer aux risques de cette nature. A cela s'ajoute la sécurisation des résultats en évitant ou en couvrant des risques qui entraînent des pertes nettes et de la notation en évitant des « aléas » non souhaités qui peuvent avoir des impacts sur la solvabilité ou la notoriété de la banque et une plus grande compétitivité du faits des amélioration de tarif possible si les pertes constatées sur les événements à fréquence diminués.

1. c.) <u>Composants des risques opérationnels</u> :

Le risque opérationnel peut être divisé en deux types de composants que sont :

- **Risque de défaillance opérationnelle**

C'est le risque de perte directe ou indirecte provenant de défaillances potentielles de personnes employées, de processus engagés et de technologies utilisées. Ceux-ci peuvent résulter par exemple d'une destruction de données, d'erreurs de traitements, de fraudes humaines, d'une défaillance informatique, etc. De ce fait, ce risque est interne aux banques, et peut résulter d'un :

_ risque de transaction causé par des erreurs pouvant survenir dans les opérations telles que : transferts, virements, encaissements, paiements et déblocage des fonds.

_ risque de contrôle opérationnel provenant d'un défaut de contrôle dans les activités

_ risque de système dû à des erreurs ou des défauts pouvant survenir dans le maintien du système informatique et de l'organisation.

Les défaillances opérationnelles ne se produisent pas souvent mais leur impact et leur fréquence sont incertains. C'est pourquoi leur anticipation est fondamentale pour l'atténuation de leurs conséquences.

❖ **Risque opérationnel stratégique**

Ce risque est lié à des évènements extérieurs non maîtrisables comme : des perturbations politiques, la concurrence d'un nouveau venu sur le marché capable de changer les règles du jeu, des catastrophes naturelles ou d'autres facteurs non contrôlables par l'établissement bancaire. Le risque opérationnel stratégique appelé aussi « risque de dépendance extérieure » est un risque non négligeable pour les banques. Toutefois, et en tenant compte de notre réflexion, on va s'intéresser seulement au risque de défaillance opérationnelle, lequel est interne et peut être quantifié, voire maîtrisé par les banques, ceci dans la mesure où l'on peut consacrer une partie des fonds propres.

1. d.) Typologie de risques opérationnels :

Selon le dispositif prudentiel en vigueur en Janvier 2018, il existe sept (7) catégories de risques opérationnels :

Fraude interne : informations inexactes sur les positions, vols, soustraction de fonds, faux en écritures, manipulations frauduleuses d'informations, usage frauduleux de moyens de paiements etc… ;

Fraude externe : Holdup, attaque à main armée, faux en écriture, piratage informatique, cybercriminalité, etc… ;

Pratique en matière d'emploi et de sécurité sur le lieu de travail : demande d'indemnisation des travailleurs, violation des règles de santé et de sécurité au travail, plaintes pour discrimination et responsabilité civile, harcèlement moral.

Pratique concernant les clients, les produits et l'activité commerciale : violation de l'obligation fiduciaire, violation de secret professionnel, blanchiment d'argent (ou complicité de blanchiment), ventes de produits non autorisés, etc… ;

Dommages aux biens physiques : acte de terrorisme, vandalisme, incendie, inondations, catastrophe naturelle, etc… ;

Interruption d'activité et pannes de système : pannes de matériel et de logiciel informatique autres anomalies techniques (GAB, téléphones, serveurs, etc…);

Exécution des opérations, livraisons et processus : erreur d'enregistrements de données / imputations erronées, défaillance dans la gestion des sûretés, lacune dans la documentation juridique, erreur d'accès aux comptes de la clientèle, défaillance / conflits avec des fournisseurs.

2.) La cartographie des risques opérationnels par catégorie baloise :

Dans ce chapitre, nous aborderons l'ensemble des risques considérés comme opérationnels selon Bâle II ; toutefois, il serait d'abord nécessaire de comprendre la notion de cartographie des risques, les phases qu'elle compose mais surtout de pouvoir appréhender la mission du comité de Bâle et les répartitions de pertes (par catégorie bâloise) qui découlent de ces risques.

2. a.) Mission du comité de Bâle :

Le comité de Bâle est une institution créée en 1974 par les gouverneurs des banques centrales des pays du « groupe des dix »(G10) à savoir : la France, Belgique, canada, Italie, japon, Luxembourg, Pays-Bas, Suisse, Espagne, Suède, Royaume-Unis et les Etats- unis. Depuis sa création, le comité de Bâle poursuit deux objectifs fondamentaux : renforcer la sécurité des systèmes bancaires et promouvoir une égalisation des conditions en concurrence entre les grandes banques internationales.

Le comité de Bâle a pour missions essentielles d'assurer :

- le renforcement de la sécurité et de la fiabilité du système financier ;
- l'établissement de standards minimaux en matière de contrôle prudentiel ;
- la diffusion et la promotion des meilleures pratiques bancaires et de surveillances et ;
- la promotion de la coopération internationale en matière de contrôle prudentiel.

Les travaux du comité de Bâle ont fait état de trois piliers majeurs. En effet, le ratio de Cooke imposait aux banques de disposer d'un montant de fonds propres au moins égal à 8% de leurs risques pondérés. Un travail de refonte de l'accord a été engagé depuis 1998 et a débouché en janvier sur la publication d'un nouveau dispositif appelé « accord de Bâle II » ou « ratio de Mac Donough » du nom du président de la Federal Reserve Bank of New York, William J.Mcdonough. Cette refonte permettra de prendre en compte l'ensemble des risques auxquels les banques peuvent être exposées, de renforcer la sur la surveillance prudentielle et celle d'une plus grande transparence financière ; et d'assurer la convergence entre l'exigence en fonds propres réglementaires et l'exigence de capital économique propre à chaque établissement. Aussi, le nouvel accord repose sur une approche non seulement quantitative mais aussi qualitative en s'appuyant sur les trois piliers :

- **Pilier 1 : exigence minimale en fonds propres**

L'objectif ici est d'assurer que la mesure du besoin en fonds propres d'un établissement de crédit correspond au niveau de risque qu'il porte. Le nouveau ratio modifie les principes mais il crée non seulement une nouvelle exigence de charge en fonds propre pour les risques opérationnels mais aussi, préconise trois approches de calcul des fonds propres en ce qui concerne ces risques.

- **Pilier 2 : surveillance prudentielle**

Le régulateur pourra, en fonction du profil du risque, imposer les exigences supérieures à celles imposées par le ratio. L'objectif ici est d'assurer que les banques appliquent des procédures internes saines et efficaces pour évaluer l'adéquation de leurs fonds propres grâce à une évaluation approfondie des risques encourus. Ce processus doit s'appuyer sur deux principes essentiels :

_ Existence au sein de la banque d'un processus d'évaluation du niveau global des fonds propres et d'une stratégie permettant de maintenir ce niveau ;

_ Vérification et évaluation du processus par les autorités et du niveau des fonds propres que l'adaptation de mesures correctives en cas de non-respect des principes ;

- **Pilier 3 : discipline de marché :**

Ce pilier a pour objectif :

_ D'améliorer la transparence et la communication financière des banques et ;

_ De permettre aux investisseurs de connaître leurs profils de risques, la gestion et la couverture de ces risques.

Les réalisations les plus connues du comité ont été le premier et le second accord de Bâle. Les accords sont nés de la refonte du premier et adopté en juin 2004. Ils imposent l'unification de la gestion des risques ainsi que la mise en place de processus de modélisation.

2. **b.) Notion de la cartographie des risques :**

La cartographie des risques est la phase primitive du processus de management des risques. Elle a pour but d'établir le profil de vulnérabilité d'une entreprise ou d'une de ses composantes par une identification et une évaluation des risques. Son caractère essentiel découle de la

réglementation bancaire de l'UEMOA qui en fait une exigence pour les établissements financiers.

D'après **l'article 9 de la circulaire 004/2017/CB** relative à la gestion des risques : « Le dispositif de gestion des risques doit comporter une cartographie des risques validée par l'organe délibérant qui recense, évalue et hiérarchise l'ensemble des risques de l'établissement. L'établissement est tenu de se doter de cet outil de pilotage aux fins d'assurer une bonne gestion et un suivi adéquat des risques. La mise à jour de la cartographie doit être dynamique avec une revue globale au moins une fois par an ».

Selon **Christelle & Villepin** (2005 :102), « les risques doivent être représentés de manière à identifier les risques les plus significatifs (probabilité et/ou impact ou le plus élevé (é)) et les moins significatifs (probabilité et/ou impact ou le plus faible ». Elle doit permettre l'analyse du risque suivant deux variables : la fréquence ou probabilité de survenance du risque sur une période donnée et les impacts ou gravité, c'est à dire les conséquences financières et les effets sur l'image de la banque.

2. c.) <u>Les phases de la cartographie des risques</u> :

Les six phases de la cartographie des risques :

Etape 1 : clarifier les rôles et responsabilités dans le projet de la cartographie des risques,

Dans une organisation, c'est **l'instance dirigeante** qui prend la décision et endosse la responsabilité, au nom de l'organisation, d'engager une démarche de pilotage de gestion des risques.
A ce titre, elle impulse l'exercice de cartographie des risques et désigne un risk-manager. L'instance dirigeante valide la stratégie de gestion des risques mise en œuvre et veille à ce que les acteurs de la gestion des risques disposent des moyens humains et financiers suffisants pour exercer leurs responsabilités.

Les responsables des processus managériaux, opérationnels et support rendent compte des risques spécifiques au périmètre relevant de leur responsabilité afin qu'en soient tirées les conséquences sur la probabilité d'occurrence, les potentiels facteurs aggravants et la cotation des risques.

L'ensemble du personnel apporte sa contribution à l'exercice de cartographie en rendant compte des facteurs spécifiques dues aux fonctions exercées afin qu'en soient tirées les

conséquences sur la probabilité d'occurrence, les potentiels facteurs aggravants et la cotation des risques.

Etape 2 : identifier les risques inhérents aux activités des organisations concernées

Cette étape vise à dresser la typologie des risques à laquelle les organisations sont exposées dans le cadre de leurs activités.

Il ne s'agit pas de décliner la typologie théorique des risques auxquels une organisation est exposée mais de procéder à un état des lieux précis permettant d'identifier, de manière circonstanciée et documentée, les risques qui lui sont propres.

De ce fait, le recensement exhaustif des risques inhérents aux activités nécessite, outre la connaissance de l'organisation mobilisée et des rôles impartis, une maîtrise fine des processus mis en œuvre.

Étape 3 : évaluer l'exposition aux risques de corruption, en identifiant des facteurs de risques liés au pays, à l'activité, au client, au produit ou à des facteurs internes (tels que le turnover),

Cette étape vise à évaluer le niveau de vulnérabilité de l'organisation en cause pour chaque risque identifié à l'étape précédente. Il s'agit ici de déterminer les risques «bruts» auxquels cette organisation est exposée du fait de ses activités, c'est à dire les risques considérés en amont des moyens de prévention mis en œuvre.

La méthodologie et les modalités de calcul des risques «bruts» devront figurer dans une annexe à la cartographie des risques, rappelant les définitions retenues et décrivant les procédures d'identification des risques et les conventions de comptabilisation adoptées.

Étape 4 : évaluer l'adéquation et l'efficacité des moyens visant à maîtriser les risques,

Cette étape vise à évaluer le niveau de maîtrise par l'organisation des risques afin de déterminer les risques «nets» ou « résiduels » auxquels elle est exposée du fait de ses activités. Il s'agit donc de réévaluer les risques «bruts» en prenant en considération les moyens de prévention mis en œuvre.

A ce stade d'élaboration de la cartographie, le risk-manager s'attachera à évaluer l'efficacité des mesures de prévention existantes afin de maîtriser les risques.

Etape 5 : hiérarchiser et traiter les risques nets et résiduels, positionner chaque direction évaluée sur une matrice de risques résiduels pour prioriser les actions en fonction des directions, et définir parmi les éléments existants ceux qui s'avèrent défaillants ou insuffisants,

Une fois les risques déterminés, il convient de les hiérarchiser en distinguant les risques que la direction ne veut pas prendre et ceux auxquels elle assume de s'exposer.
Une fois cette limite d'acceptabilité fixée et définie dans la procédure annexe, il s'agit de déterminer, dans le cadre de la stratégie de gestion des risques, les mesures à mettre en œuvre afin de corriger les lacunes du dispositif de prévention et ainsi limiter la probabilité d'occurrence et le défaut d'anticipation de facteurs aggravants.

Sur la base de ces éléments, un plan d'actions sera élaboré. Le calendrier et les modalités de mise en œuvre de ce plan d'action, ainsi que son suivi et les modalités de compte-rendu associés, sont confiés au risk-manager.

Etape 6 : formaliser la cartographie des risques et la tenir à jour.

La cartographie des risques est écrite et structurée. Son résultat est présenté de manière synthétique. A cet égard, il est rappelé que la forme de la cartographie des risques facilite son appropriation comme outil de pilotage des risques.

La documentation peut être organisée par métier et par processus. Elle est accompagnée d'une annexe décrivant les modalités d'élaboration de la cartographie des risques et la méthodologie de classification des risques.

Enfin, la nécessité d'actualiser la cartographie est évaluée chaque année. En tout état de cause, la cartographie des risques doit être mise à jour en fonction de l'évolution de l'activité. Parmi les évènements nécessitant de réévaluer la cartographie figurent notamment : l'évolution du modèle économique, de nouveaux processus ou leur transformation, un changement affectant l'organisation, une évolution significative du contexte réglementaire ou économique.

2. d.) <u>La cartographie des risques opérationnels</u> :

Partant du contexte général, la cartographie des risques est une restitution annuelle du processus d'identification des risques d'une entité. L'identification des risques s'inscrit dans la démarche globale d'évaluation du profil de risque de l'entité. Préparée par la Direction des risques sous l'autorité de la Direction générale, la cartographie est présentée une fois par an au Comité des

risques du Conseil d'administration. Cette démarche vise à estimer les pertes potentielles significatives pour les principaux types de risques auxquels le groupe est exposé (risques de crédit, de marché, opérationnels etc…). Elle permet d'associer une perte potentielle à des scénarios spécifiques sur des périmètres identifiés. Cette évaluation résulte de la combinaison d'approches statistiques, utilisant des historiques d'observations, et des validations à dire d'experts.

La cartographie des risques opérationnels quant à elle prend assise au dispositif prudentiel en vigueur et peuvent être classifiés en sept catégories telles que nous l'avons cité dans la partie « typologie des RO » ; mais dans cette rubrique nous tenterons de donner les définitions respectives de chacune de ces risques en fonction de la répartition des pertes par catégories bâloise.

Fraude interne : La fraude interne se définit comme une tromperie ou une dissimulation intentionnelle dans le but d'obtenir un gain financier personnel. L'ensemble des services de l'entité peuvent être concernés.

Exemple de fraudes internes : Détournement de chèques, Erreur de caisse, détournement d'actif, vol et extorsion falsification des documents financiers, communication d'informations confidentielles, corruption etc….

Fraude externe : Elle a pour objectif de tromper l'entreprise par des manœuvres, des attaques commises par des personnes extérieures à l'entreprise. Ces personnes peuvent être des professionnels qui dirigeront les attaques pour leur compte ou pour celui d'autres personnes (par exemple des concurrents).

Exemples de fraudes externes : Usurpation d'identité, holdup, attaque à main armée, faux en écriture, piratage informatique, cybercriminalité, etc… ;

Pratique inapproprié en matière d'emploi et de sécurité sur le lieu de travail : Elle a pour objectif de fournir un gain. En effet, évoluer dans un monde du travail capable de garantir à chacun de ne subir aucun dommage physique ou moral dans le cadre du travail permets aux employés d'être et de rester productif. Une entreprise qui fournit le nécessaire à la protection de ses travailleurs réduit considérablement les arrêts maladie, les accidents de travail etc….

Exemples : demande d'indemnisation des travailleurs, violation des règles de santé et de sécurité au travail, plaintes pour discrimination et responsabilité civile, harcèlement moral.

Pratique concernant les clients, les produits et l'activité commerciale : d'après le circulaire 004/2017, elle se définit comme un risque de pertes résultant 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.

Exemples de pratiques : violation de l'obligation fiduciaire, violation de secret professionnel, blanchiment d'argent (ou complicité de blanchiment), ventes de produits non autorisés, etc… ;

Dommages aux biens physiques : C'est un risque de pertes lié à des destructions ou dommages résultant d'une catastrophe naturelle ou des causes externes.

Exemples de dommages aux biens physiques : acte de terrorisme, vandalisme, incendie, inondations, catastrophe naturelle, etc… ;

Interruption d'activité et pannes de système : c'est un risque de pertes résultant d'interruptions de l'activité ou de dysfonctionnements des systèmes technologiques ;

Exemples : pannes de matériel et de logiciel informatique autres anomalies techniques (GAB, téléphones, serveurs, etc…);

Exécution des opérations, livraisons et processus : Elle peut être définit comme 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.

Exemples : Erreur d'enregistrements de données / imputations erronées, défaillance dans la gestion des sûretés, lacune dans la documentation juridique, erreur d'accès aux comptes de la clientèle, défaillance / conflits avec des fournisseurs.

3.) Notion de la gestion des risques :

Depuis Juin 2004, le nouvel accord de Bâle II a adopté la modification de l'assiette des risques qui prévoit désormais la prise en compte du risque opérationnel ; à cela s'ajoute l'exigence de la BCEAO d'un comité des risques qui est un des comités spécialisés exigés aux banques selon l'article 22 de la circulaire 001/BC/C ainsi que la circulaire 004 relative aux règles en matière de gestion des risques. La gestion des risques bancaires fait donc intervenir le dispositif de contrôle interne de la banque qui prend assise sur les dispositions réglementaires du secteur.

Elle comprend également la surveillance et la revue du système afin de permettre son amélioration continue. La maîtrise des risques opérationnels est le principal levier d'efficacité des processus.

3. a.) <u>Définition de la gestion ou management des risques</u> :

Selon **COSO II (cadre de référence du management des risques dans l'entreprise)**, le management des risques est un processus mis en œuvre par le Conseil d'Administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation.

Par ailleurs, le management des risques tel que défini par la FERMA (**Federation of European Risk Management Association)** « est constitué par un ensemble de concepts, démarches et outils, qui se concrétise par un processus continu et itératif visant successivement, à identifier et analyser les risques stratégiques et opérationnels, les évaluer et les hiérarchiser, à envisager les moyens de les maîtriser, à les suivre et les contrôler et enfin, à capitaliser le savoir-faire et l'expérience acquis dans ce domaine ». Le management des risques fait ainsi partie intégrante de la mise en œuvre de la stratégie de toute organisation.

En effet, la gestion des risques est une démarche qui consiste à identifier, prévenir et résoudre les risques. C'est un processus itératif consistant à établir de manière rationnelle et méthodique le profil de vulnérabilité d'une organisation ou d'une de ses composantes à appliquer les traitements appropriés de manière à réduire leur impact et leur probabilité.

Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.

Le management définit ensuite les actions nécessaires qui permettent d'aligner les risques avec le seuil de tolérance et l'appétence de l'organisation pour le risque.

3.b) <u>Objectifs de la gestion des risques</u> :

La gestion des risques a pour but de créer un cadre de référence aux entreprises afin d'affronter efficacement le risque et l'incertitude. Les risques sont présents dans presque toutes les activités économiques et financières des entreprises. Le processus d'identification, d'évaluation et de gestion des risques fait partie du développement stratégique de l'entreprise et doit être conçu et planifié au plus haut niveau, soit au conseil d'administration. Une approche intégrée de la gestion des risques doit évaluer, contrôler et faire le suivi de tous les risques auxquels l'entreprise est exposée.

Les **Normes IIA-2005** relatives à la nature du travail de l'audit interne et plus particulièrement la **MPA 2110-1** précise que la gestion des risques est une responsabilité majeure du

management qui doit s'assurer de la mise en place et du bon fonctionnement de processus rigoureux de management des risques pour atteindre ses objectifs. Alors, il incombe au Conseil et au comité d'audit de veiller à ce que des processus de management des risques appropriés, suffisants et efficaces, soient mis en œuvre.

Le management et le Conseil sont responsables des processus de management des risques et de contrôle de leur organisation. Ils doivent maîtriser la méthodologie générale et s'assurer que le processus de management des risques de l'organisation répond aux objectifs fixés.

3. c) <u>Les éléments du dispositif de management des risques et ses limites</u> :

Le management des risques ne doit pas être assimilé à de l'inspection ou de l'audit. C'est avant tout une démarche de progrès continu et un état d'esprit supporté par des méthodes formalisées

Un dispositif de management des risques comprend 8 éléments :

- ✓ **Environnement interne:** Implication des dirigeants, ressources dédiées, langage commun, démarche structurée
- ✓ **Fixation des objectifs**: fixation des objectifs en phase avec la mission de l'entreprise et son appétence pour le risque
- ✓ **Identification des évènements** (facteurs de risque) interne et externe qui affecte l'atteinte des objectifs
- ✓ **Évaluation des risques** pour déterminer le traitement adéquat
- ✓ **Traitement des risques** conformément au seuil d'appétence
- ✓ **Activités de contrôle** : déclinaison des actions de traitement des risques
- ✓ **Information et communication** : collecte des informations nécessaires au processus de management des risques
- ✓ **Pilotage et reporting** : évaluation ponctuelle du dispositif

Toutefois, nous ne pouvons aborder le management des risques sans citer quelques-unes de ses limites telles que :

- ✓ Une erreur de jugement dans la prise de décision,
- ✓ Des faiblesses potentielles dans le dispositif, susceptibles de survenir en raison de défaillances humaines (erreurs),
- ✓ Des contrôles susceptibles d'être déjoués par collusion entre deux ou plusieurs individus

- ✓ De la possibilité qu'a le management de passer outre les décisions prises en matière de gestion des risques.

Section II : Revue critique de littérature

Dans cette phase, nous aborderons certains travaux antérieurs et semblables à notre étude.

En effet nous allons soulever quelques points relatifs à ces travaux ; les points soulevés seront ainsi matérialisés par l'abréviation PS.

II. 1.) Etude descriptive de la revue critique de littérature:

PS 1 : Le risque opérationnel et la gestion du risque opérationnel

Le risque opérationnel est défini selon Bale II comme « tout risque de perte résultant de la défaillance ou de l'inadéquation des processus internes, des ressources, des systèmes ou d'événements extérieurs, matérialisant les fragilités des cycles d'exploitation et de l'activité courante d'une structure » (Paragraphe 644 de l'accord de Bâle II), Ils sont donc nombreux. Selon Darsa et Jean-David (2013), « Cette définition se montre équilibrée dans son champ d'application parce que tout en restant large dans son objet, elle fait référence à une identification précise des éléments couverts ». En effet, le Comité de Bâle a classifié les types de pertes liées au risque opérationnel à savoir : « la fraude interne, la fraude externe, les pratiques en matière d'emploi sur le lieu travail, les clients, produits et pratiques commerciales inappropriées, les dommages aux actifs corporels, les dysfonctionnements et interruptions d'activité et pannes de système et l'exécution des opérations, livraison et gestion des processus » (classification du comité de Bâle). Ces événements ne se rattachent pas à une ligne de métier particulière et sont susceptibles d'être observés dans toutes les activités de la banque.

PS 2 : Les banques islamiques, entre ressemblance et spécificité par rapport aux banques classiques dans la gestion des risques :

(ATTAR, 2005, pp. 12-13) Rapport aux banques classiques dans gestion des risques : La gestion des risques dans les banques islamiques a la même importance que pour sa consœur classique. En effet, et dans les deux cas, le management de risque se trouve au cœur de l'activité bancaire. Toutefois, il existe des différences émanant de la spécificité des modes opératoires avec des risques partagés avec les banques classiques, et ceux qui font la spécificité des banques islamiques.

Les banques islamiques sont exposées aux risques bancaires traditionnels similaires à leurs contreparties conventionnelles à savoir le risque de crédit, le risque de liquidité, le risque de marché et le risque opérationnel. En plus, ces institutions font face à des risques de nature unique dus à leurs modes de fonctionnement particuliers.

PS 3 : Enjeu des risques opérationnels selon Bâle II

Le comité de Bâle 2, source des réglementations bancaires, établit que les plus grandes pertes résultent d'une mauvaise surveillance du contrôle interne ou d'un manque de respect des procédures existantes. Il soutient que « la gestion du R.O devient un enjeu important pour le développement du Risk Management dans l'évolution des marchés financiers » et que « les banques sont invitées à partager avec les autorités de surveillance du système financier de nouvelles techniques pour identifier, mesurer, gérer et contrôler les R.O dans le but de les éliminer ». Ainsi, la mesure et le contrôle du risque opérationnel sont devenus le sujet de réflexions profondes pour les institutions bancaires et les autorités de surveillance. Le contrôle du R.O est un problème clairement qualitatif (pilier 2 et 3). Mais, depuis peu, c'est la quantification de ce risque qui devient la question primordiale. En effet, la mesure de l'exposition à ce risque a été introduite dans le nouvel accord de Bâle 2 (pilier1).

PS 4 : La nature financière du risque opérationnel selon Culp (2001)

Culp (2001) compare le risque (stratégique) de business et les risques de crédit et de marché. Il conclut que la difficulté d'identifier le risque opérationnel revient aux différents processus d'organisation utilisés par les entreprises pour agir face à ce risque. Culp rejette la nature financière du risque opérationnel et considère que même si les entreprises financières ont récemment commencé à s'intéresser au risque opérationnel sous l'aspect organisationnel, les entreprises non financières ont toujours souffert des risques de management de produit et de la labilité du produit. Culp note que le risque opérationnel est un vaste problème qui peut se produire n'importe où et conclut que la stratégie ne consiste pas à identifier tous les risques opérationnels, mais à retenir ceux dont la perte potentielle associée est conséquente pour l'entreprise.

PS 5 : Méthodes de gestion des risques opérationnels selon Hiwatashi (2002)

Hiwatashi (2002) classe des méthodes de mesure qui peuvent être utilisées sous chacune des deux catégories : Top down et Bottom up. Dans la catégorie Top-down, il considère 3 approches. Dans l'approche de l'indicateur, les variables comme le « Gross Income ou le coût » sont des approximations pour la performance et un certain pourcentage représente alors, l'exposition au risque opérationnel de la banque. La deuxième approche est reliée au MEDAF (CAPM). Tout risque est estimé par le modèle du MEDAF et après la soustraction des risques de marché et de crédit, on obtient le risque opérationnel comme le reste (résidu).

Dans la troisième approche, la volatilité des revenus est vue comme le risque. Dans ce cas, une certaine volatilité, celle des revenus non financiers est considérée comme étant le risque opérationnel.

PS 6 : Interaction entre l'audit interne et la maîtrise des risques opérationnels selon Brody & lowe (2003)

La gestion des risques est une responsabilité conjointe entre le service d'audit interne et le département du risk management (Brody & lowe, 2003). Les agents de gestion des risques sont responsables de tous les processus qui fourniraient une gestion complète des risques. L'auditeur interne est chargé de vérifier si les recommandations faites en matière de gestion des risques sont appliquées correctement (William, 2015). L'audit interne a un rôle efficace dans la gestion des risques (Frigo & Anderson, 2011). Aujourd'hui, cette dernière occupe une place de plus en plus importante dans les préoccupations des dirigeants. A ce titre ces derniers essaient de les identifier et les réduire à des proportions acceptables tous ceux qui menacent la vie de leurs organisations. Pour ce faire, plusieurs conditions doivent être réunies pour mettre en place un système efficace capable de détecter les risques et de les éliminer comme l'audit interne.

II.2) <u>Etude prescriptive de la revue critique de littérature</u> :

Suite à nos recherches, nous avons constaté que quelques rares chercheurs à travers le monde se sont intéressés à l'étude de la gestion des risques opérationnels. Leurs analyses se sont penchées sur les spécificités des risques opérationnels dans les banques islamiques, l'enjeu des risques opérationnels, la nature financière du risque opérationnel, ses méthodes de gestion, l'interaction entre l'audit interne et la maitrise des risques opérationnels entre autres.

Toutefois, parmi les différents points soulevés, certains présentent des limites et nous nous devons de faire une analyse critique sur certains auteurs.

Ainsi, la définition du risque opérationnel a d'abord été mise en exergue selon Bâle II**.** Cependant, l'utilisation de cette définition sans aucune extension amène à des difficultés d'application dans les banques, telles que le risque opérationnel représente seulement une possibilité de perte, le potentiel de gain est négligée. La définition indique que les personnels 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. De plus, le document de travail de Bâle centré sur la perte, ne permet pas de représenter les anciennes pertes des banques, ni les éventuelles à venir.

Aussi, sur ATTAR 2005 l'auteur a développé les ressemblances et spécificités entre les banques islamiques et les banques classiques mais il a plutôt mis en exergue le système de management des risques entre les deux institutions alors qu'il pouvait soulever aussi les risques opérationnels liés à l'aspect religieux et au manque de personnel qualifié capable de mener à bien les opérationnels financiers islamiques qui sont à l'origine de beaucoup de pertes financières issues des erreurs d'exécutions et pratiques inappropriées.

Nous allons également émettre une analyse critique sur l'enjeu des risques opérationnels selon Bâle II qui a accentué cet enjeu sur les pertes résultant d'une mauvaise surveillance du contrôle interne au un manque de respect des procédures en omettant la non qualification du personnel qui est l'une des principales causes du risque opérationnel et la formation du personnel devient ainsi un des enjeux de la gestion des risques opérationnels.

En outre, nous allons parler de Culp qui rejette la nature financière du risque opérationnel en y ajoutant qu'il s'agit d'un vaste problème qui peut se produire n'importe où et conclut que la stratégie ne consiste pas à identifier tous les risques opérationnels mais à retenir ceux dont la perte potentielle associée est conséquente pour l'entreprise.

Cependant, nous ne pouvons pas être d'accord avec l'auteur car dans le processus de gestion des risques, les risques à faible criticité peuvent devenir des risques à criticité élevée s'ils ne sont pas traités et minimisés. Donc selon nous, même les risques les moins importants doivent être identifiés et maîtrisés par le risk-manager.

L'auteur Hiwatashi quant à lui considère trois approches sur la méthode de gestion des risques opérationnels. Il s'agit de l'approche par indicateur, le MEDAF et l'approche sur la volatilité des revenus ; mais les trois approches qu'il a développées ne se limitent qu'à la méthode quantitative ; alors que la plupart des institutions financières font usage de la méthode par approche qualitative.

Nous allons terminer notre résumé et analyse critique sur l'étude des auteurs Brody & Lowe (2003) sur l'interaction entre l'audit et la maîtrise des risques opérationnels. En effet, les auteurs étudient le rôle de l'audit interne dans le processus de gestion des risques opérationnels mais selon nous, l'étude est plutôt limitée car n'ayant pas abordé le système de contrôle interne dans sa globalité à savoir le lien hiérarchique et la collaboration entre les acteurs des différents niveaux de contrôle (premier, second et troisième niveau). Cet aspect aurait rendu leur étude plus enrichissante.

L'ensemble de nos recherches sur différents auteurs ayant traités des sujets en similarité avec notre étude, nous a permis de faire une revue littéraire enrichissante et d'avoir une connaissance transversale sur le thème. Toutefois, nous avons critiqué objectivement ces auteurs dans cette partie tout en reconnaissant qu'ils ont développé des thèmes intéressants qui constituent des perspectives de sujets que nous pourrions éventuellement traités dans la suite de notre cursus et carrière professionnelle.

Chapitre 2 : CADRE CONCEPTUEL

Section I : Définition conceptuelle des variables

L'un des objectifs majeurs de toute organisation est d'assurer son activité dans les conditions d'efficacité, d'efficience, de qualité et de conformité ; mais au quotidien tout ne se passe pas comme prévu.

En effet, l'organisation est assujettie à des risques avec des impacts qui peuvent venir remettre en cause le bon fonctionnement de l'activité ; maîtriser son activité revient donc à avoir une connaissance sur ses processus que l'on peut définir comme l'enchainement des activités et des rôles associés à ses activités mais aussi sur les risques qui peuvent venir influencer sur le bon déroulement des processus.

Il s'agit donc d'une part de comprendre puis d'agir e proposant des plans d'actions pour renforcer des contrôles et limiter les risques : c'est ce qu'on appelle la gestion des risques.

Selon le référentiel ISO, sur le vocabulaire du management des risques, le risque est défini comme l'effet de l'incertitude sur l'atteinte des objectifs. Le risque est ainsi associé à la notion de probabilité et de conséquence plus ou moins grave. Il peut être appréhendé, c'est-à-dire connu au préalable et c'est d'ailleurs ce qui le distingue à l'incident.

Ainsi, toute organisation souhaitant par nature atteindre ses objectifs et réaliser son activité dans les meilleures conditions doit nécessairement disposer d'un processus qui lui permet de comprendre et de gérer efficacement les risques dans l'ensemble de l'organisation.

Cela s'inscrit dans une démarche globale que l'on appelle le management des risques de l'entreprise ou ERM (Entreprise Risque Management).

Ainsi, pour mettre en place une gestion des risques efficace, il faut une méthode ; la plus courante définit un cycle en quatre phases dans une logique d'amélioration continue.

1.) <u>Processus de management ou gestion des risques</u> :

Plusieurs entreprises proposent des dispositifs de management des risques. Ces méthodes et référentiels diffèrent sur certains points mais convergent globalement vers une méthode commune s'appuyant sur quatre grandes actions : l'identification, la priorisation, le traitement et le pilotage des risques.

- **La phase d'identification :**

Cette étape consiste à identifier les risques pouvant avoir un impact sur l'activité de l'entreprise. Les risques peuvent provenir d'un référentiel de risques ; c'est-à-dire un document présentant les risques majeurs recensés pour un métier donné comme le cas de notre étude où les risques opérationnels bancaires prennent assise sur la répartition des risques opérationnels par catégories bâloise qui les répartit en sept catégories.

En effet, les acteurs des processus analysés de l'entreprise sélectionne dans le référentiel les risques qui les concernent et peuvent proposer des risques supplémentaires en lien avec leur activité.

- **La phase de priorisation :**

Une fois les risques recensés, il s'agira ensuite de les prioriser. La gestion des risques consiste ensuite à limiter les risques à un niveau que l'organisation juge acceptable. Alors, pour définir les risques qui seront tolérés et ceux sur lesquels il faudra agir, la méthode consiste à juger la criticité de chaque risque en fonction de deux critères : l'impact ou la gravité en d'autres termes quels seront les conséquences du risque.

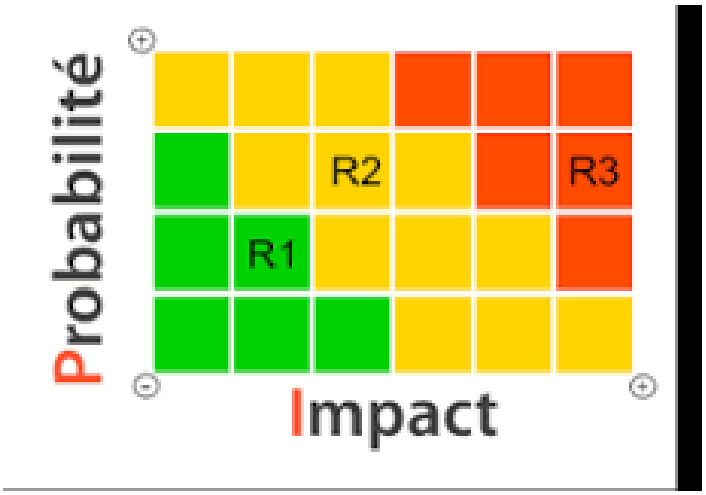
On comprend ainsi que plus les conséquences sont importantes plus le risque est critique. Un risque peut avoir un impact sur l'ensemble des processus ou plus spécifiquement sur l'une de ses activités mais il faut également coupler l'impact à la notion de probabilité (quelles sont les chances pour que le risque se produise).

C'est en effet la réunion de l'impact et de la probabilité qui définit la criticité de l'impact et de la probabilité qui définit la criticité d'un risque. Une échelle de mesure est proposée pour chaque critère ; ce qui permet de positionner chaque risque dans une matrice de criticité.

On identifie alors les risques négligeables, les risques intolérables et les risques avec une criticité intermédiaire.

Un risque critique pourrait être considéré comme acceptable si par exemple l'impact financier est inférieur au coût à investir pour réduire ce risque.

Figure 1 : MATRICE D'ANALYSE DES RISQUES



Source : www.exam-pm.com

R1 : Risques négligeables

R2 : Risques avec une criticité intermédiaire

R3 : Risques intolérables

- **La phase de traitement :**

Le moment d'agir arrive en 3eme étape. L'objectif est de diminuer dans la mesure du possible la criticité d'un risque en le ramenant à un niveau tolérable pour l'entité. Certaines actions pourront tendre vers la suppression du risque ; mais cela reste rare.

Les deux stratégies classiques sont : mettre en place des actions de protection en réduisant l'impact et mettre en place des actions de prévention en réduisant la probabilité.

Cette logique se veut proactive ; analyser et gérer le risque avant qu'il ne se produise.

Il est également possible de réfléchir à des plans d'actions réactifs. C'est-à-dire que le risque est accepté en l'état mais que la procédure de l'entreprise définit des actions à mener en cas de survenance du risque.

Ceux sont naturellement les acteurs métiers qui sont impliqués dans la recherche de solutions proactives dans une démarche participative.

- **La phase de pilotage :**

Lorsqu'on définit un plan d'action pour agir sur un risque, on espère que ses actions auront des conséquences sur la criticité du risque.

L'impact et la probabilité évoluent en fonction de l'efficacité du plan d'action. Il est donc indispensable de réévaluer périodiquement les risques.

Aussi, en fonction du contexte certains risques peuvent apparaître d'autres qui avaient été jugés acceptables peuvent voir leur criticité augmenter. Il est donc important de piloter et suivre l'évaluation du cycle de vie de chaque risque et de savoir adapter sa stratégie si besoin.

Tous les acteurs de l'organisation sont concernés par la mise en place efficace de la gestion des risques.

Tableau 1 : Plan d'action de la phase de pilotage des risques opérationnels

ACTEURS	PLAN D'ACTION
GOUVERNANCE / DIRECTION	Définit les orientations stratégiques et arbitre certains choix de tolérance face à des risques plus ou moins critiques.
MANAGEMENT	Organiser et piloter la gestion des risques; mettre en place les méthodes, les plannings et les outils. Il encourage la démarche participative en collaboration avec les opérationnels pour le recensement des risques, la recherche des solutions et la définition des plans d'actions.
OPÉRATIONNELS	Ils constituent les impactés des plans d'actions sur leurs activités.

Source : Nous-même

Chaque niveau de l'organisation a donc un rôle clé dans la démarche de la gestion des risques.

2.) Définitions de quelques concepts relatifs à la gestion des risques opérationnels :

Pour mieux comprendre la gestion des risques, la définition de certains concepts est primordiale.

a.) La criticité :

Elle correspond au produit de la probabilité de survenance et de gravité des conséquences. C'est un indicateur qui permet d'établir une hiérarchie entre les risques et une priorité dans l'ordre chronologique de prise en charge et d'allocation de ressources.

b.) L'indicateur de risque :

C'est une variable de l'environnement interne ou externe qui permet de mesurer les facteurs générateurs ou aggravant de risques. Les indicateurs influent par conséquent sur la probabilité de survenance d'un risque ou sur la gravité du risque.

On peut citer l'exemple du facteur « opérations de caisses » qui peut accroître la probabilité d'erreur de caisses.

c.) La probabilité d'occurrence :

Elle est également appelée probabilité de survenance et peut être définie comme la possibilité qu'un évènement se réalise au regard des facteurs internes et externes. Elle est l'un des deux caractéristiques d'un risque.

d.) L'impact d'un risque :

Elle correspond à un niveau de préjudice estimé sur les objectifs et les actifs de l'organisation. Un risque est ainsi caractérisé par sa gravité ou impact et sa probabilité d'occurrence

e.) L'incident :

Un incident peut être défini comme la matérialisation d'un risque opérationnel. Un incident est une interruption non planifiée d'un service ou de réduction de la qualité d'un service. Autrement dit, un incident est une défaillance effective d'un processus.

3.) Les risques spécifiques aux banques islamiques :

Les banques islamiques encourent des risques qui leur sont spécifiques en raison de leur caractère islamique qui les différencient des banques conventionnelles. Dans cette rubrique nous tenterons de lister les risques majeurs spécifiques aux banques islamiques.

Le risque opérationnel :

Étant des institutions de création récente, les banques islamiques encourent un risque opérationnel provenant essentiellement du manque de personnel qualifié capable de mener efficacement des opérations financières islamiques. Le caractère spécial des banques islamiques fait que les logiciels informatiques disponibles sur le marché ne soient pas utiles pour les banques islamiques car ils sont conçus pour les banques traditionnelles. Cela ajoute un nouveau type de risque lié à l'utilisation de la technologie informationnelle au niveau des banques islamiques.

Risque de taux de référence :

Comme les banques islamiques ne pratiquent pas de taux d'intérêt, il semble qu'elles sont à l'abri des risques de marché liés à la fluctuation des taux d'intérêt. Toutefois, les variations des taux de marché présentent certains risques pour les gains des institutions financières islamiques.

Les institutions financières utilisent un taux de référence pour déterminer le prix des différents instruments financiers. Ainsi, dans un contrat Mourabaha, la marge de profit est déterminée par le rajout d'une prime de risque au taux de référence. La nature de l'actif à revenu fixe fait que la marge soit fixée pour la durée du contrat. Par conséquent, si le taux de référence varie, les taux de marge fixés dans les contrats Mourabaha ne peuvent pas faire l'objet d'ajustement. Les banques islamiques ont donc à faire face à des risques émanant des variations de taux d'intérêt.

Le risque de liquidité :

Il provient des difficultés à mobiliser des fonds à coût raisonnable (emprunts) ou à vendre des actifs financiers. Le risque de liquidité émanant de ces deux sources est d'une importance particulière pour les banques islamiques. Sachant que les emprunts à intérêt sont prohibés par la Charia, les banques islamiques ne peuvent pas recourir à ce mécanisme pour se ressourcer, le cas échéant, en argent liquide. De même, la Charia n'autorise pas la vente d'une créance en dehors de sa valeur nominale. Par conséquent, il est exclu pour les institutions financières islamiques de s'alimenter en argent liquide en vendant des actifs financiers.

Le risque juridique :

Sachant que les contrats financiers consacrés par les banques islamiques ont un caractère un peu spécifique, celles-ci encourent des risques liés à leur documentation et leur mise en application. En l'absence de formalisation de ces contrats pour les différents instruments financiers, les banques islamiques continuent de les concevoir en fonction de leur appréhension de la Charia, des lois nationales, de leurs besoins et leur intérêt. Cette manque d'uniformisation des contrats et l'absence de cadre juridique destiné à résoudre les problèmes liés à l'exécution de ces contrats pour toutes les parties concernées font augmenter les risques d'ordre juridique associés aux engagements contractuels des banques islamiques.

Le risque fiduciaire :

L'AAOIFI (Accounting and Auditing Organisation of Islamic Financial Institutions) (1999) identifie également le risque fiduciaire comme le risque que les clients perdent confiance en leur banque suite à la non-conformité des opérations bancaires avec les principes de la finance islamique ou bien à cause d'une mauvaise gestion des fonds. Ceci engendre généralement une dégradation de l'image de la banque et une perte de confiance de la part des titulaires des dépôts qui peuvent être amenés à retirer leurs dépôts.

Le risque d'investissement :

Les banques islamiques offrent un financement sous les principes du partage de profit et des risques avec ses déposants. A ce titre, le risque d'investissement dans les banques islamiques découle des choix de placement de la banque, puisqu'en investissant en capital, la banque encourt le risque d'une perte de ses apports, perte qu'elle partage avec ses déposants.

Le risque religieux ou de non-conformité :

Les écoles de pensée musulmanes se rejoignent dans l'interprétation de la plupart des textes religieux et dans la promulgation de la quasi-majorité des opinions juridiques. Cependant, il n'est pas exclu que certaines d'entre elles émettent un avis différent concernant un même questionnement juridique ou qu'elles produisent des décisions divergentes. Ces situations sont rares mais peuvent, quand elles se produisent, entraver par exemple le lancement d'un produit par une institution financière islamique.

4.) Les principaux enjeux des risques opérationnels :

Le premier qui apparaît dans la mise en place d'un dispositif de maîtrise des risques opérationnels est la nécessité de se mettre en conformité avec la réglementation bancaire et ainsi optimiser le montant des fonds propres (non lié à des activités rémunératrices) à allouer aux risques de cette nature. Comme autres enjeux, outre de la performance, nous pouvons citer : la sécurisation des résultats en évitant ou en couvrant des risques qui entraînent des pertes nettes et de la notation en évitant des « aléas » non souhaités qui peuvent avoir des impacts sur la solvabilité ou la notoriété de la banque et une plus grande compétitivité du fait des amélioration de tarif possible si les pertes constatées sur les événements à fréquence diminués.

Le risque opérationnel est donc un enjeu financier considérable et sa concrétisation peut avoir d'énormes conséquences sur l'activité bancaire notamment une perte financière, un manque à gagner considérable, un problème d'image et de réputation etc….

Ainsi, l'enjeu majeur pour une banque est de trouver un système de gestion global et efficace des risques opérationnels tout en se conformant à la réglementation bancaire.

5.) Les approches de mesure du risque opérationnel selon Bâle II :

La réglementation prévoit trois (03) approches de calcul : approche de base ; approche standard et approche des mesures avancées (Basel committee supervision).

a.) Approche indicateur de base (basic indicator approach) :

Elle consiste en l'utilisation d'un indicateur unique pour l'exposition d'une banque au risque opérationnel global. Le comité de Bâle propose que les banques appliquent un pourcentage fixe

(alpha= 15%) à un indicateur sur lequel sont évalués les fonds propres réglementaires et qui présente l'exposition potentielle aux risques opérationnels.

Cet indicateur est le produit bancaire (PNB) moyen des trois dernières années.

Fonds propres (capital requis)= à*PNB total= 15%* PNB

Aux fins de calcul de l'exigence des fonds propres au titre du risque opérationnel, les différentes composantes du PNB sont : les intérêts perçus et produits assimilés, les intérêts versés et charges assimilées, les revenues des titres, les commissions perçues et celles versées, le résultat provenant d'opérations financières et les autres produits d'exploitation.

b.) Approche standard (standard approach) :

Dans cette approche, l'activité est décomposée en métiers et produits. Les banques, ici, doivent détenir des fonds propres correspondant à chacun des huit métiers à un pourcentage fixe (beta β) de leur produit net bancaire moyen des trois dernières années.

Tableau 2 : coefficients du risque opérationnel par métier bancaire

Lignes de métiers	Coefficient βi (%)
Financement des entreprises	18%
Négociation et vente industrielle	18%
Paiements et règlements	18%
Banque commerciales	15%
Service d'agence	15%
Banque de détail	12%
Gestions d'actifs	12%
Courtage de détail	12%

Source : Jiménez & al (2008 : 29)

c.) Approche avancée (Advanced measurement approach ou AMA) :

Il ne s'agit plus d'une approche unique, définie par le régulateur, mais d'un ensemble de modèles internes réunies sous le vocable « d'approche de mesures complexes » ou AMC (Advanced measurement approach ou AMA) approuvé par les autorités de contrôle sur la base d'une série de critère.

Selon l'AMA, l'exigence de fonds propres réglementaire équivaut à la mesure du risque opérationnel produite par le système interne de la banque, sur base de critères quantitatifs et qualitatifs.

Le Comité de Bâle propose plusieurs alternatives au sein du régime AMA : la méthode Scorecard, l'analyse de scénarios (Scenario-based AMA), et enfin, la méthode LDA (Loss Distribution Approach), la plus sophistiquée au plan technique. La pratique de chacune de ces méthodes est soumise au respect d'un ensemble de critères qualitatifs, notamment en termes d'évaluation du risque opérationnel et de procédure de collecte des données de perte. C'est là leur dénominateur commun. Sur le fonds, la différence concerne essentiellement le type d'information privilégié dans le calcul du capital réglementaire.

Les accords de Bâle II n'imposent aucune méthode particulière de calcul pour les banques adoptant l'approche de mesures complexes (AMA). Ce choix est laissé à la discrétion des banques, pourvu qu'elles satisfassent aux critères qualitatifs et quantitatifs énoncés dans l'accord.

Deux principales méthodologies sont utilisées pour le déploiement de ces approches de mesures avancées.

- **La méthodologie Top -DOWN :**

La méthodologie Top down donne une estimation du risque opérationnel sur la base des variations historiques des résultats après intégration de facteurs tels que l'évolution de l'activité où le coût lié aux changements. L'hypothèse sous-jacente est que les pertes historiques sont une bonne mesure des pertes futures.

Dans cette approche, certaines banques ont tendance à évaluer l'exigence de fonds propres pour le risque opérationnel en prenant simplement un pourcentage d'un indice d'activité comme le produit brut bancaire.

D'autres estiment le risque opérationnel selon un pourcentage fixe correspondant aux coûts opérationnels de l'établissement où de la ligne métier.

Selon cette approche, on peut envisager un schéma dans lequel le montant alloué en fonds propres pour couvrir le risque opérationnel serait égal :

Indice d'activité * multiplicateur de la ligne d'activité*k

Avec k est un score représentant l'environnement.

Cette approche présente l'avantage de sa facilité à mettre en place, une fois que l'élément inconnu de volatilité des résultats historiques des activités est résolu. Toutefois elle présente une faible valeur analytique ; un rapport difficile à établir entre perte et revenu variable et entre risque opérationnel et revenu variable.

On peut dire que les modèles proposés par cette méthode ne sont pas propices à la mise en œuvre d'un contrôle interne, d'où son ignorance à la qualité du contrôle. Dans ce cadre et pour mieux maîtriser le risque opérationnel les établissements s'orientent d'avantage vers des approches à forte valeur ajoutée type " Bottom Up ".

- **Méthodologie Bottom -Up :**

Les modèles Bottom -Up correspondent à une approche structurelle dans laquelle l'identification, l'évaluation des pertes et risques sont définis à l'intérieur de la banque en fonction de la logique de comportement, en séparant tout ce qui peut provenir des personnes, des processus et de la technologie.

En effet, lors d'une telle approche, chaque opération est analysée de son initiation jusqu'à sa comptabilisation. A chaque étape les tâches et contrôles clés sont décrits, testés et évalués.

Le recensement et l'évaluation des risques opérationnels se faisant selon une cartographie (zones géographiques, ligne métier, entité, activité et productivité) qui se décline de la plus globale à la plus exhaustive.

Cette approche apparaît plus utile pour comprendre la nature du risque opérationnel et pour permettre un contrôle interne. Elle est à forte valeur ajoutée car elle intègre des cartographies des risques opérationnels liés aux activités et processus comprenant l'identification, l'analyse et l'évaluation des risques.

Elle permet de contribuer à la connaissance des risques opérationnels au niveau des activités, et au changement comportemental des différents acteurs et notamment les opérationnels.

Toutefois elle présente l'inconvénient de la subjectivité et la consistance des évaluations.

Les approches de mesures avancées sont :

- **La Loss Distribution Approach :**

L'idée de base de LDA est assez simple : on considère que la perte annuelle totale d'une banque due au risque opérationnel se compose de deux éléments, la fréquence et la sévérité. Chacune se présente sous la forme d'une distribution statistique. La distribution de fréquence représente l'occurrence d'événements de pertes opérationnelles, c'est-à-dire le nombre de pertes observées. La distribution de sévérité traduit quant à elle l'amplitude de ces pertes, à savoir le montant, en unités monétaires, des pertes individuelles subies par la banque.

L'idée générale de la méthode LDA (Loss Distribution Approach) est de modéliser la perte liée au risque opérationnel pour une période donnée (par exemple, un an) et d'en déduire la valeur en risque. Frachot et al. (2003) proposent de procéder en cinq étapes pour implémenter cette méthode :

- Estimation de la distribution de sévérité ;

- Estimation de la distribution de la fréquence ;

- Calcul de la charge en capital;

- Calcul des intervalles de confiance;

- incorporation des avis d'experts.

Pour cette approche, on ne va pas entrer dans la formulation mathématique de ces différentes étapes, mais simplement de comprendre l'idée générale de la méthode LDA.

A l'instar de la plupart des modèles de mesure du risque opérationnel, la LDA se fonde sur une approche actuarielle (fréquence/sévérité) très ancienne largement utilisée dans le domaine de l'assurance pour modéliser des problèmes similaires.

Pour que le modèle LDA puisse tourner, il faut lui fournir deux éléments essentiels : la distribution de la sévérité des pertes (loss severity distribution) et la distribution de la fréquence des pertes (loss frequency distribution). Ces deux distributions, qui forment l'historique des pertes, sont ensuite combinées par une technique statistique appelée « convolution » (Monte

Carlo) afin d'obtenir la distribution de la perte totale. Celle-ci étant le résultat de plusieurs pertes successives, il s'agit d'une perte agrégée (aggregate loss distribution).

A partir de la perte totale, on dérive ensuite la perte attendue ou moyenne (expected loss) et la perte exceptionnelle (unexpected loss), pour un niveau de confiance donné.

L'accord stipule qu' « un établissement doit faire la preuve que sa mesure du risque opérationnel répond à un critère de solidité comparable à celui de l'approche NI pour le risque de crédit (correspond à une période de détention d'un an et à un intervalle de confiance de 99, 9éme percentile de la distribution de perte agrégées). On utilise souvent cette notion en matière de gestion des risques financiers sous le terme de Valeur-au-risque avec un intervalle de confiance de 99,9%.

Afin de différencier le risque opérationnel du risque de marché ou ce terme est né, nous utiliserons la terminologie « valeur-au-risque opérationnel » ou Op Var.

Le comité de Bâle a décomposé les Op Var en deux éléments : la perte attendues PA et les pertes inattendues(PI).

- **L'approche Scorecard :**

L'appellation « scorecard » regroupe un ensemble d'approche visant à identifier, mesurer et surveiller les risques opérationnels. Ces approches traduisent une évaluation qualitative des risques et des contrôles en une valeur numérique ou score.

L'un des objectifs poursuivis par les banques ayant développé et implémenté une approche Scorecard est de se doter d'un outil permettant de faire le lien entre la mesure et la gestion du risque opérationnel.

Les grandes étapes de mise en œuvre de la démarche scorecard sont les suivantes :

Evaluation du capital initial en se basant sur une autre approche : celle-ci pourrait être l'approche LDA, l'approche des scénarios, l'utilisation du benchmarking ou une méthode forfaitaire. Il est crucial à ce stade de considérer ce capital initial crédible.

Définition de la structure de la scorecard et sa mise en œuvre, permettant d'aboutir à un score pour chaque catégorie de risque et pour chaque ligne de service.

Allocation du capital initial aux lignes de service sur base du score et donc des performances de l'organisation en matière de maîtrise du risque opérationnel. Par la suite, le capital alloué à chaque ligne de service va varier en fonction de l'évolution des résultats de scorecard. Dans cette approche, le capital initial n'est pas recalculé à chaque évaluation.

Conformément aux exigences du comité de Bâle, les données internes ont également un rôle à jouer dans l'approche scorecard.

Ces données internes et externes sont utilisées à plusieurs niveaux. En effet, elles peuvent être utilisées de la détermination du capital initial en utilisant une approche de distribution de pertes. Une autre utilisation intéressante de ces pertes est leur analyse afin d'identifier les facteurs de risques ayant amené à la réalisation de ces pertes est leur analyse afin d'identifier les contrôles internes permettant de réduire l'impact ou de contrôler les facteurs de risque identifiés.

Une fois la scorecard établie et utilisée, les pertes internes et externes peuvent être utilisées afin de valider la qualité des réponses apportées aux questionnaires. De plus, leur analyse régulière permet de s'assurer que les risques et facteurs de risque associés sont actualisés, ce qui permet de prendre en compte l'apparition de nouveaux facteurs de risque dans l'analyse. La validation des résultats de la scorecard avec des donnés objectifs est importante, compte tenu des nombreux éléments subjectifs intervenant dans sa construction.

Le Comité de Bâle n'a fourni aucune formulation mathématique pour cette approche. Néanmoins, les groupes de travail au sein des banques ont proposé des formules de calcul du capital réglementaire (K) de la forme :

K Scorecard = EI ij × ù ij × RS ij

Avec EI l'indicateur d'exposition (Exposure Indicator), RS le score de risque (Risk Score) et où un facteur d'échelle (Scale Factor).

- **L'approche par les scénarios :**

L'approche scénarios est en fait un prolongement de l'approche scorecard. Le risque y est envisagé comme une combinaison de la sévérité et de la fréquence des pertes potentielles sur une période donnée. La fréquence et la sévérité (potentielles) de la perte peuvent être mesurées en unités monétaires et en nombre d'occurrences annuelles. Le risque reflète en quelque sorte

la vulnérabilité de la banque. L'évaluation du risque devrait par conséquent se focaliser sur les vecteurs de cette vulnérabilité. Or, celle-ci provient pour l'essentiel des facteurs de risque sous-jacents. Réduire le niveau de risque opérationnel impose donc une bonne lisibilité de l'exposition du portefeuille de la banque aux différents facteurs de risque préalablement définis.

L'un des objectifs de l'utilisation de cette approche dans la quantification des risques opérationnels est de fournir une évaluation prospective du risque opérationnel.

En fait, on pourrait considérer que l'évaluation du risque est intrinsèquement liée à l'analyse de scénarios, qui s'applique d'ailleurs également aux risques de marché et de crédit.

De manière générale, les scénarios sont des événements susceptibles de se produire dans l'avenir. Ils expriment l'idée selon laquelle les experts d'une banque ont certaines intuitions ou des informations sur le risque qui ne sont pas contenues dans l'historique de données. Pour être réellement utile à des fins de décision en matière de risque, une analyse de scénarios doit être en mesure de répondre à ces deux questions : à quelle fréquence le scénario X est-il susceptible de se produire ? Quel est le montant de la perte si le scénario X se produit ?

L'axe principal de développement de cette approche est le développement et l'évaluation des scénarios, ces derniers doivent permettre d'évaluer les deux paramètres caractérisant le risque : la fréquence et la sévérité potentielle d'un événement générateurs de pertes.

Cette évaluation nécessite la constitution de scénarios, chaque scénario prenant en considération l'ensemble des facteurs de risque opérationnel.

Parmi les facteurs de risque opérationnel les plus courant, on recense le niveau de compétence/qualification du personnel, l'organisation interne/transferts d'information, l'infrastructure IT (sécurité des systèmes), les procédures de contrôle des activités non autorisées/vol et fraude/erreurs non intentionnelles (saisie, exécution et suivi des transactions), les mesures de protection contre des catastrophes et autres sinistres, ou encore, le respect des obligations légales (conformité, diffusion d'informations et devoir fiduciaire).

En considérant ces différents éléments, la banque va donc générer des scénarios sous forme de questions « what if ».

Pour chaque scénario, l'évaluateur considère plusieurs hypothèses, dont par exemple un cas normal, un cas extrême et un cas catastrophique.

En effet, les scénarios vont se construire en fonction de l'organisation de la banque et de la catégorisation d'événement de pertes. Les facteurs de risque et les indicateurs de risque associés serviront de contexte et de base à l'évaluation des scénarios.

6.) Dispositif de maîtrise des risques opérationnels :

Selon la circulaire 004/2017/CB de la BCEAO, le dispositif de gestion des risques doit être basé sur des stratégies, politiques et procédures bien documentées qui permettent d'identifier, de mesurer, d'évaluer, de suivre, de déclarer et de contrôler ou d'atténuer l'ensemble des risques significatifs de l'établissement. Les stratégies, politiques et procédures doivent être dynamiques, de manière à refléter l'évolution du degré d'appétence au risque de l'établissement, son profil de risque ainsi que les conditions de marché et l'environnement macroéconomique. L'établissement doit veiller à la mise en œuvre de stratégies, politiques et procédures permettant d'avoir une vision globale, à l'échelle de l'organisation, de ses expositions sur chaque type de risque.

Il s'agit d'une procédure combinant plusieurs facteurs dont la finalité est soit de réduire la probabilité de survenance du risque, soit de limiter les impacts. Le but du dispositif de maîtrise des risques opérationnels est de ramener le niveau jugé acceptable face aux objectifs fixés en termes de processus de gestion des risques.

Section II : Modèle conceptuel d'analyse

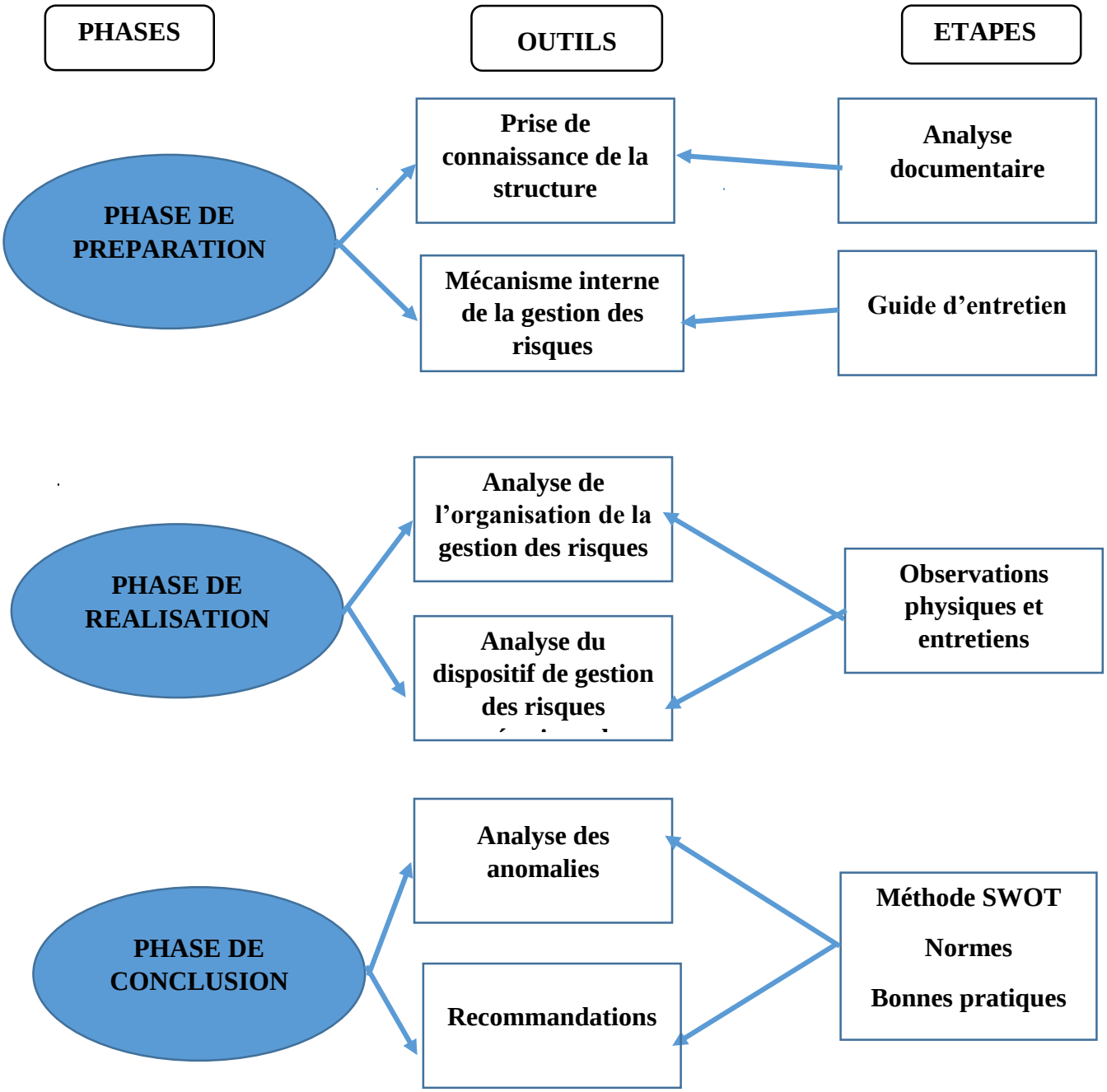
Le modèle d'analyse consiste en une représentation schématique de la démarche utilisée pour l'obtention des informations et l'élaboration de notre étude. Notre démarche est divisée en trois phases. Chaque phase comprend des étapes et pour la matérialisation de ces étapes des outils sont utilisés.

_ La phase de préparation : cette phase permettra de mieux connaître la structure à travers son historique, ses missions, ses activités et son organisation. Cette étude prendra aussi compte les mécanismes internes de gestion des risques opérationnels mis en place. Pour ce faire, les outils utilisés sont : l'analyse documentaire, le guide d'entretien et l'observation ;

_ La phase de réalisation : cette phase sera consacrée à l'évaluation de la gestion des risques à la BIS. Cette évaluation consistera à analyser l'organisation, la gestion des risques ainsi que le dispositif de gestion des risques opérationnels. Cette phase est ainsi une phase terrain ;

_ La phase de conclusion : le but de cette phase sera d'analyser des anomalies et faire les recommandations qui vont aider la Direction à une meilleure gestion des risques opérationnels.

Figure 2 : Modèle d'analyse



Source : Nous même

DEUXIÉME PARTIE : Cadre méthodologique et analytique

CHAPITRE 1 : CADRE MÉTHODOLOGIQUE

Section I : Présentation de l'entreprise ou du secteur

1.) Historique de la Banque Islamique du Sénégal :

En mars 1981 se créait une association musulmans sous forme de holding, dénommé Dar Al Maal Al Islami (DMI) qui fixe son siège à Genève. Devenu très vite un puissant groupe financier islamique installé dans plusieurs pays du monde, elle fera sa pénétration en Afrique en 1983 avec la création de trois filiales dans trois pays d'Afrique de l'Ouest à majorité musulmane : la Guinée, le Sénégal et le Niger.

La création des banques islamiques nécessitait une dérogation spéciale sur la loi N° 76-52 portant réglementation bancaire de l'UMOA. En septembre 1982, après plusieurs investigations, le Conseil des Ministres de l'UMOA autorisait la dérogation et dès mai 1983 les banques islamiques démarrèrent leurs activités sous la dénomination de Massraf Fayçal al Islam (MFI).

En 1983, le groupe financier Dar Al Mal Islami crée une filiale au Sénégal sous l'appellation de Masraf Fayçal Al Islami.

Le capital lors de la constitution de la société s'élevait à 1813 millions de FCFA.

Le 06 Février 1996, une restructuration du capital est réalisé sous la forme d'une opération 'd'accordéon' réduction du capital suivi de son augmentation. Cette restructuration est réalisée avec l'entrée de nouveaux actionnaires et le changement de dénomination de la structure qui devient la Banque Islamique du Sénégal (BIS). Le capital est porté à FCFA 2 705 640 000 (deux milliards sept cent cinq millions six cent quarante mille).

En 2009, Dar Al Maal Al Islami de Genève cède sa participation à la Société Islamique pour le Développement du Secteur Privé (SID) qui devient actionnaire de BIS.

En 2010, le capital social est augmenté et porté à FCFA 10 000 000 000 (dix milliards).

En 2011, SID cède la totalité de sa participation à Tamweel Africa holding (TAH), qu'elle a créée pour gérer sa participation dans les banques islamiques. TAH devient actionnaire de la BIS.

En 2014, TAH cède des actions qu'elle détenait dans le capital de la BIS à la BID. Le capital de la banque a été porté à 20 milliards.

Depuis l'année 2020, le capital est de 30 milliards.

La BIS va bientôt fêter ses 40 ans. Elle se positionne aujourd'hui sur l'échiquier bancaire sénégalais comme une banque de référence. Son actionnariat est composé de diverses entités, parmi lesquelles le groupe de la Banque Islamique de Développement qui est l'actionnaire majoritaire à hauteur de 77%. La seule institution financière sénégalaise dotée d'un actionnariat composé d'une institution financière multilatérale cotée triple A.

L'État du Sénégal est également actionnaire à hauteur de 6%, enfin le secteur privé est représenté à hauteur d'environ 17%.

Depuis Janvier 2021, le capital de la BIS s'élève à peu près 50 milliards et son réseau d'agence actuel est composé de 32 agences et trois points avec une prévision d'ouverture d'autres agences d'ici la fin de l'année 2022.

2.) Objectifs de la Banque Islamique du Sénégal :

Forte de l'appui des principaux actionnaires, la BIS entend contribuer au développement économique du Sénégal à travers la réalisation des objectifs fondamentaux repris à l'article 3 de ses statuts à savoir :

- Mener des activités de collectes d'épargne et de distribution de crédits sur la base des principes édictés par l'islam, répondant ainsi aux besoins et aspirations d'une grande partie de la population sénégalaise.
- Offrir aux entreprises et opérateurs économiques des services bancaires modernes et compétitifs en conformité avec les prescriptions islamiques

« Le secteur bancaire sénégalais est en effet très concurrentiel; ce qui fait la différence entre les banques, c'est d'abord la qualité de service. A ce niveau, la BIS a mis en place un certain nombre de dispositifs pour améliorer et enrichir le parcours client, qu'il soit un particulier, une entreprise ou un institutionnel. L'objectif ultime est de permettre à ce client d'accéder au crédit et aux services bancaires de qualité dans un délai le plus court possible » dixit Monsieur Mouhamadou Madana Kane actuel Directeur Général de la BIS lors d'un entretien avec le Magazine Business Africa N°176 paru au mois de Juillet 2022.

3.) La spécificité de la BIS vis-à-vis des banques conventionnelles :

La banque islamique est une banque qui s'engage à appliquer les principes de la charia et la sunna du prophète Mohammad PSL dans ses transactions bancaires. Elle est aussi définie comme une institution financière qui a pour tâche principale d'attirer les fonds monétaires et de les utiliser efficacement de sorte à garantir leur augmentation en conformité avec les règles de la charia. C'est ce qui fait sa spécificité par rapport aux banques conventionnelles.

Ainsi, les principes de la Banque Islamiques sont : l'interdiction de l'usure considérée comme du riba, la banque Islamique n'offre pas ses services à des activités interdites (haram) mais également prône l'honnêteté et la transparence.

Cependant, des non musulmans peuvent pratiquer des activités de finance islamique car la finance islamique découle du FIQH; c'est-à-dire le relationnel, les rapports sociaux entre les hommes.

Pour rappel, depuis 2018, les autorités de la Banque Centrale des États de l'Afrique de l'Ouest ont adopté une nouvelle réglementation régissant les conditions d'exercice des activités de finance islamique par les banques islamiques ou par les fenêtres islamiques ouvertes au sein des banques conventionnelles.

A ce jour, la BIS est la seule banque habilitée à réaliser exclusivement des opérations de finance islamique au Sénégal. Un dispositif de gouvernance existe au sein de la banque pour garantir la conformité islamique de ses opérations avec la mise en place d'un Conseil de Conformité Interne (Shariah Board) composé d'experts nationaux et internationaux en finance islamique.

4.) Les défis de la Banque Islamique du Sénégal :

Les défis de la BIS reposent sur une stratégie quinquennale portant principalement sur deux piliers.

Le premier pilier c'est la consolidation de son développement interne avec l'ambition claire de devenir la première banque au Sénégal. Pour se faire, la BIS poursuit la modernisation de son outil de travail avec comme pierre angulaire la digitalisation de l'ensemble de ses processus clés. La croissance de la banque sera accompagnée d'une efficacité opérationnelle et d'une meilleure compréhension des besoins de ses clients.

Le second pilier est une stratégie de croissance externe avec l'ambition de créer un écosystème de services financiers islamiques autour de la BIS. D'ici les cinq prochaines années, la banque

souhaite ouvrir des filiales ou succursales bancaires dans d'autres pays de l'UEMOA et mettre sur pied d'autres filiales dans le domaine notamment de l'assurance TAKAFUL et de la microfinance islamique.

Tous ces chantiers constituent un ensemble de défis à relever et la seule ambition de la BIS est de jouer son rôle principal qui est de financer l'économie étant donné que la finance islamique est une finance de développement.

5.) Les produits et services offerts par la BIS :

Dans le but de satisfaire sa clientèle, la Banque Islamique offre un large choix de produits et services adaptés à chacun des segments de son portefeuille clientèle.

a.) Comptes courant et épargnes :

La BIS propose aux clients un compte courant islamique avec plusieurs packs disponibles et adaptés à tous les particuliers et entreprises; ainsi que plusieurs types d'épargne.

- **ISLAMIQUE :**

Le compte courant islamique est un compte de dépôt à vue non rémunéré. Il peut être ouvert en monnaie locale ou en devise. Les comptes étrangers sont soumis aux dispositions de la réglementation des changes. Les titulaires de comptes courants islamiques ne perçoivent aucune rémunération dans la mesure où ils peuvent disposer à tout moment de leur avoir.

- **YAXANAL :**

Le compte d'épargne est régi par les mêmes règles que le compte courant islamique en ce qui concerne la disponibilité des fonds et l'absence de rémunération.

Cependant, le compte d'épargne peut avoir un objet spécifique (épargne logement, épargne équipement, épargne pèlerinage…) permettant au titulaire d'obtenir un financement complémentaire au bout d'une certaine période. Ce produit contribue à la collecte des ressources. Toute personne physique majeure ou mineure autorisée peut en bénéficier.

Le versement initial de 15 000 FCFA à l'ouverture du compte représente le solde minimal.

Avantages clients : épargne rémunérée, rémunération halal, pas de frais de gestion, carte GIM gratuit.

❖ **TAALIB :**

TAALIB est un compte d'épargne rémunéré suivant les principes de la finance islamique. Ce compte vous permet de sécuriser vos économies tout en les fructifiant. L'épargne TAALIB est un produit destiné aux élèves et étudiants dans le but de familiariser les futurs salariés et chefs d'entreprises à la BIS. Ce produit contribue à la collecte des ressources.

Toute personne physique majeure ou mineure (avec autorisation parentale si nécessaire) peut en bénéficier.

Le solde initial du compte et minimal du compte s'élève à 5 000 FCFA et la rémunération se fait suivant les performances de la BIS en fin d'année.

Avantages clients : gratuité de la carte GIM, rémunération de l'épargne suivant le principe islamique, exonération de frais de gestion, accès au financement à marge préférentiel dès le premier salaire domicilié.

❖ **GOU'NGUE**

L'épargne GOU'NGUE est un produit destiné aux particuliers et leur permet de constituer une épargne destinée au financement des études et/ou projets futurs de leurs enfants. Toute personne physique majeure titulaire d'un compte courant.

Le versement initial minimum est de 20 000 FCFA avec des prélèvements mensuels de 10 000 FCFA minimum. La rémunération du compte se fait suivant les performances de la BIS.

Avantages client : épargne rémunérée (rémunération halal), pas de frais de gestion, préparation sereine des études des enfants, frais gratuit pour une attestation de prise en charge pour l'enfant.

❖ **HAJJ :**

HAJJ est un plan d'épargne dont le but est de permettre aux particuliers d'effectuer le pèlerinage à la Mecque. Toute personne physique majeure ou mineure avec un versement initial de 30 000 FCFA et des versements mensuels minimums de 25 000 FCFA. La rémunération du compte se fait suivant les performances de la BIS.

Avantages client : constitution souple des fonds nécessaires au hajj.

b.) Les produits de financement :

La BIS propose plusieurs modes de financements adaptés à tout type de client.

- **PRÊT'0**

Le financement 0% est un financement QARDH HASSAN qui permet aux particuliers de bénéficier d'un financement halal. Ce produit offre à sa clientèle la possibilité d'accéder à des crédits sur le court terme à l'occasion d'évènements comme les fêtes religieuses. Le client ne rembourse que le capital emprunté.

Toute personne physique salariée ayant domicilié ses revenus à la BIS et éligible à ce type de financement peut en bénéficier.

Les frais fixes de 11 700 FCFA TTC, pas de souscription d'assurance vie.

Avantages client : satisfaction d'un besoin de financement, financement à marge de profit nulle, mise à disposition rapide des fonds (comité restreint).

- **NOFLAY :**

C'est un financement qui permet aux particuliers salariés en CDI (Contrat à durée déterminée) ayant domicilié leur salaire et étant éligible à ce type de crédit (employeur listé dans la classification des entreprises) d'acquérir des équipements sur le moyen terme. Le montant du crédit peut aller jusqu'à 10 000 000 FCFA pour une durée maximum de 6 ans avec une marge de 9% plus TAF (Taxe sur les Activités Financières).

Avantages client : satisfaction d'un besoin de financement, financement sur le moyen terme, mise à disposition rapide des fonds.

- **MAKAANE :**

Le plan d'épargne logement MAKAANE est un placement conçu pour la préparation d'un projet immobilier. Il permet à terme d'obtenir un prêt avec une marge préférentielle pour l'acquisition, la construction ou rénovation de la résidence principale ou secondaire.

Toute personne physique majeure ou mineure autorisée (autorisation parentale) titulaire d'un compte courant peut en bénéficier et une durée de 20 ans maximum.

Garanties : Hypothèque sur le bien financé, délégation d'assurance vie (si acceptation du client)

Avantages client : satisfaction d'un besoin de financement immobilier, financement à marge faible et sur la longue durée, épargne et financement halal.

- **COMMODITY**

C'est un mode de financement de type commodity mourabaha (tawarruq) par lequel la banque achète une marchandise pour le compte du client et la revend pour lui permettre d'avoir de la trésorerie.

Le mode de financement Commodity mourabaha est destiné aux particuliers, professionnels et entreprises titulaires d'un compte courant.

Avantages client : Financement respectant les principes de la finance islamique, satisfaction d'un besoin de trésorerie

- **FIN AUTO**

C'est un mode de financement de type Mourabaha par lequel la BIS achète au près du fournisseur le véhicule de votre choix et vous le revend au prix de revient majoré d'une marge bénéficiaire fixée d'accord parties.

Le mode de financement Mourabaha Véhicule est destiné aux particuliers, professionnels et entreprises titulaires d'un compte courant.

Avantages client : Financement respectant les principes de la finance islamiques, financement à marge compétitive.

- **IMMOBIS**

C'est un mode de financement de type mourabaha à travers lequel la BIS finance l'acquisition d'un bien immobilier.

Le mode de financement Mourabaha immobilier est destiné aux particuliers, professionnels et entreprises titulaires d'un compte courant.

Avantages client : Financement respectant les principes de la finance Islamique, financement à marge compétitive.

- **IJARA :**

L'Ijara consiste pour la Banque à acquérir des biens qu'elle met à la disposition du client en location simple. Dans ce cas, la Banque perçoit un loyer pour le service rendu.

Ijara est un contrat de location de biens assorti ou non d'une promesse de vente au profit du locataire.

Il s'agit d'une technique de financement qui fait intervenir trois acteurs principaux :

1. Le fournisseur (fabricant ou vendeur) du bien.
2. Le bailleur (en l'occurrence la banque qui achète le bien pour le louer à son client).
3. Le locataire qui loue le bien.

Le droit de propriété du bien revient à la banque durant toute la période du contrat, tandis que le droit de jouissance revient au locataire.

c.) <u>Les produits d'investissement</u> :

La BIS propose trois types de comptes d'investissements à sa clientèle.

❖ **INVESTIS**

C'est un compte participatif à travers lequel le client remet les fonds à la BIS qui se chargera de les faire fructifier en les investissant dans des projets rentables et conformes aux principes de la finance islamique. Le client est rémunéré en fonction des performances de la banque.

Qui peut en bénéficier

Toute personne physique et morale.

Quelles sont les conditions ?

- Être titulaire d'un compte
- Montant minimum d'investissement : 5 000 000 FCFA

Quels sont les avantages

- Sécurité des fonds
- Gestion efficace
- Possibilité de consultation via le service banque en ligne BIS
- Possibilité de faire plusieurs versements et retrait sur le compte
- Les fonds déposés génèrent une rémunération conformément aux principes de la finance Islamique
- Gratuité des frais de gestion

❖ **ISLAMIK :**

ISLAMIK est un compte d'investissement moudharaba qui vous permet de placer une somme d'argent pour la rentabiliser.

Qui peut en bénéficier ?

Toute personne physique ou morale.

Caractéristiques d'islamik :

Minimum de placement de 5 000 000 FCFA.

Renouvellement des placements par tacite reconduction.

- Rémunération suivant les performances de la BIS
- Placement sécurisé
- Rémunération halal

❖ **PLACECO :**

C'est un compte d'investissement sous forme de contrat de mandat par lequel le client (investisseur) mandate la banque de lui faire fructifier ses fonds. Une clé de répartition est fixée d'accord parties.

Qui peut en bénéficier

Toute personne physique et morale.

Quelles sont les conditions ?

- Être titulaire d'un compte
- Montant minimum d'investissement: **5 000 000 FCFA**

Quels sont les avantages ?

- Sécurité des fonds
- Régie d'investissement conforme aux principes de la finance islamique
- Rémunération compétitive fixée d'accord parties

d.) <u>La banque électronique</u> :

La BIS offre des produits et services digitaux à sa clientèle.

❖ **CARTE GIM-UEMOA :**

La Banque Islamique du Sénégal vous propose une carte GIM-UEMOA de retrait et de paiement. Avec cette carte vous pourrez retirer de l'argent et consulter votre solde en toute sécurité et cela dans plus de 100 banques affiliées d'où plus de 1500 GAB. Aussi les clients peuvent effectuer leurs paiements avec leur carte dans les commerces affichant le logo du GIM-UEMOA.

Cibles : particulier (compte courant ou épargne), entreprise individuelle, profession libérale, PME/PMI.

- **CARTE VISA :**

La Banque Islamique du Sénégal met à votre disposition une carte Visa qui vous permet de régler vos achats ou de retirer de l'argent au Sénégal comme partout dans le monde, grâce au réseau mondial VISA. Elle vous permet également de régler vos dépenses en toute sécurité.

Cibles : particulier (compte courant ou épargne), entreprise individuelle, profession libérale, PME/PMI.

- **TAMWEEL TOUCH**

L'application Tamweel touch permet au client de suivre son compte en permanence en effectuer des consultations de solde, des virements bancaires, une commande de chéquier, de consulter le réseau d'agences, le taux de change, de demander un rendez-vous etc….

- **SMS BANKING**

Cette fonctionnalité permet aux clients de recevoir via leur téléphone mobile un SMS qui les renseigne sur le solde de leurs compte(s), la disponibilité d'un chéquier, la réception d'un virement, l'alerte d'un retrait ou versement, etc. Ce service est accessible par téléphone mobile quel que soit l'opérateur et l'abonnement téléphonique.

- **E-BANKING :**

Le client reçoit un E-mail instantanément à chaque opération effectuée. Tous les clients dotés d'un compte courant peuvent en bénéficier. Le client reçoit un E-mail en cas de débit ou de crédit sur son compte.

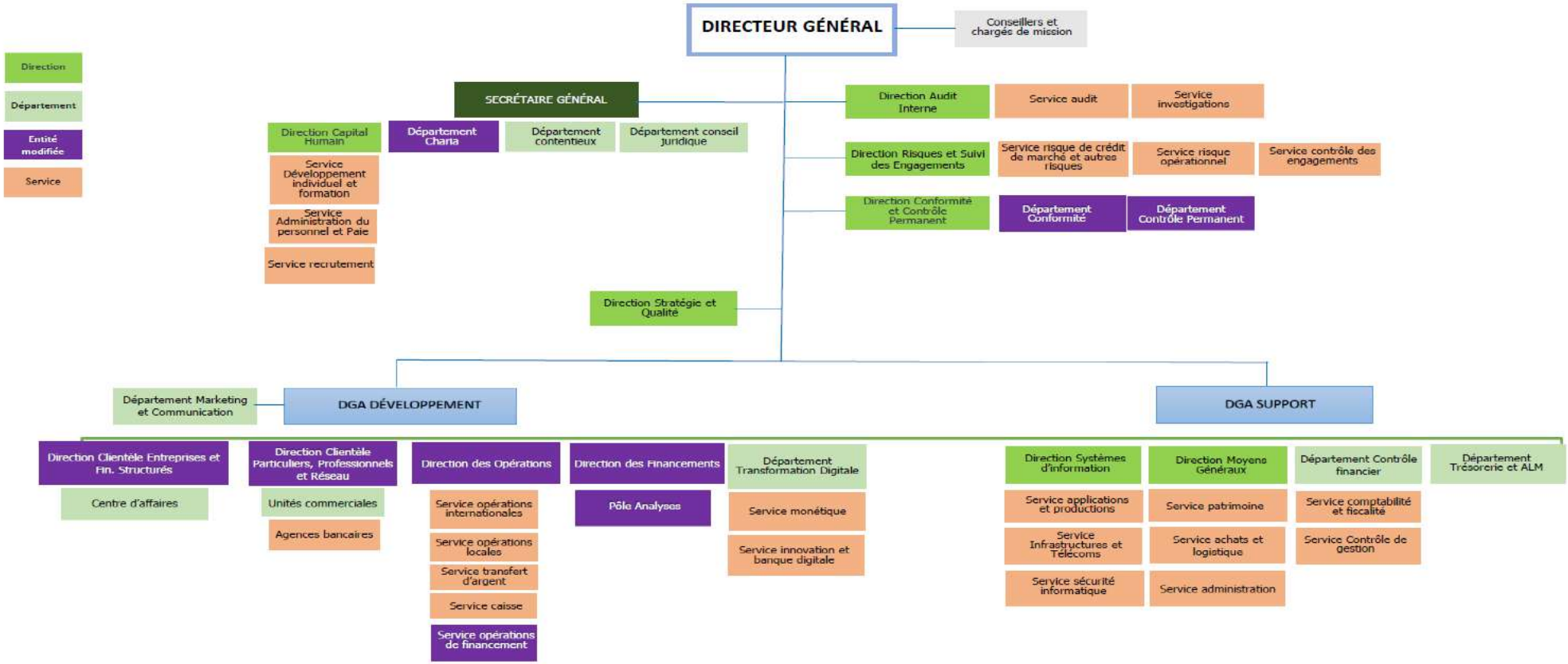
- **AUTRES SERVICES :**

La BIS offre à la clientèle tous les autres services bancaires classiques ne comportant pas perception ou paiement d'intérêt : opérations de change, de transfert rapide d'argent, d'encaissement, de portefeuille, d'aval, de cautionnement, de confirmation ou de domiciliation, d'opérations de commerce extérieur.

6.) L'organigramme de la BIS :

La BIS a mis en place une nouvelle organisation le 05 Septembre 2022 représentée sur l'organigramme suivant :

Figure 3 : Organigramme de la Banque Islamique du Sénégal (les différentes directions)



Section II : Stratégie de recherche

Notre étude suit une démarche d'audit avec une méthodologie d'investigation qui s'articule sur le fonctionnement de la gestion des risques opérationnels à la BIS à travers un guide d'entretien, une revue documentaire, des entretiens, une observation physique…etc.

La démarche d'investigation est une démarche hypothético-déductive qui fait appel au questionnement et à la construction de savoirs par le biais d'expérimentations.

La démarche d'investigation est essentielle car elle s'inscrit dans une démarche purement scientifique**.**

On valorise dans cette démarche la réflexion, l'expérience, la création d'outils, la communication et les capacités de synthèse.

La démarche d'investigation n'est pas unique, elle n'est pas non plus exclusive et tous les objets d'étude ne se prêtent pas à sa mise en œuvre. Cette démarche s'appuie sur le questionnement sur le monde réel et sur la résolution de problème. Les investigations réalisées avec l'élaboration de réponses et la recherche d'explications ou de justifications débouchent sur l'acquisition de connaissances, de compétences méthodologiques et sur la mise au point de savoir-faire techniques. Une démarche d'investigation doit être conclue par des activités de synthèse.

Elle s'apparente à l'approche inductive qui est l'approche choisie pour notre étude.

En effet, la démarche inductive, aussi appelée approche empirico-inductive, est une méthode de travail qui part de faits, de données brutes réelles et observables, pour aller vers l'explication de celles-ci.

À partir des phénomènes particuliers observés sur le terrain, le chercheur peut comprendre un phénomène général. On va du particulier au général.

L'approche inductive réunit des articles évalués par les pairs portant sur l'induction en méthodologie du travail intellectuel, c'est-à-dire dans les enjeux méthodologiques de la recherche scientifique et les enjeux pédagogiques reliés à la construction des connaissances. Les contributions empiriques, théoriques, historiques, conceptuelles et critiques concernent le projet épistémologique qui renverse, en quelque sorte, l'ordre traditionnel de la démarche hypothético-déductive. Une approche inductive, autant en recherche qualitative qu'en recherche

quantitative, consiste à donner priorité aux données, à l'expérience vécue, au terrain, pour ensuite avoir recours aux savoirs constitués dans un processus de construction de connaissance.

Ainsi, pour mener à bien notre étude, nous avons entrepris une stratégie bien définie en commençant d'abord à mener nos recherches sur Google scholar pour consulter d'anciens mémoires en adéquation avec le nôtre mais aussi nous avons parcourus plusieurs circulaires et documents sur la réglementation de la BCEAO en rapport avec la gestion des risques bancaires plus précisément le risque opérationnel tels que les circulaires 001, 003 et 004/2017, le document récapitulatif des accords de Bâle etc….

Nous avons également consulté les processus internes de la BIS plus particulièrement ceux concernant la gestion des risques opérationnels.

A cela s'ajoutent nos entretiens téléphoniques et par échanges de mails avec nos collaborateurs de la BIS pouvant nous aider dans nos recherches.

Ces recherches sont accompagnées par le soutien de l'administration, de notre professeur encadreur, du responsable de la cellule vérification opérationnelle et du chef de service de la gestion des risques opérationnels de la BIS.

Section III : Outils de recueil de données

Les outils de collecte et d'analyse des données ont pour objectifs de recueillir des informations sur la banque et les procédures appliquées qui nous permettront d'apprécier les dispositifs mis en place et de recenser les risques. Dans le cadre de nos recherches, les outils utilisés sont : l'analyse documentaire, les entretiens, la description narrative de procédures, le guide d'entretien sur la gestion des risques opérationnels, l'observation physique, le tableau des forces et faiblesses apparents, les bonnes pratiques et les normes. Ces outils sont présentés selon les étapes ci-après.

1.) La phase de prise de connaissance et du fonctionnement de la BIS :

Cette phase est constituée d'une seule étape : la présentation de la BIS et de ses activités. Deux outils ont été utilisés pour la collecte des informations.

1. a.) L'analyse documentaire :

C'est le traitement intellectuel des documents de l'entreprise. Elle nous a permis de connaitre la banque, son organisation, son fonctionnement et son dispositif de gestion des risques. Pour obtenir les informations nécessaires à notre étude, nous avons consulté l'organigramme qui présente l'organisation de l'entité, et aussi le lien interne des procédures, chartes et produits de la BIS.

1. b.) L'entretien :

Selon MADERS & al (2006 : 55), « l'objectif des entretiens est d'obtenir une description des processus du domaine sous l'angle de ses risques et de son dispositif de gestion de ces risques ». L'entretien nous a permis d'obtenir des informations sur les activités et les procédures de la banque. Les questions posées ont été de nature ouvertes et fermées selon la disponibilité du personnel et la confidentialité de certaines informations. Nous avons eu un premier entretien avec le responsable de la cellule de vérification qui nous a aussi apporté son support sur le choix du thème, ensuite avec le chef de service de la gestion des risques opérationnels qui était réactif par rapport à notre guide d'entretien et enfin avec certains des agents.

2.) La phase de prise de connaissance de la gestion des risques :

Le manuel de procédures est un document d'une grande importance dans l'exploitation des données internes. A la BIS, toutes les fonctions disposent d'un manuel de procédures complet et bien défini, aussi le manuel de procédures apparait comme notre deuxième source d'information après l'entretien.

2. a.) Le guide d'entretien sur la gestion des risques opérationnels à la BIS :

Pour MADERS & al (2006 : 57), le guide d'entretien a pour objectif " à la moulinette" un domaine pour en déterminer les forces et les faiblesses apparentes ». Il s'agit d'un document élaboré à partir du découpage de l'activité en tâches élémentaires. Il part comme étant le tableau d'analyse des risques du découpage fondamental. Il permet de réaliser sur chacun des points soumis à appréciation critique, une observation sur le fonctionnement normal ou non de l'activité. Il s'articule autour de cinq questions fondamentales : Qui ? Quoi ? Où ? Quand ? Comment ?

2. b.) La description de la procédure de gestion des risques :

Deux outils ont été utilisés pour la collecte des informations relatives à la description du dispositif de gestion des risques à la Banque Islamique du Sénégal.

- **L'observation physique**

L'observation a notamment porté sur l'exécution des tâches dans les procédures de la gestion des risques. Pour ce faire des observations tant directes qu'indirectes ont été effectuées. Les observations physiques ont consisté à l'observation des agents chargés de la maîtrise des risques opérationnels dans l'exécution de leur tâche quotidienne.

- **L'analyse documentaire**

Nous nous sommes référés aux textes existants à la BIS; des fiches de description des postes, du manuel de procédures, du guide d'entretien etc…. Nous avons repéré dans les documents des informations pertinentes. Les documents émanant des entités objet de nos recherches.

3.) <u>La phase d'analyse du rôle du dispositif de gestion des risques dans le processus de management à la BIS</u> :

Les informations collectées dans le manuel de procédures et celles obtenues pendant nos entretiens nous ont permis de procéder à l'analyse du rôle de la gestion des risques opérationnels mise en place à la BIS. Trois outils ont été utilisés pour l'analyse des résultats.

3. a.) Tableau des forces et faiblesses :

Ce tableau constitue un état des lieux des forces et des faiblesses réelles ou potentielles, et nous a permis d'identifier les risques dans le but de formuler des recommandations. Ces forces et faiblesses sont exprimées par rapport aux caractéristiques normalement attendues pour assurer le bon fonctionnement du dispositif de contrôle interne.

3. b.) Bonnes pratiques :

Une bonne pratique désigne un processus, un procédé, une attitude professionnelle qui représente le moyen le plus pertinent pour atteindre un objectif, accomplir une mission. Les bonnes pratiques concernées par notre étude sont celle relatives au processus de management des risques et celles relatives à l'activité de chaque service de la banque.

4.) Les recommandations :

Les recommandations ont été formulées sur la base des normes professionnelles et des bonnes pratiques.

4. a.) Normes :

Les nouvelles normes impliquent une responsabilité accrue des organes de contrôle dans le processus de management des risques. L'utilisation de ces normes permet de formuler des recommandations en vue d'augmenter les performances du dispositif de gestion des risques dans le processus de management à la BIS.

4. b.) Bonnes pratiques :

Les bonnes pratiques sont utilisées pour la formulation de recommandations pertinentes, en vue d'une amélioration du processus de management de la BIS. La définition et la mise en œuvre des recommandations appropriées permettront d'obtenir un processus de management efficace. Le modèle d'analyse présenté ci-dessus montre les outils utilisés pour l'obtention et le traitement des informations. L'analyse des informations collectées permet donc d'appréhender le rôle du contrôle interne dans le management de la BIS.

CHAPITRE 2 : CADRE ANALYTIQUE

Section I : Présentation des résultats

Dans le cadre de la collecte des données que nous avons faites, nous avons mis l'accent sur le dispositif de maîtrise des risques opérationnels à la BIS à savoir : l'appréciation de la hiérarchisation de la fonction RO (Risques opérationnels) à la BIS, de la méthodologie de gestion des RO, du rapport entre la fonction RO et les autres corps de contrôle de la BIS et de la fréquence de survenance des RO à la BIS au courant de l'exercice 2021.

Tableau 3 : Résultats relatifs à la hiérarchisation de la fonction RO

QUESTIONS	OUI	NON
Existe-t-il une fonction de gestion des RO à la BIS ?	X	
Si oui, quelle est la périodicité des reporting effectués ?		
Ø Mensuel	X	
Ø Trimestriel		
Ø Semestriel		
Ø Annuel		
La fonction des RO est –elle rattachée à la direction des risques	X	
Si non, à quelle direction est _elle rattachée ?		
Existe-t-il un comité de gestion des risques à la BIS ?	X	
Si oui, qui y participe ? Les membres du comité sont : ● Administrateur Président du comité ; ● Administrateur N°2 Les participants sont : ● Directeur Général BIS ; ● Directeur Adjoint support BIS ; ● Directeur des risques et Contrôle des engagements ; ● Directeur Contrôle permanent et conformité ;		

Tableau 4 : Résultats relatifs à la méthodologie de la gestion des RO à la BIS

QUESTIONS	OUI	NON
Disposez-vous d'une cartographique des RO ?	X	
Si oui, quel est son état d'avancement ? La BIS dispose d'une cartographie des risques opérationnels qui est mise à jour au moins une fois dans l'année comme préconisée par la circulaire N°04-2017/CB/C relative à gestion des risques dans les établissements de crédits et les compagnies financières de l'UMOA.		
Avez-vous mis en place une base de collecte de pertes et incidents ?	X	
Utilisez-vous des sources de données externes ?		X
Si oui, lesquelles ? ……		
Avez-vous un plan de continuité d'activité (PCA)	**X**	
Si oui, la démarche de mise en place du PCA est-elle coordonnée ou suivi par le responsable de RO ? La démarche de mise en place du PSCA est lancée. Effectivement le coordinateur du PSCA est le Directeur des risques ; le responsable des risques opérationnels participe à la démarche de mise en place. Le processus est encadré par des normes qui exigent au préalable des prérequis (mise en place d'un comité de projet, définir les rôles des acteurs, identifier les ressources critiques, etc.)		
Si non, par quel organe le suivi de la démarche est–elle faite ? …… Comment la banque compte gérer les situations de crise ? Les situations de crise sont gérées à travers un comité de crise qui est mis en place ou les décisions y sont discutées et prises. Les normes de gouvernance du comité sont définies et bien encadrées.		

Tableau 5 : Résultats relatifs au rapport entre la fonction RO et les autres corps de contrôle

QUESTIONS	OUI	NON
La cartographie des RO intègre-t-elle les risques de non-conformité ?	X	
Le contrôle interne, l'audit interne, la conformité et le RO sont-ils considérés comme des entités de contrôles à la BIS ?	X	

Quels sont les organes de contrôle qui participent à la maîtrise des risques opérationnels à la BIS ? Dans la pratique, tous les acteurs de la banque participent à la maîtrise des risques, mais les acteurs les plus importants concernant la maîtrise des risques sont respectivement le contrôle de premier et de second niveau et enfin le troisième niveau.		
Existe-t-il des points de surveillance fondamentaux concernant certains types d'évènement défini par Bâle II ou III et susceptibles d'engendrer le RO ?	X	
Si oui, lesquels ? Toutes les catégories Bâloises définies sont susceptibles d'engendrer des risques opérationnels. Les points de surveillance sont plus accès sur les erreurs d'exécution, les deux cas de fraude (interne et externe) et les interruptions d'activité et de processus.		
Disposez-vous d'un système d'alerte pendant le traitement des données ?	X	
Si oui, en quoi consiste ce dispositif ? Tout système d'information dispose d'alertes pour le traitement de certaines opérations. Il s'agit de points de contrôle nécessitant plus de vigilance pour ne pas exposer la banque à des évènements risques opérationnels.		
Si non, pourquoi et comment êtes –vous alertés des pertes éventuelles ? …… ..		
Le dispositif de gestion de RO fait-il l'objet d'audit régulier ?	X	

<u>Tableau 6</u> : Résultats relatifs à la fréquence de survenance des RO à la BIS au courant de l'exercice 2021

QUESTIONS	0 à 25 %	26 à 50 %	51 à 75 %	76 à 100%
Quelle est la fréquence de survenance des fraudes internes ?	1%			
Quelle est la fréquence de survenance des fraudes externes ?	0%			
Par quelle fréquence avez-vous rencontrés des incidents en rapport avec les pratiques en matière d'emploi et de sécurité sur le lieu de travail ?	1%			
Par quelle fréquence avez-vous rencontré des incidents liés aux clients, produits et pratiques commerciales ?	0%			
Par quelle fréquence avez-vous rencontré des incidents liés aux dommages aux actifs corporels ?	0%			
Par quelle fréquence avez-vous rencontré des incidents liés au dysfonctionnement de l'activité et des systèmes?	3%			
Par quelle fréquence avez-vous rencontré des incidents liés à l'exécution ou à la gestion des processus ?				95%

Section II : Analyses et interprétations des résultats

Nos analyses vont porter sur les résultats issus de notre guide d'entretien. Les analyses et interprétation des résultats obtenus vont également nous permettre de justifier notre hypothèse de recherche.

- **Hiérarchisation de la fonction Risques Opérationnels de la BIS :**

Il existe une fonction dénommée Service Risques Opérationnels dirigé par un chef de service et rattaché à la direction des risques et suivi des engagements. Ce service a pour mission de mettre en place et animer le dispositif de maîtrise des risques opérationnels au sein de la Banque Islamique du Sénégal mais exerce également une fonction clé en charge de l'identification de la mesure et du monitoring des risques opérationnels.

En plus de la direction des risques, la BIS a aussi un comité de gestion des risques conformément à la réglementation bancaire de l'UEMOA qui exige aux banques d'avoir un comité des risques à travers la circulaire 001 relatif à la gouvernance des établissements de crédits. Au sein de la BIS, ce comité est composé d'un administrateur président du comité, d'un administrateur N°2 et de quatre participants dont le Directeur Général de la BIS, le Directeur Adjoint Support de la BIS, Directeur des risques et contrôle des engagements, Directeur contrôle permanent et conformité.

Par ailleurs, le Service Risques Opérationnels est chargé des reportings mensuels des risques opérationnels. Ce reporting RO est un système de reporting interne conforme aux besoins de monitoring du risque opérationnel et permet d'examiner périodiquement la stratégie de maîtrise des RO et d'ajuster leur profil dans les limites de leur appétit pour le risque.

Ce reporting se fait en six rubriques et chacune des rubriques est essentielle à la gestion des RO à savoir :

_L'évolution du nombre d'évènements RO collectés au courant de l'exercice

_ La répartition des pertes par catégorie bâloise

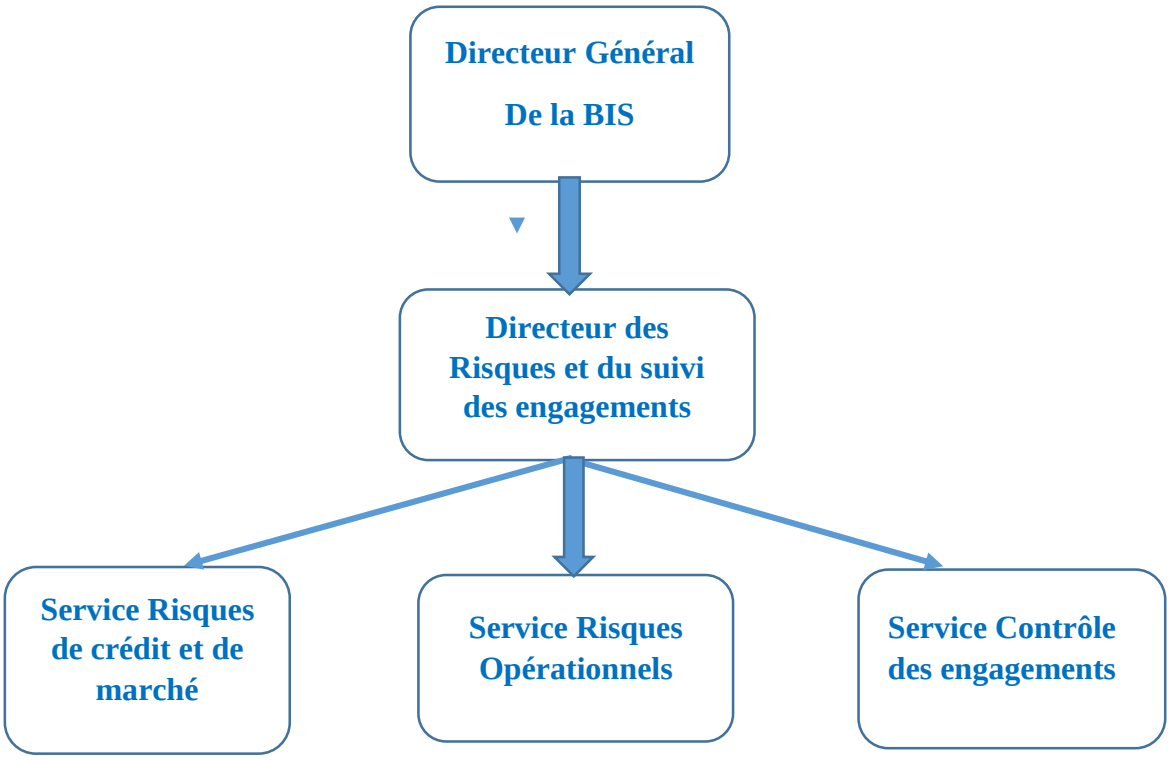
_ La déclaration des incidents par entité

_ La répartition des pertes par processus impactés

_ Les faits marquants au courant du mois

_ Un aperçu sur le niveau d'appétence risque opérationnel au courant de l'exercice

Figure 4 : Organisation de la direction des risques et suivi des engagements



Source : Organigramme de la BIS

- **Méthodologie de gestion des risques opérationnels :**

A ce niveau, nous analysons les méthodes de collecte et de gestion des risques opérationnels de la BIS. La BIS dispose de plusieurs méthodes lui permettant de collecter et de gérer ses RO.

Elle dispose d'une cartographie des risques qui est mise à jour au moins une fois dans l'année comme préconisée par la circulaire N°04-2017/CB relative à la gestion des risques dans les établissements de crédits et les compagnies financières de l'UEMOA.

A cela s'ajoute une base de collecte des pertes et incidents qui permettent au service risques opérationnels d'appuyer les entités opérationnelles dans la déclaration de leurs incidents et les sensibiliser sur l'importance de leur remontée ; mais aussi de mener des analyses et d'assurer un suivi des investigations effectuées par l'audit sur les incidents suspects de cas de fraude.

Le service risques opérationnels assure une animation et une coordination dans le but d'une vulgarisation de la culture du risque opérationnel au près du personnel à travers des formations et des formats de communication interne appropriés afin de mieux gérer ses risques opérationnels. Le reporting est également un outil de gestion des risques.

Toujours dans le cadre de la maîtrise de ses RO, la BIS a mise en place un Plan de Continuité d'Activité (PCA) et le coordinateur est le Directeur des risques ; le chef de service des risques opérationnels participe à la démarche de mise en place et d'améliorer du PCA. Le processus est encadré par des normes qui exigent aux préalables des prérequis (mise en place d'un comité de projet, définir les rôles des acteurs, identifier les ressources critiques etc...).

En outre, la BIS prévoit un dispositif de gestion des situations de crise qui consiste à la mise en place d'un comité de crise ou les décisions y sont discutées et prises. Les normes de gouvernance sont définies et bien encadrées.

- **Rapport entre la fonction RO et les autres corps de contrôle :**

Cette partie sera analysée avec approfondissement en raison de l'importance des corps de contrôle dans le dispositif de gestion des risques opérationnels.

Dans la pratique, tous les acteurs de la banque participent à la maîtrise des risques mais les acteurs les plus importants concernant la maîtrise des risques sont respectivement le contrôle de premier niveau, le second niveau et le troisième niveau.

En effet, ces niveaux de contrôle constituent le dispositif de contrôle interne de la banque.

Selon COSO, le contrôle interne est un processus mis en œuvre par les dirigeants et personnel d'une entreprise afin d'assurer la réalisation des objectifs et visant à limiter les tentatives de fraudes dans les rapports financiers des entreprises.

En d'autres termes, nous pouvons définir le contrôle interne comme un dispositif mise en œuvre par les dirigeants de l'entité pour s'assurer de la régularité des comptes, une utilisation efficace des ressources et une maîtrise des risques dans le but d'atteindre les objectifs de ladite entité.

Ainsi, le dispositif de contrôle interne de la BIS se fait à trois niveaux : les opérationnels qui assurent le contrôle de premier niveau ; la direction contrôle permanent et conformité, et la direction des risques qui s'occupent du contrôle de deuxième niveau et en fin l'audit interne qui assure le contrôle de troisième niveau.

Toutefois, chaque composante a un rôle bien défini dans le processus de gestion des risques opérationnels.

- **Premier niveau : Les opérationnels**

A la BIS, les opérationnels s'auto contrôlent et effectuent des pointages exhaustifs sur toutes les transactions passées dans le système. Ils font une classification de toutes les pièces comptables

de façon permanente et chronologique afin de détecter leurs anomalies et procéder à leur correction (pour minimiser les risques opérationnels) avant de transférer les pièces comptables aux contrôleurs permanents qui à leur tour font des vérifications d'usages.

En plus de l'autocontrôle, le premier niveau regroupe aussi les contrôles automatisés et les contrôles hiérarchiques.

A ce niveau, les supérieurs hiérarchiques doivent s'assurer que leurs équipes effectuent les contrôles de premier niveau.

Deuxième niveau : Contrôle Permanent, Risque et Conformité

Le deuxième est la vérification opérée par un agent n'ayant pas participé au processus de création et de validation d'une transaction. Ce niveau de contrôle regroupe la Direction du Contrôle Permanent et de la Conformité et la Direction des Risques et Suivi des Engagements.

Le contrôle permanent et la conformité vient en appoint à la direction des risques pour une maîtrise efficace des risques.

La conformité : elle se charge des risques de conformité et assure la veille réglementaire, la lutte anti-blanchiment (LAB/FT), l'anti-corruption et évite à la banque des sanctions pécuniaires ou judiciaires ou encore un risque d'image et de réputation.

Le contrôle permanent : c'est une fonction incontournable dans le processus de gestion des risques opérationnels, elle doit d'abord s'assurer que les opérationnels font les contrôles de premier niveau, veiller ensuite à la fiabilité des informations, de la conformité des opérations vis-à-vis de la réglementation en vigueur, de l'efficacité des informations, du suivi de l'éthique et des bonnes pratiques du personnel afin d'éviter les fraudes internes et la matérialisation des risques d'exécution des opérations, livraisons et processus. Les contrôleurs permanents assurent aussi les missions de contrôles inopinés en agence sur une périodicité mensuelle pour contrôler les encaisses physiques des caissiers et du GAB, les moyens de paiement (chèques et cartes bancaires), le respect des procédures internes telles que le principe de la garde des clés, la tenue des registres, l'affichage des conditions de banques, les risques d'interruption d'activité et pannes de systèmes et la bonne pratique du personnel en vue de pouvoir les sensibiliser sur la culture risque.

Le contrôle permanent de la BIS participe activement à la gestion des risques opérationnels à travers leurs reportings :

- Journaliers tels que le suivi des chambres forte de la banque, des états GAB, des comptes manquants et excédents de caisses, des pointages des pochettes comptables etc…
- Hebdomadaires tels que le suivi des arrêtés hebdomadaires de caisses qui sont des contrôles inopinés des caisses effectués par les responsables d'agence toutes les semaines du mois, le suivi des rejets de cartes commandées, le suivi des numéros de téléphones des clients modifiés par l'exploitation, le suivi des moyens de paiement mis en opposition et du prélèvement des frais, le suivi des comptes en interdit bancaire, etc…
- Mensuels tels que les analyses de compte internes, le suivi des constats mensuels des unités, les comptes rendus des contrôles inopinés, etc…

Dans les missions qui lui sont assignées, le contrôle permanent assure la surveillance globale et permanente des risques de crédit, financiers, opérationnels, comptables, informatiques, physique, …etc.

Toutes ces vérifications permettent aux contrôleurs de détecter toutes les anomalies qui engendrent des risques opérationnels et donc des pertes financières pour une meilleure efficacité de la gestion des risques opérationnels. Les indicateurs de contrôle permettront de mesurer et d'apprécier les résultats des contrôles dans l'objectif d'informer régulièrement la Direction Générale pour une correction rapide des anomalies et de prévenir les risques.

Les risques : ils assurent le processus de management des risques et ont pour mission une maîtrise des risques de la banque en faisant usage des outils et méthodes précédemment cité tout en étant conforme aux principes, lois et règlements en vigueur relatifs à la gestion des risques.

C'est dans ce sillage que **le service risques opérationnels** est chargé d'évaluer et d'analyser les risques opérationnels susceptibles d'affecter la réalisation des objectifs. Il assure l'évaluation des RO par approche qualitative qui consiste à analyser un risque opérationnel sur une double échelle de criticité (prenant en compte cumulativement la probabilité de survenance et l'impact) et la maîtrise.

Figure 5 : Échelles d'évaluation des risques opérationnels à la BIS

Échelle de maîtrise :

Valeur	Qualification	Explication
1	**Efficace**	Le dispositif de contrôle interne est efficace et suffisant
2	**Acceptable**	Quelques corrections doivent permettre de porter le dispositif de contrôle interne au niveau
3	**A renforcer**	Le dispositif de contrôle interne doit être renforcé et le processus mieux surveillé
4	**Défectueuse**	Le dispositif de contrôle interne du processus doit être réorganisé sans délai

Ces facteurs peuvent être des facteurs internes ou externes.

Échelle de criticité :

Valeur	Qualification	Explication
1	**Faible**	Impact faible ou inexistant et probabilité
2	**Moyenne**	Impact faible et probabilité
3	**Critique**	Impact fort et probabilité faible
4	**Très critique**	Impact et probabilité forts

Source : documentation de la BIS sur la gestion des risques opérationnels

Cette évaluation va donc permettre au service risques opérationnels de positionner le risque sur un repère orthonormé entre l'impact ou la gravité et la probabilité afin de déterminer la qualification du risque. Elle prend en compte les facteurs internes et externes qui constituent des variables d'environnement ou des indicateurs de risques (ou Key Ris Indicator - KRI).

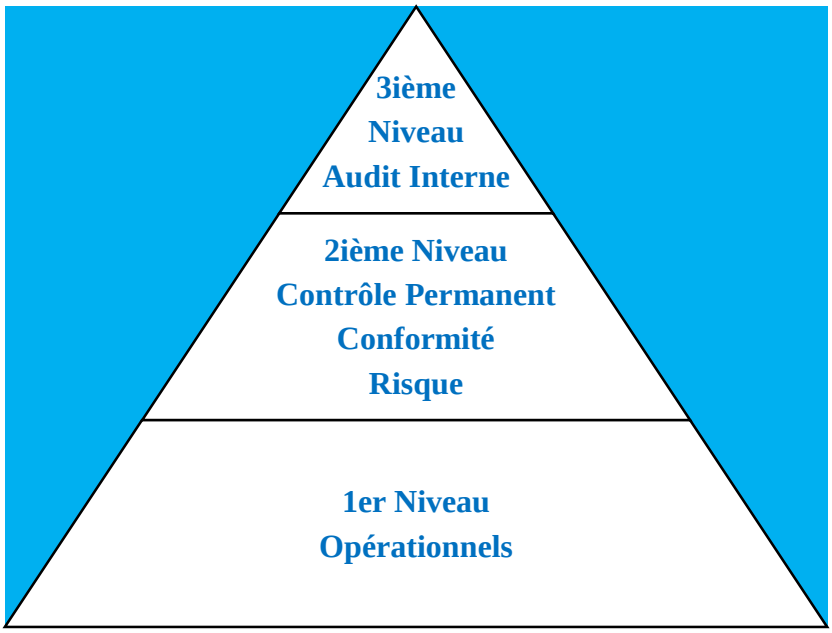
Ces indicateurs sont classés en deux catégories : les indicateurs d'exposition et les indicateurs de survenance. L'indicateur d'exposition peut permettre la description d'un contexte (caractère manuel d'une transaction, absence de formation du personnel, le volume d'activité, etc…) et les indicateurs de survenance sont des évènements de risques qui se sont matérialisés.

Les indicateurs de risques donnent une orientation sure « l'attitude » d'un process et permettent aux corps de contrôle d'augmenter de vigilance et d'intensifier leurs contrôles sur une nature d'opération. De ce fait, à partir d'un certain niveau, ils doivent impérativement générer une alerte qui indique qu'une opération ou un facteur de risque a atteint un niveau anormal : c'est ce qu'on appelle seuil d'alerte.

Troisième niveau : l'Audit Interne

L'audit interne intervient au troisième niveau du dispositif de contrôle interne et se charge des contrôles périodiques qui évalue en toute indépendance l'efficacité des processus de contrôle mis en place par la première et la deuxième ligne de défense et fournit une assurance sur ces processus. La fonction d'audit indépendamment des deux autres niveaux de contrôle effectue des contrôles périodiques sur toutes les composantes du système de contrôle interne.

Figure 6 : Dispositif de contrôle interne de la BIS



Source : Nous même

Concernant les points de surveillance fondamentaux de certains types d'évènements définis par Bâle II ou III et susceptibles d'engendrer le RO, ils sont plus accès sur les erreurs d'exécution, les deux cas de fraudes (interne et externe) et les interruptions d'activité et de processus.

Le service risques opérationnels dispose d'outils pour la collecte et le suivi des incidents risques opérationnels.

Ainsi, tout système d'information dispose d'alertes lors du traitement de certaines opérations. Il s'agit de point de contrôles nécessitant plus de vigilance pour ne pas exposer la banque à des évènements risques opérationnels.

Il faut noter également que le dispositif de gestion de RO fait objet d'audit régulier.

- **Fréquence de survenance des RO à la BIS au courant de l'exercice 2021**

Les résultats issus de notre guide d'entretien nous ont relatés d'une part la fréquence de survenance des fraudes internes et externe qui sont respectivement à 1% et 0%; ceci indique qu'au courant de l'exercice 2021, il n'y avait pas de fraudes externes et les fraudes internes étaient à un faible niveau de l'échelle. Cependant nos échanges avec le chef de service risques opérationnels ont révélé qu'il y avait des cas de fraudes externes constatés en 2021 mais qu'au vu de l'échelle du guide d'entretien que nous lui avons proposé le pourcentage est sensiblement nul.

D'autre part, il y a les incidents liés aux clients, produits et pratiques commerciales puis ceux liés aux dommages des actifs corporels qui étaient inexistants soit un taux de fréquence de 0% en 2021. Le taux de fréquence des incidents en rapport avec les pratiques en matière d'emploi et de sécurité sur le lieu de travail était à 1%.

En revanche, les incidents liés au dysfonctionnement de l'activité et des systèmes sont légèrement fréquents soit un taux de 3% ; mais les incidents liés au risque opérationnel beaucoup plus fréquent à la BIS est la catégorie des évènements liés à l'exécution ou à la gestion des processus avec un taux significatif de 95%.

Nous allons également analyser les forces et faiblesses de la gestion des risques de la BIS à travers deux tableaux récapitulatifs.

Tableau 7 : Présentation des forces

ÉLÉMENTS	FORCES
Structure organisationnelle	Le responsable RO est rattaché à la direction des risques opérationnels de la banque
Existence d'un comité de gestion des risques opérationnel	Le comité passe en revue la politique de gestion des risques opérationnels définie avant l'approuver
Mesure de risque par approche qualitatif	Cette approche évalue les RO en fonction de leur gravité et leur probabilité de survenance
Cartographie des risques	Existence d'une démarche d'identification des risques opérationnels ;
	La typologie des risques opérationnels de la BIS est inspirée de celle proposée par le comité de Bâle. Elle est conforme à la typologie de Bâle II
Conception d'une base d'incidents pour la collecte de données internes et externes	Existence d'un système de collecte des pertes et incidents
Indicateurs clés de risque	Existence d'indicateurs clés bien définis et suivis par la banque
	Le seuil critique de chaque indicateur est bien défini
PCA	Le PCA est approuvé par le DG et tous les directeurs de chaque département avant validation
	Le suivi du PCA est assuré par le directeur des risques et le responsable RO participe à la démarche de mise en place
Reporting	Un reporting des RO est mis à la disposition du personnel tous les mois Le reporting permet d'avoir une vision globale et consolidée du profil des risques opérationnels au niveau de la banque,
Gestion des risques	Suivi continu des risques opérationnels
Contrôle Interne	Existence d'un dispositif de contrôle interne
Gestion des situations de crises	Existence d'un comité crise
Contrôle permanent	Renforcement du personnel du service contrôle permanent

Source : Nous-même

Tableau 8 : Présentation des faiblesses

ÉLÉMENTS	FAIBLESSES
Système d'information	Récurrence des anomalies techniques (GAB Hors Service, instabilité du réseau de la connexion internet dans certaines agences, problème de serveur, problème de licence et de certificat des transferts rapides et…)
Exécution des opérations et processus	Erreur d'enregistrement de données (Anomalies sur les transactions des caisses et guichet, anomalies sur la gestion des moyens de paiement en agence)
	Non-respect des procédures dans certains cas de figures (Principe de garde des clés, contrôles hiérarchiques, seuils d'encaisses en agence…)
	Seuils d'alerte des retraits d'épargne non paramétrés pour certains caissiers
Formation du personnel	Défaut de formation du personnel sur la réglementation bancaire en générale et les process internes sur les métiers
Biens physiques	Dysfonctionnements des matériels informatiques, des compteuses de billets et détecteurs de faux billets, absences de meubles de rangements adaptés pour les dossiers des clients, absence de caissons pour certains caissiers, mal dispositions des box de caisses dans certaines agences etc...
Comptes internes	Omissions et lenteurs de régularisation des suspens sur les comptes internes de la banque (comptes manquants-excédents, chèque de banque, stock de timbres fiscaux)
Système Monétique	Le système monétique fait face à quelques défaillances et enregistre aussi des anomalies telles que les débits à tort, des retraits GAB intégrés tardivement par le système

Source : Nous-même

Section III : Recommandations managériales

Après étude de la gestion des risques opérationnels de la BIS, nous avons ressortis des points de satisfaction mais aussi quelques points à améliorer. C'est dans ce sens que nous avons formulé des recommandations afin d'optimiser le dispositif de maitrise des opérationnels.

❖ Recommandation relative au système d'information :

La présentation des faiblesses a fait ressortir une récurrence des anomalies techniques telles que l'instabilité du réseau de connexion internet dans certaines agences, les GAB qui sont souvent hors service etc…. Nous recommandons ainsi au top management de la BIS de faire un diagnostic de l'ensemble des GAB du réseau qui sera effectué par les agents de contrôles internes, du service monétique au niveau de l'informatique et du prestataire chargé de l'entretien des GAB afin de fournir un rapport détaillé sur l'environnement des GAB, leur état de vétusté dans le but de minimiser les risques opérationnels qui affectent la qualité de service et constituent un manque à gagner pour la banque.

D'autre part, nous recommandons à la direction d'optimiser leur serveur et de diversifier ses prestataires pour le réseau de connexion internet.

❖ Recommandation relative à l'exécution des opérations et processus :

Concernant l'exécution des opérations et processus nous avons relevé plusieurs anomalies auxquelles nous avons émis des recommandations.

- Les anomalies sur les transactions des caisses et du guichet et sur la gestion des moyens de paiement : Sur ce cas précis, nous préconisons une édition de guides d'usage relatifs aux différents postes concernés pour les opérationnels pour une maîtrise des processus de traitement des transactions et des renforcements de capacité sur ces métiers ;
- Le non-respect des procédures dans certains cas de figure par exemple le non-respect du principe de garde des clés, des contrôles hiérarchiques et des seuils d'encaisses en agence, nous recommandons ainsi la Direction Générale de prendre des mesures et d'inciter le personnel à respecter les procédures et les recommandations du contrôle permanent. Il y'a aussi le fait que certaines procédures ne sont pas uniformisés au niveau du réseau; une mise à jour des procédures doit être effectuée.
- Les seuils d'alerte des retraits d'épargne ne sont pas paramétrés pour certains caissiers, nous recommandations au management plus particulièrement la direction d'exploitation et la direction informatique de collaborer avec les responsables d'agences afin de recenser tous les caissiers qui ont des défauts de contrôles automatisés dans le système.

❖ **Recommandation relative à la formation du personnel :**

Nous avons ressorti ce point en raison de certaines anomalies et incidents qui sont parfois dû à un défaut de maîtrise de la réglementation bancaire et des procédures internes de la banque. Nous préconisons alors à la Direction Générale et la Direction du Capital Humain en collaborations avec les chefs de département d'organiser des formations sur les processus internes et la réglementation bancaire de la BCEAO mais aussi sur les risques opérationnels dans le but de les sensibiliser à avoir une culture risques pour tout collaborateur de la banque et de toujours se conformer aux procédures et à la réglementation.

Ces formations seront ainsi assorties d'évaluations en ligne qui seront pris en compte sur les fiches d'évaluation annuelle en étant considérées comme objectif.

❖ **Biens physiques :**

Sur ce point, des dysfonctionnements récurrents sont notés sur les matériels informatiques (ordinateurs, imprimantes etc…), des compteuses de billets et détecteurs de faux billets etc… ; et nous recommandons au top management une révision du processus de gestion des moyens généraux puis prendre des mesures corrections afin d'éviter le manque à gagner et le risque d'image de ses défauts de fonctionnement.

❖ **Comptes internes :**

Nous avons cité ce point comme faiblesse en raison des omissions et lenteurs de régularisation des suspens sur les comptes internes de la banque (comptes manquants-excédents, chèque de banque, stock de timbres fiscaux). Les comptes internes sont sensibles et susceptibles de faire objet de fraudes internes, nous recommandons à la Direction Générale, la Direction de la Comptabilité et de la Finance ainsi que les différentes lignes de défense de la banque de prendre les dispositions nécessaires afin d'apurer les comptes dans la mesure du possible ; par exemple certains suspens constatés sur les comptes manquants-excédents de certaines agences sont dus à des erreurs de fermetures de caisses ou d'écart de caisse retrouvé mais qui sont non apurés pour un défaut de suivi pour régularisation de ces suspens.

❖ **Système monétique :**

Le système monétique de la BIS fait face à quelques défaillances et enregistre aussi des anomalies telles que les débits à tort, des retraits GAB intégrés tardivement par le système.

En effet, le système monétique de la BIS est sous-couvert de GIM-UEMOA alors que la banque a beaucoup grandi~~e~~ en termes de production et de portefeuille clientèle. Nous avons ainsi jugé nécessaire de recommander au management la mise en œuvre du projet de création d'un

système monétique autonome étant donné que ce projet fait partie des objectifs stratégiques de la Direction Générale.

Tableau 9 : Tableau récapitulatif des recommandations émises

REF	Recommandations	Objectifs Visés	Responsables mis en œuvre
R1	Diagnostic de l'ensemble des GAB du réseau	_ Réduire considérablement les dysfonctionnements des GAB du réseau _ Améliorer la qualité de service	DG DCCP Service Monétique
	Optimiser le serveur et diversifier les prestataires de télécommunication (Service internet)	Éviter les arrêts de services dus à une instabilité de connexion interne ou du serveur	DG IT
R2	Edition de guide d'usage pour les opérationnels	Minimiser les anomalies sur les transactions traitées par les opérationnels	DG en collaboration avec les directeurs et chefs de services
	Prise de mesures et incitation au personnel à respecter les procédures et les recommandations du contrôle permanent	Respect des procédures et réduction des risques opérationnels	DG
	Recenser tous les caissiers qui ont des défauts de contrôles automatisés dans le système	Paramétrer les seuils d'alerte des retraits d'épargne pour renforcer le dispositif de maîtrise des RO	DG IT CA
R3	Formation du personnel sur les process internes et la réglementation bancaire de la BCEAO et sur les risques opérationnel	Permettre d'avantage au personnel d'avoir une culture risques sur chacun des métiers de la banque et de toujours se conformer aux procédures et à la réglementation.	DG DCH Chefs de départements
R4	Révision du processus de gestion des moyens généraux Prise de mesures correctrices	Éviter le manque à gagner et le risque d'image et de réputation	DG Direction Audit Interne
R5	Prise de mesures correctrices	Apurement des suspens sur les comptes internes afin d'éviter des fraudes internes sur ces comptes et des risques de non-conformité avec la réglementation bancaire	DG DFC Contrôle Interne
R6	Mise en œuvre du projet de création d'un système monétique autonome	Améliorer la qualité de service et minimiser les charges financières	DG

Conclusion Générale

Nous voilà à la dernière phase de notre étude sur la gestion des risques opérationnels à la BIS notamment sur la problématique d'une gestion optimale des risques opérationnels. De cette problématique découle trois questions de recherches qui ont fait l'objet de notre étude et qui nous ont permis d'obtenir des résultats et d'en tirer les forces et faiblesses de la BIS en termes de gestion des risques opérationnels afin de formuler des recommandations managériales à l'endroit de la Direction Générale.

Nous avons mené ce travail sur la base d'une démarche structurée en trois phases (phase de préparation, phase de réalisation, phase de conclusion) et d'un ensemble d'outils de recherches (analyse documentaire, entretien, observation physique).

En effet, cette méthodologie a abouti à des résultats concrets qui nous ont guidé sur le fonctionnement du service risques opérationnels qui occupe une place importante dans la structuration de la banque sachant que l'atteinte des objectifs de la BIS est confronté aux risques opérationnels ; mais aussi sur les méthodes utilisées par la BIS pour gérer ses risques opérationnels à savoir une cartographie des risques, une base de collecte des pertes et incidents, un plan de continuité d'activité et une évaluation des risques par approche qualitative.

Nous avons également ressorti de cette étude l'efficacité du dispositif de contrôle interne de la BIS en matière de gestion des risques opérationnels et la place qu'occupe la fonction risque dans ce dispositif.

C'est ainsi qu'au cours de la première partie, nous avons d'abord clarifié tous les concepts et notions relatifs aux risques bancaires en général et aux risques opérationnels en particulier puis leur gestion; ensuite nous avons développé dans cette partie une revue littéraire.

Dans ce sillage, nous avons aussi abordé la deuxième partie pour démontrer la méthodologie et les outils d'analyse pour obtenir des résultats que nous avons présentés, analysés puis interprétés pour préconiser des solutions face aux faiblesses issues de notre analyse. Aussi, nous avons étayé dans cette partie le cadre organisationnel de la BIS qui a fait office d'exemple de notre étude.

Cependant, fournir ce travail n'a pas été sans difficultés car notre étude porte sur le cas d'une banque et les banques sont régies par une charte de confidentialité raison pour laquelle beaucoup d'informations ne peuvent être à la portée du public. A cela s'ajoute la rareté des documents à propos de notre sujet et l'inaccessibilité aux rapports annuels récents de la BIS.

Ces difficultés ont été d'une part sources de limites pour nous permettre de faire une étude beaucoup plus approfondie dans l'objectif d'identifier plus de limites et d'émettre plus de recommandations.

A l'issue des faiblesses que nous avons énumérées sur la gestion des risques opérationnels à la BIS, nous pensons qu'il est nécessaire pour la banque d'autonomiser son système monétique, de réévaluer la gestion des moyens généraux, de former le personnel sur la réglementation bancaire de la BCEAO et les processus internes de la banque dans le but de réduire les incidents les plus fréquents liés à l'exécution ou la gestion des processus qui était estimé à 95% en 2021.

Par ailleurs, la banque doit sensibiliser le personnel et prendre des mesures nécessaires pour un respect strict des procédures et un suivi rigoureux des recommandations du contrôle permanent.

En fin, ce mémoire qui a été fructifié par notre année d'expérience passée à la BIS recèle plusieurs perspectives et on peut en citer une qui est la maîtrise des risques de fraudes internes et externes qui deviennent de plus en plus fréquentes dans le secteur bancaire sénégalais et qui fragilise l'atteinte des objectifs des banques. Ces fraudes font parties des causes du faible taux de bancarisation au Sénégal car certains acteurs économiques peinent à faire confiance aux banques à cause des risques d'image et de réputation liées à ces deux cas de fraudes.

BIBLIOGRAPHIE

OUVRAGES

1. Circulaire 001/2017/CB
2. Circulaire 003/2017/CB
3. Circulaire 004/2017.CB
4. 2ème Édition « Les Topos + » Dunud Paris 2008 d'Olivier Hassid sur la gestion des risques
5. Pilier 03-16/03/2017-FR du Groupe Société Générale Sur la Gestion des Risques
6. Rapport du Séminaire de Frédéric Visnovsky sur Bâle 1,2 et 3 publié à Grenoble le 25 Janvier 2017
7. Revue de l'étude des risques dans le système financier islamique présenté par Ahmed Ouazzani Professeur à l'Université Abdelmalek Essaadi du Maroc
8. Rapport annuel de la BIS, édition 2016
9. Manuel des procédures internes de la BIS
10. Magazine Business Africa N°176 paru en Juillet 2022 (Interview du DG de la BIS)

WEBOGRAPHIE

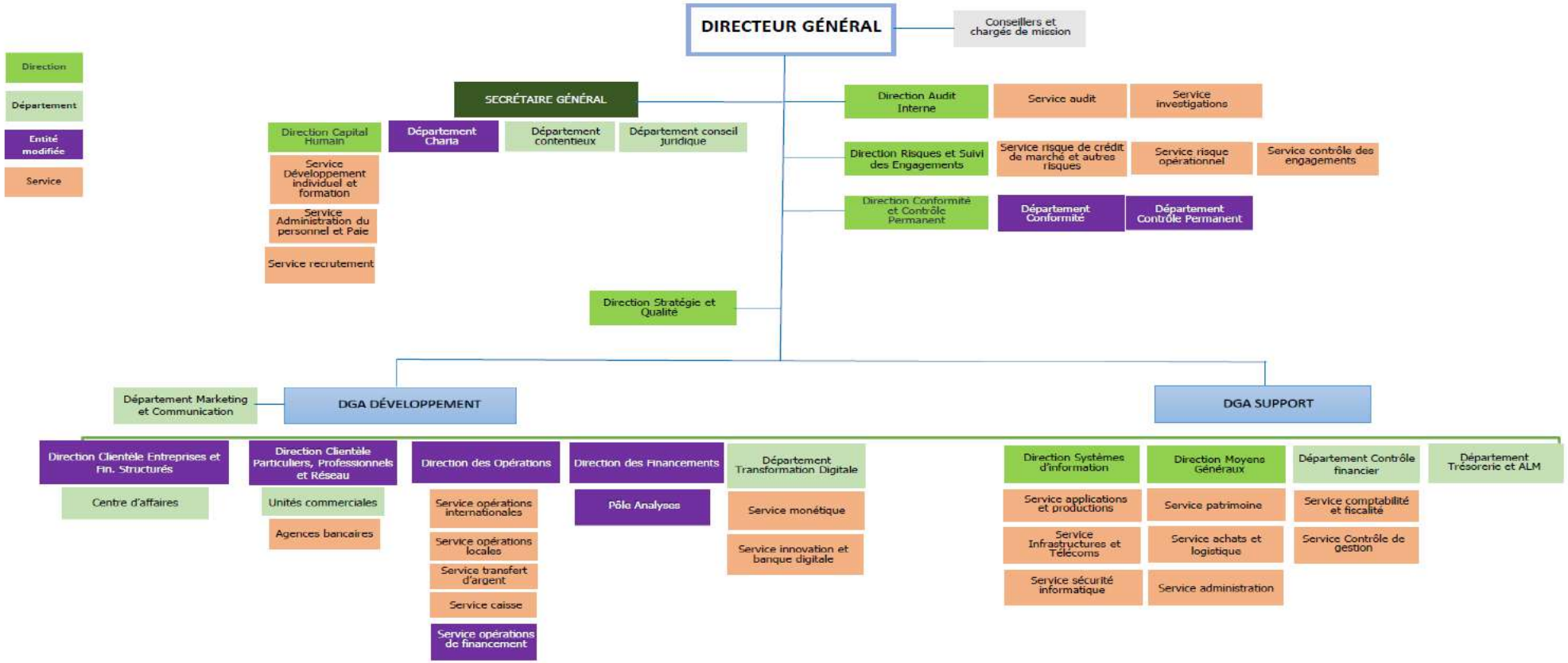
1. Google Scholar
2. www.acpr.banque-france.fr
3. www.denud.comhttp : //revue.imist.ma/?journal
4. africabusinessmag.com
5. www.bis-bank.com

MÉMOIRES ET TRAVAUX DE FIN DE CYCLE

1. MAHBOUB, SENOUSSI. Ali (2019), Gestion du risque opérationnel état d'avancement des banques Algérienne cas de la BADR Laghouat.
2. DJIOUA Kamelia, ATMANI Lamia (2017-2018), Le concept de gouvernance et la gestion des risques bancaires Cas : de la « BADR » direction régionale de Tizi-Ouzou
3. Alexis RENAUDIN (2012), Modèle de capital économique pour le risque opérationnel bancaire : estimation, diversification

ANNEXES

Annexe 1 : Organigramme de la BIS (Les différentes directions



Annexe 2 : Guide d'entretien sur la gestion des risques opérationnels à la BIS

Bonjour,

Dans le cadre de la rédaction de notre mémoire de fin de cycle, nous vous invitons à répondre à ce questionnaire de notre étude qui porte sur « La gestion des risques opérationnels dans une banque : Cas de la BIS ».

Merci d'avance !

Questions sur la gestion des risques opérationnels (RO) et leur fonction à la BIS

<u>Objectif 1</u> : Apprécier la hiérarchisation de la fonction RO de la BIS

QUESTIONS	OUI	NON
Existe-t-il une fonction de gestion des RO à la BIS?		
Si oui, quelle est la périodicité des reporting effectués ?		
Ø Mensuel		
Ø Trimestriel		
Ø Semestriel		
Ø Annuel		
La fonction des RO est –elle rattachée à la direction des risques		
Si non, à quelle direction est _elle rattachée ?		
Existe-t-il un comité de gestion des risques à la BIS ?		
Si oui, qui y participe? …… ……		

<u>Objectif 2</u> : apprécier la méthodologie de gestion des RO

Questions	Oui	Non
Disposez-vous d'une cartographique des RO ?		
Si oui, quel est son état d'avancement ?		

Avez-vous mis en place une base de collecte de pertes et incidents ?		
Utilisez-vous des sources de données externes ?		
Si oui, lesquelles? ……		
Avez-vous un plan de continuité d'activité (PCA)		
Si oui, la démarche de mise en place du PCA est-elle coordonnée ou suivi par le responsable de RO ?		
Si non, par quel organe le suivi de la démarche est–elle faite ? .... Comment la banque compte gérer les situations de crise? ……..... ..		

<u>Objectif 3</u> : Rapport entre la fonction RO et les autres corps de contrôle

QUESTIONS	OUI	NON
La cartographie des RO intègre-t-elle les risques de non-conformité ?		
Le contrôle interne, l'audit interne, la conformité et le RO sont-ils considérés comme des entités de contrôles à la BIS ?		
Quels sont les organes de contrôle qui participe à la maîtrise des risques opérationnels à la BIS? …… ……		
Existe-t-il des points de surveillance fondamentaux concernant certains types d'évènement défini par Bâle II ou III et susceptibles d'engendrer le RO ?		
Si oui, lesquels ?		
Disposez-vous d'un système d'alerte pendant le traitement des données ?		

Si oui, en quoi consiste ce dispositif ?		
Si non, pourquoi et comment êtes –vous alertés des pertes éventuelles ? …… ..		
Le dispositif de gestion de RO fait-il objet d'audit régulier ?		

<u>Objectif 4</u>: fréquence de survenance des RO à la BIS courant de l'exercice 2021

QUESTIONS	0 à 25 %	26 à 50 %	51 à 75 %	76 à 100%
Quelle est la fréquence de survenance des fraudes internes ?				
Quelle est la fréquence de survenance des fraudes externes ?				
Par quelle fréquence avez-vous rencontrés des incidents en rapport avec les pratiques en matière d'emploi et de sécurité sur le lieu de travail ?				
Par quelle fréquence avez-vous rencontré des incidents liés aux clients, produits et pratiques commerciales ?				
Par quelle fréquence avez-vous rencontré des incidents liés aux dommages aux actifs corporels ?				
Par quelle fréquence avez-vous rencontré des incidents liés au dysfonctionnement de l'activité et des systèmes?				
Par quelle fréquence avez-vous rencontré des incidents liés à l'exécution ou à la gestion des processus ?				

TABLE DES MATIÈRES