Remerciement

Je tiens à exprimer toute ma reconnaissance à mon Directeur de mémoire Monsieur CHIHEB GHANMI. Je le remercie de m'avoir encadrée, orientée, aidée et conseillée.

Je tiens à remercier également tous les collaborateurs à la direction de commerce extérieur, en particulier mon tuteur de stage Monsieur HEDI SIDAOUI, pour leur soutien, collaboration et conseils.

Toute ma gratitude reviens à mes chers professeurs ainsi que l'ensemble du personnel de notre prestigieux institut de financement du développement du Maghreb arabe I.FI.D , pour l'aide qu'ils m'ont apporté, mais aussi et surtout pour le savoir qu'ils ont eu la générosité de me transmettre, & pour toute les leçons qu'ils m'ont chaleureusement appris durant cet inoubliable parcours.

J'exprime ma sincère gratitude à Messieurs les jurys qui me font l'honneur de juger ce travail.

Table des matières

Liste des abréviations

ATB	Arab Tunisian Bank
Bâle	Comité de Bâle sur le contrôle bancaire
BCT	Banque Centrale de Tunisie
COSO	Committee Of Sponsoring Organizations of the Treadway Commission
ERM	Entreprise Risk Management
HSBC	Hongkong and Shanghai Banking Corporation Limited
IFACI	Institut Français de l'Audit et du Contrôle Interne
ISO	Organisation Internationale de Normalisation
IT	Information Technology
PCA	Plan de Continuité d'Activité
PNB	Produit Net Bancaire
RUU	Règles et Usances Uniformes
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TNN	Tunisie Trade Net

Liste des figures

Liste des tableaux

INTRODUCTION GENERALE

Introduction générale

Les banques sont exposées à une multitude de risques (risque de crédit, risque de marché, risque opérationnel et risque lié à la conformité). Tout risque se caractérise par un coût. En réalité, le coût des risques opérationnels est loin d'être négligeable[1]. Ce risque est présent d'une façon ou d'une autre dans chacune des activités de la banque. Il peut donner lieu à des pertes financières, à des sanctions réglementaires ainsi qu'à des atteintes à la réputation de la banque.

Conscientes de ce grand risque, les autorités réglementaires ont lancé le débat sur la définition, l'identification, la mesure et la gestion du risque opérationnel à partir de juin 1999. Depuis 2004, elles imposent aux banques de mettre en place un système de gestion propre au risque opérationnel et de détenir un capital permettant de couvrir les pertes opérationnelles non anticipées, comme c'est le cas pour le risque de marché et de crédit.

En Tunisie, le risque opérationnel a fait l'objet d'une attention particulière tant à travers son intégration dans le calcul de ratio de solvabilité que les circulaires 2006/19 et 2013/15. La première oblige les banques de se doter d'un système de gestion du risque opérationnel, de mettre en place un système de contrôle interne et l'institution d'un comité permanent d'audit interne. La seconde est relative à la mise en place des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme.

A cet égard, la mise en place d'un système de gestion des risques opérationnels intéresse de plus en plus les banques ayant pour objectif de rendre leurs dispositifs de contrôles plus simples et plus efficaces. Or, la clé de toute gestion est la connaissance, et pour gérer les risques opérationnels, il faut les connaitre, c'est-à-dire les identifier et les évaluer. Cela se fait grâce à des processus, des outils et des méthodes qui ont été progressivement développés dans la banque. Le caractère général et diffus du risque opérationnel, ses divers impacts et la difficulté liée à son identification ont rendu délicate sa gestion. A ce titre, la cartographie des risques se présente comme une démarche bien structurée et efficace pour la gestion des risques opérationnels.

C'est une composante essentielle du processus de gestion des risques. Son objectif est de disposer d'un état des lieux global des vulnérabilités pour l'ensemble des champs

[1] Les développements récents de la mesure du risque opérationnel, Frantz Maurer, Université Montesquieu-Bordeaux IV.

d'activité. La démarche de cartographie est primordiale. En effet, elle suscite le recensement général des risques, leur évaluation et leur hiérarchisation. En outre, elle détermine si les le mesures de maîtrise des risques en place sont appropriées ou s'il faut en instaurer d'autres. Elle offre des représentations simples, donnant une vision d'ensemble aux dirigeants pour orienter leurs choix stratégiques d'action. Les cartographies des risques sont ensuite utilisées pour suivre l'efficacité des stratégies mises en œuvre et forment enfin un outil très pertinent de communication sur l'état des lieux.

La cartographie globale consiste à réunir et hiérarchiser tous les risques opérationnels de la banque. Son élaboration passe par la réalisation des cartographies thématiques, spécifiques à des processus distincts. Dans le cadre de ce travail de recherche, noua avons choisi d'élaborer la cartographie des risques opérationnels inhérents au processus du crédit documentaire.

Etant la plus utilisée dans le commerce international, cette technique de paiement vise à réduire le risque lié à la non-exécution ou à l'exécution tardive des obligations des parties contractantes. Les banques étant tenues de vérifier exclusivement que les documents de livraison sont conformes aux clauses du contrat, mais non que ces documents correspondent à une livraison effective, le crédit documentaire fait l'objet d'abus de la part d'organisations criminelles, qui peuvent ainsi transférer des sommes d'argent en simulant une livraison de marchandises[2]. De ce fait, la banque est tenue de s'assurer de la régularité de l'opération avant de s'y engager. Autrement dit, l'opération d'import ou d'export ne doit pas impliquer des parties « black listées » ou porter sur des produits illicites. En outre, elle ne doit pas violer les règles d'embargo.

A l'instar des autres banques, les banques tunisiennes font face au risque de manquer à leurs engagements à cause de l'erreur ou la négligence humaine, dysfonctionnement des processus et des systèmes ou des événements externes. Par suite, elles seront menacées de pénalités, amendes et sanctions règlementaires. Depuis 2009, une dizaine de grandes banques ont payé des centaines de millions de dollars pour avoir violé ou cherché à contourner les embargos mis en place par Washington sur plusieurs pays. Évidemment, l'amende la plus forte est celle de BNP Paribas. En juin 2014, la banque a dû payer près de 9 milliards de dollars. Standard Chartered, le Crédit Agricole et Deutsche Bank ont également payé des lourdes pénalités aux autorités américaines. Les banques sont sanctionnées aussi, pour ne pas avoir respecté les engagements de lutte contre le blanchiment d'argent et financement de

[2] Document de travail sur le blanchiment de capitaux, Commission spéciale sur la criminalité organisée, la corruption et le blanchiment de capitaux, parlement Européen 2009-2014.

terrorisme. En 2012, la banque sino-britannique HSBC a accepté de payer un montant de 1,9 milliard de dollars. Elle était accusée de complicité de blanchiment d'argent sale appartenant à des cartels de la drogue au Mexique et de financement du terrorisme au Moyen-Orient.

Certes, la banque fait face aux risques de blanchiment d'argent et de viol des règles d'embargo ainsi que plusieurs autres risques opérationnels. Dans le cadre de cette étude nous cherchons à répondre à la question suivante : **quelle démarche à suivre pour élaborer la cartographie des risques opérationnels inhérents au processus du crédit documentaire** ? Afin de répondre à cette question axiale, nous allons apporter des réponses aux questions de recherche suivantes :

1- Quels sont les risques opérationnels liés au processus du crédit documentaire ?
2- Quels sont les contrôles mis en place afin d'atténuer ces risques ?
3- Comment peut-on évaluer ces risques et ces contrôles ?
4- Quels sont les risques résiduels nécessitant des actions de gestion ?
5- Quels sont les actions proposées pour gérer les risques nets ?

L'objectif d'une telle étude est d'établir un recensement et une évaluation des risques au regard des contrôles en place, en vue de mettre en valeurs les défaillances des contrôles et les risques résiduels. De fait, ce travail est une contribution au processus de gestion des risques qui s'articule en trois chapitres :

1- Le premier chapitre présente brièvement l'activité bancaire et les risques qui y sont associés. En suite, l'accent est mis sur le risque opérationnel bancaire. Nous allons le définir et expliciter ses spécificités. La dernière section est consacrée aux méthodes de gestion du risque opérationnel.
2- Le deuxième chapitre, nous allons expliquer la démarche d'élaboration d'une cartographie des risques. Cette démarche commence par la mise en place des préalables nécessaires à sa réussite. Elle passe par un certain nombre d'étapes : cartographie des processus, identification et évaluation des risques et des contrôles, hiérarchisation des risques nets, communication et actualisation des risques et mise en place d'un plan d'actions et d'un plan d'audit.
3- Dans le troisième chapitre, nous allons suivre cette démarche pour l'élaboration d'une cartographie des risques liés au processus du crédit documentaire au sein de l'ATB. Avant cela, nous allons présenter brièvement la banque, ses indicateurs d'activité.

CHAPITRE I :

LA GESTION DU RISQUE OPÉRATIONNEL DANS LA BANQUE

Introduction

De par l'essence de leur métier qui consiste à prendre des risques, les banques sont les plus concernées par leur maîtrise. Ces dernières opèrent dans un environnement en pleine mutation où la maitrise des risques devient une priorité absolue. De plus, la solidité des banques étant un souci majeur pour les pouvoirs publics, des mesures ont été prises pour limiter les faillites bancaires et les réactions de panique qui peuvent en résulter.

Les régulateurs du domaine bancaire sont de plus en plus conscients de risques opérationnels inhérents aux activités bancaires et qui sont susceptibles d'engendrer des pertes financières importantes pour la banque. Ces pertes peuvent avoir des retombées négatives sur la stabilité financière.

A cet égard, depuis l'année 2004, les banques internationales sont soumises à une nouvelle réglementation prudentielle connue sous le nom d'Accords de Bâle II. En particulier, elles doivent appliquer le nouveau ratio de solvabilité international qui remplace le ratio Cooke mis en place en 1988 pour en pallier les défaillances. Les acteurs du domaine bancaire veulent élaborer un cadre de gestion de risque opérationnel. Une gestion efficace de ce risque nécessite une gouvernance d'entreprises et des contrôles internes rigoureux, des politiques et procédures des fiables et du personnel qualifié.

Toutes ces idées que nous venons d'avancer et autres, seront détaillées davantage dans ce premier chapitre, scindé en trois sections :

Section 1 : Les établissements bancaires : activités et risques ;

Section 2 : les spécificités du risque opérationnel ;

Section 3 : la gestion des risques opérationnels.

Section 1 : Les établissements bancaires : activités et risques

Cette première section a pour objectif d'introduire notre sujet en présentant quelques spécificités du domaine bancaire. Nous mettons l'accent sur les principales activités bancaires ainsi que les risques qui y sont inhérents.

1.1 Les activités bancaires

La banque remplit une multitude de fonctions dont nous pouvons les regrouper dans quatre grandes catégories :

- **Activité d'intermédiation bancaire** : le rôle traditionnel des banques consiste à collecter des dépôts et à octroyer des prêts. Le taux d'intérêt facturé sur les prêts est supérieur au taux d'intérêt payé sur les dépôts. Cette différence doit couvrir les différentes charges de la banque (les coûts administratifs, les provisions…), tout en générant une rentabilité en capital satisfaisante.
- **Activité de trésorerie** : la banque intervient sur le marché monétaire interbancaire pour emprunter des fonds, si elle présente un déficit de trésorerie. Dans le cas où la banque a un excédent de trésorerie, elle le place sur le marché interbancaire. Les opérations de prêts et d'emprunts sur le marché monétaire se font au taux de marché monétaire.
- **Activité de prise de participation** : les banques peuvent participer dans le capital des autres entreprises sous centaines conditions ou souscrire dans des emprunts obligataires. Cette activité est rémunérée par des intérêts, des dividendes et éventuellement des plus value sur cession.
- **Activité de services** : les banques offrent également une multitude de services tels que la mise à disposition de la clientèle et la gestion des moyens de paiements, le conseil et assistance en matière de gestion de patrimoine, d'ingénierie financière et d'une manière générale tous les services destinés à faciliter la création, le développement et la restructuration des entreprises. Elles assurent aussi des opérations de commerce international pour le compte des opérateurs économiques ainsi que l'intermédiation en matière de change. L'activité de services génère pour la banque des commissions.

Les banques sont des organisations globalisées et complexes qui interviennent dans différents types d'activités. Les grandes banques collectent des dépôts, octroient des prêts, souscrivent des titres et fournissent une multitude de services comme les moyens de paiements, la banque en ligne et les guichets automatiques de banque. Ainsi, une banque qui rassemble toutes ces activités, gère toute une typologie de risques.

1.2 Les risques bancaires

Plusieurs définitions du risque ont apparus. Selon l'Organisation internationale de normalisation (ISO) le risque est « la possibilité d'occurrence d'un événement ayant un impact sur les objectifs, il se mesure en terme de conséquences et de probabilité ». L'Institut Français de l'Audit et du Contrôle Interne (IFACI) définit la notion de risque comme étant « un ensemble d'aléas susceptible d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer sa maîtrise ».

Généralement, les risques se matérialisent par la baisse des résultats de la banque et par conséquent la dégradation du rating, des difficultés à se procurer de la liquidité nécessaire à l'activité, la hausse du coût de ressources, le problème de solvabilité de l'établissement et des pertes importantes. Malgré cette connotation négative généralement affectée au risque, il est une occasion pour saisir une opportunité. Ainsi, la prise de risque est fortement liée à se doter des moyens nécessaires pour le maitriser.

Par ailleurs, la raison d'être d'une banque est de prendre des risques, d'en accepter les conséquences et de mettre en place les moyens de protection nécessaires. Néanmoins, l'ampleur des risques menaçant l'activité bancaire est clairement montrée dans les dernières crises financières et les cas de faillites ou de quasi-faillites de certaines banques. Quelle que soit l'activité exercée par la banque, celle-ci doit donc faire face à plusieurs risques.

La nature de risque diffère selon l'activité rendue par la banque. En effet, les intérêts rémunèrent les prêts accordés par celle ci à ses clients. Elle y intègre une prime de risque considérant que certains clients ne rembourseront pas leurs crédits. Dans ce cas, il s'agit donc d'**un risque accepté** que la banque cherche à encadrer pour éviter toute dérive. A l'inverse, certaines de ses activités peuvent l'exposer à des risques qu'elle ne souhaite pas, par exemple la fraude. Ces risques existent du fait même de son activité. Il s'agit ici de **risques subis**.

1.2.1 Les risques acceptés et rémunérés

Comme précisé, le métier de la banque est de prendre des risques de plusieurs natures. La banque est donc rémunérée pour cette prise de risque.

– Le risque de crédit : c'est le risque de pertes financières consécutives à l'incapacité des clients ou autres contreparties à honorer leurs engagements financiers.
– Le risque de marché : c'est le risque pour la banque de subir des pertes financières consécutives aux variations des prix des instruments financiers (actions, obligations…), des taux de change, des taux d'intérêt, etc.

1.2.2 Les risques subis

A l'inverse des risques pris volontairement par la banque sur lesquels elle se rémunère, certaines activités peuvent l'exposer à des risques qu'elle ne souhaite pas. Il s'agit de risques subis.

– **Les risques stratégiques** : ce sont les risques liés aux prises de décisions des organes décisionnels de la banque pouvant générer une perte économique imprévue ;
– **Le risque de non-conformité** : le risque de non-conformité constitue un risque de sanction judiciaire, disciplinaire ou administrative, de perte financière significative ou d'atteinte à la réputation, qui naît du non-respect de dispositions propres aux activités bancaires, qu'elles soient de nature législatives ou réglementaires, ou qu'il s'agisse de normes professionnelles et déontologiques ;
– **Le risque opérationnel** : le risque opérationnel se définit, selon le comité de Bâle, comme étant « le risque de perte directe ou indirecte résultant d'une inadéquation ou d'une défaillance attribuable aux procédures, au facteur humain, systèmes internes ou à des événements extérieurs». Le risque opérationnel exclut les risques stratégiques et le risque de réputation. La présentation de ce risque fait l'objet de la section suivante.

Section 2 : Les spécificités des risques opérationnels dans la banque

Dans la deuxième section, nous allons définir les risques opérationnels, en mettant l'accent sur leurs spécificités et en présentant des exemples de pertes qu'ils ont engendrées.

2.1 Les risques opérationnels : des risques d'une importance croissante

Le risque opérationnel est un risque dont l'importance et la perception se sont accrues au cours des dernières années, sous l'effet conjoint des principaux facteurs suivants :

- **Les mutations dans le fonctionnement des marchés** : les risques associés aux domaines d'intervention des banques s'est accrus suite à la déréglementation et la désintermédiation bancaire, associées à la globalisation des marchés et des produits. Par ailleurs, l'accroissement des acquisitions, fusions et autres regroupements entre banques constitue également des défis importants, en matière, par exemple, d'intégration des différents systèmes de gestion ;

- **La sophistication des techniques financières** : les nouvelles activités des banques sont de plus en plus complexes à gérer et rendent certains risques plus présents. Par exemple, le développement du commerce électronique soulève de nouvelles questions en matière de fraude ou de sécurité informatique, alors que les montages financiers, de plus en plus élaborés, exposent les établissements à un risque juridique accru ;

- **L'évolution des processus internes**: l'automatisation croissante du fonctionnement interne des établissements, avec un rôle de plus en plus central accordé aux outils informatiques en particulier, renforce les risques de nature technique. Le recours croissant à l'externalisation peut également contribuer à l'accroissement des risques opérationnels ;

- **Les événements extérieurs :** ces risques ne sont en aucun cas nouveaux, mais leur perception est aujourd'hui beaucoup plus forte qu'auparavant. Les risques exceptionnels (de faible occurrence mais de forte intensité), comme les catastrophes naturelles ou les actes terroristes, font ainsi l'objet d'une attention accrue.

2.2 Le risque opérationnel : composantes, dimensions et particularités

Pour une gestion efficace du risque opérationnel, il est indispensable de définir avec précision ce type de risque ainsi que ses particularités.

2.2.1 Les composantes du risque opérationnel

Une des définitions du risque opérationnel consiste à le considérer comme un risque résiduel qui n'est un risque de crédit n'est un risque de marché. Cette définition reste trop générale. Elle inclut les risques associés à l'entrée de nouveaux marchés, au développement de nouveaux produits, aux facteurs économiques, etc. Une autre définition possible admet que le risque opérationnel provient des risques d'erreurs dans les transactions et les paiements. Cette définition est trop réductrice, car elle n'inclut pas d'autres risques tels que les dommages aux actifs corporels.

Hull (2010) estime qu'on peut définir le risque opérationnel comme la totalité des risques internes. Dans ce cas, ce risque englobe plus que les risques associés aux opérations et inclut désormais les risques provenant de contrôle inadéquat et tout autre risque associé à la fraude des employés. A coté des risques internes, les régulateurs préfèrent inclure dans leur définition l'impact d'évènements externes, tels que : les catastrophes naturelles, le risque politique ou réglementaire, les failles de sécurité.

Malgré son caractère diffus, quatre composantes essentielles se dégagent de la définition du risque opérationnel proposée par l'accord de Bâle II :

- Une défaillance due aux processus (non-respect, contrôle absent ou incomplet) ;
- Une défaillance due aux personnes (erreur, malveillance et fraude);
- Une défaillance due aux systèmes d'information (panne informatique);
- Une défaillance due aux événements extérieurs (inondation, incendie).

Chacune de ces sources du risque opérationnel est à l'origine des sous-catégories de ce risque. Leurs fréquences de manifestations varient d'un établissement à un autre. L'enquête réalisée en 2002 par le Comité de Bâle auprès de 89 institutions financières (COUCHOUD, 2004 :60), a permis d'obtenir, pour 8 milliards d'euros de pertes dues aux risques opérationnels, une ventilation dans laquelle la fraude et les erreurs en matière d'exécution, de livraison et de gestion des traitements sont les plus importants. Cependant, cela ne devrait pas servir de base

de répartition. En effet, l'ordre de ventilation est en plein mutation avec le développement des systèmes d'information et la naissance de nouveaux domaines d'activité.

L'accord de Bâle II classe les risques opérationnels en sept sous-catégories différentes :

- ***Fraude interne :*** pertes dues à des actes visant à frauder, détourner des biens ou à contourner les règlements, la législation ou la politiques de l'entreprise impliquant au moins une partie interne à l'entreprise. Par exemple, le vol commis par un employé, la falsification de documents, le délit d'initié d'un employé opérant pour son propre compte, les informations inexactes communiquées sur ses positions de marché ;
- ***Fraude externe :*** pertes dues à des actions visant à frauder, à détourner des biens ou à contourner des règlements, la législation de la part d'une partie extérieure à la banque. Par exemple, le détournement de fonds, les faux en écriture, l'usurpation d'identité, le vol de données, les dommages dus au piratage informatique, les chèques de cavalerie[3] ;
- ***Pratiques en matière d'emploi et de sécurité sur le lieu de travail :*** pertes résultant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, de demandes d'indemnisation ou d'atteinte à l'égalité ou actes de discrimination. Par exemple, la violation des règles de santé et de sécurité des employés, les activités syndicales, les plaintes pour discrimination à l'embauche ;
- ***Clients, produits et pratiques commerciales :*** pertes résultant d'un manquement non intentionnel ou du à la négligence, à une obligation professionnelle envers des clients spécifiques ou de la nature ou conception d'un produit. Par exemple, le défaut de conseil, le défaut d'information, l'utilisation frauduleuse d'informations confidentielles sur la clientèle, la vente de produits non autorisés et le blanchiment d'argent;
- ***Dommages aux actifs corporels :*** destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres. Par exemple, actes de terrorisme, vandalisme, séismes, incendies et inondations ;

[3] Chèques tirés sur une société inexistante.

- ***Interruption de l'activité dysfonctionnement des systèmes :*** cette composante couvre les interruptions et dysfonctionnements des systèmes informatiques et de télécommunications. Par exemple, les pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité ;
- ***Exécution, livraison et gestion des processus :*** pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs. Par exemple, erreur d'enregistrement de données, défaillance dans la gestion des sûretés, lacunes dans la documentation juridique, erreur d'accès aux comptes de la clientèle et défaillances des fournisseurs ou conflits avec eux.

2.2.2 Les dimensions du risque opérationnel

Le risque opérationnel se calcule selon la formule suivante :

Risque opérationnel= probabilité x impact

- **La probabilité du risque** : elle désigne les possibilités de réalisation du risque. Elle peut être désignée par le terme voisin de fréquence d'occurrence. Son échelle peut être quantitative (échelle de valeur de 0 à 1 ou encore de fréquence ou pourcentage) ou qualitative (probabilité importante à probabilité faible) (DE MARESCHAL, 2003 : 9).
- **L'impact ou la gravité** : il s'agit de la quantification de la réalisation du risque. Son échelle peut également être quantitative (pertes monétaires, amendes) ou qualitative (gravité faible à gravité forte).

A ces deux dimensions de mesure généralement utilisées, s'ajoutent les notions de « risk timing » et de « risk duration » (MCNAMEE ; 1998 : 39). En effet, le poids de risque dépend également de sa période d'occurrence c'est-à-dire de l'étape du processus à laquelle il se manifeste, ainsi que la durée de ses conséquences sur les activités de la banque.

Il convient de faire la distinction entre le niveau de risque brut du risque opérationnel et son niveau résiduel après application des mesures de contrôles. En fait, il s'agit d'une évaluation plus affinée du risque opérationnel intégrant une évaluation de la qualité du dispositif du contrôle interne.

2.2.3 Les spécificités du risque opérationnel

Le risque opérationnel présente certaines particularités par rapport aux autres risques bancaires :

- Le risque opérationnel est réputé moins fréquent que les autres risques, même si la complexité et la grande taille des institutions financières, ainsi que la sophistication des produits financiers augmentent sa probabilité d'occurrence ;
- Le risque opérationnel est considéré comme très grave. Il engendre des pertes financières désastreuses. Contrairement aux autres types de risques, l'exposition au risque opérationnel ne peut être ni plafonnée, ni échangée. De surcroît, étant donné son caractère imprévisible, son impact financier ne peut être limité ni couvert par des contrats de couverture ;
- Le risque opérationnel est un risque diffus, présent dans tous les départements d'une banque, y compris ceux n'ayant pas une activité commerciale. Il concerne toutes les personnes employées par la banque sans distinction. À cet égard, ce risque est encore plus difficile à gérer et à évaluer ;
- Le risque opérationnel est un risque multiforme. Il regroupe un ensemble de risques variés, tels que :
    - Des risques de nature qualitative : les risques stratégiques, juridiques, administratifs ;
    - Des risques d'ordre technique : les risques associés aux systèmes d'information, aux procédures ;
    - Des risques environnementaux : les risques économiques, politiques, climatiques.
- L'identification précise du risque opérationnel est délicate. De plus, ses manifestations sont souvent difficiles à isoler. Par exemple, un événement, comme une position non autorisée d'un trader, peut résulter de plusieurs causes, à savoir une fraude interne (dépassements de limites autorisée) et/ou des carences du contrôle interne et/ou d'un système informatique inadapté. D'autant plus, ce même événement peut avoir plusieurs effets tels que des pertes financières, atteinte à la réputation, baisse du cours des titres ;
- Le risque opérationnel peut engendrer des pertes financières élevées pour les institutions financières. Parmi les types d'incidents de nature opérationnelle

susceptibles d'occasionner de lourdes pertes, il existe notamment le risque de fraude interne (vol commis par un employé), de fraude externe (piratage informatique) ou la panne de systèmes informatiques.

2.3 Exemples des pertes inhérentes aux risques opérationnels

En 1999, les régulateurs du secteur bancaire ont exigé la mise en place d'une allocation en fonds propres pour le risque opérationnel dans le cadre de nouvel accord de Bâle II. Les banques ont exprimé leurs réticences à l'égard de cette décision. Malgré cela, les régulateurs ont persisté, en argumentant que le risque opérationnel était important pour les banques. Ils ont répertorié plus de 100 pertes dues au risque opérationnel, tous dépassants 100 millions de dollars, au cours de dix ans. . Plus généralement, les pertes subies par les établissements au titre du risque opérationnel sont évaluées à plus de 200 Md d'euros sur la période 1980-2000. Certaines de ces pertes, listées par la Banque des Règlements Internationaux, sont :

- Fraude interne : Allied Irish Bank, Barings et Daiwa ont perdu 700 millions de dollars, 1 milliard de dollars et 1.4 milliard de dollars respectivement sur la base de transactions frauduleuses.
- Fraude externe : Republic New York Corporation a perdu 611 millions de dollars en raison de fraudes commises par un client.
- Pratiques en matière d'emploi et de sécurité sur le lieu de travail : Merrill Lynch a perdu 250 millions de dollars suite à une décision de juste dans une affaire de discrimination à l'embauche.
- Pratiques concernant les clients, les produits et l'activité commerciale : Household International a perdu 484 millions de dollars à cause de prêts frauduleux ; Providian Financial Corporation a perdu 405 millions de dollars en raison de ventes et de facturations frauduleuses.
- Dommages aux biens : Bank of New York a perdu 140 millions de dollars à cause des attaques terroristes du 11 septembre 2001.
- Interruption d'activité et pannes de systèmes : Salomon Brothers a perdu 303 millions de dollars en raison d'une modification du système informatique.

- Exécution des opérations, livraison et processus : Bank of America et Wells Fargo Bank ont perdu 225 millions de dollars et 150 millions de dollars respectivement en raison de défaillances des systèmes d'intégration et des processus de transaction.

Par ailleurs, selon une étude du comité de Bâle en 2001, sur un panel de 89 banques internationales, en moyenne, une banque a été affectée par 528 occurrences du risque opérationnel, majoritairement sur la banque de détail, engendrant une perte unitaire moyenne de 10000 euros. Il s'ensuit une perte brute moyenne de 90 millions d'euros par établissement.
En réalité, il est beaucoup plus difficile de quantifier et de gérer le risque opérationnel que les risques de crédit ou de marché. Les banques prennent des décisions d'octroi de prêts ou de prise de risque de marché de façon consciencieuse. Alors que, de nombreux produits de marché existent pour réduire ces risques, le risque opérationnel fait partie intégrante de l'activité quotidienne. A cet égard, le risque opérationnel fait l'objet d'un encadrement législatif et réglementaire et d'une surveillance accrue de la part des banques.

Section 3 : La gestion des risques opérationnels

La dernière section de ce chapitre va mettre l'accent sur les processus et les méthodes de gestion de risques opérationnels prévues par la réglementation nationale et prudentielle et les organisations internationales spécialisées telles que Committee Of Sponsoring Organizations of the Treadway Commission (COSO) et L'Organisation Internationale de Normalisation.

3.1 Le cadre de référence de la gestion des risques COSO 2

Le référentiel COSO 2 « The Enterprise Risk Management Integrated Framework» (2004) propose un cadre de référence pour la gestion des risques de l'entreprise en détaillant le processus de management des risques et en complétant le référentiel COSO 1 de 1993. Selon COSO 2, 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. 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. On distingue quatre catégories d'objectifs :

- Les objectifs stratégiques : servant la mission de l'organisation ;
- Les objectifs opérationnels : visant l'utilisation efficace et efficiente des ressources ;
- Les objectifs de reporting : liés à la fiabilité de reporting ;
- Les objectifs de conformité : liés aux lois et aux réglementations en vigueur.

L'implémentation d'un ERM au sein de l'entreprise est primordiale. L'ERM soutient la création de valeur en permettant la direction de traiter efficacement les incertitudes futures susceptibles de constituer un obstacle devant la réalisation des objectifs et d'y répondre de manière efficace en augmentant la valeur de l'entreprise.

Le dispositif de management des risques comprend huit éléments. Ils sont les suivants :

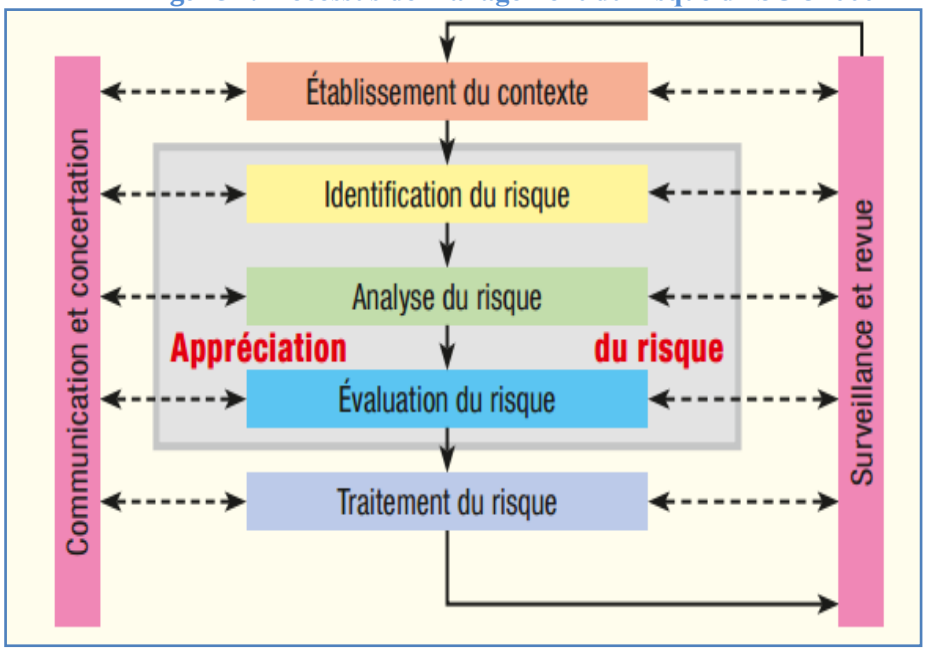
- **L'environnement interne** : il établit la philosophie et la culture de l'entreprise en matière de gestion des risques. Il reconnait l'idée stipulant que les événements attendus ainsi que ceux inattendus peuvent se produire. Il détermine le niveau de sensibilisation du personnel de l'entreprise au contrôle.
- **La fixation des objectifs** : les objectifs de l'entreprise doivent être préalablement fixés. Ainsi, le management peut identifier les incertitudes potentielles, liées à ces objectifs, susceptibles d'en affecter la réalisation. Les objectifs à définir doivent être compatibles avec son appétence pour le risque.
- **L'identification des événements** : il s'agit d'identifier les événements internes et externes susceptibles d'affecter l'accomplissement des objectifs d'une entreprise. La distinction entre risques et opportunités doit être établie.
- **L'évaluation des risques** : les risques identifiés sont évalués en fonction de leur probabilité de survenance et de l'étendue du sinistre au cas où ils se concrétisent.
- **Le traitement des risques** : le cadre COSO définit quatre types de traitement des risques : évitement, réduction, partage et acceptation. Le choix de traitements adéquats nécessite la prise en compte de leur effet sur la probabilité d'occurrence et l'impact des risques et du rapport coût /bénéfice des traitements à envisager.
- **Les activités de contrôle** : elles sont constituées des politiques et des procédures permettant de s'assurer de la mise en place effective des mesures de traitement des risques.
- **Information et communication** : toutes les informations pertinentes sont identifiées, collectées et diffusée convenablement pour permettre aux collaborateurs d'exercer leurs responsabilités.
- **Le pilotage** : il permet de détecter les problèmes, d'identifier les disfonctionnements affectant le processus de management de risque et d'entreprendre les actions correctrices de façon efficace.

3.2 Norme ISO 31000

La norme ISO 31000 *Management du risque- Principes et lignes directrices* publiée en 2009, propose un processus générique de gestion des risques. Ce processus reprend les activités classiques d'appréciation des risques (identification, analyse, évaluation) et de leur traitement. La norme les complète par 3 autres activités.

- **L'établissement du contexte** oblige de définir en amont de ces activités, les paramètres fondamentaux caractérisant l'environnement (interne et externe) dans lequel s'effectue la gestion des risques et la valeur de ces paramètres. Des seuils stipulés par une réglementation ou des critères d'appréciation des risques issus des parties prenantes constituent deux exemples de paramètres de l'environnement externes. Par contre, les pratiques propres à l'organisme sont des exemples de paramètres de l'environnement interne.

Figure 1:Processus de management du risque d'ISO 31000



Source : Management des risques, par Reinhard Weissinger, ISO Focus+ Février 2013

- La norme met également en valeur la tâche de **Communication et concertation** et son couplage avec l'ensemble des autres tâches du processus. Ces échanges concernent les parties prenantes externes et internes à l'organisme. Cette tâche facilite la compréhension de ses changements par les activités de management des risques.
- Enfin, elle distingue la tâche intitulée **Surveillance et revue** ayant par exemple pour but de réévaluer le déroulement des activités de gestion des risques. Cette tâche peut ainsi mesurer l'efficacité de l'emploi des moyens mis en œuvre afin d'améliorer leurs utilisations futures.

3.3 La gestion du risque opérationnel selon la réglementation nationale

Selon l'article 46 de la circulaire la BCT n° 2006 – 19, les banques doivent être dotées d'un système de gestion du risque opérationnel permettant de s'assurer que les risques qui pourraient découler de défaillance ou d'insuffisance de procédures et d'erreurs humaines ou techniques sont identifiés et mesurés périodiquement. Ce système doit permettre d'évaluer l'adéquation de leurs fonds propres au regard de ce risque. Il doit faire l'objet d'un examen périodique et d'une vérification par les commissaires aux comptes. Ces examens doivent porter sur les activités des unités et sur la fonction indépendante de gestion du risque opérationnel.

Conformément à l'article 47 de la même circulaire, les banques doivent enregistrer systématiquement les données relatives au risque opérationnel, notamment les pertes significatives par catégorie d'activité. Le système d'évaluation doit être étroitement intégré aux processus de gestion des risques au sein de la banque. Les données qu'il produit doivent faire partie intégrante de ses processus de surveillance et de contrôle du profil de risque opérationnel. En outre, l'exposition au risque opérationnel (et notamment les pertes importantes subies), doit être régulièrement notifiée à la direction de l'unité concernée, à l'organe de direction et au Conseil d'Administration ou de Surveillance. En fin, les banques doivent disposer de procédures leur permettant de prendre les mesures correctrices à la lumière des rapports à l'organe de direction.

3.4 La gestion du risque opérationnel selon la réglementation prudentielle

L'Accorde de Bâle II impose aux banques de calculer l'exigence en capital relative au risque opérationnel en proposant trois méthodes de calcul. En outre, il propose des saines pratiques de gestion et de surveillance du risque opérationnel.

3.4.1 Bâle II

Le premier Accord de Bâle a été conclu en 1988. Il a établi le premier ratio prudentiel, baptisé ratio Cooke. Ensuite, il s'est apparu que ce ratio n'est plus adapté au nouvel environnement sous la conjugaison de plusieurs facteurs :

- Les fonds propres calculés selon les règles de Bâle I donnent une insensibilité aux risques. En effet, les divers degrés d'exposition au risque de crédit ne sont pas suffisamment différenciés ; par exemple toutes les entreprises sont pondérées à 100% ;
- L'Accord de Bâle I ne prend en compte que les risques opérationnels ;

- La seule exigence d'un capital minimum, pour inciter les banques à gérer sainement leurs opérations, était insuffisante. En effet, elle n'a pas empêché la faillite des banques respectant parfaitement le ratio Cooke. Donc, il est nécessaire d'introduire des exigences qualitatives.

A partir de 1999, le comité de Bâle a réalisé une réforme de l'Accord débouchant sur l'Accord de Bâle II en 2004. Selon lequel, les banques doivent prendre en compte le risque opérationnel dans le calcul du ratio de solvabilité. Actuellement, ce ratio appelé ratio McDonough a la forme suivante :

$$\frac{\boldsymbol{Fonds\ propres}}{\boldsymbol{Risque\ crédit + Risque\ de\ marché + Risque\ opérationnel}} > 8\%$$

Dans le même Accord, le Comité a instauré un processus de surveillance prudentielle. Ce processus impose à la banque d'analyser l'ensemble de ses risques, de calculer ses besoins de fonds propres. Il exige la confrontation par l'autorité de contrôle bancaire, au sein du pays, de sa propre analyse du profil de risque de la banque avec celle conduite par la banque elle-même, en vue d'adapter son action prudentielle, que ce soit via des fonds propres supérieurs aux exigences minimales ou toute autre technique appropriée. En outre, l'Accord prescrit aux banques de communiquer les informations nécessaires, concernant la composition de leurs fonds propres, l'évaluation et la gestion des risques, ou encore l'allocation des fonds propres, pour permettre à des tiers d'apprécier l'adéquation de leurs fonds propres.

L'Accord de Bâle II propose trois approches de calculs des exigences en fonds propre en couverture du risque opérationnel. Les institutions financières ont la possibilité de choisir l'approche qui leur paraît correspondre le mieux à la spécificité de leur activité, ainsi qu'à leur capacité globale d'action. En effet, elles doivent s'assurer qu'elles disposent de l'ensemble des moyens nécessaires à la mise en œuvre effective de la solution retenue. Le degré de complexité de chacune de ces trois approches est variable, allant d'une méthodologie grossière jusqu'à des modèles de sensibilité au risque techniquement très sophistiqués. Les trois méthodes de calcul disponibles sont :

- **L'approche de l'indicateur de base** : c'est l'approche la plus simple, mais elle induit un capital économique important. Elle préconise que les fonds propres dédiés au risque opérationnel correspondent à 15% du produit annuel brut moyen de l'établissement sur les trois dernières années. Ce produit correspond aux produits d'intérêts créditeurs nets et autres

produits d'exploitation[4]. Il exclut les provisions, les plus ou moins values liées au portefeuille titres et les éléments exceptionnels. La règle peut donc être exprimée à partir de l'équation suivante :

Capital réglementaire = 15% x Produit Annuel Brut Moyen

Cette approche très simplifiée correspond à l'idée sous-jacente que l'ampleur du risque opérationnel est une fonction positive du volume des activités estimé par les différents éléments du revenu annuel brut. Les données de produits annuels bruts, puisées dans la comptabilité officielle, ont l'avantage d'être disponibles pour toutes les institutions, à la différence d'autres indicateurs plus directs du volume, comme le nombre de clients ou le nombre de transactions.

Le chiffre de 15% a été retenu suite aux deux premières études quantitatives d'impact réalisées lors de calibrage de l'Accord. En effet, il apparaît qu'en moyenne, 15% du revenu annuel brut représente le montant cible de capital réglementaire opérationnel, pour les 29 établissements ayant répondu aux premières études quantitatives d'impact lancées par le Comité de Bâle en mai 2001. L'approche de base n'est soumise à aucune condition d'agrément. Cependant, quelle que soit l'approche adopté, le calcul du capital réglementaire opérationnel doit être complété par des éléments contenus dans le document « Sound Prictices for the Management and Supervision of Operationnal risk », publié en février 2003 par le Comité.

- **L'approche standard :** légèrement plus compliquée, cette approche décompose les activités bancaires en huit lignes de métier. Elle permet de calculer séparément pour chaque ligne de métier le capital économique associé, en se basant essentiellement sur le revenu brut de la ligne en question. Le produit brut moyen des trois dernières années pour chacune de ces métiers est multiplié par un « facteur β » (voir tableau 1) selon le niveau de risque opérationnel estimé de chaque activité. Puis, la somme totale permet de déterminer les fonds propres nécessaires, afférent au risque opérationnel. Les facteurs de multiplication dans le calcul du capital réglementaire proviennent de la deuxième étude quantitative d'impact menée par le Comité de Bâle.

[4] Le produit d'intérêt net correspond à l'excès des produits perçus sur prêts par rapport aux produits versés les dépôts et les autres ressources qui financent les prêts.

Tableau 1 : Facteur bêta par ligne d'activité

Métiers	Exemples	β
Financement d'entreprise	Collectivité locale et administration publique, les banques d'affaires, service et conseil	18%
Activité de marché	Vente, tenu de marché, prise de participation sur compte propre, trésorerie	18%
Banque de détail	C'est l'activité pour les particuliers : prêt et dépôt ; les carte ; banque privé	12%
Banque commerciale	Le financement des exportations et du commerce ; affacturage ; crédit bail et les prêts	15%
Paiements et règlements	La clientèle extérieur ; transfert de fond, compensation et règlement	18%
Fonction d'agence	Conservation, prestation d'agent aux entreprises	15%
Gestion d'actifs	La gestion des portefeuilles	12%
Courtage de détail	Exécution et services complets	12%

Source : Bâle 2

- **L'approche de mesures complexes** : c'est l'approche la plus sophistiquée et la plus exigeante techniquement. Dans le cadre de cette approche, le superviseur peut autoriser une banque à utiliser sa propre méthode d'évaluation du capital économique lié au risque opérationnel, sous réserves de valider certains critères d'agrément. Différentes méthodes sont

possibles. Elles sont fondées sur les données internes de perte de la banque, éventuellement complétées avec des données externes. Elle comporte trois méthodes de mesure de risque opérationnel produite par le système interne de la banque, sur la base des critères quantitatifs et qualitatifs propres à l'organisation interne et à l'activité de la banque.

- **L'approche « distribution des pertes »** : cette approche constitue une méthode avancée de calcul de la perte non anticipée. Elle s'appuie sur une base de données de pertes provenant de l'établissement ou de sources externes. Il s'agit d'établir pour chaque ligne de métier et chaque type d'événement de perte deux courbes de distribution de probabilités, l'une représentant la fréquence des événements de pertes et l'autre la sévérité de ces mêmes événements sur un intervalle de temps donné. Pour ce faire, on trie les événements de pertes par fréquence d'une part, et par coût d'autre part, et l'on représente le résultat sous forme graphique (histogrammes). Pour chacune des distributions obtenues, on recherche ensuite le modèle mathématique qui rend le mieux compte de la forme de la courbe. Pour valider le choix d'un modèle mathématique, on met en relation le résultat (fréquence ou perte) prédit par le modèle mathématique et le résultat de la courbe issue des données réelles : si les deux courbes se superposent, le modèle est réputé fiable.

  Les 2 distributions sont combinées, en utilisant une simulation de Monte-Carlo afin d'obtenir, pour chaque ligne métier et chaque type d'événement, une courbe agrégée de distribution des pertes pour un horizon de temps donné. Pour chacune, la Value At Risk (VAR) est la perte maximale encourue avec une probabilité de 99,9%. Le capital requis dans le cadre de Bâle II est alors la somme des VAR ainsi calculées.

- **L'approche par les scénarios** : elle consiste à mener des enquêtes systématiques auprès d'experts de chaque ligne métier et de spécialistes de la gestion des risques. Le but est d'obtenir de ces experts une évaluation de la probabilité et du coût d'incidents opérationnels identifiés conformément aux grilles d'analyse proposées par le comité de Bâle. La construction des scénarios combine l'ensemble des facteurs de risques d'une activité donnée. On effectue ensuite des simulations en faisant varier les facteurs de risque.

  Cette approche constitue un complément intéressant lorsque les données historiques ne sont pas suffisantes pour appliquer une méthode purement statistique. Elle trouve en particulier son application pour évaluer les impacts d'événements de risque de sévère

amplitude, ou l'impact de la survenance simultanée de plusieurs événements. L'intérêt de cette méthode est de pouvoir capter des événements singuliers dont les conséquences pourraient être graves pour l'établissement et qu'une approche statistique aurait du mal à être envisagée.

- **La méthode de scorecard** : elle consiste à donner un score aux différents risques associés aux processus. Ce score peut évoluer en fonction des différents critères qui le composent et ainsi faire varier le montant en risque qui lui-même détermine les fonds propres nécessaires à sa couverture. Cette méthode procède par une série de questions pondérées, dont certains peuvent s'apparenter à des scénarios. Cette méthode nécessite l'intervention d'experts afin d'évaluer le degré de maîtrise et de proposer les actions correctrices.

3.4.2 Les saines pratiques pour la gestion et la surveillance du risque opérationnel

Dans le but de définir les meilleures pratiques s'appliquant aux établissements de crédit dans leur appréhension des risques opérationnels, le Comité de Bâle a rédigé, en 2003, un document intitulé « saines pratiques pour la gestion et la surveillance du risque opérationnel » scindé en quatre grandes parties. Chaque partie propose des principes à appliquer.

- ***L'élaboration d'un environnement adéquat pour la gestion du risque :***

Principe 1 : le conseil d'administration doit considérer le risque opérationnel comme une catégorie distincte de risque à gérer. Il doit approuver et réexaminer périodiquement le dispositif de gestion de ce risque.

Principe 2 : le dispositif de gestion du risque opérationnel de la banque doit être soumis à un audit interne efficace et complet, effectué par un personnel fonctionnellement indépendant et compétent.

Principe 3 : le dispositif de gestion du risque opérationnel mis en place par la direction générale doit être appliqué de façon cohérente dans la banque. En outre, la direction générale doit élaborer des politiques de gestion du risque opérationnel.

- ***Gestion du risque : identification, évaluation, suivi et maîtrise/atténuation du risque***

Principe 4 : les banques doivent identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. L'identification des risques opérationnels doit prendre en compte à la fois les facteurs internes (la structure de la banque, la nature de ses activités, la qualité de ses ressources humaines) et externes (les évolutions du secteur bancaire, les progrès technologiques). Les outils d'évaluation des risques opérationnels sont l'autoévaluation, la cartographie des risques, les indicateurs du risque et la quantification du risque.

L'autoévaluation : La banque évalue ses opérations et ses activités en fonction d'une liste de points potentiellement exposés au risque opérationnel.

La cartographie des risques : c'est un processus qui cartographie par type de risque les diverses fonctions organisationnelles. Il peut repérer les zones de faiblesse et permet d'établir des actions à entreprendre par la direction.

Les indicateurs de risque : ce sont des statistiques ou des mesures, souvent d'ordre financier, donnant une idée sur l'exposition d'une banque au risque opérationnel, notamment, le nombre d'opérations non exécutés, le taux de rotation du personnel, la fréquence et la gravité des erreurs et omissions.

La quantification du risque : pour quantifier leur exposition au risque, certains établissements utilisent les séries historiques sur les pertes opérationnelles, dont les gravités et les fréquences sont enregistrées systématiquement, croisées avec des données externes de pertes.

Principe 5 : un processus de suivi régulier des profils de risque opérationnel et des expositions importantes à des pertes doit être mis en œuvre. La communication des informations utiles à une gestion dynamique du risque à la direction générale doit être régulière

Principe 6 : Les banques doivent adopter des politiques pour maîtriser et atténuer les sources importantes de risque opérationnel. Ces politiques doivent être réexaminées périodiquement.

Principe 7 : Les banques doivent mettre en place des plans de secours et de continuité d'exploitation pour garantir un fonctionnement sans interruption et limiter les pertes en cas de perturbation grave de l'activité.

En 2010, le comité de Bâle a eu pour mission d'adapter la réglementation prudentielle au contexte post-crise des Subprimes. Le risque opérationnel n'a pas suscité un intérêt

approprié lors de la réforme de Bâle III, qui s'est davantage focalisée sur les conséquences (crise de liquidité, crise systémique) que sur l'origine (risque opérationnel) des problèmes. Or, pour mettre en place une réglementation prudentielle efficace, il ne suffit pas de réguler les symptômes de la crise, il est indispensable de surveiller également les causes.

Conclusion

Dans ce premier chapitre, nous avons présenté brièvement les activités de la banque ainsi que les risques qui y sont inhérents. En suite, nous avons mis l'accent sur la définition et les particularités du risque opérationnel bancaire. La dernière section du présent chapitre est consacrée à la gestion de risques opérationnels dans la banque. Pour cela, nous avons mis en exergue tant les processus de gestion des risques que les réglementations nationales et prudentielles relatives à ce sujet.

Evidemment, pour gérer les risques opérationnels, il faut les identifier, les évaluer et recenser les dispositifs de maîtrise existant pour les couvrir. En suite, il faut préparer un plan d'action destiné au traitement des risques majeurs. Cette démarche est la cartographie des risques. Elle fera l'objet du chapitre suivant.

CHAPITRE 2 :

LA DÉMARCHE D'ÉLABORATION D'UNE CARTOGRAPHIE DES RISQUES OPÉRATIONNELS

Introduction

La cartographie des risques constitue un outil de gestion des risques opérationnels. Elle permet, selon RENARD (2008), d'identifier, d'évaluer et de hiérarchiser les risques en tenant compte des dispositifs de maîtrise mis en place au sein de la banque. Son élaboration requiert une démarche méthodologique à suivre. Etant établie, la cartographie des risque permet de déterminer les actions à entreprendre pour traiter les risques majeurs. Elle sert d'un moyen de communication sur les risques qui doit être mis à jour en continue.

Dans ce chapitre, nous avons mettre l'accent sur la démarche d'élaboration de la cartographie des risques. Pour ce faire, nous allons commencer par un préalable à la cartographie des risques. En suite, nous allons passer à la présentation de la démarche de son élaboration. Ainsi, ce chapitre sera scindé en trois sections :

Section 1 : préalable à la cartographie des risques
Section 2 : démarche d'élaboration de la cartographie des risques opérationnels
Section 3 : Après cartographie des risques opérationnels

Section 1 : Préalable à la cartographie des risques

La section actuelle s'occupera de certains concepts de cartographie des risques. Elle abordera tout d'abord la définition et les types de la cartographie des risques. Par la suite, elle présentera ses objectifs, les avantages visés par son élaboration et les conditions de sa réussite.

1.1 Définitions de la cartographie des risques

Plusieurs auteurs et groupes professionnelles ont défini la cartographie des risques. La multitude de définitions relatives à ce terme tournent autour du même objectif : une représentation visuelle des risques de l'entreprise servant de support à leur maîtrise. Selon l'IFACI (2003), la cartographie des risques est « le positionnement des risques majeurs selon différents axes, tels que l'impact potentiel, la probabilité de survenance ou le niveau actuel de maîtrise des risques.» Par ailleurs, selon DE MARESCHAL (2003) « la cartographie des risques est un mode de représentation et de hiérarchisation des risques d'une organisation. Cette représentation s'appuie sur une identification des risques effectuée sur la base de la définition des risques. »

Une définition plus récente de L'IFACI (2005) estime que la cartographie des risques est une représentation graphique de la probabilité d'occurrence et de l'impact d'un ou plusieurs risques. Les risques sont représentés de manière à identifier les risques les plus significatifs (probabilité et/ou impact la ou le plus élevé(e) et les moins significatifs (probabilité et /ou impact la ou le plus faible).» Cependant, la définition de Bernard et al. (2008) va plus loin. Ils définissent la cartographie des risques comme étant « un outil de pilotage vivant qui doit permettre de mesurer régulièrement la progression de l'entité dans son niveau de maitrise des risques ».

Hassid (2008) présente la cartographie des risques comme « un processus d'identification, de hiérarchisation et d'évaluation des risques permettant de les positionner sur des échelles afin de les traiter ». BERENARD et Al, (2010) proposent une définition semblable à cette dernière. En effet, ils estiment que la cartographie des risques permet d'identifier, d'analyser, de classer, de comparer et de hiérarchiser les risques afin de pouvoir

mettre en place des méthodes et procédure dans le double but de les prévenir et de les maîtriser, voire de les éliminer.

De ces définition il en ressort que la cartographie des risques permet de recenser les risques majeurs d'une organisation et de les présenter de façon synthétique sous une forme hiérarchisée. Cette hiérarchisation s'appuie sur les critères suivants :

- L'impact potentiel ;
- La probabilité de survenance ;
- Le niveau actuel de maitrise de risque

Après avoir défini la cartographie des risques, nous allons présenter ses types dans le paragraphe suivant.

1.2 Les types de cartographie des risques

Avant de mettre en place une cartographie des risques, il est indispensable de définir son type. D'une part, LENEL et Al (2009) préconise l'existence de deux types de cartographie des risques à savoir la cartographie globale et la cartographie thématique. D'autre part, DE MARSCHAL (2003) affirme que le choix de type de la cartographie est directement lié au type de risque étudié.

1.2.1 La cartographie globale

DE MARESCHAL (2003) estime que la cartographie globale des risques tend à recenser, quantifier et cartographier l'ensemble des risques d'une organisation, tous sujets confondus. En effet, établir une cartographie globale consiste à réunir et hiérarchiser les principaux risques auxquels est exposée une organisation.

La connaissance de ces risques et de leurs caractéristiques est essentielle pour les gérer de manière efficace. Cela diffuse une vision partagée des risques au sein de l'organisation ainsi qu'une culture de gestion des risques auprès de la direction. De plus, grâce à la cartographie globale des risques, l'organisation peut avoir une base permettant de classer les actions à entreprendre pour atténuer ses risques majeurs.

Par ailleurs, l'élaboration d'une cartographie globale des risques conduit à l'amélioration de la communication sur les risques au sein d'une organisation en particulier vers la direction générale. Cela répondra à des demandes extérieures telles que les marchés

financiers, les partenaires ou à des obligations de la réglementation prudentielle ainsi qu'à la demande grandissante de transparence sur les risques. De plus, avoir une cartographie globale des risques permet d'optimiser l'allocation des ressources entre les actions visant à atténuer les risques et l'achat des contrats d'assurance.

1.2.2 La cartographie thématique

A la différence de la cartographie globale, celle thématique se limite à un domaine particulier. DE MARESCHAL (2003) définit la cartographie thématique comme étant un outil de recensement et d'hiérarchisation des risques liés à un thème précis. Elle peut être réalisée, par exemple, sur les risques des systèmes d'information, les risques juridiques, ou les risques liés à la mise en place d'un projet particulier au sein de l'entreprise.

Elle peut constituer un premier pas vers une cartographie globale. D'une part, elle permet d'avoir une vision synthétique mais précise des différents domaines de risques pour un thème déterminé. D'autre part, elle a pour intérêt de pouvoir réunir et comparer sur un thème donné soit des différentes organisations pour un même risque soit des différents domaines de risques liés au thème étudié pour une même organisation.

Après avoir défini les types de la cartographie des risques, nous allons définir ses objectifs.

1.3 Objectifs de la cartographie des risques

La cartographie des risques constitue un véritable inventaire des risques d'une organisation. Elle permet d'atteindre les objectifs suivants:

- Inventorier, évaluer et classer les risques de l'entreprise par domaine, fonction ou processus de gestion;
- Informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités au sein de son département ;
- Permettre à la direction générale ou au département d'audit interne d'élaborer une politique de risque ;
- Permettre aux responsables opérationnels de mettre à jour leur système de contrôle interne en corrigeant l'aspect spécifique du risque identifié se rapportant à leur unité ;
- Permettre aux auditeurs internes et externes d'élaborer leur plan d'audit afin d'identifier la pertinence et l'efficacité des contrôles mis en place ;

- Aider le management dans l'élaboration de son plan stratégiques et sa prise de décision ; il s'agit alors d'un outil de pilotage interne ;
- Améliorer ou développer une culture de management des risques dans une entreprise grâce à l'établissement, notamment d'outils d'auto-évaluation ;
- Respecter les lois ou les bonnes pratiques en matière de gouvernement d'entreprise.

Les objectifs étant définis, nous allons présenter les motivations conduisant à l'établissement d'une cartographie des risques.

1.4 Les motivations de l'élaboration d'une cartographie des risques

Plusieurs facteurs peuvent amener les dirigeants d'une banque à élaborer une cartographie des risques plutôt qu'à chercher à user d'autres outils de gestion des risques.

- **Le plan d'audit** : la cartographie des risques permet le pilotage de la gestion du risque en identifiant les domaines d'actions prioritaires. En effet, elle oriente le plan d'audit interne en mettant en lumière les processus ou les activités où se concentrent les risques majeurs ;
- **Un référentiel des risques** : La cartographie des risques est établie pour permettre autant aux dirigeants ainsi qu'aux opérationnels d'avoir un référentiel homogène en matière de risques. D'une part, elle fournit une définition commune de risque pour l'entreprise. D'autre part, elle propose une méthode partagée d'évaluation des risques ainsi que des contrôles et des plans d'action.
- **La communication en matière des risques** : la cartographie est un outil de communication interne. En effet, les dirigeants l'utilisent pour maitriser l'évolution des risques majeurs susceptibles d'affecter gravement leurs activités et pour lesquels des actions préventives et correctives doivent être menées en priorité. La cartographie des risques est aussi un outil de communication externe. Elle vise à rassurer l'ensemble des parties prenantes (Etat, assurance, commissaires aux comptes, marchés financiers) quant à la capacité de l'entreprise à honorer ses engagements en toutes circonstances. De plus, elle permet de répondre à la demande grandissante de transparence en matière de risques (DE MARSCHAL, 2003).

- **La réglementation bancaire** : les banques doivent constituer des fonds propres réglementaires pour la couverture de leurs risques bancaires. Cela impose aux banques de disposer d'outils aidant à l'identification et à l'évaluation des risques inhérents aux activités des banques. A cet égard, la cartographie des risques représente une étape préalable en matière de gestion des risques pour faciliter le développement des méthodes d'évaluation des risques.

Etant un outil essentiel de gestion des risques au sein de l'entreprise, la cartographie des risques exige un certain nombre de facteurs de réussite.

1.5 Les facteurs clés de succès d'une cartographie des risques

La réussite de la cartographie des risques dépend de certains facteurs (FONTUGNE et AL, 2001) :

- **Un soutien motivé et une implication de la part de la direction générale :** étant une décision stratégique, l'élaboration de la cartographie des risques dans une entreprise doit être prise par la direction générale. Ainsi, il est fondamental pour sa réussite que les dirigeants s'impliquent et soutiennent l'équipe travaillant sur le sujet. De plus, un tel projet comporte souvent une forte composante de changement. Il est par conséquent impératif que les opérationnels se sentent obliger d'y participer.
- **Des objectifs clairs et biens communiqués :** afin de réussir le projet de cartographie des risques, une définition claire et précise des objectifs est un pré-requis essentiel. Elle détermine l'approche à suivre. Une fois ces objectifs sont bien définis, ils doivent être compris parfaitement par l'équipe de travail afin de favoriser une vision cohérente de la démarche à adopter.
- **La désignation d'un chef de file :** étant un projet, l'élaboration d'une cartographie des risques doit avoir un responsable. Ainsi, il est impératif de désigner un responsable qui peut être un risk manager, un membre du département de l'audit interne ou de la direction générale.
- **Une équipe de travail de qualité :** la mise en place d'une équipe de qualité est un facteur important de succès de la cartographie de risques. Une telle équipe doit être composée de responsables opérationnels ayant une meilleure vision des processus et activités de la banque, ainsi que des membres de la direction générale ayant à charge d'adapter la stratégie de la banque et de prendre les décisions en matière de politique

de risque. L'intervention des spécialistes outillés tels que les cabinets de conseil externes peut être très bénéfique dans la prise de décisions.

- **La disponibilité des moyens** : outre la constitution d'une équipe dynamique et expérimentée, la cartographie des risques nécessite des fonds, ainsi que des ressources humaines et des moyens informatiques pour sa réalisation.

Après avoir présenté la notion de cartographie des risques en mettant l'accent sur ses types, objectifs et les facteurs clés pour réussir son élaboration, nous allons passer dans la section suivante à présenter la démarche à suivre afin de réaliser une cartographie des risques opérationnels au sein de la banque.

Section 2 : Démarche d'élaboration de la cartographie des risques

Il n'existe pas une démarche standard d'élaboration de cartographie des risques. Les démarches varient selon les auteurs. Cependant, nous pouvons identifier trois phases primordiales dans chaque démarche à savoir : la phase de préparation, la phase de conception et la phase après cartographie.

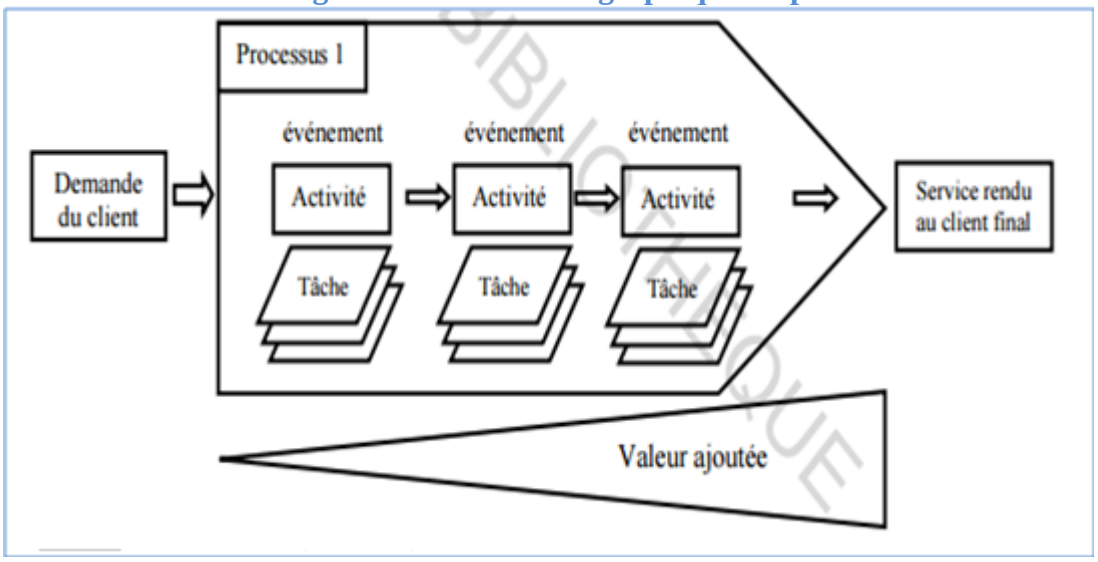
2.1 La phase préparatoire :

Selon Moreau (2003), De Marschal (2003) la phase préparatoire comprend :

- La constitution d'une équipe de qualité pour les travaux ;
- La préparation des fonds nécessaires à la réalisation de ces travaux ;
- La recherche du soutien de la direction générale ;
- La définition du périmètre de la cartographie ;
- Le choix d'une typologie des risques.

Par ailleurs, il faudra procéder à une étude documentaire sur les pratiques existantes en matière de cartographie des risques et construire une démarche contenant les meilleures pratiques. Selon Baron (2001), cette phase peut se poursuivre jusqu'à la segmentation de l'organisation en processus, sous processus et tâches élémentaires. Un processus peut être défini comme étant un enchaînement ordonné d'un ensemble d'activités, produisant une valeur ajoutée croissante, et qui conduit à un produit délivré à un client, correspondant à sa sollicitation initiale (Jiménez et al : 2008).

Figure 2: Présentation graphique du processus



Source : Jiménez & al (2008)

L'inventaire des processus peut se faire en distinguant les processus de métier, les processus supports et les processus managériaux. Les processus de métier sont ceux qui interviennent dans la réalisation du produit ou de la prestation. En ce qui concerne les processus support, ils sont ceux qui fournissent les ressources (humaines, matérielles, financières…) à tous les processus. Par contre les processus managériaux comprenant notamment les processus liés à la planification stratégique, à l'établissement des politiques, à la fixation des objectifs, à la mise en place de la communication, à la mise à disposition des ressources nécessaires et aux revues de direction.

Au sein de la banque, l'identification des processus devrait être faite en respectant le découpage de Bâle. En effet, afin que la démarche de cartographie des risques réponde aux objectifs de la gestion du risque opérationnel, les processus doivent être explorés tout en prenant en considération les lignes de métiers existants au niveau de la banque.

Une fois ce travail est achevé, il s'agit de déterminer pour chaque processus les sous processus qui lui sont rattachés. Les processus doivent être décrits avec un niveau de granularité permettant de mettre en évidence les éventuelles zones de risque opérationnel et de conduire l'analyse des facteurs et événements de risque correspondants ainsi que des contrôles existants. L'étape suivante consistera à l'identification des risques opérationnels inhérents à chaque processus.

2.2 La phase de conception

Elle constitue la phase clé de la démarche d'élaboration de la cartographie des risques opérationnels. Elle comprend plusieurs étapes. La première étape constitue l'identification des risques opérationnels.

2.2.1. Identification des risques opérationnels

Il s'agit d'associer à chaque ligne de métier les évènements de risque opérationnel pouvant l'affecter directement ou indirectement selon le même découpage en famille de risque de Bâle. Tous les événements à risques qui peuvent se produire lors d'un processus et qui pourraient avoir des conséquences sur son déroulement sont répertoriés. Par ailleurs, certains événements types peuvent se retrouver comme événement à risque dans un grand nombre de processus, par exemple l'erreur humaine ou l'interruption du système d'information. Pour entreprendre ce recensement, plusieurs approches peuvent être suivies.

- **Les approches d'identification des risques**

Les approches d'identification des risques sont diverses. Elles varient d'un auteur à un autre. Selon IFACI (2006), DE MARESCHAL (2003), il existe trois approches de cartographie des risques à savoir l'approche bottom-up, l'approche top-dow et l'approche combinée. Pour JIMENEZ et al (2008), à coté ces trois approches, il existe l'approche par le benchmarking.

- **L'approche bottom-up**

Dans le cadre de cette approche, les risques opérationnels sont identifiés par les opérationnels. En suite, ils seront communiqués via un dispositif de reporting au management et aux personnes chargées de l'élaboration de la cartographie des risques et la détermination des plans d'action. Ce type de recensement des risques se fait généralement par l'intermédiaire des entretiens. L'utilisation d'une grille des risques potentiels, préparée à l'avance, permet de s'assurer que tous les risques ont bien été évoqués. Cette approche est souvent utilisée dans une cartographie globale.

L'approche bottom-up est basée sur le principe selon lequel les opérationnels étant les plus proches de l'activité de l'entreprise. Pour cela, ils sont les premiers acteurs impliqués dans le processus de cartographie des risques. Elle permet de fournir aux dirigeants ainsi qu'aux

opérationnels un outil leur permettant de visualiser les risques auxquels leurs processus sont confrontés afin de mieux les gérer. L'identification des risques selon cette approche se fait de manière relativement libre et ouverte (DE MARESCHAL 2003). Cela renforcera la communication entre les différents acteurs de l'entreprise.

Cependant, cette approche d'identification des risques s'avère couteuse en termes de temps et de compétences. En effet, elle requiert la tenue de nombreux entretiens et la collecte d'informations en masse.

- **L'approche top-down**

Cette approche se présente comme l'inverse de l'approche précédente. La hiérarchie détecte les risques susceptibles d'empêcher l'atteinte des objectifs stratégiques de l'entreprise. Puis, elle les soumet pour avis aux collaborateurs opérationnels. Cette approche est souvent utilisée dans une cartographie thématique et peut se faire par questionnaire.

Elle présente l'avantage de la facilité de mise en œuvre. En effet, le nombre d'entretiens nécessaires est réduit. De plus, elle permet d'améliorer le processus décisionnel. Elle favorise aussi l'instauration d'une culture des risques dans l'entreprise propice à l'amélioration continue des processus. Cependant, elle présente l'inconvénient d'être mois précise dans l'identification des risques.

- **L'approche combinée**

Dans le cadre de cette approche, les risques sont déterminés parallèlement par la hiérarchie et les opérationnels. Elle est considérée comme la plus efficace par rapport aux deux premières approches. En effet, ces dernières sont complémentaires. Elles doivent être combinées et développées afin de couvrir aux mieux l'ensemble des risques. Le schéma ci-dessous illustre la complémentarité des deux approches.

- **L'approche par le benchmarking**

Cette approche consiste à étudier et analyser les meilleures pratiques d'élaboration d'une cartographie des risques des entreprises exerçant des métiers similaires et ayant les mêmes processus afin de s'en inspirer et d'en retirer le meilleur (JIMENEZ et al, 2008).

Après la présentation des approches d'identification des risques, nous allons définir quelques outils utilisés pour le recensement des risques.

Les outils d'identification des risques

Divers outils sont utilisés dans le cadre de la collecte des données relatives aux risques. Nous citons les outils suivants.

- **Le questionnaire**

Le questionnaire est un ensemble de questions construit dans le but d'obtenir l'information correspondant aux questions de l'évaluation. L'enquête par questionnaire est un outil d'observation qui permet de quantifier et comparer l'information. Elle combine souvent deux formes de questionnaires à savoir le questionnaire fermé et le questionnaire ouvert.

Dans un questionnaire fermé, les questions imposent au répondant une forme précise de réponse et un nombre limité de choix de réponse. Dans un questionnaire ouvert, la personne interrogée développe une réponse que l'enquêteur prend en note. Dans ce cas, l'enquête par questionnaire ouvert ressemble à un entretien individuel de type directif.

- **Le questionnaire d'audit interne**

C'est un outil indispensable dans l'identification des vulnérabilités au niveau des processus opérationnels. Il s'agit d'une grille d'analyse. Elle permet d'apprécier le niveau du dispositif de contrôle interne du processus audité et d'y apporter un diagnostic.

- **L'interview**

C'est un moyen de collecte d'informations. Il permet d'expliquer et de commenter le déroulement des opérations afférentes à un processus ainsi que les risques y sont inhérents.

- **Les tableaux d'identification des risques**

Ce tableau a la particularité de donner une évaluation sommaire des risques inhérents à la tâche ainsi que les dispositifs de contrôle mise en place pour les couvrir comme le montre le tableau suivant :

Tableau 2: Tableau 2:Tableau d'identification des risques de RENARD (2010)

Tâches	Objectifs	Risques	Evaluation	Dispositif du contrôle interne*	Constats**

* les dispositifs de contrôle interne devant exister pour couvrir les risques identifiés.
** l'existence ou l'absence des dispositifs identifiés.

Source : RENARD (2010)

Commentaire du tableau : pour chaque tâche identifiée, nous déterminons ses objectifs (sécurité, conformité), les risques auxquels la banque est exposée en cas de mauvaise

exécution (pertes financières, pertes juridiques ou de réputation). En suite, nous évaluons ces risques (insignifiant, faible, moyen, élevé) ainsi que les dispositifs de contrôle envisagés afin de les couvrir en mettant l'accent sur leur maitrise dans les constats.

À coté des approches et des outils d'identification des risques, il existe des techniques permettant d'effectuer ce recensement.

- **Les techniques d'identification des risques**

Afin d'identifier de manière la plus complète possible tous les évènements générateurs de risques opérationnels pour l'entreprise, plusieurs techniques peuvent être utilisées.

- **Identification basée sur l'atteinte des objectifs**

Les risques potentiels sont déterminés en fonction des objectifs de l'entreprise. Ainsi, il s'agit d'identifier d'abord les objectifs et leur affecter les menaces inhérentes. L'efficacité de cette technique se base sur une identification claire et partagée des objectifs en amant.

- **Identification basée sur l'analyse historique**

Dans cette technique, il s'agit d'identifier les risques en se basant sur ceux déjà survenus au sein de l'entreprise.

- **Identification basée sur les check-lists**

Cette technique permet de passer en revue les risques classiques d'un domaine ou d'un processus. Elle a l'avantage de lister d'une manière exhaustive les risques.

- **Identification basée sur l'analyse des activités**

Il s'agit de décomposer les processus en activités afin d'identifier les risques qui y sont associés. Autrement dit, il s'agit des conséquences potentielles de la non-exécution ou la mauvaise exécution de ces activités.

- **Identification basée sur l'analyse de l'environnement**

Cette technique prend en compte les risques potentiels par anticipation de l'évolution future de l'environnement externe et interne.

- **Identification basée sur la décomposition en tâches élémentaires**

Elle consiste à découper les activités de l'entreprise en tâches élémentaires et à recenser les risques essentiels rattachés à chaque tâche (RENARD, 2008).

- **Identification basée sur les scénarios**

Cette technique consiste à faire recours à des experts ou des bases de données externes pour identifier les risques.

Il faut noter que le choix de la technique d'identification des risques opérationnels dépendra des objectifs définis par l'entreprise. Ces techniques peuvent être utilisées en combinaison les unes avec les autres selon les préférences de l'entreprise.

Après l'identification des risques, il est nécessaire de procéder à leur évaluation et à leur classement suivant leurs cotations.

2.2.2. Evaluation des risques inhérents

L'évaluation des risques est une étape centrale de la cartographie des risques. Elle consiste à évaluer la probabilité d'apparition de chaque risque recensé et à estimer l'impact de sa réalisation. L'impact du risque est apprécié en se basant sur l'atteinte à l'image de la banque, les pertes financières et les poursuites judiciaires.

Il s'agit d'évaluer de manière brute, sans tenir compte des dispositifs de contrôle, l'exposition de l'entreprise à l'univers des risques (BERNARD et al, 2008). Il convient d'introduire la distinction entre le risque inhérent et le risque résiduel. Pour DE MARESCHAL (2006) :

- le risque inhérent est le risque brut considéré sans les éventuels moyens de protection ou de contrôle mis en place par l'organisation.
- Le risque résiduel (ou risque net) est celui qui résulte du risque brut en tenant compte des protections et des contrôles mis en place.

Dans un premier temps, l'évaluation doit porter sur les risques inhérents. Dans un deuxième temps, il faudra estimer les risques résiduels après évaluation des mesures de contrôles mises en place afin de réduire leurs impacts. Pour évaluer les risques inhérents, deux techniques sont utilisées à savoir l'estimation quantitative et l'estimation qualitative (IFACI, 2006).

L'estimation quantitative des risques *:* c'est une estimation où la probabilité et l'importance des conséquences sont exprimées numériquement (mesures de probabilités et données de pertes financières). Elle suppose la disponibilité des données fiables permettant d'estimer la probabilité d'occurrence et la gravité des risques provenant de sources aussi bien internes qu'externes (LANDWELL, 2005). L'estimation de probabilité de survenance d'un

risque donné peut se faire par l'exploitation des taux de défaillance grâce à des modèles statistiques. Quant à la mesure de l'importance de ses conséquences, elle est obtenue en utilisant les pertes causées par ce risque.

L'estimation qualitative des risques : c'est une estimation où la probabilité et l'importance des conséquences sont exprimés en termes qualitatifs : élevé, moyen ou faible. Ainsi, des échelles d'appréciation contenant des cotations de 1 à 5 peuvent être utilisées. Cette méthode d'estimation est utilisée lorsque :

- Le risques sont difficiles à appréhender ou à quantifier ;
- Les données statistiques nécessaires à une estimation quantitative sont insuffisantes ;
- La collecte et l'analyse de ces données n'est pas rentable au regard du bénéfice attendu (LANDWELL et al, 2005).

Avant de présenter les échelles de cotation de la probabilité d'occurrence et de l'impact de risque, il convient de définir ces deux termes.

La probabilité de survenance de risque (fréquence d'occurrence) : elle représente le nombre de fois où le risque pourrait se produire sur une période donnée. Pour évaluer la probabilité de survenance d'un risque, nous proposons l'échelle de cotation suivante. Cette échelle est donnée à titre indicatif. Elle peut être adaptée aux spécificités de l'entreprise.

Tableau 3: Echelle d'évaluation de la probabilité d'occurrence du risque

Note	Qualificatif	Probabilité de survenance
1	Rare	Très faible.
2	Peu probable	Faible
3	Possible	Modérée
4	Probable	Elevée
5	Quasiment certain	Très élevée

–L'impact du risque (sévérité de ces conséquences sur l'entreprise en cas de manifestation) : il représente la quantification de la perte engendrée par la réalisation du

risque. Il s'agit de l'impact financier ou l'impact que peut avoir un incident sur la réputation de l'établissement et la conformité des opérations. Les risques peuvent être classés selon leur importance : « élevé », « moyen » ou « faible » (IFACI, 2004) ou d'une manière quantitative selon les pertes financières engendrées. Le tableau ci-dessus présente un exemple d'échelle d'évaluation de la gravité des risques.

Tableau 4:Echelle d'évaluation de l'impact des risques

Note/Score	Impact	Description
1	Insignifiant	Sans aucune conséquence remarquable sur la qualité des opérations.
2	Mineur	conséquences tolérables sur la qualité des opérations.
3	Modéré	Impact sur l'optimisation des opérations
4	Majeur	Impact très grave et doit impérativement être traité.
5	Catastrophique	Conséquences financières, atteinte grave à l'image de la banque

Le produit de la fréquence et de la gravité des risques désigne la criticité. C'est l'appréciation globale du risque. La représentation graphique de cette mesure est une matrice dont l'abscisse correspond à la gravité et l'ordonné à la fréquence.

$$\textbf{Criticité du Risque} = \textbf{Probabilité} * \textbf{Gravité}$$

2.2.3. Hiérarchisation des risques inhérents

Il s'agit d'un classement en fonction du criticité de chaque risque inhérent en tenant compte du seuil de tolérance aux risques de l'organisation ainsi que son risque intrinsèque (risque maximum possible) RENARD (2004). La hiérarchisation des risques inhérents devrait être affinée par l'appréciation des contrôles internes ayant déjà été mis en œuvre pour la réduction des effets de ces différents risques.

2.2.4. Identification et appréciation des contrôles internes existants

L'identification des contrôles internes existants est la mise en valeur de tous les contrôles ayant été mis en place pour pallier les conséquences négatives des risques avant l'élaboration de la cartographie des risques. Il s'agit donc de procéder à un listage des différentes procédures existantes de la manière détaillée et précise. Par la suite, il faudra vérifier si elles sont adaptées à la nature des risques et si elles peuvent atténuer leurs conséquences négatives. L'appréciation du dispositif de maitrise se fait pour chaque couple risque/ processus à l'aide de quelques critères. Selon IFACI (2006), les critères les plus utilisés sont :

- L'efficacité : l'aptitude de contrôle à atteindre les objectifs pour lesquels il est mis en place ;
- La pertinence : l'utilité du contrôle et rapport coût/utilité ;
- La fiabilité : la capacité du contrôle à fonctionner de façon continue ;
- La qualité de la conception et de la mise en œuvre ;
- L'efficience : il s'agit de rapprocher les trois critères à savoir coût, rendement et délai d'obtention des résultats.

Comme les risques inhérents, les contrôles internes sont évalués sur la base d'une échelle allant de 1(non adéquat ou inefficace) à 5 (adéquat ou efficace). Les outils généralement utilisés pour l'évaluation du contrôle interne sont les questionnaires de contrôle interne, la feuille de révélation des risques, la grille d'analyse des risques, etc.

L'évaluation des risques inhérents et des contrôles internes permettra d'évaluer et de hiérarchiser les risques résiduels sur lesquels se construisent toutes les stratégies de gestion des risques.

2.2.5. Evaluation des risques résiduels

Il s'agit d'évaluer les risques résiduels qui résultent des risques bruts en tenant compte des contrôles mis en place. Les risques nets sont donc largement fonction du dispositif de contrôle interne mis en place pour atténuer les événements à risque. Dés lors, l'analyse doit être complétée par l'identification des contrôles.

2.2.6. Hiérarchisation des risques résiduels et formation de la cartographie des risques

Les risques résiduels sont hiérarchisés en fonction de leurs scores. A ce niveau, il est essentiel de prendre en considération le seuil de tolérance aux risques de l'entreprise. Ensuite,

les risques seront représentés de manière à identifier les risques les plus significatifs et les moins significatifs (IFACI, 2006). A cet égard, la matrice des risques est une représentation graphique de la probabilité d'occurrence et de la gravité de l'impact des risques identifiés.

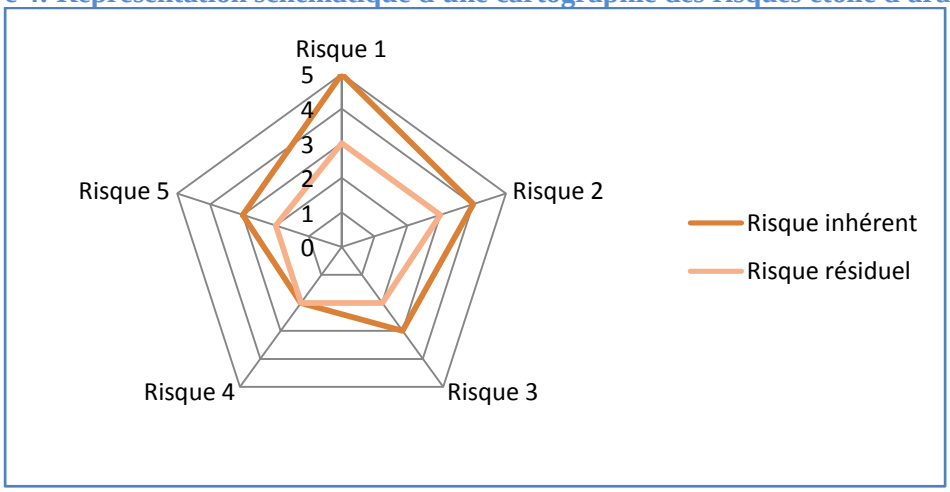
Figure 3: matrice des risques

probabilité					
	Fréquent 4	4	8	12	16
	Probable 3	3	6	9	12
	Rare 2	2	4	6	8
	Improbable 1	1	2	3	4
		Négligeable 1	**Moyenne 2**	**critique 3**	**catastrophique**
	gravité				

Source : Elaboré par nos soins.

Les risques inhérents et les risques résiduels peuvent être représentés dans un seul graphique afin de mettre en valeur le rôle des contrôles internes dans l'atténuation des risques. Cela est montré dans la figure ci-après.

Figure 4: Représentation schématique d'une cartographie des risques étoile d'araignée



Source : Elaboré par nos soins.

La cartographie des risques étant établie, les risques critiques de chaque processus sont mis en évidence. Ainsi, la direction peut s'orienter vers les plans d'action dans la phase après cartographie. Cette phase fera l'objet de la section suivante.

Section 3 : Après cartographie des risques opérationnels

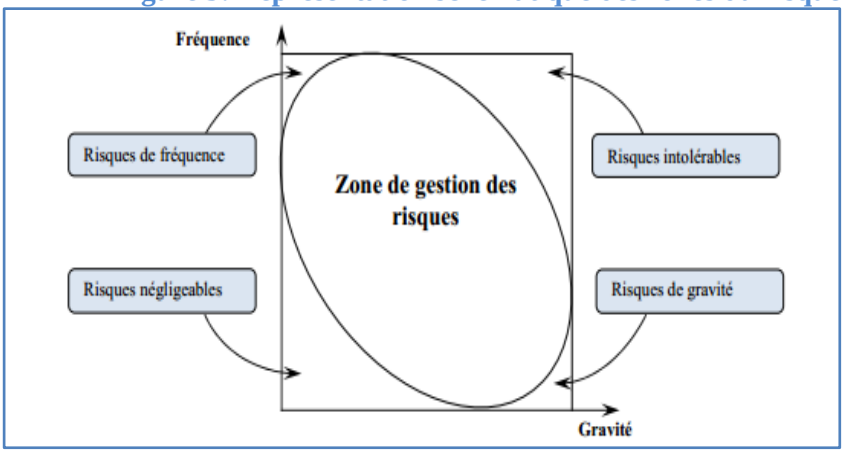
La cartographie n'est pas une fin en soi. Elle procure des outils dont la finalité est l'aide à la décision et surtout les actions d'amélioration.

3.1 Interprétation de la cartographie des risques

Il faut noter que nous pouvons distinguer cinq zones de risques sur le diagramme fréquences*gravité. Elles sont représentées dans la figure suivante. Ces cinq zones sont :

- la zone « des risques de fréquence », caractérisée par une fréquence assez élevée et une gravité relativement faible ;
- la zone « des risques de gravité », qui au contraire auront une gravité forte, mais une probabilité d'occurrence faible ;
- la zone « des risques négligeables », de fréquence et de gravité faibles ;
- la zone « des risques inacceptables », de gravité et fréquence élevées, et pour lesquels le seul traitement est l'évitement ou la suppression de l'activité à risque ;
- Enfin, la zone « des risques à fréquence et gravité moyennes », qui constitue le vaste champ d'application de la gestion des risques.

Figure 5: Représentation schématique des zones du risque



Source : B. Barthélémy, gestion des risques, édition d'organisation 2002

Ces zones de risques constituent, à degré divers, le champ d'application de la gestion des risques. A ce titre, nous pouvons distinguer deux natures de risque.

3.2 Elaboration d'un plan d'action

Le plan d'action a pour objectif de réduire au maximum les risques jugés majeurs pour la banque, c'est-à-dire d'obtenir un risque résiduel le plus faible possible. La constitution de ces plans comprend en général deux grandes étapes. La première consiste à déterminer la meilleure façon de traiter le risque en se basant sur la criticité du risque net. La seconde comprend la sélection et la planification d'un traitement adapté en fonction des ressources disponibles. Généralement, ces traitements sont au nombre de quatre.

3.2.1. Eviter le risque

Lorsqu'il s'agit d'une tâche ou une activité très risquée même après le traitement du risque, il est impératif de l'éliminer. Cette solution peut être envisagée quand le traitement du risque est très coûteux par rapport aux bénéfices rapportés par cette activité.

3.2.2. Transférer le risque

Il s'agit de diminuer la probabilité ou l'impact d'un risque en le transférant ou le partageant. D'une part, l'entreprise a la possibilité de transférer ses risques tels que le vol, l'incendie par le biais de l'assurance (achat de contrats d'assurance). D'autre part, elle peut sous-traiter les activités jugées très risquées outrés peu rentables à développer en interne en s'assurant de l'efficacité des contrôles chez les sous-traitants.

3.2.3. Accepter le risque

Il s'agit de ne prendre aucune mesure pour modifier la probabilité du risque ou son impact (IFACI, 2005). Cette action est valable pour les risques de niveau relativement faible ou jugés acceptables (niveau de risque est inférieur à l'appétence de l'entreprise) et qui offrent des opportunités considérables.

3.2.4. Réduire le risque

La réduction de risque consiste à prendre des mesures pour réduire sa fréquence (la prévention) ou son impact (la protection) ou les deux à la fois. Ces mesures peuvent être de différents types : suppression des causes, partage de responsabilités, limitation des conséquences, acceptation du risque tout en le surveillant, etc. Le choix des actions à engager est effectué en comparant les coûts de leur mise en œuvre avec les coûts des conséquences du risque, en tenant compte de leur probabilité d'apparition.

- **la protection** : les mesures de protection visent à limiter les conséquences d'un sinistre en limitant les pertes supportées. On distingue les instruments de protection avant le sinistre (mettre un système d'alarme pour le risque de vol), et les instruments de protection au moment de sinistre (mettre des extincteurs pour le risque d'incendie) ;
- **la prévention** : les mesures de prévention visent à réduire la probabilité d'occurrence des risques récurrents. Ces mesures agissent au moins sur l'un des événements de la chaine conduisant à l'événement dommageable. Par exemple, pour un risque de vol la mesure de prévention pourrait être la mise en place des contrôles d'accès.

3.3 Plan de continuité de l'activité

Pour des raisons qui peuvent échapper au contrôle de la banque, un incident peut l'empêcher d'exécuter entièrement ou partiellement ses obligations, en particulier quand ses infrastructures physiques, de télécommunications ou d'informatique ont été endommagées. Cette situation peut provoquer de lourdes pertes financières pour la banque. Cette éventualité nécessite que les banques mettent en place des programmes de reprise et de continuité d'exploitation, prenant en compte divers types de scénarios plausibles auxquels la banque peut être exposée.

A ce titre, la gestion de la continuité d'activité est un processus de management holistique qui identifie les menaces potentielles pour une organisation et les impacts sur les opérations liées à l'activité de l'organisation. Il fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs. L'intérêt du Plan de Continuité d'Activité est :

- D'assurer la pérennité des activités vitales de l'entreprise,
- D'assumer financièrement sa part de rétention,
- De protéger l'entreprise d'une perte d'activité,
- De renforcer son image face à ses clients, partenaires.

Sa mise en place passe généralement par quatre étapes :

- **l'étude des risques et besoins en matière de continuité** : à partir de la cartographie des risques et des données fournies par les responsables des activités en terme de délai

maximum d'interruption possible (DMIA) et de ressources nécessaires à la continuité de l'activité, le gestionnaire des risques va identifier et hiérarchiser les besoins en termes de continuité ;

- **Le dispositif de prévention et solutions envisageables en cas de sinistres** : les responsables des ressources vont proposer des solutions de continuité aux responsables d'activités, en tenant compte des DMIA de chaque activité ;
- **La mise en place du dispositif de continuité** : la figure ci-après illustre les étapes de mise en place du dispositif de continuité ;
- **Le maintien en condition opérationnelle** : c'est la partie la plus difficile. Les plans de secours doivent être testés périodiquement et après chaque modification majeure de l'environnement organisationnel. Cela est fait dans le but d'évaluer leur efficacité et de s'assurer qu'ils sont à jour et que les collaborateurs connaissent le dispositif et sauront réagir de manière adéquate en cas de sinistre réel.

Les banques devraient revoir périodiquement leurs programmes de reprise et de continuité d'exploitation pour s'assurer qu'ils restent adaptés au niveau de leurs activités et stratégies. En outre, ces programmes devraient être testés périodiquement pour vérifier que la banque serait en mesure de les mettre en œuvre même dans le cas improbable d'une grave perturbation de l'activité.

3.4 La cartographie des risques au service de l'audit interne

« L'Audit Interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. » IFACI (2000).

La cartographie des risques, une fois approuvée, doit servir au responsable de l'audit interne pour confectionner son plan d'audit qui établira une relation entre les risques significatifs qui pèsent sur l'entreprise et les processus à auditer. En outre, le rôle de l'auditeur est d'apporter un jugement sur le contrôle interne mis en place, et de proposer des solutions pour l'améliorer. De ce fait, la cartographie des risques constitue l'outil au

service de l'auditeur interne pour planifier ses travaux, car elle met l'accent sur les défaillances des fonctions de la banque

3.5 Le suivi des actions de traitement des risques

Cette activité régulière permet de suivre l'évolution de la probabilité d'apparition des risques (stable, à la hausse, à la baisse), de contrôler la pertinence des actions préventives engagées et éventuellement de corriger les dispositions prévues. Egalement, de nouveaux facteurs de risques peuvent apparaître ; il faut les ajouter à la liste initiale. Enfin, il s'agit de surveiller le déclenchement des événements redoutés et leurs conséquences réelles. Le changement par l'entreprise de certaines de ses activités peut aussi entrainer une actualisation de la cartographie.

3.6 Communication de la Cartographie des risques

La cartographie des risques constitue un moyen de communication sur ceux-ci. La communication doit être efficace aussi bien à l'intérieur de la banque qu'avec les partenaires externe tels que les actionnaires, les autorités publiques.

- **La communication de la cartographie des risques en interne :** elle peut être ascendante ou descendante. La communication ascendante est généralement réalisée par les lignes de reporting habituelle. Elle est destinée aux dirigeants. Cependant, la communication descendante est destinée aux opérationnels. Dans les deux cas, elle a permet de se rendre compte des risques susceptibles de survenir au sein de la banque ainsi que les défaillances de contrôles recensées et pour les quels il faut mettre en place des actions correctives.
- **La communication de la cartographie des risques en externe :** la cartographie des risques constitue un moyen de reporting externe concernant l'identification et l'évaluation des risques et des mesures de contrôle mis en œuvre auprès de l'autorité de contrôle et les actionnaires.

Conclusion

Dans ce chapitre, nous avons défini la notion de cartographie des risques, ses objectifs et motivations et les facteurs clé de sa réussite. Ensuite, nous avons établi la démarche de son élaboration.

Cette démarche commence par une phase préparatoire. Il s'agit de définir le périmètre de la cartographie et mettre en place les moyens humains et financiers nécessaires et de segmenter les processus en sous processus et tâches élémentaires. Ensuite, il s'agit d'identifier et évaluer les risques susceptibles de survenir et les contrôles associés à chaque tâche. La dernière étape consiste à hiérarchiser les risques nets et la représentation de la cartographie. L'analyse de résultat trouvé permet d'élaborer un plan d'actions à entreprendre pour faire face aux défaillances de contrôle existantes. Egalement, ce résultat sert de base pour la planification d'un plan d'audit fondé sur les risques. En outre, la cartographie des risques doit être communiquée dans toute la banque pour que le personnel et les dirigeants se rendent compte des risques et des défaillances de contrôle.

Il est impératif qu'elle soit mise à jour pour suivre l'évolution de l'activité de la banque et de son environnement.

Le chapitre suivant a pour objet l'élaboration d'une cartographie des risques opérationnels liés au processus du crédit documentaire au sein de l'ATB.

CHAPITRE 3 :

CARTOGRAPHIE DES RISQUES OPÉRATIONNELS INHÉRENTS AU PROCESSUS DU CRÉDIT DOCUMENTAIRE AU SEIN DE L'ATB

Introduction

Le dernier chapitre est consacré au cas pratique. En effet, après avoir exposé de manière théorique la démarche d'élaboration d'une cartographie des risques, nous essayons d'élaborer une cartographie des risques opérationnels liés au processus de crédit documentaire au sein de l'ATB.

Pour cela, nous avons passé un stage pratique à la direction de commerce extérieur de 45 jours. Nous avons commencé par la compréhension du processus ainsi que l'organisation de travail au niveau de cette direction. Ensuite, nous avons passé à l'identification des risques et des contrôles. En fin, et après la détermination des risques nets, nous avons proposé un plan d'action pour les couvrir.

Ce chapitre est scindé en trois sections :

Section 1 : Analyse descriptive
Section 2 : Méthodologie de travail
Section 3 : Résultat et plan d'action.

Section 1 : Analyse Descriptive

Dans cette section, nous allons présenter, de manière succincte, la banque ATB et exposer ses indicateurs d'activité. Le dernier paragraphe est consacré à la définition du crédit documentaire, ses intervenants, ses modes de réalisation.

1.1 Présentation de l'ATB

L'Arab Tunisian Bank a été créée en 1982. Son capital s'élève à 100 millions dinars. Au 31 décembre 2014, le capital est détenu à hauteur de 64,24% par l'Arab Bank et 24,37% par divers groupes privés. L'agence de notation Fitch Rating a confirmé le premier avril 2015, les notes émetteur à long terme de L'ATB en monnaie étrangère et locale, respectivement à 'BB' et 'BB+', relevant la perspective pour la première note de négative à stable et maintenant la dernière sous surveillance négative.

1.2 Les indicateurs d'activité

Dans la banque, le risque opérationnel est fonction croissante des indicateurs d'activités tels que le volume des crédits, des dépôts, le total actif, le produit net bancaire, le nombre d'agences et les ressources humaines. Les graphiques suivants montrent l'évolution de ces indicateurs depuis l'année 2009 jusqu'à l'année 2014.

Tableau 5- Les indicateurs d'activité

Années	2010	2011	2012	2013	2014
Dépôts de la clientèle	2893	3230	3544	3713	3555
Créances nettes sur la clientèle	2252	2233	2482	2690	3117
Total actif	4016	4313	4603	4865	5036
Produit net bancaire	144	146	158	167	174
Nombre d'agence	110	115	119	120	126

Source : Rapports d'activité ATB.

- **Les dépôts**

Les dépôts de la clientèle se sont établis au 31/12/2014 à 3555 millions de TND contre 2893 millions de TND à fin décembre 2010, soit un taux de croissance annuel moyen de 5.3%.

- **Les crédits**

Les crédits nets à la clientèle se sont établis à fin décembre 2014 à 3117 millions de TND contre 2252 millions de TND au terme de l'exercice 2010, soit taux de croissance annuel moyen de 8.5%.

- **Le total actif**

Au terme de l'année 2014, le total actif s'est établi à 5036 millions de TND contre 4016 millions de TND en 2010, soit un taux de croissance annuel moyen de 5.8%.

- **Le produit net bancaire**

Le produit net bancaire a atteint à fin décembre 2014 un montant de 174 millions de TND contre 144 millions de TND au terme de l'année 2010. Il a réalisé un taux de croissance annuel moyen égal à 4.8%.

- **Le nombre d'agences**

Le nombre d'agences ouverts en 2010 est égal à 110 agences. Ce chiffre a atteint 126 agences en 2014, soit un taux de croissance annuel moyen de 3.5%.

- **Ressources humaines**

L'effectif global de la banque a dépassé les 1000 employés au terme de l'année 2011. Au 31/12/2014, il totalise 1234 employés.

1.2.1. Le nombre de crédits documentaires traités à l'ATB

Le tableau suivant indique le nombre de crédits documentaires traités à la direction de commerce extérieur à l'ATB entre 2012 et 2014. Malgré sa baisse, le volume des dossiers traité reste élevé (en moyenne 11 dossiers par jours). Traiter un volume important par jour est susceptible d'augmenter la fréquence des risques opérationnels et leur sévérité. Cela peut avoir des conséquences négatives sur le résultat de la banque.

Tableau 6: Le nombre de crédits documentaires traités

Années	2012	2013	2014
Nombre de crédits documentaires traités	2839	2736	2587

Source : données de la banque

De ce fait, élaborer une cartographie des risques opérationnels liés au processus du crédit documentaire revêt d'un intérêt particulier. Il s'agit d'un processus métier qui participe dans la formation du produit net bancaire. Cependant, c'est processus qui demande de la vigilance et la stabilité des conditions de travail.

1.3 Le crédit documentaire

1.3.1. La définition du crédit documentaire

Le crédit documentaire est l'opération par laquelle une banque (banque émettrice) s'engage, à la demande et pour le compte de son client importateur (donneur d'ordre), à régler à un tiers exportateur (bénéficiaire), dans un délai déterminé, un certain montant contre remise des documents strictement conformes et cohérents entre eux, justifiant de la valeur et de l'expédition des marchandise ou des prestations de services.

Pendant la négociation du contrat commercial, les parties contractantes doivent impérativement se mettre d'accord sur la nature du crédit documentaire, en fonction des risques que l'on désire couvrir. On distingue le crédit documentaire irrévocable et le crédit documentaire irrévocable et confirmé.

- Le crédit documentaire irrévocable : Depuis les nouvelles « RUU 600 », tous les crédits sont automatiquement irrévocables, c'est à dire qu'un crédit documentaire ne peut être annulé qu'avec l'accord des deux parties.
- Le crédit documentaire irrévocable et confirmé : lorsque la banque notificatrice s'engage à régler le bénéficiaire si ce dernier présente des documents conformes aux termes du crédit documentaire.

Le crédit documentaire est régi par les Règles et Usances Uniformes (RUU) de la Chambre de Commerce Internationale. Ces règles sont reconnues et adoptées au niveau international à l'égard de tous les intervenants qui participent à des opérations effectuées au moyen d'une lettre de crédit. Elles ont été publiées pour la première fois en 1993. Révisées régulièrement pour suivre et accompagner les évolutions de la pratique, leur dernière version les « RUU 600 » remplaçant la précédente version les « RUU 500 » datant de 1993 est entrée en vigueur le premier juillet 2007.

1.3.2. Les intervenants

Le crédit documentaire met en relation les intervenants suivants :

- Le donneur d'ordre : c'est la partie qui donne les instructions d'ouverture du crédit documentaire ;
- La banque émettrice : c'est la banque de l'acheteur (située en général dans le pays de celui-ci). Elle procède à l'ouverture du crédit documentaire ;
- La banque notificatrice : c'est la banque correspondante de la banque émettrice (située en général dans le pays du vendeur). Elle avise le bénéficiaire de l'opération de crédit documentaire, sans prendre d'engagement de paiement vis-à-vis de celui-ci ;
- La banque confirmatrice : c'est, en général, la banque notificatrice. Le cas échéant, elle accepte de prendre un engagement de paiement vis-à-vis du bénéficiaire ;
- Le bénéficiaire : c'est la partie en faveur de laquelle un crédit documentaire est émis.

1.3.3. Les modes de réalisation du crédit documentaire

Un crédit documentaire doit indiquer s'il est réalisable par paiement à vue, paiement différé, acceptation ou négociation.

- Crédit documentaire réalisable par paiement à vue : le bénéficiaire obtient le paiement sur remise et après contrôle des documents stipulés dans la lettre d'ouverture. La banque dispose d'un délai maximum de cinq jours ouvrables suivant le jour de présentation des documents pour les opérations de vérification et pour honorer, négocier ou refuser les documents.
- Crédit documentaire réalisable par acceptation: l'exportateur tire une traite à terme, selon les dispositions prescrites, sur la banque émettrice ou sur celle qui confirme, ou

encore sur une autre banque désignée. A la présentation des documents, il n'y a pas de paiement, mais acceptation d'effet de change.

- Crédit documentaire réalisable par paiement différé : sur présentation des documents conformes, la banque autorisée (banque émettrice, confirmatrice ou toute autre banque désignée) s'engage par écrit à effectuer le paiement à l'échéance. Le terme de l'échéance doit être clairement stipulé dans le crédit documentaire. Les paiements différés sont possibles, tant pour les crédits confirmés que non confirmés.
- Crédit documentaire réalisable par négociation : un crédit est réalisable par négociation à vue ou à terme. La négociation s'effectue par la banque désignée. Le crédit est utilisé par le bénéficiaire sur présentation d'une traite (tirée le plus souvent sur la banque émettrice), accompagnée des documents spécifiés, ou contre remise de document uniquement. Une traite n'est donc pas indispensable (RUU Art.2). le bénéficiaire obtient les fonds après déduction d'un escompte avant ou au plus tard le jour ouvrable où le remboursement est dû à la banque désignée

1.4. Description du processus du crédit documentaire

D'abord nous allons décrire les étapes du processus du crédit documentaire import. Puis, nous passons au deuxième processus, le crédit documentaire export.

1.4.1. Le processus du crédit documentaire import

Pour réussir à identifier les risques opérationnels majeurs inhérents au processus du crédit documentaire import, il est primordial de découper ce processus en des sous processus et en tâches élémentaires.

- Le sous processus « Instruction d'ouverture du crédit documentaire » : conformément aux termes du contrat commercial prévoyant le règlement par voie de crédit documentaire, l'initiation de la transaction appartient à l'acheteur (le donneur d'ordre). Il demande à sa banque d'émettre un crédit documentaire en faveur du vendeur étranger (le bénéficiaire). Pour cela, le donneur d'ordre doit se déplacer à l'agence bancaire pour :
  - Remplir un formulaire pré-imprimé où il détaille les caractéristiques et les conditions de réalisation du crédit documentaire ainsi que les documents requis pour l'importation de la marchandise ;

- Fournir un ensemble de documents justificatifs de l'importation : le certificat d'importation ou autorisation d'importation, la facture proforma.

- Le sous processus vérification de la solvabilité du client, de la conformité de la signature et des termes de la demande : avant de transmettre la demande à la division de domiciliation, on doit s'assurer de la solvabilité du donneur d'ordre, la cohérence et la complétude des termes de la lettre de crédit

- Le sous processus domiciliation du titre de commerce extérieur

Le titre de commerce extérieur est domicilié s'il respecte la réglementation des changes. Ses données sont saisies et transmises à la Banque Centrale via le système Tunisie Trade Net (TTN).

- Le sous processus ouverture du crédit documentaire : afin de procéder à l'ouverture du crédit documentaire, la banque a besoin du formulaire qui lui a été soumis. Ce dernier constituera l'outil principal de travail pour la rédaction de l'ouverture du crédit à transmettre au bénéficiaire par l'intermédiaire d'une banque de son pays. Cette transmission se fera en général par un message SWIFT conforme aux instructions contenues dans la demande d'ouverture.

- Le sous processus suivi du crédit documentaire : la modification d'un crédit documentaire consiste à changer un ou plusieurs de ces termes. Il existe deux types de modifications :
  - Les modifications touchant l'engagement des banques (émettrice et confirmante) : annulation ou réduction du montant ou de la devise, prorogation de la durée de l'engagement par exemple ; Dans pareil cas, les frais liés à ces modifications sont indexés sur ces nouvelles données.
  - Les modifications ne touchant pas l'engagement des banques : annulation ou addition d'un document, annulation de spécifications de certains documents, modification des risques couverts par le document d'assurance etc. ; dans ce cas, les charges sont moindres et sont fixées selon le barème propre à la banque.

Le bénéficiaire et le donneur d'ordre se mettent d'accord sur les amendements à apporter au crédit documentaire. Le donneur d'ordre donne instruction à la banque d'effectuer les modifications nécessaires : Si elle en a convenance, elle procède à la transmission du message testé Swift MT 707 « modification d'un crédit documentaire » à son correspondant ; dès lors elle est liée aux amendements qu'elle vient de transmettre.

- Le sous processus vérification des documents **:** dès réception des documents de la part de la banque remettante (la banque notificatrice/confirmatrice), la banque émettrice procède à leur examen. Elle dispose à cet effet d'un délai de cinq jours ouvrés pour fixer leur sort. A l'issue de cet examen, ils peuvent s'avérer conformes ou irréguliers :
    - Si les documents sont conformes : la banque émettrice est tenue de lever les documents et de rembourser la banque confirmante, à vue ou à terme selon les modalités de réalisation du crédit documentaire.
    - Si les documents comportent des anomalies**,** deux alternatives sont possibles:
        - Si les réserves constatées lui paraissent acceptables, elle peut demander au donneur d'ordre de l'autoriser à lever les documents et à honorer ses engagements vis-à-vis de la banque remettante.

        - Si les réserves sont inacceptables, elle refuse de lever les documents et le notifie à la banque remettante, sans délai, par message testé Swift, tout en indiquant les raisons du refus. Toutefois, elle doit préciser si elle tient les documents à la disposition de la banque correspondante ou s'ils lui seront réexpédiés.

Dans tous les cas, il est possible que l'importateur donne l'ordre, de façon expresse, à la banque émettrice de lever les documents en dépit des irrégularités qu'ils contiennent. Celle-ci, agissant dans l'intérêt de son client, autorisera alors son correspondant à réaliser le crédit ou le fera elle-même si le crédit est valable à ses guichets. Le compte du donneur d'ordre est débité de la commission de réalisation pour l'examen des documents, plus la commission de suivi en cas de paiement différé et des frais éventuels de Swift.

- Le sous processus règlement de crédit documentaire : après avoir examiné et jugé les documents conformes aux stipulations du crédit documentaire, la banque émettrice est dans l'obligation de rembourser la banque confirmante selon les instructions de remboursement indiquées dans la lettre d'ouverture de l'accréditif. L'opération de remboursement fait intervenir trois banques : la banque émettrice, la banque de remboursement, la banque réclamante. Ces trois parties interagissent selon le processus suivant :

- Lors de l'émission du crédit documentaire, la banque émettrice indique sur la lettre d'ouverture (à la banque réclamante) que le remboursement se fera auprès de la banque de remboursement (nommément désignée), pourvu que les termes et conditions du crédit soient respectés.
- Une fois la banque confirmante ayant réalisé le crédit en conformité avec les stipulations y afférentes, elle demande à la banque émettrice l'autorisation de débiter son compte sous bonne date valeur, chez la banque de remboursement, tout en prenant soin d'adresser à cette dernière une demande de remboursement par message Swift testé.
- Si la banque émettrice consent à effectuer le paiement, elle enverra un message Swift à la banque de remboursement l'autorisant à débiter son compte au profit de la banque réclamante tout en indiquant la date de valeur ; si non, elle mettra en instance le remboursement pour des raisons de non respect des instructions de la lettre d'ouverture par la banque remettante.
- Dès réception de l'autorisation de payer, la banque de remboursement vérifiera la concordance des données y figurant avec la demande qu'elle a reçue de la banque réclamante. Si les deux messages concordent, elle débitera le compte de la banque émettrice et créditera celui de la banque réclamante. Si les messages ne concordent pas ou si le compte de la banque émettrice ne présente pas une provision suffisante pour honorer le paiement, elle avisera les banques concernées par message Swift en précisant les motifs de l'inexécution du remboursement.

Le compte de donneur d'ordre est débité du montant du crédit documentaire, ainsi que la commission de règlement.

1.4.2. Le processus du crédit documentaire export

- Le sous processus réception du message SWIFT (MT700) : dés la réception du message SWIFT (MT700), la banque examine les termes du crédit documentaire. Elle notifie l'ouverture du crédit au bénéficiaire. Et, elle prend position en ce qui concerne son degré d'engagement (notificatrice ou confirmante). Elle envoie par message SWIFT sa décision à la banque remettante.

- Le sous processus suivi de crédit documentaire : la banque reçoit les nouvelles instructions et en informe le bénéficiaire si elle estime que les modifications apportées ne constituent pas un risque pour elle du fait de son engagement antérieur. Le bénéficiaire reçoit les modifications voulues et exécute ses obligations contractuelles.
- Le sous processus vérification et transmission des documents : la banque reçoit les documents requis. Avant de les transmettre à la banque émettrice, elle est demandée de les examiner pour s'assurer qu'ils sont conformes aux termes du crédit, s'il s'agit d'un Crédit documentaire irrévocable et conformé.
- Le sous processus règlement du crédit documentaire : ayant réalisé le crédit documentaire en conformité avec les stipulations y afférents, la banque demande à la banque émettrice l'autorisation de débiter son compte sous bonne date valeur, chez la banque de remboursement, tout en prenant soin d'adresser à cette dernière une demande de remboursement par message SWIFT testé. Si la banque de remboursement débitera le compte de la banque émettrice et créditera celui de la banque réclamante, cette dernière crédite le compte de bénéficiaire par la contre valeur en TND du montant de la lettre de. Dans le cas d'un Crédit documentaire irrévocable et confirmé et si la présentation des documents est conforme, la banque confirmante s'engage de payer le bénéficiaire à la date convenue. Elle est tenue de créditer le compte du bénéficiaire à la date de règlement par la contre valeur en TND du montant de la lettre de crédit. Ensuite, elle réclame le remboursement chez la banque émettrice. Le paiement se fait en déduisant les frais applicables.

Après la description des deux processus, nous allons présenter le cadre méthodologique de l'étude.

Section 2 : Méthodologie de travail

La définition du cadre méthodologique est fondamentale pour fixer de façon claire et objective tous les éléments qui serviront aux travaux d'analyse ultérieurs. Le cadre méthodologique devra notamment définir les outils de collecte et d'analyse de données, la démarche de la cartographie des risques opérationnels liés aux processus étudiés, la méthode d'évaluation et les échelles de valorisation des risques et des contrôles.

2.1 Les outils de collecte et d'analyse de données

Afin d'identifier les risques opérationnels liés au processus du crédit documentaire, nous avons retenu l'approche combinée. Ainsi, les risques sont déterminés parallèlement par la hiérarchie et les opérationnels. En outre, les outils utilisés peuvent être regroupés en deux catégories à savoir ceux qui permettent de collecter des données et ceux qui permettent d'analyser ces données collectées.

2.1.1. Les outils de collecte de données

Les outils de collecte de données utilisés sont l'analyse documentaire, l'observation et les entretiens.

- **Les entretiens** : nous avons procéder à des entretiens avec les collaborateurs intervenant dans la réalisation du processus du crédit documentaire (import et export), ainsi qu'avec les collaborateurs à la direction de conformité et la division des risques opérationnels pendant la période de stage. Cela nous a permis de comprendre les différentes tâches qui entrent dans le cadre de ce processus ainsi que les événements sources de risques opérationnels et le dispositif de contrôle interne mis en place.
- **L'observation : c**et outil consiste à suivre le traitement d'une demande de crédit documentaire dés l'ouverture jusqu'à le règlement. L'observation permet de voir concrètement le déroulement du processus du crédit documentaire. Elle permet également de vérifier que les contrôles prévus à chaque étape du processus sont effectivement réalisés.

- **L'analyse documentaire :** les documents consultés sont essentiellement :
  - le manuel de procédure de la banque décrivant le processus de crédit documentaire ;
  - Des circulaires internes à la direction de conformité ;
  - les Règles et Usances Uniformes relatives au crédit documentaire, établies par la Chambre de Commerce Internationale.
- **Le tableau d'identification des risques :** ce tableau nous a servi au recensement des risques pour l'élaboration de la cartographie. Il nous a permis d'identifier à chaque tâche, les risques susceptibles de se manifester et les mesures de contrôles susceptibles de les atténuer.

2.1.2 Les outils d'analyse de données

- **Le test de conformité :** pour s'assurer de l'application réelle de la procédure et les dispositifs de contrôles internes, nous avons réalisé le test de conformité. Pour cela, nous avons choisi au hasard dix dossiers. Ensuite, nous avons observé les documents et les justificatifs de chaque dossier. Nous avons constaté que le traitement de tous les dossiers choisis est conforme aux exigences de la procédure.

2.2 Le modèle d'analyse

La démarche suivie pour la cartographie des risques opérationnels inhérents au processus du crédit documentaire commence par la prise de connaissance de la direction de commerce extérieur au sein de l'ATB et en particulier les divisions de crédit documentaire import et export. La deuxième étape consiste à identifier et évaluer les risques bruts. L'étape suivante concerne l'identification et l'évaluation des mesures de contrôle interne. La dernière étape comprend la formation de la cartographie des risques.

2.2.1. Phase de préparation

- Organisation des divisions de crédit documentaire import et export

Les divisions de crédit documentaire import et export sont rattachées à la direction de commerce extérieur. La cartographie des risques opérationnels inhérents au processus du crédit documentaire nécessite la connaissance de l'organisation et le fonctionnement des ces

deux divisions (voir annexe n°1). Pour cela, nous avons effectué des entretiens avec les collaborateurs intervenant dans les processus étudiés afin de mieux comprendre l'organisation de travail et la gestion d'un dossier de crédit documentaire en segmentant ces processus en sous processus et tâches élémentaires. En outre, nous avons préparé la typologie des risques à utiliser dans cette étude en s'appuyant sur celle du Comité de BâleII (voir annexes 2).

2.2.2. La phase de conception

Elle comprend les étapes suivantes :

- **Identification des risques :** cette étape consiste à identifier les principales zones de vulnérabilité des processus. A ce niveau, notre démarche a consisté à mener une réflexion sur les risques opérationnels pouvant naître au niveau des processus étudiés, complétée par les réponses des collaborateurs (opérateurs et responsables) à l'issue des entretiens.
- **Evaluation des risques :** dans cette étape nous avons déterminé la probabilité d'occurrence des risques et la gravité de leurs conséquences grâce aux différents entretiens réalisés avec les collaborateurs concernés. Les évaluations sont faites sur un fichier Excel (voir annexe n°3). Le tableau suivant fournit les cotations des fréquences possibles à l'aide d'une échelle à 6 niveaux.

Tableau 7: Echelle d'évaluation de la fréquence des risques

Cotation chiffrée	Fréquence	Libellé
1	Très rare	Moins d'une fois par an
2	Rare	Quelques fois par an
3	Occasionnel	Moins d'une fois par mois
4	Probable	Quelques fois par trois mois
5	Fréquent	Quelques fois par mois
6	Très fréquent	Plusieurs fois par semaine

Le Tableau suivant fournit les cotations des gravités possibles à l'aide d'une échelle à 6 niveaux.

Tableau 8: Echelle d'évaluation de la gravité des risques

Cotation chiffrée	Gravité	Libellé
1	Trais faible	Perte inférieure à 5000 TND
2	Faible	Perte supérieure à 5000 TND et inférieure à 20000 TND
3	Moyen	Perte supérieure à 20000 TND et inférieure à 100000 TND
4	Important	Perte supérieure à 100000 TND et inférieure à 500000 TND
5	Majeur	Perte supérieure à 500000 TND et inférieure à1000000 TND
6	Catastrophique	Perte supérieure à 1000000 TND

- **Identification et l'évaluation des contrôles internes**

L'évaluation du dispositif de maîtrise est la dernière étape avant d'obtenir la cotation du risque résiduel. Le tableau suivant fournit les cotations de la conception des mesures de contrôle grâce à une échelle de 5 niveaux.

Tableau 9: Evaluation de la conception des contrôles

Cotation chiffrée	Caractéristiques
1	Le contrôle est limité (au niveau de son étendue) ou n'est pas correctement conçu.
2	Quand ce contrôle est correctement appliqué, il offre une protection très limitée.
3	La conception du contrôle permet d'atténuer la majorité des aspects liés au risque.
4	Toutefois quelques risques mineurs demeurent non couverts par la conception du contrôle.
5	La conception du contrôle a été effectuée de manière à atténuer substantiellement ou complètement le risque.

Ce tableau fournit les cotations de l'application des mesures de contrôle grâce à une échelle de 6 niveaux.

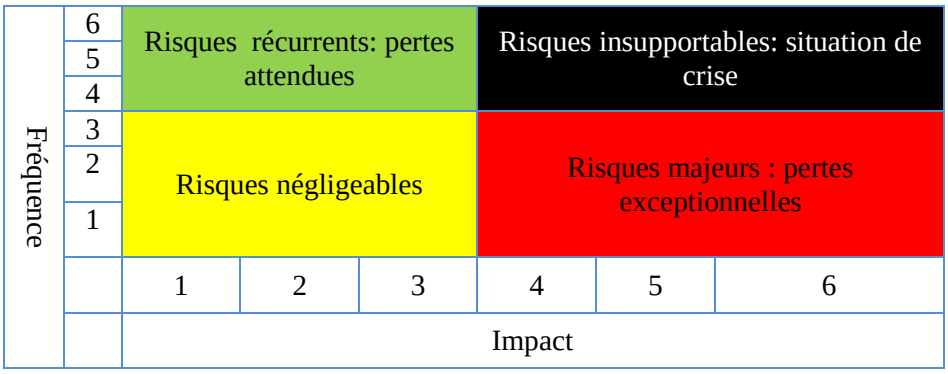
Tableau 10: Evaluation de l'application des contrôles

Cotation chiffrée	Caractéristiques
1	Le contrôle n'est pas appliqué
2	Le contrôle n'est pas appliqué correctement.
3	Le contrôle est normalement opérationnel.
4	Dans certaines situations le contrôle n'est pas appliqué d'une manière permanente ou il n'est pas appliqué adéquatement.
5	Le contrôle est appliqué conformément à sa conception.
6	Le contrôle est opérationnel d'une manière quasi-permanente.

- **Hiérarchisation et formation de cartographie**

Hiérarchiser ou classer les risques permet de déterminer quels sont les risques graves qu'il faut maitriser en premier lieu. La priorité est établie en tenant compte des criticités des risques nets selon la matrice suivante.

Figure 6: Matrice des risques nets



L'étape qui suit la définition de la méthodologie est l'identification des risques et des contrôles existants ainsi que les mesurer afin de repérer les risques nécessitant une action prioritaire.

Section 3 : Résultats et plan d'action

Cette section met l'accent sur l'identification et l'évaluation des risques opérationnels liés au processus du crédit documentaire conformément à la méthodologie déjà définie. En suite, il s'agit de déterminer les risques nets, représenter les cartographies des risques et définir un plan d'actions pour atténuer les risques non maitrisés.

3.1 Identification des risques opérationnels inhérents au processus : crédit documentaire import

Les risques opérationnels et les mesures de contrôles sont identifiés dans les tableaux suivants. Chaque tableau est consacré à un sous processus. L'annexe n° 6 présente une identification des risques opérationnels par métier.

Tableau 11: le sous processus « Instruction de la demande »

Spécification du risque	Les mesures de contrôles
La falsification des documents justificatifs	La compétence du personnel à détecter et reporter les opérations frauduleuses, les mesures de contrôles appliquées par direction de conformité.
La falsification des signatures	La compétence du personnel à détecter et reporter les opérations frauduleuses, le scannage des Spécimens de signature.
les documents juridiques absents ou incomplets : le dossier présenté par le client est incomplet	L'opérateur est tenu de vérifier la complétude des documents, le contrôle du supérieur hiérarchique.
Ignorance de la procédure : les opérateurs à l'agence ignorent les tâches à effectuer à la réception de la demande du client	La formation continue du personnel portant sur tous les métiers de la banque
Transaction de type non autorisé : le personnel à l'agence risque d'être impliqué dans des opérations illégales (falsification, faraude)	La vérification du supérieur hiérarchique, le contrôle des opérations, audit interne et inspection.

Spécification du risque	Les mesures de contrôles
Le blanchiment d'argent : La banque n'applique pas ses obligations en matière de lutte contre le blanchiment d'argent	La compétence du personnel de détecter et reporter les opérations frauduleuses, les mesures de contrôles appliquées par direction de conformité.
Absence de provision : le personnel accepte la demande sans blocage de fonds nécessaires	le contrôle du supérieur hiérarchique.
Retard d'exécution : l'envoie de la demande à la direction de contrôle réglementaire et suivi se fait en retard	un coursier chargé de la transmission des dossiers à la direction de contrôle réglementaire et financier.
Perte de documents : la perte du dossier avant de sa transmission à la direction de contrôle réglementaire et suivi	Une copie du dossier est gardée à l'agence
Dommages dus au piratage informatique.	Le dispositif de sécurité informatique
Les pertes provenant de catastrophes naturelles (inondation)	Les polices d'assurance : mesure de transfert de risque
Les pertes dues à des causes externes (vandalisme, terrorisme).	Les polices d'assurance : mesure de transfert de risque, le dispositif de sécurité des agences et des sièges centraux : le système de surveillance (les gardiens, les caméras de surveillance, système d'alarme)

Tableau 12: le sous processus « Domiciliation du titre de commerce extérieur »

Spécification du risque	Les mesures de contrôle
Les pertes provenant de catastrophes naturelles.	Les polices d'assurance : mesure de transfert de risque
Les pertes dues à des causes externes (vandalisme, terrorisme).	Les polices d'assurance : mesure de transfert de risque, le dispositif de sécurité des agences et des sièges centraux : le système de surveillance (les gardiens, les caméras de surveillance, système d'alarme).
Les pertes dues au dysfonctionnement du matériel informatique : par exemple, la défaillance du service rendu par le scanner.	Garder du matériel informatique en stock pour l'utiliser en cas de besoin.
Les pertes provenant des interruptions ou perturbations du système informatique: le problème de discordance, par exemple la matricule fiscale d'une société ne correspond pas à son numéro de compte.	La vérification après la saisie.
Indisponibilité de l'électricité.	Le système de stockage d'énergie électrique
Erreurs dans la saisie, le suivi ou le chargement: le risque de saisir des données erronées pour la domiciliation du titre de commerce.	Garde fou du système informatique, Contrôle hiérarchique.
Retard d'exécution: à cause du volume de travail élevé ou des pannes du système informatique, le traitement des demandes de domiciliation est retardé.	Personnel compétent, respect de l'organisation du travail au sein de la direction.

Tableau 13: le sous processus « Ouverture de crédit documentaire »

Spécification du risque	Les mesures de contrôle
Saisir des données sans vérification : l'opérateur peut saisir des données incohérentes et/ou incorrectes.	les formulaires d'ouverture sont lus par le supérieur hiérarchique avant de saisir l'ouverture sur le système informatique.
Erreurs dans la saisie, le suivi ou le chargement : le risque de saisir des données erronées.	La vérification du supérieur hiérarchique avant la validation.
Les pertes dues au dysfonctionnement du matériel informatique.	Garder du matériel informatique en stock pour l'utiliser en cas de besoin
Les pertes dues aux interruptions ou perturbations du système informatique.	Le système de sauvegarde des données.
Indisponibilité de l'électricité.	Le système de stockage d'énergie électrique
Non-respect des règles d'embargo ou de Black listes.	Les mesures de contrôles de la direction de conformité.
Validation sans vérification : le supérieur valide la transaction sans vérifier le message SWIFT ou les autres données saisies par l'opérateur.	

Tableau 14: le sous processus "Suivi du crédit documentaire"

Spécification du risque	Les mesures de contrôle
Saisir des données sans vérification : saisir les données de la modification sans les vérifier	Les demandes de modification sont lues par le supérieur hiérarchique.
Retard d'exécution : retard dans le traitement de la modification au point de notifier le correspondant après la date limite de livraison.	L'organisation de travail : les demandes sont traitées le jour de leur réception.
Erreurs dans la saisie, le suivi ou le chargement : commettre une erreur dans la saisie des termes de modification ou des commissions.	La vérification du supérieur hiérarchique.
Les pertes dues au dysfonctionnement du matériel informatique.	Garder du matériel informatique en stock pour l'utiliser en cas de besoin
Les pertes dues aux interruptions ou perturbations du système informatique.	Le système de sauvegarde des données.
Indisponibilité de l'électricité.	Le système de stockage d'énergie électrique
Non-respect des règles d'embargo ou de Black listes.	Les mesures de contrôles appliquées direction de conformité.
Validation sans vérification : le supérieur valide la transaction sans vérifier le message SWIFT ou les autres données saisies par l'opérateur.	

Tableau 15: le sous processus "vérification des documents"

Spécification du risque	Les mesures de contrôle
Vol des documents	Le coffre fort
Destruction des documents à cause des incendies ou des inondations dues à des fuites internes.	Le coffre fort
Les pertes dues au dysfonctionnement du matériel informatique.	Garder du matériel informatique en stock pour l'utiliser en cas de besoin
Les pertes dues aux interruptions ou perturbations du système informatique : panne du réseau interne retardant la réalisation du crédit documentaire (le crédit sera réalisé après les délais convenus).	Le système de sauvegarde des données.
Indisponibilité de l'électricité.	
Erreurs dans la saisie, le suivi ou le chargement : commettre une erreur de saisie	La vérification du supérieur hiérarchique.
Accepter des documents non conformes	La double vérification : les documents sont vérifiés par deux personnes, la vérification de hiérarchique.
Retard d'exécution : retard dans le traitement de la modification / notifier le correspondant après la date limite de livraison	L'obligation de traiter la demande de modification le jour de sa réception
Validation sans vérification	

Tableau 16: le sous processus « le règlement du crédit documentaire »

Spécification du risque : niveau 3	Les mesures de contrôle
Retard d'exécution : effectuer le règlement après le délai convenu	L'utilisation de deux échéanciers (automatique et autre manuel).
Erreurs dans la saisie, le suivi ou le chargement : commettre une erreur dans la saisie des commissions ou des autres données (taux de change, les numéros de comptes, etc.)	La vérification du supérieur hiérarchique
Les pertes dues au dysfonctionnement du matériel informatique.	
Les pertes dues aux interruptions ou perturbations du système informatique : panne du réseau interne retardant le règlement du crédit documentaire (le règlement se fait après les délais convenus)	Le système de sauvegarde des données
Indisponibilité de l'électricité.	Le système de stockage d'énergie électrique
Détournement des fonds (au moment du règlement)	La vérification du supérieur hiérarchique, le contrôle des opérations, audit interne et inspection.
Validation sans vérification	

3.2 Identification des risques opérationnels inhérents au processus : crédit documentaire export

Les risques opérationnels inhérents au processus du crédit documentaire export ainsi que les mesures de contrôles susceptibles de les atténuer sont présentés dans les deux tableaux suivants.

Tableau 17: le sous processus « la saisie de l'ouverture »

Spécification du risque	Les mesures de contrôle
Retard d'exécution : retard dans la réception du message SWIFT provenant de la direction SWIFT,	L'obligation de transmettre les messages SWIFT le jour de leur réception
Saisir des données sans vérification	Le supérieur hiérarchique lit le message SWIFT avant de le transmettre à l'opérateur.
Erreur dans la saisie : le numéro de compte de bénéficiaire, le montant, etc.	La vérification du supérieur hiérarchique.
Le blanchiment d'argent : La banque n'applique pas ses obligations en matière de lutte contre le blanchiment d'argent	Les mesures de contrôles de la direction de conformité.
Non-respect des règles d'embargo ou de Black listes.	Les mesures de contrôles de la direction de conformité.
Validation sans vérification	

Tableau 18: « le sous processus vérification et règlement »

Spécification du risque	Les mesures de contrôle
Accepter des documents non conformes	Double vérification des documents, la vérification du supérieur hiérarchique
Destruction des documents à cause des incendies ou des inondations	Le coffre fort.
Vol des documents	Le coffre fort.
Les pertes dues au dysfonctionnement du matériel informatique.	Garder du matériel informatique en stock pour l'utiliser en cas de besoin
Les pertes dues aux interruptions ou perturbations du système informatique : panne du réseau interne retardant la saisie de l'ouverture de la LC, le règlement du crédit documentaire (après les délais convenus)	Le système de sauvegarde des données
Erreurs dans la saisie, le suivi ou le chargement : commettre une erreur dans la saisie des commissions ou des autres données (taux de change, les numéros de comptes, etc.)	La vérification du supérieur hiérarchique
Détournement des fonds	La vérification du supérieur hiérarchique, le contrôle des opérations, audit interne et inspection.
Validation sans vérification	

Le paragraphe suivant est destiné à la définition des mesures de contrôle identifiées.

3.3 Les mesures de contrôles

- **Le développement continu du système d'information :** l'ATB a un système d'information développé. C'est le système utilisé par l'Arab Bank (maison mère). Il est responsable, selon les collaborateurs à la direction du commerce extérieur, de la limitation des risques opérationnels menaçant la banque, en particulier ceux liés au processus du crédit documentaire. l'ATB n'a pas cessé de développer son système d'information en mettant l'accent sur la sécurité, la prémunition contre le piratage et la protection des données personnelles (Rapport annuel 2013).
- **L'organisation :** au sein des divisions de crédit documentaire, l'organisation est bien conçue. La procédure écrite et l'organigramme définissent la place et les tâches de chaque collaborateur, ses pouvoirs, ses responsabilités et les schémas de circulation. Cela favorise

la maitrise des processus et réduit le nombre des erreurs et assure la traçabilité des opérations.

- **La séparation des tâches**: l'organisation de travail au sein de la division de crédit documentaire import favorise la traçabilité des opérations.
- **Le contrôle permanent** : le supérieur hiérarchique assure le contrôle de la conformité et la validation des opérations réalisées. Cela contribue à la minimisation des erreurs.
- **Le contrôle périodique :** le contrôle inopiné et/ou planifié vise principalement à vérifier le respect des procédures. Les missions d'audit réalisées ont pu mettre en relief et apprécier les différents risques auxquels la banque est exposée est en particulier les risques opérationnels. En outre, la sécurité informatique, la continuité de l'activité, la gestion des accès, les mesures de secours et la protection des données personnelles ont été le focus des travaux de l'audit informatique. (le rapport d'activité 2014)
- **Le dispositif du contrôle de conformité** : dans le cadre du renforcement des règles de contrôle interne, la direction de conformité a mis en place une politique pour la lutte contre le risque de blanchiment d'argent et financement du terrorisme. Les opérations de commerce extérieur avec les pays sous embargo passent impérativement par la direction de conformité pour des vérifications préalables.
- **La qualité et la formation du personnel :** le personnel en place a la compétence et l'expérience nécessaires. Il passe des sessions de formation continuellement en interne et en externe. Ces sessions couvre les services bancaires étrangers, la réglementation des changes, la langue anglaise.
- **La centralisation du traitement des opérations du commerce extérieur** :la centralisation de ces opérations au niveau de l'Unité Centrale des Opérations est de nature à garantir la traçabilité des opérations, de réduire le nombre d'erreurs et les délais de réponse et de renforcer le contrôle ce qui aura un impact réel sur l'efficacité opérationnelle.
- **La sauvegarde des données** : l'ATB a mis en place un back up IT en Mirroring permettant la sauvegarde des données de la banque dans un endroit très fortement sécurisé. Cela préserve l'activité de la banque, notamment en cas de défaillance du système informatique. En outre, il sauvegarde son image de marque auprès de ses clients ou de ses partenaires. Il assure une productivité constante et évite la perte d'informations sensibles.

3.4 Les risques nets

L'évaluation des risques nets selon la méthodologie décrite dans la première section du présent chapitre a donné les deux matrices de risques suivantes. Le processus crédit documentaire import présente des risques nets acceptables, récurrents et un risque majeur. Cependant, le processus crédit documentaire export ne présente que des risques acceptables ou négligeables. Ces résultats reflète la qualité des contrôles mises en œuvre.

Figure 7: Cartographie des risques nets"processus crédit documentaire import"

<table>
<tr><td rowspan="8">fréquence</td><td>6</td><td colspan="3" rowspan="3">R613, R612, R623, R612, R512</td><td colspan="3" rowspan="3"></td></tr>
<tr><td>5</td></tr>
<tr><td>4</td></tr>
<tr><td>3</td><td colspan="3" rowspan="3">R411, R213, R214, R622, R112, R311, R121, R221, R511, R513, R611, R412, R615, R611, R512, R312, R616, R312, R122, R413, R614, R611, R512, R513, R612, R123</td><td colspan="3" rowspan="3">R412</td></tr>
<tr><td>2</td></tr>
<tr><td>1</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td colspan="7">Impact</td></tr>
</table>

Figure 8: Cartographie des risques nets "processus crédit documentaire export"

<table>
<tr><td rowspan="8">Fréquence</td><td>6</td><td colspan="3" rowspan="3"></td><td colspan="3" rowspan="3"></td></tr>
<tr><td>5</td></tr>
<tr><td>4</td></tr>
<tr><td>3</td><td colspan="3" rowspan="3">R612, R126, R615, R611, R311, R312, R511, R512, R513, R616, R612, R614, R122, R123</td><td colspan="3" rowspan="3">R412</td></tr>
<tr><td>2</td></tr>
<tr><td>1</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td colspan="7">Impact</td></tr>
</table>

Le tableau suivant présente les risques récurrents du processus du crédit documentaire import. Les autres tableaux d'évaluation des risques et des contrôles sont en Annexe n°5.

Tableau 19: les risques récurrents processus "crédit documentaire import"

Risques	F	I	C	c	Risques nets	
Les pertes dues à des causes externes : vandalisme, vol, incendies	4	6	24	4	15	Risque majeur
Les pertes dues à des interruptions ou des perturbations du système informatique : problème de discordance des données, sous processus de domiciliation	4	4	16	1	13	risque récurent
La perte des documents (agence-division de domiciliation)	3	5	15	1	13	risque récurent
Les pertes dues au retard d'exécution (sous processus vérification et envoie de la demande de domiciliation)	2	6	12	-	12	risque récurent
Les pertes dues à l'ignorance de la procédure (à l'agence)	4	3	12	2	8	risque récurent
Les pertes dues au retard d'exécution (sous processus de domiciliation du titre de commerce extérieur)	2	5	10	1	8	risque récurent

Le risque majeur :

- **Les pertes dues à des causes externes : vandalisme, vol, incendies :** la communication financière de l'ATB, en mars 2011, indique que les opérations de pillage et de vandalisme ont touché plusieurs agences de ladite banque. En effet, 14 agences ont été incendiées et 14 autres endommagées, soit des dégâts évalués à 6 millions de dinars, couverts à hauteur de 80%. Le coût total des dégâts est donc estimé à 2 millions de dinars. Le 12 janvier 2015, l'agence bancaire ATB à Hammam–Lif a été braquée par un homme armé d'un révolver. L'agresseur a eu 7 mille dinars en espèces[5].

Les risques récurrents

- **Les pertes dues au dysfonctionnement ou perturbation du système informatique :** le système d'information fait face à deux risques importants : le risque de dysfonctionnement de système informatique et le risque de perturbation de la base de données. En effet, à la division de domiciliation des titres de commerce extérieur, la fréquence de panne de système informatique est assez élevée. Cela retarde les opérations de domiciliation et diminue la satisfaction des clients cherchant le traitement rapide de

[5]Le site internet de l'Association professionnelle tunisienne des banques et des établissements financiers

leurs opérations. En outre, cette division est exposée au risque de perturbation de la base de données liée au logiciel utilisé. Lorsque le collaborateur saisit des données concernant le client (tel que la matricule fiscale) d'autres informations sont données directement par le système informatique (tel que le numéro de compte). Il arrive que ce dernier ne corresponde pas au client en question. Ainsi, si le collaborateur ne vérifie pas les informations saisies et les compare à celles inscrites sur la demande de domiciliation, les frais de domiciliation seront soustraits du compte d'un autre client. Ce dernier demande une ristourne quand il se rend compte du débit injustifié de son compte.

- **La perte des documents :** pendant le transfert des demandes de domiciliation de l'agence à l'Unité Centrale des Opérations, la banque fait face au risque de perte des demandes. La perte implique la non exécution de la domiciliation du titre de commerce extérieur.
- **Les pertes dues au retard d'exécution :** la transmission des demandes de domiciliation des titres de commerce extérieur, à la division de domiciliation, se fait par courrier. La banque est exposée au risque d'envoi tardif se manifestant par des retards dans la réception desdites demandes à la division de domiciliation.
- **Les pertes dues à l'ignorance de la procédure (à l'agence)** : à l'agence, généralement, il existe un collaborateur chargé du traitement des demandes d'ouverture des crédits documentaire. Lorsqu'il s'absente, la banque risque que le personnel présent ignore la procédure du traitement ou le produit lui-même (le crédit documentaire).
- **Les pertes dues au retard d'exécution (sous processus de domiciliation du titre de commerce extérieur)** : à la division de domiciliation, le collaborateur traite un volume élevé de demandes de domiciliation, cela implique plusieurs factures à scanner en cas de demande manuelle (pour envoi à la BCT). Cela risque de retarder certaines demandes de domiciliation, en particulier avec des pannes informatiques récurrentes.

Remarque :

Les risques de viol des règles d'embargo ou des black listes et le risque de blanchiment d'argent ne constituent pas un risque récurrent pour l'ATB. Il s'agit des risques négligeables car la conception du contrôle mis en place a été effectuée de manière à atténuer substantiellement le risque et le contrôle est opérationnel d'une manière permanente.

3.5 Plan d'actions

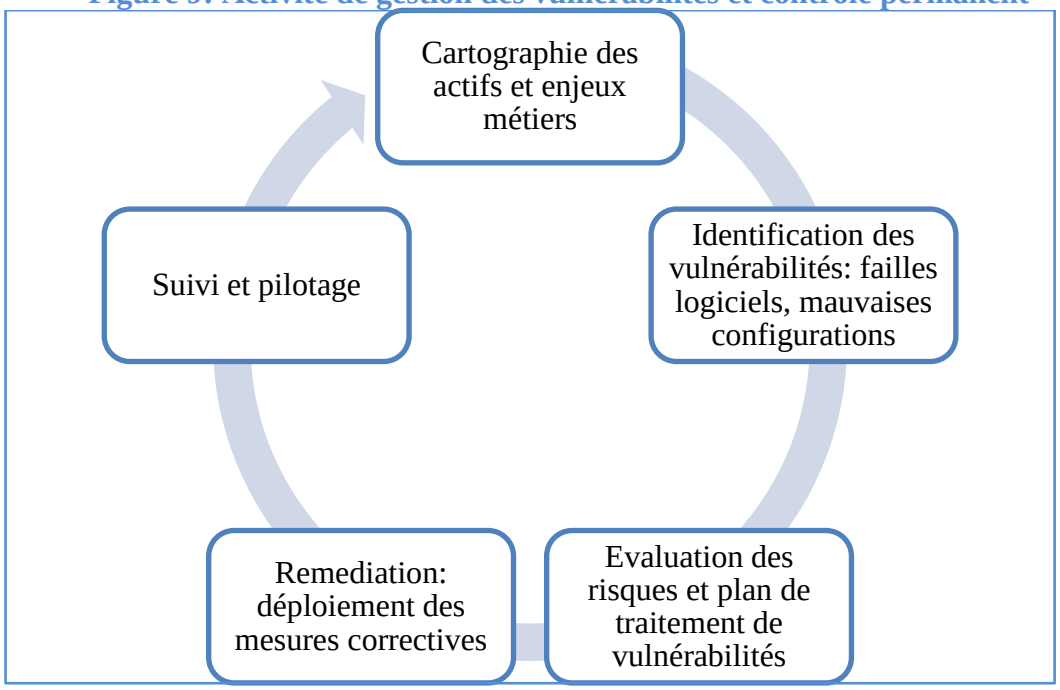
Le plan d'action a pour objectif de réduire au maximum les risques jugés majeurs pour la banque, c'est-à-dire d'obtenir un risque résiduel le plus faible possible. En règle générale, la réduction des risques se fait par la prévention ou par la protection. Le transfert des risques vers un assureur se fait après réduction de ceux-ci. Les risques récurrents demandent un suivi régulier. Nous allons proposer des actions préventives pour y remédier. Le risque majeur doit être atténué, grâce à des actions de protection et prévention, et transféré.

- **Le système informatisé d'échange de données** : l'échange de données informatisées peut être défini comme l'échange, d'ordinateur à ordinateur, de données concernant des transactions en utilisant des réseaux et des formats normalisés. Les informations issues du système informatique de l'émetteur transitent par l'intermédiaire de réseaux vers le système informatique du partenaire pour y être intégrées automatiquement.

  Les opérations de commerce extérieur sont traitées de manière centralisée à l'ATB. L'échange électronique des demandes et des documents justificatifs permet à la banque de bénéficier d'avantages significatifs tels que la réduction des coûts, l'amélioration de la vitesse de traitement, la diminution des erreurs, des pertes de dossiers et l'amélioration des relations avec ses partenaires commerciaux. En fait, les collaborateurs aux agences envoient les demandes de domiciliation instantanément à la division de domiciliation via le système d'échange de données informatisées où le collaborateur chargé de la domiciliation du titre de commerce extérieur n'est plus demandé de scanner les factures commerciales (reçues auparavant par courrier). Il vérifie la conformité de la demande à la réglementation des changes. Ensuite, il l'envoie à la Banque Centrale via le système Tunisie Trade Net.
- **Résolution du problème de perturbation de la base de données :** le collaborateur à la division de domiciliation des titres de commerce extérieur doit saisir le numéro de compte du client pour éviter l'erreur que ce dernier ne correspond pas au client en question.
- **La vérification du supérieur hiérarchique :** pour éviter le risque de confirmer une transaction (ouverture de lettre de crédit, modification, règlement) sans avoir vérifié les données saisies par l'opérateur, le supérieur hiérarchique doit être obligé de saisir des données clé telles que : le montant, la devise, le code SWIFT, etc.

- **Le processus de gestion des vulnérabilités du système informatique** : Les vulnérabilités d'une infrastructure informatique constituent un risque opérationnel majeur et nécessitant d'être adressées au plus haut niveau. La norme ISO 27000 définit une vulnérabilité comme une faiblesse, au sein d'un actif ou groupe d'actif, dont l'exploitation potentielle (par une menace) peut porter préjudice à l'organisation : fuite d'informations confidentielles, image détériorée, perte de confiance, baisse des revenus, etc. L'étude DBIR (Data Breach Investigations Report) réalisée en 2012 a révélé suite à l'examen de 855 incidents que 92% des attaques était peu complexes, et que 97% des infractions réussies auraient pu être évitées si la victime avait déployé entre autre des correctifs de sécurité et des mots de passe robustes. Le Gartner Group estime qu'en 2015, 80% des attaques réussies exploitent des vulnérabilités connues. Le risque de piratage informatique n'est pas un risque prioritaire. Cependant, nous proposons la mise en place d'un processus de gestion des vulnérabilités. Ce processus apparaît essentielle afin d'évaluer en continu et en temps réel le niveau de sécurité de la banque et de décider des actions prioritaires à conduire. La gestion des vulnérabilités renforce la sécurité intrinsèque des systèmes tout en complétant d'autres types de mesures sécuritaires (gestion des accès, filtrage des flux, détection et blocage des attaques, etc.). De ce fait, elle constitue à la fois un processus de sécurité et un moyen de contrôle permanent au sein de la banque.

Figure 9: Activité de gestion des vulnérabilités et contrôle permanent



- **L'efficacité du plan de continuité d'activité :** les plans de secours doivent être testés périodiquement pour s'assurer que leur efficacité demeure intacte.
- **Le système de télésurveillance :** ce service associe la dissuasion (alarme), le contrôle (identification à distance) et l'intervention des agents de sécurité. Il permet une détection immédiate de toute tentative d'intrusion, la dissuasion des malfaiteurs grâce au déclenchement d'une puissante sirène et télé-interpellation via le haut- parleur du système par le télésurveilleur de tout intrus. En cas d'intrusion avérée, les forces de l'ordre sont rapidement prévenues.

La banque doit continuer la mise en place des simples mesures de sécurité telles que :

- prévoir plusieurs systèmes de fermeture pour les portes, celles donnant sur la rue, les entourer d'un encadrement métallique et installer une serrure multipoints, pour les fenêtres les entourer des barreaux de fer faiblement espacés ;
- contrôler l'accès des personnes « étrangères » à la banque toute la journée sans oublier les heures de repas, vérifier leur identité et les accompagner les jusqu'au lieu de rendez-vous par le gardien de sécurité ;
- répartir les documents et les biens à protéger dans plusieurs coffres ou dans des vitrines différentes.

- **Un système de détection des fuites d'eau** : Les fuites d'eau dans la banque peuvent causer des dégâts considérables. En effet, à cause d'une fuite pareille, à l'Unité Centrale

des Opération à l'ATB, la majorité des ordinateurs a été endommagée. La solution proposée est l'installation d'un système de détection des fuites d'eau. Ce système doit être relié à une centrale pour garantir une intervention rapide.

- **La protection anti-feu** : pour conserver les documents à l'abri du feu dans la banque, il faut prévoir des armoires anti-feu.
- **Les contrats d'assurance** : tous les locaux de la banque doivent être assurés.

Recommandations en matière de gestion du risque opérationnel au sein de l'ATB.

Afin de renforcer la gestion des risques opérationnels au sein de l'ATB, la banque peut opter à :

- **La création d'une base des incidents** : la collecte de données de pertes interne par un établissement bancaire constitue la première des conditions afin d'accélérer l'étape relative à la création d'une base des incidents, l'ATB peut utiliser les informations sur les pertes disponibles. En effet, l'analyse des comptes pertes et charges, des rapports d'audit, et des rapports d'inspection permettront d'identifier et d'apprécier globalement les pertes par risque ou par opération. Actuellement la banque applique la méthode d'Indicateur de base (annexe n°7).
- **Encourager les collaborateurs à déclarer les incidents survenus** : la direction peut choisir de ne pas sanctionner les collaborateurs qui déclarent eux-mêmes leurs erreurs.
- **Le renforcement de la culture du risque opérationnel au sein de la banque** : le renforcement de la culture du risque opérationnel dans toutes les directions et les agences se fait, notamment par des formations et des cycles de conférence, afin que chaque collaborateur connaisse et maîtrise les risques opérationnels à son activité. Il doit comprendre que la gestion du risque opérationnel est une responsabilité qui incombe à tous les employés de la banque ;
- **Entamer des travaux de cartographie des risques opérationnels :** identifier et évaluer les risques opérationnels et les contrôles de processus métiers au sein de la banque et procéder à la communication des résultats trouvés et des actions à mener ;
- **Le système informatique de collecte des données de pertes opérationnelles :** dans le cadre de sa politique de gestion des risques opérationnels, la banque peut instaurer un système de collecte de pertes.

Conclusion

Ce dernier a été consacré à l'élaboration de deux cartographies des risques opérationnels liés aux processus crédit documentaire import et export au sein de l'ATB. Dans la première section, nous avons présenté la banque et ses indicateurs d'activité. En plus, nous avons défini le crédit documentaire, ses intervenants et ses modes de réalisations. Dans la deuxième section, nous avons explicité la méthodologie d'identification, d'évaluation et de classification des risques et des mesures de contrôles. Dans la troisième section nous avons présenté et analysé les risques nécessitant une intervention rapide. Nous avons proposé aussi certaines mesures de contrôle pour les atténuer.

CONCLUSION GENERALE

Ce mémoire a pour objectif principal la cartographie des risques opérationnels liés au processus du crédit documentaire au sein de l'ATB. Pour cela, noua avons consacré le premier chapitre, principalement, à la définition de risque opérationnel au sein de la banque et à l'étude de ses méthodes de gestion. La démarche d'élaboration d'une cartographie des risques a fait l'objet du deuxième chapitre. Elle consiste à mettre en place les moyens humains et financiers nécessaires, suivre les étapes d'identification, évaluation, hiérarchisation, représentation et communication des risques nets. Les résultats trouvés constituent la base d'élaboration d'un plan d'actions. Dans le dernier chapitre, nous avons mis en place une cartographie des risques opérationnels liés au processus de crédit documentaire au sein de l'ATB. Il en résulte un ensemble d'actions à entreprendre pour les risques considérés prioritaires.

Cet exercice est réalisé sur la base d'analyses et de déclarations tant des opérationnels que des supérieurs hiérarchiques aux divisions de crédit documentaire (import et export). Il s'articule autour de quatre étapes :

- La définition des processus : Cette étape consiste à diviser les deux processus en sous-processus, voire d'affiner cette division en dressant une liste des différentes fonctions les composant ;
- Le recensement et l'évaluation des risques des risques opérationnels : cette étape consiste à identifier les risques opérationnels rattachés à chaque processus. Les risques sont évalués en fonction de leurs fréquences et de leurs impacts financiers ;
- Le recensement et l'évaluation des contrôles associés : cette étape consiste à identifier les contrôles associés aux risques et évaluer leur conception et application ;
- La hiérarchisation des risques nets et présentation des la cartographie : il s'agit de hiérarchiser les risques nets et de présenter la cartographie des risques afin de prendre les mesures de gestion convenables.

L'évaluation des risques et des contrôles nécessitent la définition préalable de la méthode d'évaluation et des échelles de cotation. Dans le cadre de cette étude, nous avons appliqué l'estimation qualitative et des cotations des gravités, des fréquences, des contrôles à l'aide des échelles à 6 niveaux.

Les risques nets ont été classés en quatre zones de risques : la zone des risques négligeables, la zone des risques récurrents, la zone des risques majeurs et la zone des risques

insupportables. Il faut noter qu'aucun risque insupportable n'a été identifié. Le principal risque majeur est le risque de pertes dues à des événements externes (vandalisme, braquage). L'ATB a connu des événements pareils en 2011. Ils ont causé une perte nette de 2 millions de dinars. Pour atténuer ce risque nous avons proposé à la banque de mettre en place un système de télésurveillance. Ce système offre un triple service : dissuasion, contrôle à distance et intervention rapide des agents de sécurité. La banque doit s'assurer de l'efficacité de son plan de continuité de l'activité. Cela se fait grâce à des tests périodiques pour vérifier que la banque serait en mesure de le mettre en œuvre même dans le cas improbable d'une grave perturbation de l'activité. Les risques majeurs gérés au sein de la banque sont aussi transférés à des compagnies d'assurance. Pour ce fait, la banque doit assurer tous ses locaux contre les dommages causés par des événements externes.

Parmi les principaux risques récurrents identifiés, nous citons les pertes dues à des interruptions ou des perturbations du système informatique en particulier le problème de discordance des données au niveau du sous processus de domiciliation. Ce risque touche directement l'image de la banque, c'est pour quoi, il doit être géré immédiatement en entrant des modifications sur le système informatique. En outre, plusieurs banques dans le monde étaient victimes des attaques de piratage informatique. Pour se couvrir contre ce risque, nous proposons l'implémentation d'un système de gestion des vulnérabilités. Il renforce la sécurité intrinsèque des systèmes tout en complétant d'autres types de mesures sécuritaires (gestion des accès, filtrage des flux, détection et blocage des attaques, etc.). Quant aux risques négligeables tels que les risques de blanchiment d'argent, de falsification des documents et des signatures aucune mesure de contrôle n'est proposée. Il s'agit juste de continuer à appliquer les mesures actuelles de la même efficacité.

La cartographie des risques se révèle être l'un des instruments les plus pertinents pour identifier et analyser de façon structurée les risques opérationnels auxquels la banque doit faire face dans le cadre d'un processus d'activité. Elle permet ainsi de concevoir les actions nécessaires d'atténuation, de contrôle ou de transfert des risques. Pour cela, ce travail constitue une contribution dans le processus de gestion des risques opérationnels au sein de l'ATB. La cartographie réalisée doit être mise à jour et communiquée à l'ensemble des collaborateurs à la direction de commerce extérieur à la banque. Ces derniers doivent être impliqués dans le processus de gestion des risques opérationnels.

Bibliographie

Articles

- Comité de Bâle sur le contrôle bancaire, « Nouvel accord de Bâle sur les fonds propres », 2003.
- B. Bon-Michel, La cartographie des risques : de la rationalisation du futur à l'apprentissage du risque. Cas de l'identification du risque opérationnel au sein d'un établissement de crédit. Management & Avenir 2011/8 (n° 48).
- Comité de Bâle sur le contrôle bancaire, « saines pratiques pour la gestion des risques opérationnels », publications BRI, Février 2003.
- Commission spéciale sur la criminalité organisée, la corruption et le blanchiment de capitaux, Document de travail sur le blanchiment de capitaux, Parlement Européen 2009 – 2014.
- COSO, « Enterprise Risk Management -Integrated Framework», September 2004.
- C. Hess, The impact of the financial crisis on operational risk in the financial services industry: empirical evidence,The Journal of Operational Risk 2011.
- Club de la Sécurité de l'Information Français - La gestion des vulnérabilités informatiques : vers une meilleure gestion des risques opérationnels, mai 2014.
- D. Nouy, Le champ du risque opérationnel dans Bâle II et au-delà, Revue d'économie financière 2006 (n°84).
- É. Lamarque, F. Maurer, Le risque opérationnel bancaire : Dispositif d'évaluation et système de pilotage, Revue française de gestion 2009/1 (n° 191).
- Frantz Maurer, Les développements récents de la mesure du risque opérationnel, Université Montesquieu-Bordeaux IV.
- Gilles Motet, La norme ISO 31000 en 10 questions, Les cahiers de la sécurité industrielle, 2009 (n°5).

- IFACI, Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne, Edition 2013.
- J. Henriques et H. Khemakhem , Les meilleures pratiques en matière de gestion des risques opérationnels : une approche actuelle, CHAIRE d'information financière et organisationnelle ESG UQAM, 2015.
- M. Haouat, Risque opérationnel bancaire : le point sur la réglementation prudentielle, Revue française de gestion, 2011/8 (n° 48).
- R. Weissinger, Management du risque : L'aide des normes ISO, ISO Focus, Février 2013.
- P.DENIAU et E. RENOUX, la cartographie du risque opérationnel : Outil réglementaire ou outil de pilotage?, Revue d'économie financière, 2006.
- Société ontarienne d'assurance-dépôt, Gestion du risque d'entreprise : Guide d'application, Septembre 2011.

Ouvrages

- Ariane Chapelle, Georges Habner, Jean-Philippe Peters, Le risque opérationnel : implications de l'Accord de Bâle pour le secteur financier, 2005.
- B. Barthélémy, gestion des risques, édition d'organisation, 2002.
- Gilbert De MARSCHAL, « la cartographie des risques », Ed. AFNOR, Saint-Denis 2003.
- Jaques RENARD, « Théorie et pratique de l'audit interne », 7ème édition, Ed. d'ORGANISATION, 2007.
- John Hull, Gestion des risques et institutions financières, Pearson 2007.
- Landwell et al, Le management des risques de l'entreprise, Edition d'Organisation, 2005.
- Renard, Jacques, théorie et pratique de l'audit interne, Editions d'Organisation, 2004.

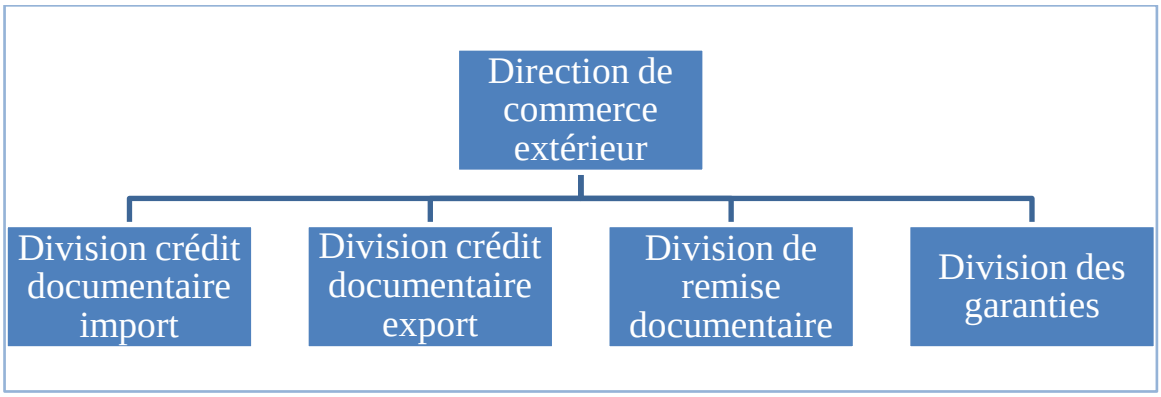
Textes juridiques

- Circulaire aux établissements de crédit n° 2006 -19 du 28 novembre 2006 relative au contrôle interne dans les établissements de crédit.
- Circulaire aux établissements de crédit n°2013-15 du 7 novembre 2013 relative à la mise en place des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme

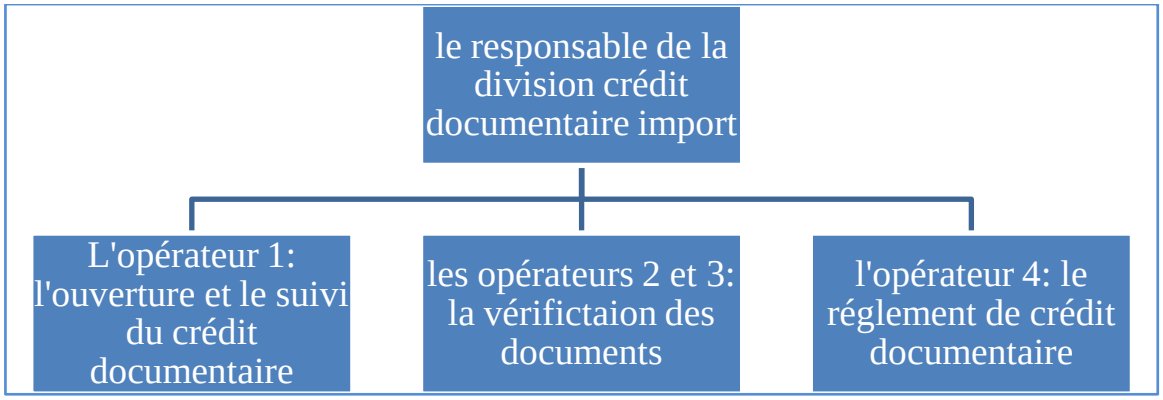
ANNEXES

Annexe n°1 : les organigrammes relatifs à la direction de commerce extérieur, la division crédit documentaire import, la division crédit documentaire import.

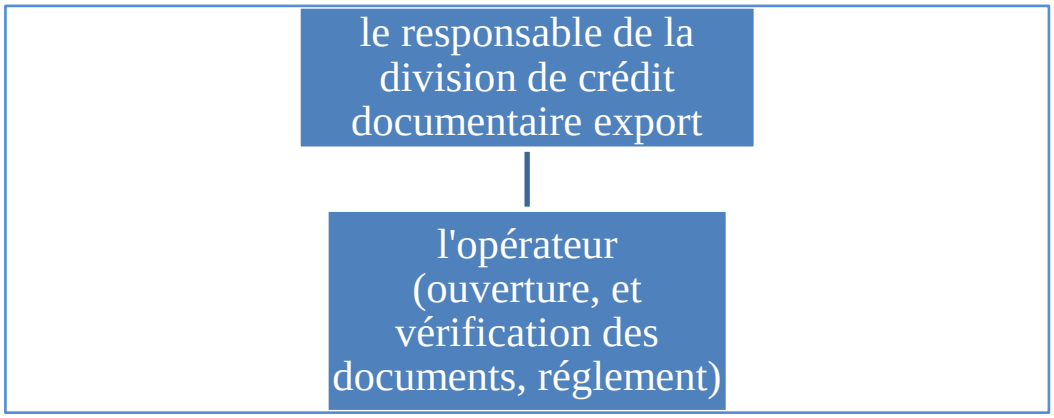
1.1 -Organigramme de la direction de commerce extérieur



1.2 - Organigramme de la division crédit documentaire import



1.3 -Organigramme de la division crédit documentaire import



Annexe n°2 : la typologie des risques opérationnels

1.1 La fraude interne

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Fraude interne	Activité non autorisée	R111	Transactions non notifiées (intentionnellement)
		R112	Transactions de type non autorisé (avec perte financière)
	Vol et fraude	R121	Fraude/fraude au crédit/absence de provisions
		R122	Vol des documents
		R123	Détournement des fonds
		R124	Destruction malveillante de biens
		R125	Contrefaçon
		R126	Falsification de documents

1.2 La fraude externe

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Fraude externe	Vol et fraude	R211	Vol/ vol qualifié
		R212	Contrefaçon
		R213	Falsification des documents
		R214	Falsification des signatures
	Sécurité des systèmes	R221	Dommages dus au piratage informatique
		R222	Vol d'informations (avec perte financière)

1.3 La négligence des règles clients

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Négligence des règles clients	Pratiques commerciales/de place Incorrectes	R311	Blanchiment d'argent
		R312	Non respect des règles d'embargos ou des black listes

1.4 Dommages aux actifs corporels

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Dommages aux actifs corporels	Catastrophe et autres sinistres	R411	pertes provenant de catastrophes naturelles
		R412	pertes dues à des causes externes (vandalisme, terrorisme).
	Pertes à cause des événements internes (inondation, incendie)	R413	Destruction des documents à cause des incendies ou des inondations dues à des fuites internes.

1.5 Dysfonctionnement des systèmes

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Dysfonctionnement des systèmes	Systèmes	R511	matériel
		R512	interruptions/perturbations d'un service
		R513	Indisponibilité d'électricité

1.6 Exécution, livraison et gestion des processus

Type de risque	Sous catégorie : niveau 2	Code de risque	Niveau 3
Exécutions, livraison et gestion des processus	Saisie, exécution et suivi des transactions	R611	Erreurs dans la saisie, le suivi ou le chargement
		R612	Retard d'exécution
		R613	Ignorance de la procédure
		R614	Accepter des documents non conformes
		R615	Saisir des données sans vérification
		R616	Validation sans vérification
	Admission et documentation clientèle	R621	Absence d'autorisation clientèle ou de déni de responsabilité
		R622	Documents juridiques absents/incomplets
		623	Perte des documents

Annexe n°3 : Identification des risques opérationnels liés au processus crédit documentaire import

3.1 Sous processus : instruction de la demande

Les tâches	Les risques opérationnels
se rendre à l'agence pour remplir la demande et présenter les documents justificatifs	**R412**: pertes dues à des causes externes (vandalisme, terrorisme).
	R411 : catastrophe naturelle - inondation
remplir et signer la demande.	**R213** : falsification des documents
	R214: falsification des signatures

3.2 Sous processus vérification de solvabilité et signature

Les tâches	Les risques opérationnels
vérifier la cohérence des données remplies, au niveau de la demande, vérifier le numéro de compte, le titulaire du compte, le montant en chiffres et en lettres, la signature apposée avec le spécimen de signature.	**R622**: les documents juridiques absents ou incomplets
	R613: Ignorance de la procédure
	R112 : Transactions de type non autorisé
vérifier l'existence de provision suffisante ou d'une autorisation, s'assurer de l'origine licite des fonds	**R311** : Le blanchiment d'argent
	R221 : Dommages dus au piratage informatique

3.3 Sous processus domiciliation

Les tâches	Les risques opérationnels
vérifier que le titre est en conformité avec la facture commerciale et avec la réglementation des changes	**R612** : retard d'exécution
Saisie de la domiciliation sur le système	**R221** : Dommages dus au piratage informatique
	R511 : Les pertes dues au dysfonctionnement du matériel informatique.
	R513: Indisponibilité d'électricité
	R512 : Les pertes provenant des interruptions ou perturbations du système informatique

3.4 Sous processus ouverture de crédit documentaire

Les tâches	Les risques
vérification de la complétude et la cohérence des données	**R615**: saisir des données sans vérification
saisie de l'ouverture de la lettre de crédit	**R612** : retard d'exécution
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R511:dysfonctionnement de matériel informatique
	R512:interruptions/perturbations du service informatique
	R513: Indisponibilité d'électricité
	R312: Non respect des règles d'embargo ou de Black listes
vérification et validation du message Swift	**R616:** validation sans vérification

3.5 Sous processus suivi du crédit documentaire

Les tâches	Les risques opérationnels
vérification de cohérence des amendements	**R615**: saisir des données sans vérification
saisie des termes de la modification	**R612** : retard d'exécution
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R511:dysfonctionnement de matériel informatique
	R512:interruptions/perturbations du service informatique
	R513: Indisponibilité d'électricité
vérification et validation du message Swift	**R616:** validation sans vérification

3.6 Sous processus vérification des documents

Les tâches	Les risques opérationnels
réception des documents	**R413**:Destruction des documents à cause des incendies ou des inondations dues à des fuites internes.
	R122: vol des documents
vérification des documents	**R614**: Accepter des documents non conformes
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R511:dysfonctionnement de matériel informatique
	R512:interruptions/perturbations du service informatique
	R513: Indisponibilité d'électricité
Vérification du message SWIFT	**R616 :** Validation sans vérification

3.7 Sous processus règlement

Les tâches	Les risques opérationnels
saisie du règlement	**R412:** pertes dues à des causes externes (vandalisme, terrorisme).
	R411 : catastrophe naturelle - incendie.
	R612 : Retard d'exécution
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R616 : Validation sans vérification

Annexe n°4 : identification des risques opérationnels liés au processus du crédit documentaire export

Les tâches	Les risques opérationnels
réception du message SWIFT	**R612 :** retard d'exécution
Saisie de la lettre de crédit sur le système informatique	**R612 :** retard d'exécution
	R615: saisir des données sans vérification
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R311 : Le blanchiment d'argent
	R312: Non respect des règles d'embargo ou de Black listes
	R511:dysfonctionnement de matériel informatique
	R512:interruptions/perturbations du service informatique
	R513: Indisponibilité d'électricité
validation de la saisie	**R616**: validation sans vérification
vérification des documents (crédit documentaire confirmé)	**R612** : retard d'exécution
	R614: acceptation des documents non conformes
	R611 : Erreurs dans la saisie, le suivi ou le chargement
	R122: vol des documents
Règlement du crédit documentaire	**R612 :** retard d'exécution
	R511:dysfonctionnement de matériel informatique
	R512:interruptions/perturbations du service informatique
	R513: Indisponibilité d'électricité
	R611 : Erreurs dans la saisie, le suivi ou le chargement

Annexe n°5 : Evaluation des risques et des contrôles, processus crédit documentaire import

5.1 Evaluation des risques et des contrôles : sous processus instruction et vérification de la demande

Les risques	F	I	R. brut	Contrôle	risque net
R412 : pertes dues à des causes externes	4	6	24	4	8
R411 : catastrophe naturelle - inondation.	1	6	6	4	2
R213 : falsification des documents	3	2	6	4	2
R214: falsification des signatures	3	1	3	4	1
R622: les documents juridiques absents ou incomplets	3	2	6	4	2
R613: Ignorance de la procédure	4	3	12	2	8
R112 : Transactions de type non autorisé	1	3	3	4	1
R311 : Le blanchiment d'argent	2	5	10	4	3
R121 : absence de provision ou d'autorisation	1	5	5	4	2
R 612 : retard d'exécution	2	4	8	1	7
R 623 : perte des documents	3	5	15	1	13
R221 : Dommages dus au piratage informatique	1	5	5	2	4

5.2 Evaluation des risques et des contrôles : sous processus domiciliation du titre de commerce

Les risques	F	I	R. brut	Contrôle	risque net
R612 : retards d'exécution	2	5	10	1	8
R221 : Dommages dus au piratage informatique	1	5	5	4	2
R511 : Les pertes dues au dysfonctionnement du matériel informatique.	2	3	6	2	4
R513: Indisponibilité d'électricité	2	1	2	4	1
R512 : Les pertes provenant des interruptions ou perturbations du système informatique	4	4	16	1	13
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	2	4
R411: Les pertes provenant de catastrophes naturelles	1	5	5	4	2
R412 : Les pertes dues à des causes externes	2	5	10	4	3

5.3 Evaluation des risques et des contrôles : sous processus ouverture du crédit documentaire

Les risques	F	I	R. brut	Contrôle	risque net
R615: saisir des données sans vérification	1	3	3	2	2
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R511:dysfonctionnement de matériel informatique	2	2	4	2	3
R512:interruptions/perturbations du service informatique	2	2	4	2	3
R513: Indisponibilité d'électricité	2	1	2	4	1
R312: Non respect des règles d'embargo ou de Black listes	1	6	6	4	2
R616: validation sans vérification	1	3	3		3

5.6 Evaluation des risques et des contrôles : sous processus suivi du crédit documentaire

Les risques	F	I	R. brut	Contrôle	risque net
R615: saisir des données sans vérification	2	3	6	2	4
R612 : Non-respect de délais ou d'obligations	1	3	3	4	1
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R511:dysfonctionnement de matériel informatique	2	2	4	2	3
R512:interruptions/perturbations du service informatique	2	2	4	2	3
R513: Indisponibilité d'électricité	2	1	2	4	1
R312: Non respect des règles d'embargo ou de Black listes	1	6	6	4	2
R616: validation sans vérification	1	3	3		3

5.7 Evaluation des risques et des contrôles : sous processus vérification des documents

Les risques	F	I	R. brut	Contrôle	risque net
R122: vol des documents	1	6	6	2	4
Destruction des documents à cause des incendies ou des inondations dues à des fuites internes.	1	6	6	2	4
R614: Accepter des documents non conformes	1	6	6	4	2
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R511:dysfonctionnement de matériel informatique	2	2	4	2	3
R512:interruptions/perturbations du service informatique	2	2	4	2	3
R513: Indisponibilité d'électricité	2	1	2	4	1
R616: validation sans vérification	1	3	3		3

5.8 Evaluation des risques et des contrôles : sous processus règlement

Les risques	F	I	R. brut	Contrôle	risque net
R612 : Non-respect de délais ou d'obligations	1	3	3	4	1
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R511:dysfonctionnement de matériel informatique	2	3	6	2	4
R512:interruptions/perturbations du service informatique	2	3	6	2	4
R513: Indisponibilité d'électricité	2	1	2	4	1
R123: détournement de fonds	1	5	5	4	2
R616: validation sans vérification	1	3	3		3

Annexe 6 : Evaluation des risques et des contrôles : processus du crédit documentaire export

6.1 Evaluation des risques et des contrôles : sous processus réception du message SWIFT et saisie de l'ouverture

Les risques	F	I	R. brut	Contrôle	R.net
R612 : retard d'exécution : retard au niveau de la direction SWIFT dans la transmission des messages SWIFT à la division crédit documentaire export	1	3	3	2	2
R612 : retard d'exécution : retard dans la notification du client	1	4	4	4	1
R615: saisir des données sans les vérifier auparavant	1	4	4	2	2
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	4	8	4	2
R311 : Le blanchiment d'argent	1	5	5	4	2
R312: Non respect des règles d'embargo ou de Black listes	1	5	5	4	2
R511:dysfonctionnement de matériel informatique	2	2	4	2	2
R512:interruptions/perturbations du service informatique	2	2	4	2	3
R513: Indisponibilité d'électricité	2	1	2	4	1
R616: validation sans vérification	1	4	4	-	4

6.2 Evaluation des risques et des contrôles : sous processus vérification des documents

Les risques	F	I	R. brut	Contrôle	R.net
R612 : retard d'exécution	1	4	4	4	1
R614: acceptation des documents non conformes	1	6	6	4	2
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R122: vol des documents	1	6	6	4	2

6.3 Evaluation des risques et des contrôles : sous processus règlement

Les risques	F	I	R. brut	Contrôle	R.net
R612 : retard d'exécution	2	3	6	4	2
R511:dysfonctionnement de matériel informatique	2	3	6	2	4
R512:interruptions/perturbations du service informatique	2	3	6	2	4
R513: Indisponibilité d'électricité	2	1	2	4	1
R611 : Erreurs dans la saisie, le suivi ou le chargement	2	3	6	4	2
R123: détournement de fonds	1	5	5	4	2
R616: validation sans vérification	1	4	4	-	4

Annexe n° 7: Calcul de l'exigence en fonds propres relative au risque opérationnel

Les exigences en fonds propres relatives aux risques opérationnels sont déterminées selon l'approche Indicateur de Base, c'est-à-dire en appliquant un pourcentage fixe de 15% au produit annuel brut moyen sur les trois dernières années.

Tableau : Evolution du PNB

Années	2012	2013	2014
Produits nets bancaires (en 1000 TND)	158 346	166 664	173 670

Le produit net bancaire moyen (en 1000 TND) = 166227 : l'exigence en fonds propres relative au risque opérationnel(en 1000 TND) = 24934

TABLE DES MATIERES