Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Ecole Supérieure de Commerce

Mémoire de fin d'études en vue de l'obtention du diplôme de magister en sciences commerciales et financières

Spécialité : Finance.

THEME :

Élaborer la Cartographie des risques opérationnels bancaires

Cas : Société Générale Algérie

Elaboré par :

GUELMA Saadia

Encadré par :

DR. KHOURI Nabil

Maitre de conférences « A »

Promotion : 2016

Remerciements

Je tiens à remercier tout d'abord « ALLAH » de m'avoir donné le courage, la volonté, la santé et la patience qui m'ont permis de réaliser ce modeste travail.

Je souhaite adresser tous mes remerciements aux personnes qui m'ont apporté leur aide et qui ont ainsi contribué à l'élaboration de ce mémoire.

Mes remerciements s'adressent également à mon encadreur, Monsieur **KHOURI Nabil** pour avoir accepté de diriger ce mémoire, tout en me conseillant, m'aidant et m'encourageant au long de ce travail.

Je remercie tout particulièrement **Madame BELARBI -Salah Dorya**, Directrice du département de l'audit Société Générale Algérie, de m'avoir accordé sa confiance et autorisé à effectuer mon stage au sein de son service, Merci également à toute l'équipe d'audit de la Société Générale Algérie qui a su trouver du temps pour m'aider dans les différentes missions et travaux que l'on m'avait confiés.

Je remercie les membres du jury d'avoir accepté de juger ce travail.

Enfin un grand merci a tous le corps de l'ESC, professeurs, administration, agents de sécurité…….ect.

Dédicaces

A la personne devant laquelle tous les mots de l'univers sont incapables d'exprimer mon amour et mon affection pour elle, à l'être qui m'est le plus cher à ma douce maman. ***Maman****, si tu savais combien je t'aime.*

A mon cher père qui m'a inculqué la discipline, les valeurs de la réussite et du respect d'autrui, ***papa*** *je te remercie d'avoir fait de mois une femme.*

A mon petit frère Abdou et mes sœurs;
A mes neveux et nièces
Pour lesquels je souhaite une belle vie.

A ***Sid Ali*** *pour son soutien moral, pour sa patience, son encouragement, et ses conseils.*

A mes chers amis ***Nabila****,* ***Imene****,* ***Ibtissem****,* ***khadidja****,* ***wassila*** *et* ***salima*** *je vous souhaite tout le bonheur et la réussite.*

SOMMAIRE

Liste des tableaux

Liste des figures

Liste des annexes

Liste des abréviations

Abréviations	significations
AMA	Approche des mesures avancées.
AS	Analyse de scénérii.
BIA	Basic Indicator Approch.
COSO	Commette of sponsoring organizations of the treadway commission.
CRBF	Comité de la réglementation bancaire et financière.
DG	Direction générale.
DMR	Dispositif de maitrise des risques.
IAS	International accounting standards.
IFACI	L'institut français de l'audit et du contrôle interne.
IIA	Institut des auditeurs internes.
ISO	International organization for standardization.
KRI	Key risk indicators.
PME	Petites et Moyennes Entreprises.
PNB	Produit net bancaire.
RCSA	Risk & control self assessment.
RI	Risque intrinsèque.
RO	Risque opérationnel.
RR	Risque résiduel.
SA	Standard approch.
SG	Groupe société générale.
SGA	Société générale Algérie.

INTRODUCTION GENERALE

Introduction générale

Le risque opérationnel n'est pas un risque totalement nouveau pour les banques, nous le constatons à partir des efforts réalisés depuis quelques années par ces dernières dans l'inventaire et l'élaboration de cartographie des risques de tout type.

Ce n'est pas non plus un risque inconnu des autorités de contrôle bancaire qui, dans leur ensemble, l'ont intégré depuis dans leur analyse du profil de risque des établissements de crédit.

Ces autorités exigent des établissements de crédit et des entreprises d'investissement la mise en place d'un système de surveillance et de maîtrise des risques opérationnels, en particulier ceux liés aux systèmes comptables et d'information.

En effet, le risque opérationnel a pris une importance croissante ces dernières années, principalement en raison des modifications du cadre d'exercice et de la conduite des activités bancaires.

Aussi, les scandales successifs et d'ampleur internationale tel que l'affaire Kerviel, l'affaire Madof et aujourd'hui encore les affaires UBS et HSBC qui se sont soldées par des pertes de plusieurs milliards d'Euros ont, depuis quelques années, accru l'attention sur l'efficacité du contrôle dans les établissements financiers.

Les autorités prudentielles et les spécialistes du métier de risque ont ainsi vu émerger une nouvelle catégorie de risques, de nature non financière au départ, mais aux conséquences tout aussi négatives. A cela, s'ajoute un risque de réputation difficilement évaluable monétairement, mais dont l'impact est jugé, par les experts, réellement significatif.

Cet essor des risques opérationnels est notamment lié au manque de prudence dans la gestion en temps réel des opérations, engendrant un risque de règlement, dans un contexte d'internationalisation des activités. Il est par ailleurs le résultat de la sophistication de ces activités, tant dans la conception de nouveaux produits que dans la mise en place de systèmes d'information de plus en plus complexes.

C'est ainsi que l'importance prise par le risque opérationnel s'explique aussi, de manière plus récente, par l'attention accrue portée aux risques extérieurs à faible probabilité d'occurrence mais à forte intensité qui peut engendrer des pertes massives comme par exemple les catastrophes naturelles ou encore les actes terroristes.

Suite à cette montée accrue du risque, les institutions bancaires doivent redoubler d'effort en vue de maintenir ou restaurer la confiance entre elles et leurs clients.

Pour ce faire, la maitrise des risques inhérents à leur activité doit se faire à l'aide d'un dispositif de contrôle interne efficace englobant l'ensemble des activités et des fonctions.

Ce dispositif doit être déployé au niveau de l'ensemble des activités de la banque et doit a son tour faire l'objet de « contrôle » et d'évaluation et ce afin de déceler les manques et de les corriger.

La fonction d'audit interne au sein de la banque donne à cet égard l'assurance raisonnable que les opérations menées ainsi que les décisions prises sont sous contrôle et qu'elles contribuent donc aux objectifs de l'établissement. Elle utilise une méthodologie rigoureuse et bien définie tout au long de ses différentes missions et vise à apporter des recommandations pour améliorer l'efficacité du contrôle interne.

INTRODUCTION GENERALE

La cartographie des risques est l'outil commun qui se dégage de l'ensemble des approches recommandées ou imposées pour la mise en place d'un dispositif de maîtrise des risques adapté et efficace.

En Algérie, à travers la réglementation prudentielle et celle relative au contrôle interne des banques et établissements financiers, exige des banques de mesurer leurs risques y compris celui comportant un caractère opérationnel et les oblige à mettre en place une cartographie permettant leur identification et leur évaluation.
La cartographie des risques est donc devenue un outil règlementaire que les banques algériennes doivent impérativement mettre en œuvre.

C'est ainsi, que nous avons opté pour le sujet «**Élaborer la Cartographie des risques opérationnels bancaires, Cas : Société Générale Algérie»**

C'est dans cette perspective que nous allons tenter d'apporter des éléments de réponse à la problématique suivante : **quelle méthodologie de cartographie des risques est la plus appropriée pour la maîtrise des risques opérationnels au sein de la SOCIETE GENERALE ALGERIE?**

De cette problématique découle un certain nombre de questions qui viendront étayer notre question centrale :

1. Comment la cartographie des risques opérationnels contribue à la maitrise des risques afférents aux processus métier ?
2. Quel sont les dispositifs mis en place pour la gestion du risque opérationnel au sein de la banque Société Générale Algérie?
3. Dans quelle optique s'inscrit la démarche de la Société Générale Algérie pour pouvoir diriger efficacement les risques opérationnels ?

Les hypothèses que l'on peut énoncer à la suite de nos différentes lectures théoriques sont :

1. Elaborer une cartographie des risques est une impérieuse nécessité. D'une part, c'est une aide précieuse à la prise de décision. D'autre part, c'est un moyen efficace permet aux banque d'avoir une bonne anticipation des risque liés à l'activité bancaire auxquels elles doivent faire face pour mettre en place les contrôles indispensables.
2. Les dispositifs de gestion des risques opérationnels mis en place par la SGA conformément aux exigences du comité de Bale.
3. pour assurer une gestion efficace du risque opérationnel, la banque doit tout d'abord procéder à une décomposition de son activité en lignes de métiers reflétant les différentes composantes de ce risque.

INTRODUCTION GENERALE

Nous examinerons les hypothèses citées à partir d'une étude de cas basée sur la Processus d'élaboration de la cartographie que nous avons effectuée au sein de la banque Société Générale Algérie « SGA ».

L'objectif de ce mémoire est d'expliquer la démarche d'élaboration de la cartographie des risques bancaires et d'analyser les résultats au sein de la banque Société Générale Algérie.

Vu le positionnement épistémologique et pratique de la problématique de recherche la **démarche méthodologique** la plus appropriée est **«** analytique descriptive », en effet une exploration des recherches antérieure sur le thème, ainsi que l'analyse des processus des banques est évidente, avant de passer au travail proprement dit d'analyse et d'identification des risques opérationnels qu'encourent SOCIETE GENERALE

Le plan ci-dessous montre l'organisation de notre travail et les points clés traités :

Un premier chapitre relatif au risque opérationnel, à sa spécificité, à ses composantes, à sa gestion et à sa couverture ; et qui se termine par La réglementation prudentielle du risque opérationnel au double plan national et international, et les différentes approches relatives à la détermination des exigences en fonds propres ;

Nous passerons ensuite dans le deuxième chapitre à la cartographie, par l'explication de la démarche d'élaboration d'une cartographie des risques. Une démarche qui commence par la mise en place des préalables nécessaires à sa réussite et qui se termine par une utilisation optimale de la cartographie élaborée (plan d'actions, plan d'audit….etc.)

Un chapitre pratique qui se déroulera sur la mise en œuvre de la méthodologie d'élaboration de la cartographie des risques opérationnels, où nous avons limité notre étude à une cartographie thématique concernant la banque de détails.

Chapitre I : Evaluation et gestion du risque opérationnel

Le risque est inhérent à toute activité humaine : la certitude de réussir ce que l'on entreprend n'est jamais absolue et il se pourrait qu'il y'ait des imprévus en cours de route, qui sont susceptibles d'altérer les résultats que l'on obtient.
Comme nous l'avons exposé en introduction, la banque ne déroge pas à la règle et elle est confrontée à une multitude de risques lors de l'exercice de ses activités.
Cependant, avant de nous plonger dans le risque opérationnel, il convient de délimiter le cadre conceptuel du risque en général, et du risque bancaire en particulier. En outre, nous traiterons de l'identification des risques en milieu bancaire.

Nous allons donc présenter dans ce chapitre l'évaluation et gestion du risque opérationnel à travers :

Une première section «**la notion de risque dans l'environnement bancaire** » permettant de présenter les différents risques bancaires et leur principales caractéristiques ;

Une deuxième section «**la spécificité des risques opérationnels dans le domaine bancaire**», qui définira le risque opérationnel et présentera la classification par catégories de risques et par types d'activités, proposée par Bâle II;

Une troisième section « **Le cadre réglementaire des risques opérationnels »** ou nous allons présenter les principales innovations apportés par le comité de Bâle en matière de recommandations et d'exigence de calcul des fonds propres ainsi que les meilleures pratiques en matière de gestion du risque opérationnel.

Section 1 : la notion de risque dans l'environnement bancaire

Par souci méthodologique. Il est impératif de définir les concepts avant de les utiliser dans leurs différents aspects. Donc, cette section est consacrée au développement de la notion de risque et la cadrer dans l'environnement bancaire**.**

1. Définition du risque

Le risque pour un investisseur c'est de perdre de l'argent ;[1]

Le risque peut être définit à partir de nombreuses sources, et pour illustrer l'ampleur de ce dernier sur les organisations, quelques définitions clés sont représentées :

Selon le dictionnaire français Le petit Larousse, le mot risque vient de l'italien risco, il s'agit de :

- Une possibilité, probabilité d'un fait, d'un évènement considéré comme un mal ou un dommage.
- Un danger, inconvénient plus ou moins probable auquel on est exposé. (Courir le risque d'un échec).
- Du fait de s'engager dans une action qui pourrait apporter un avantage, mais qui comporte l'éventualité d'un danger. (Avoir le goût du risque).

Selon la norme ISO 3100 : 2010, le risque est « l'impact de l'incertitude sur les objectifs de l'organisme »[2]

L'institut français de l'audit et du contrôle internes définit le risque comme « la menace qu'un évènement, une action ou une inaction affecte la capacité de l'entreprise à atteindre ses objectifs stratégiques et compromettre la création de la valeur ».

La dernière définition ne fait apparaitre que la menace qu'a une entreprise pour ne pas atteindre ses objectifs et mentionne pas la notion de chance (opportunité) de réalisation ou de non réalisation de cette menace.

Malgré les différentes définitions et interprétations que le mot « risque » revêt selon le domaine ou la spécialité ou il apparait, sa signification comporte le plus souvent deux dimensions :

-La probabilité de son occurrence ;

- la gravité de ses effets.

2. la Mesure du risque,[3]

Le risque est classiquement évalué sous la forme d'une combinaison des facteurs de probabilité et de gravité.

---

[1] Pierre Caron « **investir et gérer le risque** »ED presses de l'université du Québec, CANADA, 2014, P.05.

[2] Jean-Paul Louiso , « **Gestion des risques, 100 question pour comprendre et agir** », 2eme édition, édition AFNOR , paris 2014, p 214.

[3] Gilbert DE MARSHAL, « **la cartographie des risques** », Edition AFNOR, 2003, pp9-10

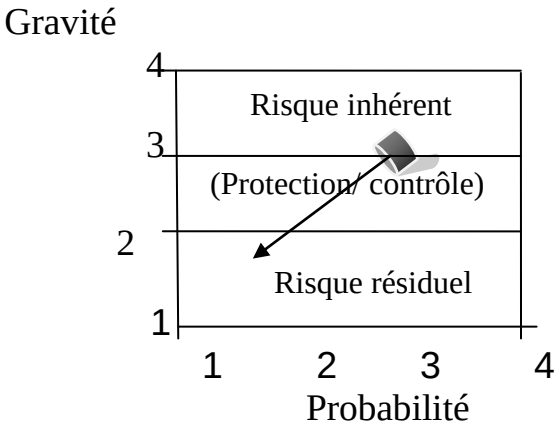
RISQUE = PROBABILITE * GRAVITE

Ces deux facteurs représentent les piliers de mesure de risque.
*La probabilité désigne les possibilités de réalisation du risque.
*La gravité désigne la quantification de la perte engendrée par la matérialisation du risque.

3. les niveaux de risques

Il est important de bien faire la différence entre un risque inhérent et un risque résiduel.
- Le risque brut ou inhérent est le risque qui existe en l'absence de mesures correctrices internes : absence de procédures, absence d'activités de contrôle, absence de système informatique, etc.
-Le risque résiduel est celui qui résulte du risque brut en tenant compte des protections et des contrôles mis en place.

Figure 1. Risque inhérent ou résiduel



Source : Gilbert de MARSHAL, « **La Cartographie Des Risques** », ED. AFNOR, 2003, p11

4. Les différentes catégories de risques bancaires

Dans cette présente partie nous nous proposons de présenter les risques relatifs à l'activité bancaire.

4.1. Définition du risque bancaire

Le risque peut se définir comme la menace qu'un évènement, une action ou une inaction affecte la capacité de l'entreprise à atteindre ses objectifs stratégiques et compromette la création de valeur [1];

[1] MOREAU FRANCK, « **Comprendre Et Gérer Les Risque** », Edition d'organisation, 2002, P3.

« Le risque correspond à l'occurrence d'un fait imprévisible, ou à tout le moins certain, susceptible d'affecter les membres, le patrimoine, l'activité de l'entreprise et de modifier son patrimoine et ses résultats ». [1]

De cette définition nous pouvons retirer deux éléments essentiels qui caractérisent le risque dans le milieu bancaire :

- L'enjeu lié aux résultats et pertes futurs de la banque (conséquence finale).
- Le caractère aléatoire et imprévisible (qui est à l'origine du risque).

Plusieurs classifications des risques bancaires peuvent être proposées. Néanmoins, les banques ont tendance à adopter la classification proposée par les différents accords de Bale qui distingue trois grandes catégories, à savoir :

· Le risque de crédit,
· Le risque de marché,
· Le risque opérationnel.

4.2 Le risque de crédit:

C'est le principal risque auquel est exposée une institution bancaire et demeure la cause première des difficultés et faillites des banques. Il est définit par le règlement de la banque d'Algérie N°11/08 du 28/11/2011 relatif au contrôle interne des banques et établissements financiers comme « le risque encouru en cas de défaillance d'une contrepartie ou de contreparties considérées comme un même bénéficier ».

Le risque de crédit peut également être définit comme étant une perte potentielle suite à l'incapacité du principal débiteur d'honorer ses engagements. Ainsi, selon le comité de Bale « la perte désigne la perte économique, qui se mesure en prenant en compte tous les facteurs concernés, notamment les effets d'escompte et les couts directs et indirects liés à la collecte des fonds relatifs à l'exposition »[2]

Mais le risque de crédit se rencontre également à l'occasion d'autres activités plus spécifiques, également exercées par le banquier [3]:

- Dans le contexte des opérations de marché (contrats dérivés hors bourse, mises/ prises en pension, prêts / emprunts de titres ou de produits de base), où il est alors qualifié de risque de contrepartie.
- Dans le contexte des opérations d'achat ou de vente au comptant (que ces opérations soient ou non par ailleurs des opérations de marché) où il est alors qualifié :

  - de risque de règlement / livraison, lorsque la transaction est effectuée selon le principe de la « livraison contre paiement », dans le cas des achats ou ventes de titres ou de produits de base, ou du «paiement contre paiement », dans le cas des achats ou ventes de devises ;

---

[1] Elie COHEN, « **Dictionnaire de gestion** », Ed La découverte, Paris, 1997, P308.
[2] Le comité de Bale sur le contrôle bancaire, « nouvelle accord de Bale sur les fond propres »(document soumis à consultation), avril 2003, point 422, page 74.
[3] Alain VERBOOMEN, Louis DE BEL, **« Bâle II et le risque de crédit »**, ED Larcier, Belgique 2011, PP .38 ,39.

- de risque sur transactions incomplètes (ou opérations non dénouées), lorsque la transaction n'est pas effectuée selon le principe sécurisé du DvP ou PvP.

4.3 Le risque de marché

« Les risques de marché sont les pertes potentielles résultant de la variation du prix des instruments financiers détenus dans le portefeuille de négociation ou dans le cadre d'une activité de marché dite aussi de " trading " ou de négoce ».[1]

L'activité de marché concentre et amplifie tous les autres risques : risque de taux (d'intérêt ou de change), de crédit, de liquidité, opérationnel. Le développement exponentiel des volumes traités sur les marchés traditionnels, et surtout sur les nouveaux marchés de produit dérivés *, a considérablement amplifié les risques. Ils ont été largement illustrés par des affaires qui mettent en exergue une étonnante faiblesse dans le contrôle que certaines banques exercent sur ces activités.

Les pertes peuvent se produire sur les compartiments des marchés financiers : marché de change, de titre de créance négociables, de titre de propriétés, de matières premières. A ces risques viennent s'ajouter ceux liés à la qualité de la contrepartie avec laquelle l'opération est traitée, qui peut s'avérer défaillante.

4 .4.Le Risque Opérationnel

La notion de risques opérationnels est extrêmement large : elle exprime tous les risques pouvant engendrer un dommage, une perte, un coût, créés ou subis lors de la réalisation de l'activité courante de l'entreprise. Ils matérialiseront tous les impacts directs ou indirects engendrés par l'entreprise dans son activité quotidienne, dans son cycle d'exploitation.

Ces pertes peuvent être liées à[2] :

- Une fraude, quelle soit interne (e.g. Nick leeson à la banque barings en 1995, ou jérome Kerviel à la société générale en 2008) ou bien externe (e.g. détournement de cartes de crédit) ;
- Des actes contraires aux dispositions législatives ou conventions en matière d'emploi (e.g. discrimination) ou de sécurité (non respect des normes) ;
- Un manquement à une obligation envers un client (e.g. vente d'un produit ne correspondant pas au profil de risque du client ou vente d'un produit en cachant au client la nature réelle du risque lié) ;
- Une catastrophe naturelle (e.g. tremblement de terre, inondation) ;
- D'autres événements externes (e.g. attentat du 11 septembre 2001 à new York) ;
- Une panne ou un dysfonctionnement des systèmes informatiques ;
- Un mauvais traitement des transactions (e.g. erreur d'encodage) ;

---

[1] Antoine SARDI, « **Audit et contrôle interne bancaire** », ED AFGES, France, Paris 2002, p. 40

*produit dérivé est un contrat dont la valeur est dérivée du prix d'autre chose, en général les actions, les obligations ou matières premières.

[2] « **Bâle II et le risque de crédit** », Op .cit, P .41

Section 2 : la spécificité des risques opérationnels dans le domaine bancaire

Après avoir présenté les risques bancaires dans leurs généralités ainsi que les interrelations entre eux, nous nous intéresserons plus particulièrement au risque opérationnel bancaire, Objet de notre travail. Pourquoi accorder tant importance à ce risque ? Que recouvre-t-il ? Comment le gérer ? C'est l'objet de la section de ce chapitre.

1. Comprendre qu'est ce qu'un risque opérationnel

La définition du risque opérationnel est la clé primordiale d'une gestion efficace. Néanmoins, il n'existe pas une définition unanime permettant d'adopter une approche commune et une méthodologie unique de gestion par toutes les banques. Toutefois, nous retiendront les plus significatives afin d'essayer de bien cerner ce concept.

1 .1. Définition selon « Bâle II » :

Le régulateur lors de l'accord de Bâle dans sa version conservatrice d'Avril 2003 a donné la définition suivante au risque opérationnel :
« Le risque opérationnel se définit comme étant le risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnes et systèmes internes ou à des événements extérieurs. Cette définition inclut le risque juridique et exclut le risque de réputation ainsi que le risque stratégique »[1].

Cette définition présente l'avantage d'être un point commun à l'ensemble des établissements. Elle sert de base de réflexion et de mise en œuvre à ces derniers et leur permet de tracer un périmètre quantifiable aux risques opérationnels.

1.2. Définition de la Banque d'Algérie :

En Algérie, la définition du risque opérationnel est donnée par l'Article 02 du règlement n° 11/08 du 28 Novembre 2011, relatif au contrôle interne des banques et établissements financiers. Cet article précise que le risque opérationnel est :

« Le risque résultant d'une inadaptation ou d'une défaillance imputables à des procédures, personnels et systèmes internes ou à des événements extérieurs.il inclut le risque de fraude interne et externe ».
Cette définition apporte un nouvel élément celui de la fraude interne et externe.

L'article 20 du nouveau règlement de la Banque d'Algérie14/01 portant, coefficients de solvabilité applicables aux banques et établissements financiers. Cet article stipule que : « On entend par risque opérationnel, le risque de perte résultant de carences ou de défaillances inhérentes aux procédures, personnels et systèmes internes des banques et établissements financiers, ou à des événements extérieurs. Cette définition exclut les risques stratégiques et de réputation, mais inclut le risque juridique»[2].

---

[1] Cette définition a été maintenue dans le dispositif révisé de juin 2004, texte disponible sur le site internet : www.bis.org

2 Http://www.bank-of-algeria.dz/html/legist014.htm, consulté le 27-12-15

Les définitions relatives au risque opérationnel diffèrent d'une banque à une autre en fonction de l'activité de chacune ainsi que de son organisation interne.

1.3. Définition du CRBF*:

Le règlement 97-02 du CRBF modifié par l'arrêté du 14 Janvier 2009 donne la définition suivante :
«Le risque résultant d'une inadaptation ou d'une défaillance imputables à des procédures, personnels et systèmes internes ou à des événements extérieurs y compris d'évènements de faible probabilité d'occurrence mais à fort risque de perte. Le risque opérationnel inclut les risques de fraude interne et externe ».

2 .Les principaux enjeux du risque opérationnel :

Le premier enjeu qui apparaît dans la mise en œuvre d'un dispositif de maîtrise des risques opérationnels est bien sûr la nécessité de se mettre en conformité avec la réglementation et par là, même d'optimiser le mentant de fonds propres (non lié à des activités rémunératrices) à allouer aux risques de cette nature.
La plupart des acteurs ont désormais en vue d'autres enjeux comme[1] :
- La sécurisation des résultats en évitant ou en couvrant des risques qui entraînent des pertes nettes ;
- Une plus grande compétitivité du fait des améliorations de tarif possibles si les pertes constatées sur les événements à fréquences diminuées ;
- Une sécurisation de la notion en évitant des « aléas » non souhaités qui peuvent avoir des répercussions sur la solvabilité ou la notoriété (avec derrière un coût supplémentaire lié à la dégradation du *rating*) ;
- Eviter la chute brutale du cours de bourse lorsque l'établissement bancaire ou une de ces filiales sont cotés ;
- Améliorer la productivité en identifiant les processus « à risque » et en menant les plans d'action nécessaires à leur amélioration.

La définition et les enjeux étant posés, nous intéresseront tout d'abord aux aspects réglementaires qui définissent désormais avec plus de précision le dispositif à mettre en œuvre, en particulier dans le cadre des méthodes avancées qui sont devenues la cible de la majorité des établissements.

En la matière même s'il existe un tronc commun donné par les textes, on constate une grande diversité aussi bien dans les organisations retenues que dans la définition des modèles de risque.

---

* Comité de la réglementation bancaire et financière.

[1] JIMENEZ .C & P.MERLIER & D.CHELLY, « **Risques Opérationnels** », Éd. Revue Banque 2008, p21

3. Classification des risques opérationnels selon Bâle II :

Le comité de Bâle, a adopté une classification assez précise des différentes catégories d'évènements opérationnels, et des lignes d'activités qui peuvent les générer. Ceci désigne une nomenclature des risques opérationnels qui constitue l'élément de base pour l'identification des risques de la banque.

3.1. Classification par type d'événement :

Selon la réglementation de Bâle II, la classification des risques opérationnels est de (07) risques, nous présentons ci-dessous les catégories de risque de niveau (1) :

- **Risque de Fraude interne** : Perte dues a des actes visant à frauder , détourner des biens ou à détourner des règlements, la législation ou la politique de l'entreprise impliquant au moins une partie interne à l'entreprise .
- **Risque de Fraude externe** : Perte dues à des actes visant à frauder, détourner des biens ou contourner la législation de la part d'un tiers.
- **Risque lié à des pratiques en matière d'emploi et de sécurité sur les lieux 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 au titre d'un dommage personnel ou d'atteintes à l'égalité /actes de discrimination.
- **Risque lié à des pratiques relatives aux clients, aux produits et à l'activité commerciale** : Pertes résultant d'un manquement, non intentionnel ou du à la négligence, à une obligation professionnelle envers des clients spécifiques (y compris exigences en matière de fiducie et de conformité) ou de la nature de conception d'un produit.
- **Risques liés à des dommages aux biens physiques** : Destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres
- **Risques de dysfonctionnement de l'activité et des systèmes** : Pertes résultante de dysfonctionnement ou de l'activité ou des systèmes.
- **Risques liés à des exécutions des opérations, les livraisons et les processus** : Pertes résultantes d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs.

3.2. Classification par type d'activités :

Afin d'assurer une identification exhaustive des risques opérationnels, il convient de découper l'activité de la banques en métiers et processus, ces derniers constituent la principale source de valeur ajoutée.
Chaque ligne de métier **(**Niveau 1**)** est détaillée en un ensemble de métiers **(**Niveau 2**),** puis découper en un groupe d'activités **(**Niveau 3**)**, le tableau ci-dessous explique ce découpage :

Tableau 1 : Ventilation des secteurs d'activité de la banque selon Bâle II.

Niveau 1	Niveau 2	Niveau 3
Financement des entreprises	Financement des entreprises	Fusion-acquisitions, engagement, privatisation, titrisation, recherche, titres de dette (Etat, haut rendement), actions, prêt consortiaux, introduction en bourse, placement sur le marché secondaire.
	Financement des collectivités locales, Administrations publiques	
	Banque d'affaire	
	Service-conseil	
Négociation et vente	Ventes	Valeurs à revenus fixes, actions, change, matières premières, crédit, financement, titres sur positions propres, prêts et pensions, courtage, titres de dettes, courtage de premier rang.
	Tenue de marché	
	Positions pour compte propres	
	Trésorerie	
Banque de détail	Banque de détail	Prêts et dépôts, services bancaires, fiducie et gestion de patrimoine.
	Banque privée	Prêts et dépôts, services bancaires, fiducie et gestion de patrimoine, conseils en placement.
	Cartes	Cartes de commerçant/ commerciales/ d'entreprises, de clientèle et commerce de détail.
Banque commerciale	Banque commerciale	Financement de projet, immobilier, financement d'exportations et du commerce, affacturage, crédit-bail, prêts, garanties, lettres de change
Paiements et règlements	Clientèle extérieure	Paiements et recouvrements, transferts de fonds, compensation et règlement
Fonctions d'agent	Conservation	Dépôts fiduciaires, certificats de titres en dépôt, prêts de titres (client), opérations de sociétés

	Prestations d'agent aux entreprises	Agents émetteurs et payeurs
	Service de fiducie aux entreprises	

Source : SAHLI EL-HACHEMI Aniss, « LE ROLE DE L'AUDIT INTERNE DANS LA MAITRISE DES RISQUES OPERATIONNELS AU SEIN DU SECTEUR BANCAIRE », MASTER 2 EN SCIENCES DE GESTION .OPTION : AUDIT COMPTABLE ET FINANCIER, MDI Business School, PROMOTION 2014 -2015, p 5

4. Risques spécifiques

Il s'agit en particulier des risques qui sont exclus de la nomenclature de Bale du fait de la difficulté de mesure qui y est associée, tels que les risques suivants :

4.1. Le risque d'image

Il consiste à donner à l'opinion publique une image assez négative de l'établissement, qui conduit à perdre des sources de financement et/ou certains de ses clients.
Certaines actions peuvent produire une impression négative durable pour l'ensemble des activités d'une banque, ce qui nuit sensiblement à sa capacité d'établir et d'entretenir des relations avec es clients. Si les pratiques utilisées, en ce qui concerne son aptitude à exécuter des fonctions vitales pour la poursuite de son activité, engendrent une perte de confiance importante, sa réputation peut être entachée.[1]

4.2. Les risques humains

L'être humain est l'une des principales ressources et valeurs de l'entreprise. Toutefois, il est nécessaire de l'encadrer et de le protéger avec attention.

Il a souvent été constaté que la survenance d'incidents suite à des causes humaines provenait d'un environnement propice qui regroupait plusieurs facteurs personnels ou associés au contexte de l'entreprise (stress permanent, surcharges, pression, insuffisance de formation et d'encadrement,….)[2].

4.3. Les risques juridiques

Les risques juridiques sont des risques qui découlent de la transgression ou du non-respect des lois, règles, règlements ou pratiques prescrites, mais aussi du fait que les droits et obligations juridiques des parties à une transaction sont mal définis.

[1] Eric LEMARQUE, «**Management de la banque : Risque, relation client, organisation** », 2éme édition, ED PEARSON, France, paris, 2008, P10.
[2] Idem.

Les banques peuvent être exposées à des risques juridiques en ce qui concerne la divulgation d'informations sur leur clientèle et la protection de la vie privée. Des clients mal informés de leurs droits et obligations peuvent engager une action en justice[1] .

4.4. Les risques stratégiques

Le comité de Bale, dans sa définition du risque opérationnel, exclu le risque stratégique.
Ce dernier est bien réel, mais peut difficilement faire l'objet d'une mesure d'impact précise.
Néanmoins, on peut le subdivisé en trois sous-catégories : les risques politiques, les risques de modification de la législation et les risques liés à l'évolution du marché.

4.5. Les risques systémiques

Le risque systémique est un événement soudain et inattendu dont la gravité est assez importante pouvant se dégénérer en crise affectant l'ensemble du système bancaire.

Le risque systémique est défini comme suit : « le risque que l'incapacité d'un acteur du marché à faire face à ses obligations entraine une réaction en chaine impliquant l'incapacité de la plupart des acteurs à assurer le bon dénouement de leurs opérations, aboutissant à la faillite de tout le système (principe de l'effet « dominons »).[2]

SECTION 3 : Le cadre réglementaire des risques opérationnels

Nous abordons à présent le volet consacré à la règlementation prudentielle en matière de risque opérationnel. Le comité de Bâle, organisme international d'où émane l'ensemble des directives et des recommandations, étoffe la réglementation prudentielle et la met à jour en réponse aux évolutions liées à l'environnement bancaire, en allouant une importance capitale aux exigences en fonds propres pour les établissements bancaires.

Trois (03) « accords » de Bâle constituent les piliers de la supervision bancaire. L'Algérie n'est pas restée en marge de cela, et les autorités de contrôle ont adapté la réglementation internationale aux spécificités du système bancaire national, notamment en matière de contrôle et de solvabilité.

1. Réglementation prudentielle internationale

Le comité de Bâle a été créé fin 1974 par les gouverneurs des banques centrales du G10 (actuellement G20*). Le Comité était initialement appelé le « Comité Cooke », du nom de Peter Cooke, directeur de la Banque d'Angleterre qui avait été un des premiers à proposer sa création et fut son premier président. Les travaux de Bâle visent à assurer la

---

[1] Idem
[2] Christian JIMENEZ et Patrick MERLIER, « **prévention et gestion des risques opérationnels** », ED REVUE-BANQUE, Paris, 2004 .P 63
* G20 : constitué de : huit principaux pays industrialisés (qui appartiennent au G-8) : Etats-Unis, Japon, Allemagne, Royaume-Uni, France, Italie, Canada et la Russie ; onze petits pays industrialisés ou pays émergents: Argentine, Australie, Brésil, Chine, Inde, Indonésie, Mexique, Arabie saoudite, Afrique du Sud, Corée du Sud, Turquie ; l'Union européenne.

stabilité et la fiabilité du système bancaire et financier. A travers l'établissement de standards minimaux en matière de contrôle prudentiel, la diffusion et la promotion des meilleures pratiques bancaires et de surveillance.

1.1 Présentation des accords de Bâle :

Afin de maintenir la stabilité du système bancaire, une évolution des accords de bale a été marquée, et cette évolution se fait en accord avec l'environnement économique ; En effet, les recommandations de Bâle sont revues régulièrement pour devenir peu à peu une obligation harmonisée à l'ensemble des banques. De Bâle I à Bâle II, puis Bâle III les banques doivent anticiper la feuille de route.

A. Accord de Bale I et ratio Cooke :

Face à la montée en puissance de la globalisation financière génératrice de véritables risques systémiques, le Comité de Bâle, a réagi en définissant un ratio de solvabilité nommé «***le ratio Cooke*** » en 1988 dit Bâle I, imposant que le ratio des fonds propres réglementaires d'un établissement de crédit par rapport à l'ensemble des engagements de crédit pondérés de cet établissement ne puisse pas être inférieur à 8% d'où sa forme s'exprime comme suit :

$$\frac{\text{Fonds propres réglementaires}}{\text{Encours risque de crédit pondérés}} \geq 8\%$$

Equation1 : Ratio de solvabilité Cook

Le succès de ce ratio est expliqué par sa simplicité. Toutefois, cette dernière ne correspond pas à la réalité des activités bancaires : trop complexe pour se traduire dans une addition de risques grossièrement pondérés. Il fallait qu'un nouveau dispositif propose aux banques des méthodes de calcul différenciées et une analyse plus fine et plus exhaustive de leurs risques.
Il devient rapidement évident par la suite qu'une refonte de l'Accord était nécessaire, ce que le Comité a réalisé à partir de 1999, débouchant sur un deuxième accord en 2004 : Bâle II.

B. Les trois piliers de Bale II :

Dans ses travaux de refonte des principes de surveillance des banques, le Comité de Bâle a décidé d'étendre les aspects de contrôle purement quantitatifs du ratio Cooke à un ensemble de mesures quantitatives et qualitatives complémentaires qui s'appuieront sur trois piliers :

Le premier pilier, qui reprend les dispositions de Bâle I, concerne les exigences minimales en fonds propres. Le deuxième pilier règle le processus de contrôle de la gestion des risques et de la couverture en capital par les autorités prudentielles nationales. Enfin le troisième pilier définit les obligations de publication imposées aux banques.

Pilier I : Exigences minimales de fonds propres :

Le ratio de solvabilité a été affiné pour donner naissance au ratio Mc Donough qui exige que les fonds propres de la banque s'élèvent au minimum à 8% du total des risques : de crédit, de marché et opérationnels. Sachant que les risques de crédit sont pondérés à 85%, de marché à 5% et opérationnels à 10%.

Ainsi la formule du ratio de solvabilité devient :

$$\frac{\text{Fonds propre réglementaires}}{\text{Risques pondérés de crédit+risques de marché+ risques opérationnels}} \geq 8\%$$

Equation2 : Ratio de solvabilité McDonough

Pilier II : surveillance prudentielle

Ce pilier repose sur une implication et une présence plus efficace des autorités de contrôle pour prévenir les défaillances des banques.

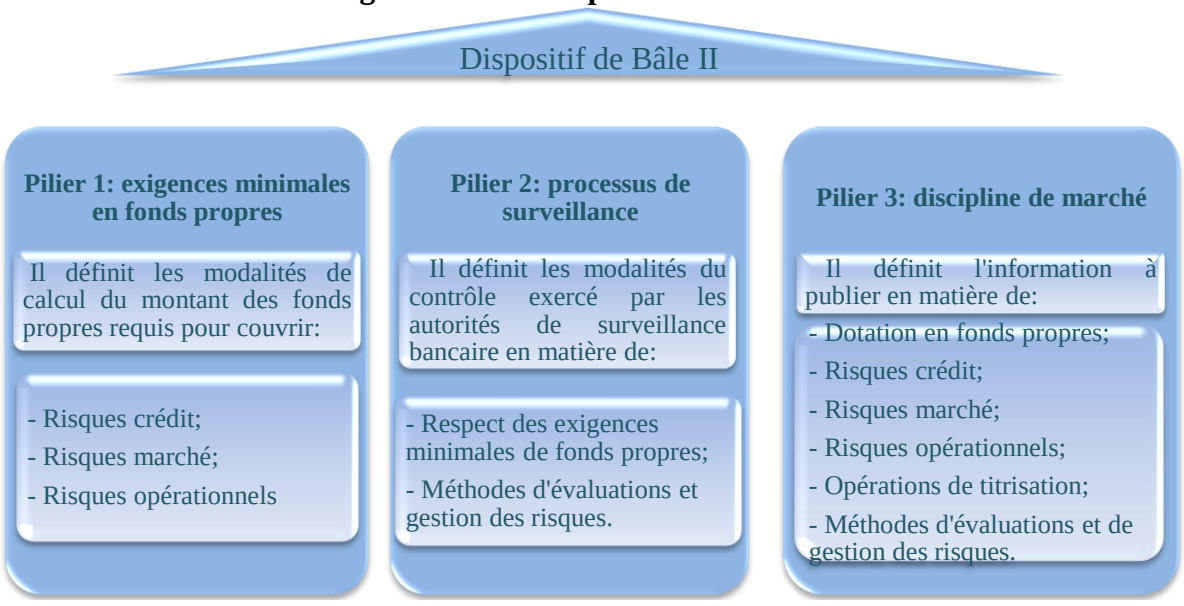
Chaque banque sera tenue de disposer d'un système permanent d'évaluation des FP (capitaux économiques) et d'une stratégie pour leur maintien. Les autorités de contrôle doivent apprécier ces dispositifs et prendre des mesures si elles ne sont pas suffisantes, elles peuvent aussi, au cas par cas, imposer des exigences de solvabilité supérieures au minimum réglementaire.

Pilier III : discipline de marché

Met l'accent sur l'amélioration de la communication financière dans une perspective de renforcement de la discipline de marché.

En effet, Une publication d'informations saines et complètes sur la nature, le volume, et les méthodes de gestion des risques, ainsi que sur l'adéquation des FP avec les risques encourus, est essentielle pour que les acteurs du marché disposant d'informations fiables puissent évaluer et comparer les banques.

Figure 2. Les trois piliers de Bale II.



Source : Pascal Dumontier et Denis Dupré ; « **Pilotage bancaire : Les normes IAS et la réglementation Bâle II** » ; Revue Banque Edition, Paris, 2005, page 124.

C. De Bale II à Bale III :

La dernière crise financière a montré les insuffisances des recommandations qu'a apportées Bale II. Ce qui a amené les autorités en charge de la régulation bancaire à en formuler de nouvelles.

Dans ce cadre, une révision du dispositif de Bale II a été réalisée dans un premier temps en Juillet 2009, sur le périmètre de la titrisation et des activités des marchés, pour aboutir en Décembre 2010 à un nouveau cadre prudentiel avec la signature des accords de Bale III. Les dispositions de cet accord visaient, le renforcement des recommandations des accords précédents, et la transition vers une nouvelle logique macro prudentielle visant à stabiliser le système financier dans son ensemble et à éviter les débordements vers l'économie[1].

Les principales mesures de Bale III sont[2] :

- Une amélioration de la qualité des fonds propres.
- Renforcement du niveau des fonds propres.
- Maitrise de l'effet de levier.
- Amélioration de la gestion de liquidité.
- Couverture des risques du portefeuille de négociation.

2 .Détermination des Exigences en Fonds Propres :

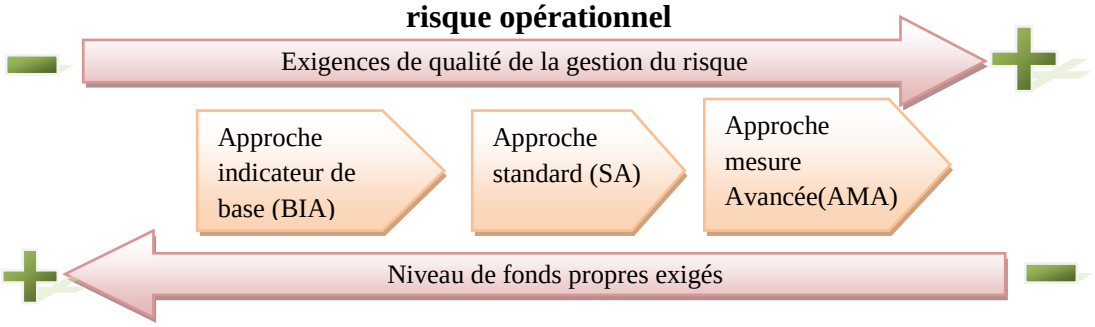
Bâle II instaure une mesure des exigences en fonds propres plus sophistiquées et plus sensibles à la qualité du risque.

Il existe trois approches pour évaluer le risque opérationnel[3] :

- Approche indicateur de base (BIA);
- Approche standard (SA) ;
- Approche mesure avancée (AMA).

Ces approches ont un ordre de sophistication croissant et plus la méthode est sophistiquée moins le capital réglementaire exigé serait élevé.

Figure 3. Classification des méthodes de calcul d'exigence en fonds propres pour le risque opérationnel



Source : C. JIMENEZ, P. MERLIER et D.CHELLY, «**Risques Opérationnels : de la mise en place du dispositif à son audit** », Edition REVUE BANQUE, 2008, p27.

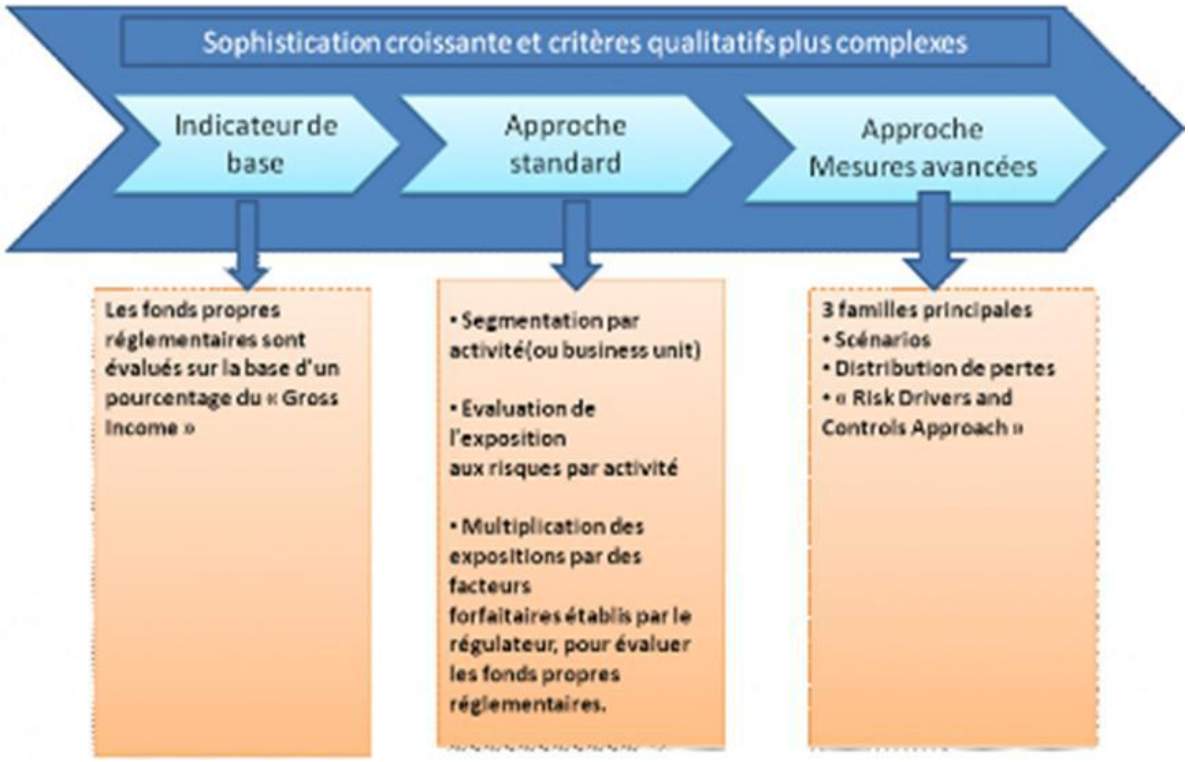
[1] Inspiré de l'article de : Bale 3 quel impact sur les métiers de la banque, EUROGROUP CONSULTING, Avril 2011, publié sur le site : http://www.eurogroupconsulting.fr/IMG/pdf/B3_M2_20110422_VF-2-2.pdf.

[2] Bale III : les impacts à anticiper, KPMG, Mars 2011 publié sur le site : http://www.kpmg.com/FR/fr/IssuesAndInsights/ArticlesPublications/Documents/Bale_III_impacts_a_anticiper_mars2011.pdf

[3] Dumontier PASCAL & Denis DUPRE, « **Pilotage bancaire : les normes IAS et la réglementation Bâle II** », Edition Revue Banque, 2005, p133.

Ces trois méthodes de calcul évolutives sont prévues par la réglementation par ordre croissant de complexité et de sensibilité au risque.

Figure 4. Les approches de mesure du risque opérationnel



Source : TANTAN Kawtar, « **Le processus de gestion et de mesure du risque opérationnel dans le cadre des règles et des saines pratiques prévues par le comité de Bâle** », thèse de master, université TIME , Tunisie, 2007/2008. Publié sur le site : http://www.memoireonline.com

L'usage de ces derniers doit impérativement être approuvé par les superviseurs nationaux (ex : Banque Centrale). L'approche retenue peut varier selon l'activité propre à la banque. Toutefois, le recours à l'approche standardisée ou à l'approche en mesures avancées est irrévocable. Ainsi, il n'est pas permis de revenir à une approche simple une fois qu'une approche plus sophistiquée a été adoptée.

2 .1. L'approche de l'indicateur de base (Basic Indicator Approch ou BIA) :

C'est la méthode la plus simple qui n'exige aucun critère d'éligibilité pour son application. Elle consiste à appliquer un pourcentage fixe (Alpha) à un indicateur représentatif de l'exposition potentielle aux risques opérationnels, et qui est le produit net bancaire moyen sur les trois dernières années :
Fonds propres risques opérationnels = $\alpha \times$ PNB total avec : $\alpha = 15\%$

2 .2. L'approche standard (Standard approch-SA) :

Cette seconde approche se situe entre l'approche BIA et l'approche de mesure complexe, ce qui revient à dire qu'elle est un prolongement de la première. Dans cette

approche, les activités des banques sont réparties en huit (08) catégories : financement des entreprises, négociation et vente, banque de détail, banque commerciale, paiement et règlement, fonctions d'agent, gestion d'actifs et courtage de détail. Le capital réglementaire est fonction d'un pourcentage du produit brut, appelé facteur Beta, établie à 12%,15%, et 18%, selon le niveau du risque opérationnel estimé de chaque activité. L'exigence de fonds propres est calculée en multipliant le produit brut par un facteur (bêta) spécifique.[1]

Identique à la précédente mais avec un pourcentage βi différencié par ligne métier :

FPRO = $\sum \beta_i$ * PNB_i

Tableau 2 : Facteurs Bêta de l'approche standardisée du risque opérationnel

Ligne d'activité	Coefficient β_i
Financement des entreprises (Corporate Finance)	**β_1=18 %**
Négociation et vente (Trading and Sales)	**β_2=18 %**
Banque de détail (Retail Banking)	**β_3=12 %**
Banque Commerciale (Commercial Banking)	**β_4=15 %**
Paiement et règlement (payment and Settlement)	**β_5=18 %**
Fonction d'agent (Agency Services)	**β6 =15%**
Gestion d'actifs (Assets Management)	**β7=12%**
Courtage de détail (Retail Brokerage)	**β8=12%**

Source : C. Jimenez, P. Merlier, «**Prévention et gestion des risques opérationnels** », Edition REVUE BANQUE, 2004, P 164.

2.3 L'approche avancée (Advanced Measurement Approaches – AMA) :

Cette approche plus complexe que les précédentes propose le calcul de l'exigence des fonds propres en s'appuyant sur un modèle interne développé par la banque et validé par l'autorité de tutelle.

L'utilisation de cette méthode suppose que la banque est capable d'exploiter les données internes de pertes liées aux risques opérationnels en se conformant à la décomposition en 8 lignes métiers et 7 catégories de risques, soit 56 couples possibles.

Le besoin en capital est calculé à partir de la mesure de la perte attendue pour chaque couple (*Expected Loss : EL*).

$EL = PE \times LGE \times E$

[1] SAIDANI Zahir, « **ANALYSE DU PROCESSUS DE GESTION DU RISQUE OPÉRATIONNEL PAR LES BANQUES** » , Mémoire en vue de l'obtention du diplôme de MAGISTÈRE EN SCIENCES ÉCONOMIQUES, OPTION : MONNAIE-FINANCE-BANQUE, UNIVERSITÉ MOULOUD MAMMERI. TIZI OUZOU , 2011/2012 ,p123

Avec :
PE : probabilité de l'évènement (probability of event).
LGE : perte en cas d'évènement (lost given by event).
E : Exposition au risque opérationnel.
PE et *LGE* sont déterminés d'après les modèles internes de la banque alors que *E* est donné par le régulateur.
Le besoin en capital s'obtient à partir de la somme des pertes attendues de chaque couple pondérées par un facteur spécifique fixé par le régulateur.
Fonds propres réglementaires = Σ_{ij} (y_{ij}× EL_{ij})

Le comité de Bâle incite les grandes banques à adopter les méthodes de calcul avancées pour développer leurs propres modèles et car elles devraient permettre un rapprochement entre les besoins de capital réglementaire et économique.

3 .Réglementation Prudentielle Nationale

La Banque d'Algérie (B.A) en tant que banque centrale a arrêté dans ce cadre de l'exercice de son autorité de régulateur, une règlementation exigeant des banques et institutions financières de surveiller les risques auxquels elles sont confrontées.
En matière de gestion des risques opérationnels, il convient de rappeler que la règlementation nationale adapte les règles prudentielles selon les spécificités du système bancaire national.
Nous citons notamment : le règlement BA 11-08 du 28 Novembre 2011 sur le contrôle interne et le règlement 14-01 du 16 Février 2014 portant coefficients de solvabilité applicables aux banques et établissements financiers.

3 .1 . Règlement Banque d'Algérie n°11/08 du 28 Novembre 2011 Portant sur le Contrôle Interne des Banques et Etablissements Financiers :

Ce règlement de la BA tenant modification et enrichissement du dispositif de contrôle interne des banques et établissements financiers, est officiellement entré en vigueur.
Publié au journal officiel du 29 Août 2012, ce règlement, qui abroge et remplace le règlement 02-03 du 14 Novembre 2002, est destiné à sensibiliser les banques et établissements financiers algériens sur la nécessité de mettre en place un contrôle interne efficace, qui leur permettra de s'aligner aux normes internationales et de se prémunir contre les risques de toute nature auxquels elles font face.

L'organisation du dispositif de contrôle interne est décrite plus en profondeur notamment dans les articles 37, 38, 58, 59 et 60, que doivent mettre en place les banques et établissements financiers pour mieux appréhender ses risques.
En matière de maîtrise des risques opérationnels, la règlementation Algérienne vient inciter cette fois-ci explicitement les banques et établissements financiers à se doter de dispositifs de gestion. Ce règlement fait référence à la cartographie des risques opérationnels qui est un outil d'appui au management de tout type de risques, cette dernière devient une solution de plus en plus appréciée à laquelle les banques et les établissements financiers Algériens doivent se mettre.

3.2. Règlement Banque d'Algérie n° 14/01 du 16 Février 2014 Portant Coefficients de Solvabilité Applicables aux Banques et Etablissements Financiers.

Ce nouveau règlement consacre les sept (7) premiers articles à la fixation des coefficients de solvabilité que les banques et établissements financiers doivent appliquer pour être en conformité avec la règlementation prudentielle.

Il porte les coefficients suivants :

- Le coefficient de solvabilité y est fixé à 9,5% par rapport aux fonds propres réglementaires ;
- La couverture des risques (crédit, opérationnel et marché) à 7% par rapport aux fonds propres de base ;
- L'établissement d'un « coussin de sécurité » à hauteur de 2,5% par rapport aux fonds propres de base.

Les articles 20 et 21 traitent du risque opérationnel. Le premier donne la définition du risque opérationnel du point de vue du législateur.

Le second article quant à lui, précise qu'en matière de couverture du risque opérationnel en Algérie, il y'a recours à l'approche dite « indicateur de base » : l'exigence en fonds propres est de 15% du PNB des trois derniers exercices.

En matière de couverture des risques opérationnels, la règlementation Algérienne vient exiger cette fois-ci rigoureusement des banques et établissements financiers à se couvrir contre toute éventualité des risques (crédits, marchés, opérationnels) par les fonds propres réglementaires tout en respectant des coefficients cités supra et dans le but de s'aligner aux normes prudentielles. La commission bancaire quant à elle, vient accorder aux banques et établissements financiers un délai supplémentaire pour qu'ils soient conformes aux nouvelles exigences comme elle peut leurs imposer d'intérêt systémique, des normes de solvabilité au-dessus à celles prévues.

Conclusion

L'importance accrue attribuée aux risques opérationnels, et due aux diverses crises ayant ébranlé le système bancaire et financier, ont incité les autorités en charge de la régulation bancaire internationale à prescrire des normes visant à atténuer les dégâts causés et à en éviter de nouveaux.

Dans ce cadre se sont inscrites les recommandations du comité de Bâle à travers la publication de trois accords visant la stabilité et le renforcement du système bancaire.

Il est à préciser que chaque publication du comité, était le fruit de la révision des différents problèmes et lacunes rencontrées par celles qui la précède.

Dans ce cadre, Bale I était le premier accord mis en place, dans le but d'instaurer des exigences réglementaires en fonds propres à travers le ratio Cooke. Cet accord a très vite montré ses insuffisances car il reposait sur des normes de calculs de fonds propres rigides.

A cet effet, s'est lancée la grande réforme de Bale II, dans le but d'élargir le champ de calcul des exigences en fonds propres des banques et des établissements financiers et d'y proposer une mesure plus fine en intégrant la notion du risque opérationnel.

Malgré les lacunes qui ont été reprochées par la suite à cette réforme avec les effets de la crise de 2008 et la mise en place d'un nouvel accord de Bale III, l'accord de Bale II reste la première base de référence en matière de risque opérationnel, à travers laquelle s'est tracé son périmètre et ses principale caractéristiques.

Ceci a été concrétisé par les différentes définitions données à ce risque par les autorités de régulation bancaires internationales ainsi que par la mise en place d'une nomenclature des risques donnant une classification des risques majeurs de la banque sur ces différentes lignes d'activités.

Chapitre II : Cartographie des risques opérationnels

La gestion des risques est devenue de nos jours, une préoccupation majeure pour les entreprises. En effet, Si une gestion infaillible des risques nécessite une identification et évaluation exhaustive.

Dans le dispositif de gestion des risques, la cartographie des risques constitue une pièce maitresse. Elle permet de disposer d'une vision globale et hiérarchisée des risques auxquels une organisation est exposée et autour de laquelle s'organise tout le management des risques.

Pour cela, Nous présentons dans ce second chapitre la Cartographie des risques opérationnels, à travers trois sections comme suit ;

Une première section «**le concept de cartographie des risques**» qui porte sur la définition du concept de la cartographie et met en avant ses objectifs, ses intervenants ces typologies et les différentes approches d'élaboration;

Une deuxième section «**Démarche d'élaboration de la cartographie des risques opérationnels**» ou nous allons présenter les fondements méthodologiques d'une démarche de cartographie des risques opérationnels en dépit de l'absence d'un référentiel commun en la matière.

Une troisième section « **Utilisation de la cartographie des risques »** ou nous évoquerons la nécessité de disposer pour l'organisme, d'un système de maintenance visant l'actualisation des résultats obtenus.

Section I : le concept de cartographie des risques

Cette section consistera à comprendre la notion de cartographie des risques, de préciser ses objectifs et son utilité.

1. Définition et objectifs de la cartographie des risques

La cartographie des risques a suscité beaucoup d'écrits. Nous allons procéder à sa définition et citer les différents objectifs qu'elle permet d'atteindre.

1.1..Définition de la cartographie des risques

Plusieurs définitions peuvent être cités, telle que :

« La cartographie est un mode de représentation et de hiérarchisation des risques d'une organisation »[1].

« La cartographie des risques est la représentation structurée d'un ensemble de risque identifiés et quantifiés dans un périmètre donné. C'est un outil visuel ayant pour objectif de donner au lecture de la cartographie une image immédiate de la situation »2.

« Une 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 les plus élevés et les moins significatifs (probabilité et /ou impact les plus faibles »3.

La cartographie des risques est, donc, un mode de représentation, d'hiérarchisation, de recensement, et d'évaluation des risques au regard des contrôles mis en place, en vue de diffuser une information qui mette en évidence d'éventuelles faiblesses résiduelles.

1.2 .l'Objectifs de la cartographie des risques

La cartographie a pour objet d'identifier, d'analyser, de classer, de comparer et de surveiller les risques susceptibles d'impacter une ligne de métier donnée et /ou l'établissement.

La cartographie des risques vise trois objectifs [4]:

- inventorier, évaluer et classer les risques de l'organisation ;

---

[1] **« la cartographie des risques** », op.cit, P15.

[2] Jean le ray, « **organiser une démarche de cartographie des risques** », AFNOR, 2008, P08.

3 IFACI et Price Water House Coopers, **« Le Management Des Risques De L'entreprise : cadre de référence et techniques d'application**», édition d'organisation, Paris, 2005, page 221

4 Serigne NDIAYE « **Elaboration d'une cartographie des risques opérationnels du cycle personnel /organismes sociaux : cas de la fondation agir pour la santé(FAES)** »institut supérieur de comptabilité, de banque et de finance, ISCBF, promotion 19 (2007-2008).

- Informer les responsables afin que chacun soit en mesure d'y adapter le management de ses activités;

- Permettre à la direction générale, et avec l'assistance du Risk manager, d'élaborer une politique de risque qui va s'imposer à tous :

- aux responsables opérationnels dans la mise en place de leur système de C.I.
- aux auditeurs internes pour élaborer leur plan d'audit, c'est-à-dire fixer les priorités.

2. Les types des cartographies opérationnelles

Le choix du type de cartographie dépend bien évidemment de la taille de l'organisation, de son portefeuille d'activité, ainsi que du type de risque étudié, toutefois, il existe deux grandes études qui peuvent se présenter :
- étudier l'ensemble des risques grevant l'organisation, donc il s'agit de réaliser une cartographie globale.
- étudier un risque spécifique lié à un domaine particulier, donc la réalisation d'une cartographie thématique.

2.1. La cartographie thématique :

« La cartographie thématique est un outil de recensement et d'hiérarchisation des risques liés à un thème précis »[1]

- soit différentes organisations (par exemple : différentes banques, ou directions) pour un même thème de risque (par exemple : le risque opérationnel)
- Soit différents domaines de risques liés au thème étudié pour une même organisation.

La cartographie thématique peut constituer un premier pas vers une cartographie globale.

2.2. La cartographie globale :

« Une cartographie globale des risques tend à recenser, quantifier et cartographier l'ensemble des risques d'une organisation, tous sujets confondus»2
On peut également la définir comme un ensemble de cartographies thématiques, car la consolidation des cartographies thématiques des différents risques pour chaque entité pourrait aboutir à une cartographie globale, sous l'hypothèse que tous les risques sont cartographiés et que toutes les entités sont prises en considération.

2. 3. Contraintes et Limites[3]:

Pour les deux types de cartographie, la principale contrainte est d'avoir une information fiable et nette pour calibrer les deux composantes du risque (probabilité et impact).

---

[1] « **La Cartographie Des Risques** », OP.cit, p18

2 Idem, p18

[3] Idem, p22

Cette contrainte pilotera, pour un thème donné, le choix du type d'axe et par conséquent, le choix du type d'information à collecter pour quantifier et cartographier ces risques. Parfois, elle résulte du refus de coopération des membres de l'entité, ces derniers peuvent refuser de fournir certaines informations ou des informations erronées craignant que leur mauvaise gestion soit dévoilée. En plus de cette contrainte, d'autres limites considérables peuvent influencer négativement une conception efficace et réussie de la cartographie des risques:

- S'agissant des processus ascendants, les résultats sont appropriés pour les opérationnels de l'organisation mais ne peuvent parler au top management ;
- Souvent, les évaluations sont beaucoup plus qualitatives que quantitatives puisqu'elles reflètent l'appréciation interne des opérationnels et la construction de base d'incidents n'est pas toujours possible ;
- La partie « moyens de maitrise » n'est en générale pas ou peu traitée ;
- Certains risques sont difficiles à évaluer et à étudier tels que le risque d'image et le risque de fraude ;
- La négligence et le désintérêt des principaux dirigeants surtout le directeur général concernant l'utilité et l'importance de la cartographie des risques.

3. les principaux facteurs de réussite d'une cartographie des risques

La réussite de la démarche d'élaboration de la cartographie des risques dépend des conditions suivantes [1]:

- Un soutien motivé de la Direction Générale ;
- Des objectifs clairs et bien communiqués ;
- La désignation du responsable du projet ;
- Une équipe de travail de qualité ;
- Et la disponibilité des moyens.

3.1. Soutien Motivé de la Direction Générale :

La décision d'application de tout outil de gestion des risques doit partir de la Direction Générale. Elle a de ce fait, une obligation d' « appropriation » de tous ces outils. Elle doit, en outre, faire comprendre et accepter sa politique de risque à toute la banque et surtout aux véritables propriétaires de ces risque (les opérationnels). Il est de ce fait impératif qu'elle s'implique dans le projet de cartographie des risques afin de faire émerger une vision consolidée, hiérarchisée et partagée des grands risques de la banque[2]

3.2. Objectifs Clairs et Bien Communiqués :

[1] FORTUGUE & al, « **cartographie des risques : quelle valeur ajoutée ? Quel processus ?** », 2001, www.amrae.asso.fr/lesrencontres/toulouse-2001.
[2] « **Comprendre et gérer les risque** », op ;cit, p9. .

La définition des objectifs est un pré requis en matière de cartographie des risques. Elle détermine l'approche qui sera menée. La définition de ces objectifs intègre également les motivations réelles. Il convient donc de savoir ce que l'on recherche[1]. Une fois ces objectifs déterminés, ils doivent, en outre, être parfaitement compris par le groupe de travail afin d'avoir une vision cohérente de la démarche à entreprendre.

3.3. Désignation du responsable du projet:

Le responsable du projet, il peut être un membre de la direction générale, du département d'audit interne ou le responsable chargé de la gestion des risques.

3.4. Equipe de Travail de Qualité :

La mise en place d'une équipe de projet chargée de piloter et de coordonner la démarche de cartographie des risques est indispensable [2] . Cette équipe doit être éventuellement 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.

3.5. Disponibilité des Moyens :

La réussite de tel projet nécessite la constitution d'une équipe disposant de tous les moyens indispensables, la mise à disposition d'un capital humain dynamique et expérimenté et des fonds (budget) pour sa réalisation.

Il n'existe aucune démarche standard de cartographie des risques. Cependant, il est question d'étapes clés d'élaboration et non de profil de risques. Les démarches de cartographie des risques s'intègrent, en effet, en général dans la culture et le fonctionnement de l'entreprise sont plutôt fonction d'autres facteurs.

4. Difficultés liées à la mise en place de la cartographie des risques :

La réalisation d'une cartographie des risques et notamment celle des risques opérationnels constituent un exercice d'introspection qui contraint chaque service. Cet exercice peut se heurter à plusieurs écueils.

- Possibilité de se heurter à un manque d'objectivité si la cartographie s'inscrit dans un cadre d'autoévaluation des risques.

- Les risques opérationnels sont par nature difficiles à appréhendés car ils ont un lien étroit avec l'organisation de la banque.
- La mesure des pertes liées aux risques opérationnels peut s'avérer être très compliquée. En effet, dans certains cas l'impact est étalé dans le temps (cas de contentieux client par exemple).
- Difficulté de maintenir une cartographie exhaustive et validée par les experts métiers.

---

[1] FORTUGUE & al, op.cit., consulté le 10/09/2015
[2] « **La Cartographie Des Risques** », op.cit., p34.

Section II : Démarche d'élaboration de la cartographie des risques opérationnels

Il est certain que la mise en œuvre d'une démarche de cartographie des risques dans l'industrie bancaire est assez spécifique puisque l'on veut aboutir au calcul de fonds propres règlementaire afin d'atteindre une gestion optimale des risques.

Nous aborderons cette section en posant la problématique suivante : quelle est la démarche suivre pour l'élaboration d'une cartographie des risques opérationnels ?

1. Approche d'Elaboration de Cartographie des Risques :

Les approches d'élaboration de la cartographie sont diverses et varient en fonction de l'activité exercée et des objectifs assignés par l'organisation, à la cartographie.
Il existe deux approches pour élaborer une cartographie des risques, à savoir:

- Le top-down ;
- Le bottom-up.

1.1. L'approche top-down « Descendante »:

Le principe de l'approche top-down consiste à désagréger une information mesurée sur la totalité des risques opérationnels de la banque et d'allouer ensuite ces fonds propres à des niveaux de plus en plus décentralisés. En d'autres termes, ce type d'approche calcule des frais financiers au niveau global de la firme. Les approches top down permettent des mesures homogènes avec celles des autres risques de crédit et de marché et ensuite permet de mesurer les corrélations entre une typologie de risques divergents. Les résultats postérieurs constituent un point de faiblesse pour l'approche top down tel que la quantification du risque opérationnel est seulement pour l'événement de risque qui a déjà eu une perte[1].

Tableau n°03 : Etapes de l'approche Top-Down

1	Identification des risques majeurs.
2	Evaluation des risques.
3	Rapprochement des risques avec la nomenclature des risques de l'organisation.
4	Rapprochement des risques avec les processus clés de l'organisation.
5	Etablissement d'une cartographie des risques.
6	Validation des risques par les principaux dirigeants.

Source : IFACI « **Cahiers de la recherche, la cartographie des risques** », 2013, page 46

[1] SAIDANI Zahir, « **ANALYSE DU PROCESSUS DE GESTION DU RISQUE OPÉRATIONNEL PAR LES BANQUES** », Mémoire en vue de l'obtention du diplôme de MAGISTÈRE EN SCIENCES ÉCONOMIQUES, OPTION : MONNAIE-FINANCE-BANQUE, UNIVERSITÉ MOULOUD MAMMERI. TIZI OUZOU , 2011/2012 ,p121

1.2. L'approche bottom-up « Ascendante » :

Dans cette approche, les risques opérationnels sont identifiés et évalués par les unités opérationnelles avant d'être portés à la connaissance du haut (La direction) via un dispositif de reporting au management.
L'identification des risques est effectuée par les personnes les plus proches de l'activité à travers des interviews. Il est souvent souhaitable d'utiliser une grille déterminée à l'avance, pour assurer que tous les risques possibles ont bien été évoqués au cours des interviews.
Cette approche est le plus souvent utilisée dans le cadre d'une cartographie globale.

L'approche bottom-up permet de fournir aux directeurs opérationnels et fonctionnels un outil leur permettant de visualiser les risques auxquels leurs services sont confrontés, pour mieux les gérer. Elle renforce également la communication entre les différents acteurs de l'organisation.

Tableau n°04 : Etapes de l'approche Bottom-Up

01	Identification des processus avec les opérationnels.
02	Identification et évaluation des risques inhérents à chaque processus.
03	Identification et cotation des éléments de maitrise de risques existants.
04	Cotation du risque résiduel.
05	Pilotage et communication.

Source : IFACI « **Cahiers de la recherche, la cartographie des risques** », 2013, page 41

2. Etapes d'Elaboration d'une Cartographie des Risques :

Il faudrait toutefois savoir qu'il n'existe pas de démarche standard de l'élaboration de la cartographie des risques imposée aux organismes, chacune doit tenir compte de ses propres spécificités pour un meilleur contrôle interne à condition qu'elle soit adaptée à la réglementation algérienne

Au terme de nos différentes lectures, on peut en déduire qu'il y a trois (03) phases lors d'une démarche d'élaboration d'une cartographie des risques :

- La phase de préparation ;
- La phase de planification ;
- La phase d'action ;

2.1. La phase de préparation

Avant de commencer une cartographie des risques, il faut, tout d'abord, déterminer son périmètre dans l'organisation. En effet, c'est la phase la plus importante, car elle permet de structurer et d'organiser la future cartographie. Elle doit nous permettre de définir avec précision :

- Le thème étudié : il s'agit de définir avec précision le périmètre qualitatif du risque étudié, c'est-à-dire définir, avec précision et exhaustivité, le risque en question.

- Le périmètre d'activité couvert : s'agit-il des risques informatiques d'un service, d'une direction spécifique, ou de l'ensemble des directions de la banque, ou l'ensemble des directions d'une région bien déterminée.

- Le niveau des réponses : selon l'objet de la cartographie, les chefs de projet doivent préciser est-ce que l'on veut une réponse par opération, par branche d'activité, par filiale, ou bien par service au sein de chaque filiale ?

- Le seuil de pertinence : pour chaque étape, le responsable devrait prendre en compte la stratégie globale de l'entreprise concernant son « appétence » au risque et devait s'assurer du soutient de la direction et des opérationnels, dans sa démarche. Pour homogénéiser les réponses, il faut déterminer des seuils d'appétences des risques parce qu'elle encadre la prise de risque en fixant les limites des impacts qu'un organisme est prêt à accepter.

- La règle de mesure du risque : il s'agit de définir le type d'axes, et pour chaque axe la métrique utilisée, c'est-à-dire la grille de notation.

Dans cette phase, il s'agit aussi de mettre en place la cartographie des processus car afin de mener à bien la démarche de management des risques dans une organisation, il faut, d'abord, la connaitre et pour cela, la disponibilité d'une cartographie des processus apparait comme un préalable logique.

2.1.1. Définition d'un processus :

Un processus est généralement défini comme :
« Un processus est un ensemble de ressources et d'activités liées qui transforment des éléments entrants en éléments sortants, autrement dit, c'est une boite noire qui a une finalité (les données de sortie) et qui, pour atteindre cette finalité, utilise des éléments extérieurs »[1].

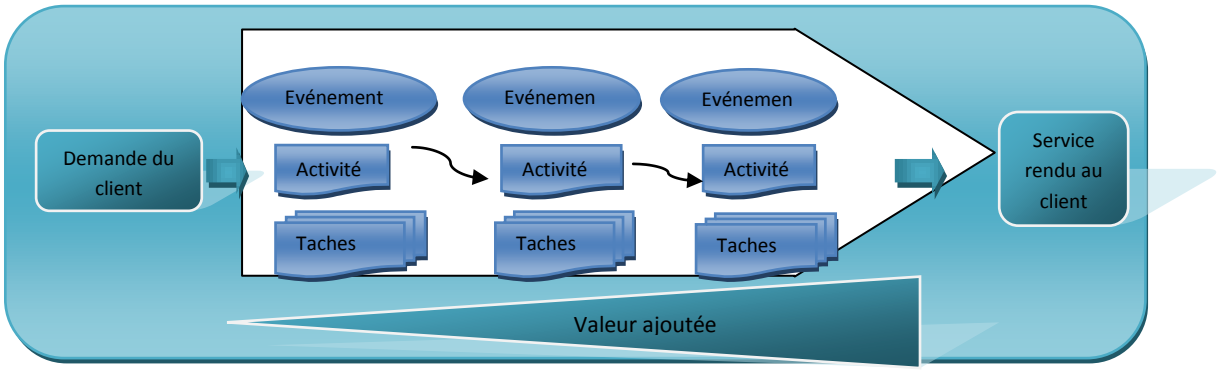
Et plus précisément on peut définir un processus comme «l'enchainement ordonné d'un ensemble d'activités, produisant une valeur ajoutée croissante, permettant de délivrer au client (interne ou externe) le produit ou service correspondant à sa sollicitation initiale »[2]

D'une manière générale, les processus donnent une image de l'ensemble des savoir-faire de l'entreprise. Et qu'il est bon de les identifier, de les décrire, de les munir d'indicateurs, pour les améliorer sans cesse, voire d'en corriger les défauts.[3]

---

[1] Y.mougin, « **la cartographie des processus, édition d'organisation** », paris 2004, P 37.
[2] C. Jimenez, P. Merlier, prévention et gestion des risques opérationnels, Revue Banque, septembre 2004, p 25.
[3] Y.Métayer, L. Hirsch, « **Premiers pas dans le management des risques** », Edition afnor, Paris, 2007, P 62

Figure 5 : Représentation schématique d'un processus



Source : C.Jimenez, P.Merlier, D.Chelly , **Risques opérationnels**, , revue banque, 2008, p57.

2.1.2 Les différents types de processus :

On peut distinguer trois types de processus :

- Les processus opérationnels (processus métier ou de réalisation) :

Ceux sont les processus dont l'objectif est de fournir des produits et services aux clients, depuis l'expression du besoin jusqu'à sa satisfaction.

- Les processus de pilotage (ou managériaux) :

Ceux sont les processus de management. Ils servent à fixer des orientations, à évaluer la situation et de définir les actions correctives.

- Les processus de support:

Qui sont relatif à la bonne gestion : la gestion de la ressource humaine, la finance, la comptabilité, l'informatique et la logistique.

2.1.3. Les caractéristiques d'un processus

« Il s'agit de définir le niveau de granularité de description. Un détail des processus trop léger amènera à une mauvaise interprétation de la nature et du niveau de risque »[1]

Ces caractéristiques sont communes à toutes les catégories de processus,

- Un point de départ : évènement déclenchant ;
- Un point d'arrivée : il s'agit du résultat final ;
- Les intervenants au cours du processus (employés, directeur, membres du directoire...) ;
- Un enchainement d'une série d'étapes regroupant chacune un ensemble de taches ;
- Création de la valeur ajoutée entre l'entrée et la sortie.

2.1.4 Lien entre risques et processus

« Afin de sélectionner les bonnes politiques face aux risques, il est nécessaire de comprendre comment les risques affectent les processus de l'organisation »[2].

---

[1] Philippe DENIAU and Etienne RENOUX , « **la cartographie du risque opérationnel : outil réglementaire ou outile de pilotage ?;** » revue d'économie financière, NO 84 ;LE RISQUE OPERATIONNEL ; juin 2006 .P164 ;

[2] Henri FRITCH, « **La maitrise des risques lié aux processus de gestion des réclamations clients** », Thèse professionnelle présentée et soutenue en vue de l'obtention du Mastère spécialisé « Audit Interne et Contrôle de Gestion », Paris, 2012, p47

En effet, le lien entre risques et processus s'exprime par la « matrice processus/risques » qui se présente comme suit :
Les processus (en ligne) se croisent avec les risques (en colonne), et afin d'évaluer les associations, pour chaque croisement (processus associé aux risques), le lien doit être qualifié soit de :
- Lien primaire : « le processus joue un rôle direct dans le management des risques ».
- Lien secondaire : « le processus contribue à gérer le risque de manière indirecte ».

2.1.5 La démarche de la cartographie des processus :

Dans le cadre d'une cartographie des risques opérationnels, il n'est pas nécessaire d'analyser les processus dans le détail. En effet, un niveau de détails trop élevé ne permet pas d'appréhender avec précision les risques et, une description trop fine peut nuire à la lisibilité du processus. Elle peut conduire à une mauvaise interprétation de la nature et du niveau de risque. L'idéal serait d'aller à un niveau de détail qui permettrait d'identifier les risques et définir des plans d'action qui serviraient à les diminuer.
Il est primordial de répertorier les processus auxquels la démarche consiste à répondre aux questions suivantes : Quoi faire ? Par qui ?

Pour quelle valeur ajoutée ? A quelle échéance ?

Il s'agit d'analyser les processus de la banque afin de faire ressortir les différentes tâches et modes opératoires ainsi que les intervenants.
Cette décomposition des processus permet non seulement de détecter les différents risques liés à chaque opération mais de déterminer en plus les points de contrôle et d'évaluer leur efficacité.

2.2. Phase de Planification :

Elle constitue la phase la plus importante dans la démarche d'élaboration de la cartographie, et citée par tous les auteurs que nous avons déjà évoqués supra, elle offre aux dirigeants la possibilité de prendre des décisions en matière de gestion et management des risques.
Cette phase se déroule en un certain nombre d'étapes, à savoir :

- Identification des risques ;
- Evaluation des risques ;
- Hiérarchisation des risques ;
- Appréciation du dispositif de maitrise des risques ;
- Détermination des risques résiduels ;
- Matrice des risques.

2.2.1. Identification des Risques :

Il s'agit d'identifier tous les évènements générateurs de risques qui peuvent se produire lors d'un processus et qui pourraient avoir des conséquences sur son déroulement ou le non atteint des objectifs[1].

[1] « **Comprendre et gérer les risqué** », op.cit, Edition d'Organisation, 2002, p42.

A .Techniques d'Identification des Risques Opérationnels :

L'identification des risques est une opération difficile et décisive dont il faut admettre, à priori et sans frustration, quelle que soient les méthodes utilisées.

Vue la gravité de l'impact engendrée par les risques opérationnels non maîtrisés, on utilise des techniques d'identification des risques potentiels dont nous citons ici quelques-unes:

- Identification basée sur les actifs créateurs de valeurs ;
- Identification basée sur l'atteinte d'objectif : Comme souligné dans la définition du risque, un risque peut entraver l'atteinte d'objectifs, il convient donc de le définir avant de le lier aux menaces correspondantes ;
- Identification par analyse historique : cet outil suppose l'enregistrement systématique des incidents et permet de garder la traçabilité ce que donne une base historique riche d'enseignements. L'existence de sinistres passés permet de mieux prévenir les risques et permet une meilleure estimation de la probabilité d'occurrence et de la gravité.
- Identification basée sur l'analyse de l'environnement : elle a pour but de souligner les menaces pouvant se présenter qu'elles soient d'origine technologique, économique, socioculturelles… ;
- Identification par analyse des activités : Après une décomposition des processus en activités, une estimation des conséquences potentielles de la bonne ou mauvaise exécution des tâches est requise.

B. Outils d'Identification des Risques Opérationnels

- **Le questionnaire :** Il permet notamment d'obtenir des informations relatives à l'exécution des tâches et de ce fait la constatation des dysfonctionnements et l'identification de celles mal comprises par les exécutants.
- **L'interview :** C'est une technique qui se base sur une grille déterminée à l'avance pour s'assurer que tous les risques possible ont été évoqués au cours de l'interview. Elle est utilisée dans le cadre d'une démarche bottom-up.[1]

2.2.2 Evaluation des Risques :

Cette approche peut être réalisée par des évaluations historiques (événements survenus) et prospectives (événements qui pourraient survenir) qui s'effectuent à dire d'expert c'est-à dire sur les déclarations des collaborateurs.
La méthodologie d'évaluation des risques d'une organisation repose sur un ensemble de techniques quantitatives et qualitatives[2]:

- La méthode quantitative *:* Cette méthode est utilisée lorsqu'il existe suffisamment d'informations (historique des incidents) permettant d'estimer la probabilité

---

[1] « **la cartographie des risques** », op.cit. p16.

[2] Idem, p 9

d'occurrence ou l'impact d'un risque sur la base d'évaluation par intervalle ou ratio.

- La méthode qualitative *:* moins fiable que la méthode précédente, elle est utilisée lorsque les risques ne peuvent pas être quantifiés ou lorsqu'il n'existe pas suffisamment de données fiables. L'évaluation, présentée sous forme d'un tableau à double entrée, va porter sur l'appréciation de l'impact du risque (financier ou d'image) ainsi que de la fréquence de survenance des événements retenus :

A. La fréquence : elle mesure la probabilité de réalisation de l'évènement de risque. Elle peut être mesurée grâce à :

- Des critères qualitatifs : une fréquence forte, moyenne ou faible ou sur une échelle de 1 à 3 par exemple.
- Des critères quantitatifs : une probabilité effective pour une période donnée (et comprise entre 0 et 1) ou la fréquence (une fois par jour, par mois , par an …etc.).

B. L'impact : c'est la quantification de la perte engendrée par la réalisation du risque, cette perte peut s'exprimer :

- De manière qualitative : impact fort, moyen ou faible ou sur une échelle de 1 à 3 par exemple.
- De manière quantitative : par des données de pertes financières ou d'exploitation.

2.2.3. Hiérarchisation des Risques :

Pour passer à la hiérarchisation des risques, il faut que l'évaluation des risques soit terminée pour simplifier leur gestion.

Il existe une multitude de risques au sein de l'organisation et il n'est pas possible de tous les contrôler, c'est pourquoi il est important de hiérarchiser les risques pour se concentrer sur les risques prépondérants afin d'améliorer le dispositif de leur gestion et préparer des plans efficaces pour définir les actions à mener en priorité pour maitriser les risques et les ramener à un niveau acceptable.

2 .2.4. Appréciation du Dispositif de Maitrise des Risques :

Pour chaque risque identifié et évalué, nous identifierons le dispositif de maitrise existant, en l'occurrence le contrôle mise en place pour parer à l'éventualité de survenance du risque.

L'efficacité du DMR réduit le risque brut et l'impact procréant une mauvaise image de la banque induit par ce dernier. Les DMR peuvent être de trois natures :

- Instructions /Dispositions
- Contrôles manuels / Visuels
- Contrôles automatiques /Outils (appareils, machines…).

L'échelle de cotation peut varier, par exemple de 1 à 5 (5 : adéquat, 3 : moyennement efficace, 1 : non adéquat, par exemple). Les outils généralement utilisées en la matière, sont en général les questionnaires de contrôles internes, les progiciels d'Audit…etc.

Le dispositif de maitrise des risques ayant été évalué, il convient de procéder à l'évaluation des risques résiduels.

2.2.5. Détermination des risques résiduels:

Le risque net mesure l'impact que l'organisation pourrait effectivement subir en termes financiers et d'impact d'image, en intégrant les dispositifs de prévention et de détection existant.
Le risque résiduel peut être évalué comme suit[1] :

Risque résiduel = impact résiduel × probabilité résiduelle
= (impact inhérent × probabilité inhérente) - évaluation du contrôle interne.
Pour la cotation, les risques résiduels, le classement se fait de la même manière que les risques inhérents (bruts).

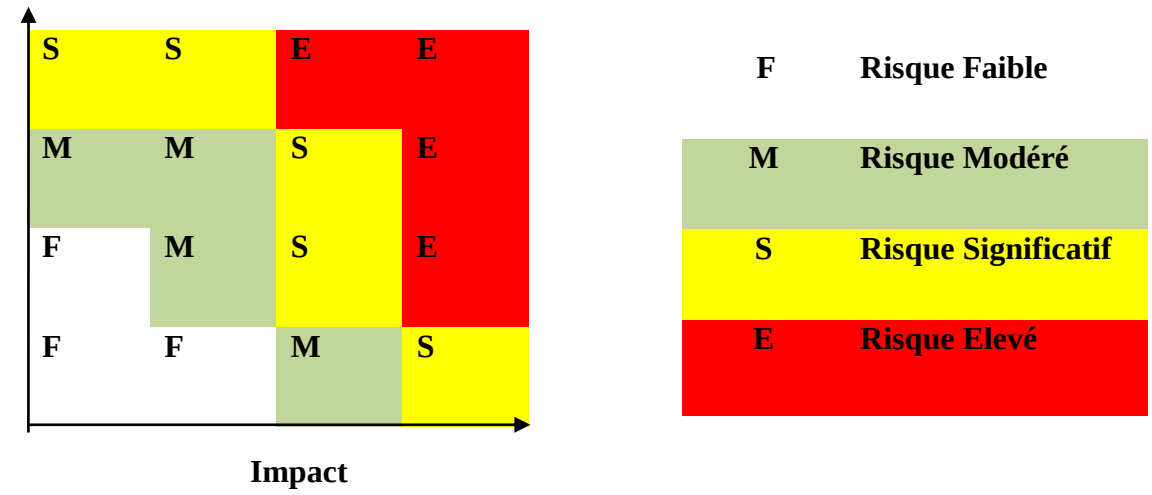
2 .2.6. Matrice des risques:

Il s'agit d'un graphique à deux axes, traditionnellement : probabilité et impact.
La représentation graphique offre une vision sur les risques majeurs et permet d'identifier les zones à traiter prioritairement.
Il existe plusieurs manières de représenter une cartographie notamment :

A. Le diagramme à deux axes :

Les risques sont représentés à l'aide des caractéristiques « fréquence » et « impact ». La gravité ou impact correspond à l'axe des ordonnés « Y» et la fréquence ou probabilité à celui des abscisses « X ».

Figure n°6 : Le diagramme à deux axes



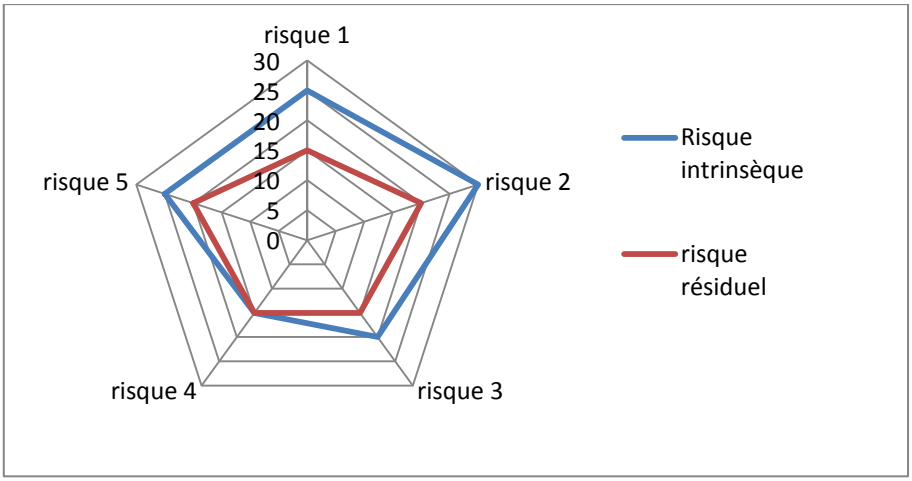
[1] IFACI, « **guide d'audit cartographie des risques** », Edition Les Cahiers de la Recherche, 2006.

Source **: « cartographie des risques »,** IFACI, op.cit, p 39

B .La représentation en mode RADAR ou toile d'araignée

Le principe de ce type de représentation est d'avoir une vue d'ensemble de l'exposition de l'organisation au risque, en fonction de son appétence. Pour ce type de cas, l'échelle représente la criticité d'un risque (coefficient multipliant la gravité par la probabilité d'occurrence. C'est un diagramme à plusieurs axes, où chaque axe représente une catégorie bien précise de risque.

Figure n°7 : Diagramme radar des risques d'une organisation



Source : « cartographie des risques », IFACI, op.cit, p 39 »

2.3. Phase d'Action :

Une fois en possession de la matrice des risques, l'entreprise peut alors décider des mesures à prendre pour chaque risque, en commençant idéalement par ceux qualifiés de majeurs à l'issue de la phase de hiérarchisation. Avant de mettre concrètement des plans d'actions, il faut effectuer un certain nombre de choix stratégiques entre les différentes alternatives que sont[1]: accepter le risque, réduire le risque, transférer le risque, l'éviter ou le supprimer.

Pour cela, il faut tenir compte de « l'appétence » de l'entreprise pour le risque, c'est-à-dire le niveau de risque que l'entreprise est prête à tolérer et assumer pour atteindre ses objectifs (niveau de risque admis) et de délimiter ainsi le risque cible, zone de risque jugée acceptable par les dirigeants. Dans la plupart des cas, les actions pour réduire le risque consistent à mettre en place des contrôles complémentaires ou différents de ceux en vigueur[2]. Mais dans ce cas, un arbitrage est nécessaire entre l'espérance d'économie de

[1] « **Comprendre Et Gérer Les Risque** »,, op.cit., p42.
[2] KERBEL Pascal, **« mise en oeuvre d'un contrôle interne efficace** », Edition AFNOR, 2007, p30.

coût résultant des mesures proposées et le coût de la mise en place et de la maintenance de ces mesures, selon les orientations stratégiques de l'organisation[1].

3. actualisation de la cartographie des risques :

La cartographie des risques est élaborée à un moment donné et constitue une image du profil de risque à un temps T déterminé, d'où le besoin de l'actualiser, la revoir et l'adapter périodiquement.
En général, cela se fait annuellement mais il est clair qu'à chaque fois qu'un incident se produit ou qu'un changement ayant un impact sur un événement à risque survient, la mise à jour de la cartographie doit s'opérer.
Dans ce cas, cela se traduira vraisemblablement par une augmentation de l'évaluation d'un risque.

En outre, s'il s'agit du lancement d'un nouveau produit ou la promulgation d'une nouvelle règlementation, les risques qui y sont liés seront introduits dans la cartographie.

Il est vrai que le projet de cartographie des risques représente un exercice qui peut être qualifié de « lourd » si l'on considère toutes les personnes mobilisées et le temps y alloué ; Cependant son actualisation est beaucoup plus simple.

Section 03 : Utilisation de la cartographie des risques :

L'objectif de Cette section est de présenter trois axes élémentaires, qui constituent le domaine d'utilisation, par excellence, de la cartographie des risques.

1 .La cartographie des risques permet une adaptation des contrôles

Une fois la cartographie des risques finalisée, elle offre une vision synthétique des risques de la banque, laquelle permettra aux managers de l'utiliser car elle représente un outil précieux d'aide à la décision et de détermination des missions de contrôle.

Le contrôle interne doit concerner toutes les fonctions de la banque, toutes ses directions, opérations et activités .Celui ci ne peut être mis en place de manière globale mais doit plutôt être composé de plusieurs sous dispositifs, chacun concernant une fonction particulière de la banque.

Il est à noter également qu'il est important de ne pas perdre de vue le caractère relatif de contrôle interne dans le sens qu'il ne peut éliminer le risque mais juste le réduite a l'égard des limites qu'il présente.

1.1 Définition du contrôle interne :

Le contrôle interne est un concept complexe qui, s'est adapté à l'évolution de la gestion d'entreprise. Afin de mieux l'appréhender, une présentation assez complète par le COSO est jugée nécessaire à présenter.

---

[1] COUCHOUD Christian, « **risques opérationnels, chronique d'une mise en place commune d'intérêt** », horizons bancaire, 2004, P53.

Il existe plusieurs définitions de l'audit interne. Nous allons citer les plus utilisées entre elles :

- **Définition du « Consultative Committee of Accountancy » de Grande-Bretagne donnée en 1978 :**« Le contrôle interne comprend l'ensemble des systèmes de contrôle, financiers et autres, mis en place par la direction afin de pouvoir diriger les affaires de l'entreprise de façon ordonnée et efficace, assurer le respect des politiques de gestion sauvegarder les actifs et garantir autant que possible l'exactitude et l'état complet des informations enregistrées ».
- **Définition de « l'American Institute of Certified Public Accountants », en la même année 1978** :« Le contrôle interne est formé de plans d'organisation et de toutes les méthodes et Procédures adoptées à l'intérieur d'une entreprise pour protéger ses actifs, contrôler l'exactitude des informations fournies par la comptabilité, accroître le rendement et assurer l'application des instructions de la direction. »
- **Définition du COSO (Committee of Sponsoring Organization of the Treadway Commission)**
  Selon COSO 3[1]Le contrôle interne est définit comme « un processus mis en œuvre par le Conseil, le management et les collaborateurs, et qui destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, aux reporting et à la conformité ».

Ces définitions nous permettent de dégager les idées principales qui suivent :

- Le contrôle interne est moyen est non une fin en soi, c'est un outil dont la dimension est universelle et relative, il concerne toutes les fonctions de l'entreprise tout en évitant les systèmes qui freinent l'évolution et nuisent à l'efficacité ;
- Le contrôle interne permet de donner une assurance raisonnable de la maîtrise des risques opérationnels, mais pas totale; le cas de l'affaire kerviel de la Société Générale où un seul homme a réussi, par le jeu des options, à causer une perte de 4,9 milliards d'euros, en fait une bonne illustration ;
- Le contrôle interne ne se superpose pas à l'organisation de l'entreprise, il en fait partie intégrante et n'a pas d'existence indépendante ou autonome. Il nait et se développe au sein de l'organisation. Il est mis en œuvre par l'ensemble du personnel, c'est l'affaire de tous, sa finalité est la maîtrise des activités.

1.2. Le Dispositif de contrôle et de maîtrise des risques opérationnels

La constitution d'un dispositif de contrôle et de maîtrise des risques opérationnels repose sur deux étapes essentielles :

[1] Le coso 2013 est une mis à jour du référentiel de 1992 portant sur le contrôle interne.

1.2.1. La construction d'un référentiel de contrôle cible :

Le référentiel du contrôle peut être présenté sous forme de points de contrôles ou d'une série de questions, il présente plusieurs avantages[1] :

- Il détermine la cible à atteindre en matière de contrôle, ainsi il permettra une réévaluation périodique du dispositif existant ;
- Il intègre les grands principes de contrôle interne, comme les séparations de fonction ainsi que l'ensemble des réglementations applicables et des normes déontologiques ;
- Il contient également les plans de continuité d'activité qui sont l'unique moyen de couvrir les risques de sinistres, à fréquence d'occurrence faible mais à impact très élevé.

La pertinence de ce référentiel cible de contrôle dépendra de sa validation par les opérationnels afin qu'il soit adapté à l'organisation de la banque.

1.2.2. L'évaluation des dispositifs de contrôle existants :

L'évaluation des dispositifs de contrôle interne et de maîtrise des risques opérationnels est basée sur la définition des écarts entre le référentiel cible préétabli et les dispositifs de contrôle existants dans la banque.
L'analyse des écarts permettra de mettre en place des plans d'action destinés à sécuriser les processus, diminuer les risques, éliminer les anomalies détectées.
En effet, la détermination des risques nets se fait à partir des risques bruts et de la qualité de contrôle interne existant**.**
L'évaluation des dispositifs de contrôle interne est donc une étape essentielle des démarches de gestion des risques opérationnels, permettant à la fois de déterminer les risques nets en justifiant le résultat obtenu et de prévoir des plans d'actions afin de sécuriser les processus.

1.2.3. L'auto-évaluation des risques opérationnels :

L'auto-évaluation est une démarche périodique à l'initiative des dirigeants, mise en œuvre par les opérationnels afin d'évaluer l'efficacité du contrôle interne de leurs propres activités ». La gestion des risques opérationnels, à travers l'utilisation de l'exercice d'auto-évaluation est une méthode utilisée par la majorité des grandes banques dans le monde afin qu'elles évaluent les risques opérationnels auxquelles elles doivent faire face.
Chaque banque a sa propre méthode d'auto-évaluation mais elles s'articulent toutes autour des points suivants :

- Identifier et évaluer les risques bruts ;
- Évaluer la qualité des dispositifs de prévention et de contrôle en place permettant de réduire ces risques ;
- Déduire l'exposition aux risques nets ;
- Mettre en place un plan d'action pour pallier aux insuffisances détectées.

---

[1]Marie-Agnès Nicolet, Michel Maignan**, « Méthodologie Contrôle interne et gestion des risques opérationnels** », Revue Banque, nº668, Avril 2005

Elle permet aux personnes qui sont impliquées dans l'exécution des contrôles de s'auto évaluer et d'identifier les faiblesses et les défaillances des contrôles qu'ils mettent en œuvre eux mêmes. Son avantage est qu'elle moins couteuse, ses inconvénients est une réduction du degré d'objectivité.

2. La cartographie des risques, un outil pour le plan d'audit interne

La cartographie sert à l'audit interne de moyen pour déterminer le plan de missions, étant donné que la fréquence des missions sur un domaine est basée sur l'importance du risque de ce dernier.

2.1. Définition de l'audit interne :

L'audit interne est une fonction qui a connue plusieurs définitions, mais celle qui parait la plus appropriée est la définition officielle présentée par l'IIA, qui a été approuvée en juin 1999 par les instances dirigeantes de ce dernier.

- **Définition internationale de l'audit interne : (IIA)**

« 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 mangement des risques, de contrôle, de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité »[1].

Cette définition fait ressortir certains points :

- L'Audit Interne est une activité indépendante qui apporte une assurance objective et des conseils pour fournir une valeur ajoutée et améliorer les opérations de l'organisation.
- Il aide l'organisation à accomplir ses objectifs en apportant une approche systématique et disciplinée pour évaluer et améliorer l'efficacité de la gestion des risques, le contrôle et le gouvernement d'entreprise.

2. 2 Caractéristiques de la fonction d'Audit Interne

À partir de la définition officielle de l'audit interne citée ci-dessus, trois caractéristiques sont associées à la fonction de l'audit :

- L'universalité :

L'audit interne est une fonction **universelle**, elle concerne toutes les entreprises quelque soit leur statut juridique et le secteur d'activité dans lequel elles activent, toutes les fonctions, les structures, et les opérations.

- **L'indépendance :**

[1] **« théorie et pratique de l'audit interne, éditions d'organisation »**, op-cit, P 73.

L'audit interne est une fonction **indépendante,** qui est une condition essentielle pour l'exercice du métier, l'auditeur doit être indépendant des activités qu'il contrôle et de toute influence qu'il peut subir. Cette indépendance va lui permettre d'apporter un jugement fondé et sans influence.

- **La périodicité :**

L'audit interne est une fonction **périodique,** ce qui veut dire qu'elle s'effectue d'une manière ponctuelle et discontinue dans le temps et cela par rapport aux auditeurs internes, qui interviennent en fonction de la nature et de l'importance du risque à auditer.

2 .3. Le rôle de l'audit interne dans l'appréciation de la cartographie des risques

Une fois la cartographie des risques est établit, elle constitue l'outil de mesure dont va s'emparer l'auditeur interne.

La cartographie des risques permettant le pilotage de la gestion du risque en identifiant les domaines d'actions prioritaires, sert de base à la programmation des missions d'audit en effet, cet outil permet, par une confrontation entre l'opinion des opérationnels et de l'audit, une rationalisation de la démarche du département d'audit.[1]

3. La cartographie des risques, Un outil d'aide à la décision

Vu que la cartographie représente le profil de risque de l'entité, elle est déterminante et sert de repère pour la gestion des risques et le choix des plans d'actions. Elle permet donc de[2]

- Déterminer les risques prioritaires et les processus jugés trop risqués ;
- Définir une nomenclature de la base d'incidents opérationnels pour le rattachement des risques avérés ;
- Définir les plans d'action pour le traitement préventif des risques en améliorant le contrôle permanent ;
- Recourir au transfert ou au financement du risque ;

Bien entendu, les plans d'action prennent en compte les dispositifs de maitrise des risques existants et une fois mis en place, ils doivent être suivis et éventuellement ajustés.

[1] ALBRAND Guy, « le risk assessement : quelques bonnes pratiques, revue française d'audit interne, 2003, P06.

[2], « **Risques opérationnels-de la mise en place du dispositif à son audit** », op-cit, p103.

Conclusion

Ce chapitre s'est voulu de démonter : l'importance de l'élaboration d'une cartographie des risques au niveau d'une organisation bancaire, la méthode à entreprendre dans son façonnement, ainsi que les différents outils et approches nécessaire à son accomplissement.

Il apparait donc que la cartographie des risques est un instrument d'identification, de quantification, et de hiérarchisation des risques qui doit être, minutieusement calibré, en raison de la différence de perception du risque entre les personnes réalisant l'évaluation des risques, et afin d'assurer le plus haut niveau d'exhaustivité et pertinence de l'évaluation.

En outre, la cartographie des risques représente un outil d'aide à la prise de décision, et se trouve à la base de plans d'audit. Son actualisation s'impose en tant que nécessité, du fait du caractère évolutif de l'environnement bancaire.

La prochaine partie, qui constitue l'étude pratique du présent mémoire, est réservée à la mise en place d'une cartographie des risques opérationnels.

Chapitre III *:* la cartographie des risques au sein de la Société Générale Algérie (SGA)

L'obligation faite aux banques d'immobiliser des fonds propres au titre des risques opérationnels les a obligées à réfléchir au dispositif de suivi et de mesure afin de pouvoir démontrer leur maitrise en la matière et de pouvoir limiter les fonds propres « non productifs » à affecter à ces risques.

Le groupe Société Générale à pris conscience de l'importance de la gestion optimale de ces risques et a mis en place un dispositif vigoureux qui lui permettra certainement d'éviter de subir d'énormes pertes qui lui-seront dommageable en termes de santé financière mais aussi en terme d'image et de réputation.

Pour compléter les aspects théoriques afférents à la gestion du risque opérationnel, nous avons élaboré une partie pratique pour mesurer les principaux dispositifs de pilotage du risque opérationnel au sein de la SGA. Et par cela nous aurons traité le dispositif pour élaborer la cartographie du risque opérationnel au sein de la société générale Algérie.

Etant donné que l'élaboration d'une cartographie des risques opérationnels est un travail très long et complexe qui s'étale sur plusieurs mois, nous avons décidé d'axer, essentiellement, notre travail sur une cartographie thématique concernant la banque de détails.

En résumé, ce chapitre est subdivisé en trois sections :
La première section de cette deuxième partie « **Présentation de la Société Générale Algérie** » portera sur la présentation de la structure d'accueil, à savoir : la Société Générale Algérie.

Dans la deuxième section **« La gestion du risque opérationnel au sein de la SGA** », nous évoquerons la manière avec laquelle le risque opérationnel est appréhendé au sein de cet organisme, ainsi que la description du dispositif de maîtrise appliqué.

La dernière section de notre mémoire est intitulée **« La cartographie des risques opérationnels liée a la banque de détail ».** Elle traite le développement d'une étude de cas, à savoir l'exercice RCSA, qui est un outil de pilotage du risque opérationnel élaboré par le Groupe tous les deux ans.

Section I : Présentation de la Société Générale Algérie

L'objectif de cette section est de présenter notre terrain de stage, nous commencerons par le groupe Société Générale, puis sa filiale en Algérie.

1. Présentation du Groupe Société Générale :

Créée en 1864 par appel public à l'épargne, la Société Générale (SG) est l'un des tout premiers Groupes Européens de services financiers.

Dés 1871, elle s'installe à l'étranger en ouvrant sa première succursale à Londres où elle développe rapidement son dispositif international à des pays du centre de l'Europe (Allemagne, Autriche, Suisse, Luxembourg), à des pays d'Afrique du Nord (1909-1911) et plus tard, aux États- Unis (1940).

Le Groupe Société Générale privatisé en 1987, est actuellement organisé en cinq pôles : Réseaux de Détail en France, Réseaux de Détail à l'International, Services Financiers, Gestions d'Actifs et Services aux Investisseurs, Banque de Financement et d'Investissement.

En 1998, le Groupe SG délègue le pouvoir de gestion des entreprises hors territoires français à la BHFM (Banque Hors France Métropolitaine) sous la tutelle de laquelle est placée la Société Générale Algérie.

Aujourd'hui la Société Générale est active dans 83 pays et compte près de 157 000 collaborateurs de 128 nationalités différentes. Elle accompagne au quotidien plus de 33 millions de clients dans le monde entier et propose une large gamme de services financiers et de conseils aux particuliers, aux entreprises et aux institutions dans trois principaux métiers :

- La banque de détail en France avec les enseignes Société Générale, Crédit du Nord et Boursorama;
- La banque de détail à l'international présente en Europe centrale & orientale et Russie, dans le Bassin méditerranéen, en Afrique sub-saharienne, en Asie et en Outre-Mer;
- La banque de financement et d'investissement avec son expertise globale en banque d'investissement, financements et activités de marché.

En Mars 2010, Le Groupe affiche une solidité financière élevée illustrée par sa notation financière à long terme : A+ chez Standard & Poor's et Fitch, Aa2 chez Moody's[1].

[1] Standard & Poor's, Moody's et Fitch sont trois des plus crédibles agences mondiales de notation financière.

2. Présentation de la Société Générale Algérie

Créée en **1999** avec un capital de 500 millions de dinars, Société Générale Algérie, filiale du Groupe Société Générale, est l'une des premières banques françaises à investir le marché algérien. Sa volonté dés le départ est de devenir la banque universelle au service de tous les agents économiques du pays .Ainsi, l'ouverture de trois agences à Alger donne le départ d'un réseau qui se veut à chaque jour plus proche de ses clients.

Allant toujours de l'avant avec l'ambition d'être une banque de proximité au service de l'économie nationale, elle introduit en **2002** « le Leasing » destiné aux entreprises avec la création d'un département qui lui est complètement dédié.

En **2003** le capital de la banque est porté à 2,5 MDS de dinars et Société Générale Algérie lance le service de banque à distance (SG@net) et le crédit immobilier. De plus son Réseau s'enrichi avec de nouvelles agences à Tlemcen, Oran, Constantine et Annaba.

C'est en **2004** que Société Générale Algérie propose à sa clientèle de particuliers le prêt Personnel ordinaire sans affectation : le crédit Bien-être[1]

Avec une croissance continue, la Société Générale Algérie adapte sa stratégie avec les orientations préconisées par les autorités, et augmente son capital à hauteur de 10 MDS de dinars en **2010**. Elle se dote d'un réseau de 70 agences réparties sur les grandes villes du pays.

Au cours de ces 15 dernières années, la Société Générale Algérie à mis tout son professionnalisme et savoir faire à la disposition d'une clientèle de plus en plus exigeante. C'est ainsi qu'en 2010, en fêtant son dixième anniversaire, Société Générale Algérie se dote d'une nouvelle signature : Société Générale Algérie, La banque de solutions.

Aujourd'hui, La SGA dispose d'un capital de plus de 12 milliards de Dinars et d'un réseau en constante croissance qui compte actuellement 85 agences dont 8 centres d'affaires ou business center dédiés à la clientèle des entreprises.

Son siège est établit à la résidence el Kerma de Bir khadem à Alger et la banque offre une gamme diversifiée et innovante de services bancaires à plus de 335000 client particuliers, professionnels et entreprises.

La SGA se doit d'être résiliente afin que la banque soit au rendez vous de ses objectifs face à un environnement économique changeant et rendu complexe par une concurrence accrue. Elle vise actuellement à promouvoir et à diversifier sa gamme de produits auprès de sa clientèle qui a dépassé les 270000 clients en 2012, entre particuliers et professionnels, PME et grandes entreprises. [2]

[1] Catalogue interne à la société Générale Algérie, 2013

[2] Site Internet : http://www.societegenerale.dz/nous_connaitre.html

Son produit net bancaire (PNB) a avoisiné, en 2013, les 14 milliards de DA, tandis que son résultat net en fin 2013 a atteint les 4 millions de DA.

2.1 Organigramme de la filiale Société générale Algérie :

L'organigramme détaillé de la filiale Société Générale Algérie se trouve en (Annexe 1) de ce mémoire.

3. L'audit interne à la Société Générale Algérie

Le Groupe SG définit le Contrôle Interne comme étant l'ensemble des moyens qui permettent à la Direction Générale de s'assurer que les opérations réalisées, l'organisation et les procédures mises en place sont conformes aux dispositions légales et réglementaires, aux usages professionnels et déontologiques, aux règles internes et aux orientations définies par la Direction Générale.

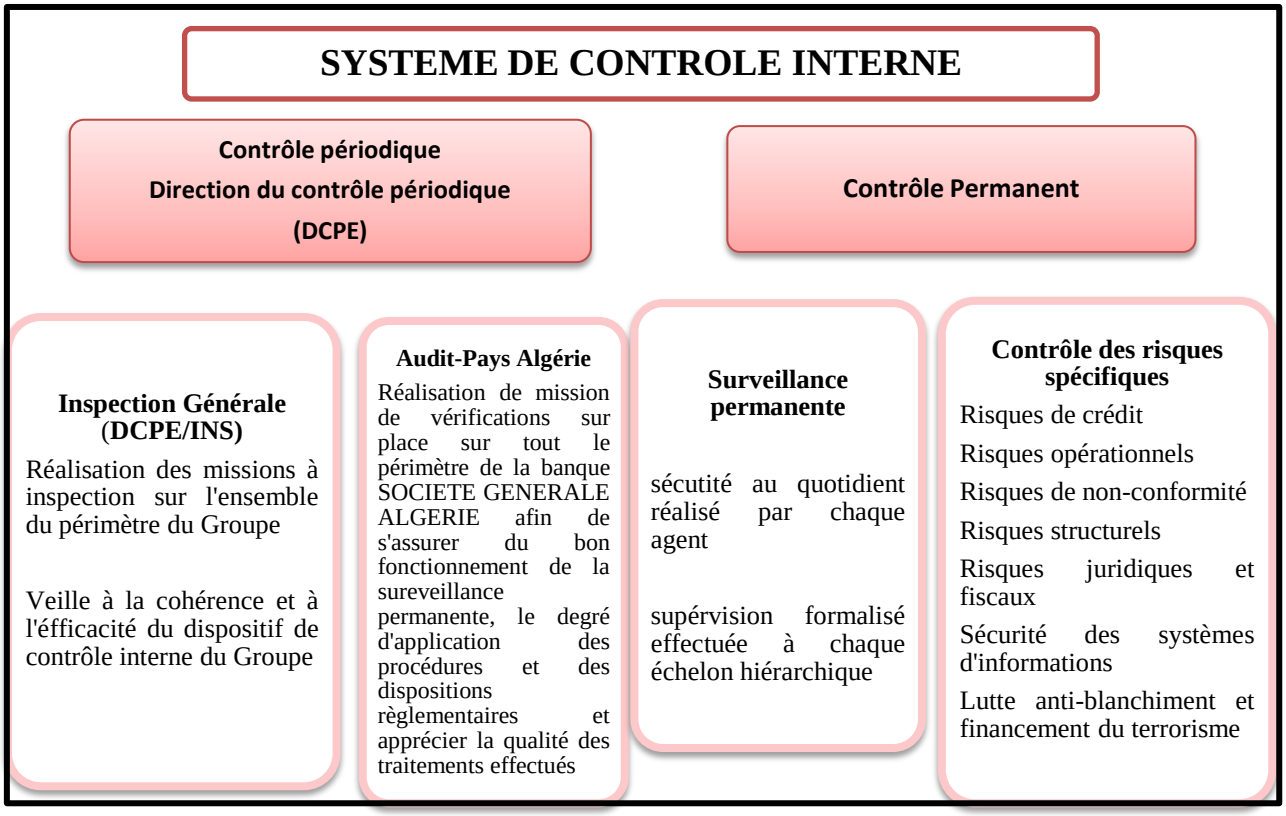
Notre stage pratique s'est déroulé au niveau de la Direction de l'Audit Interne de la SGA, qui depuis Avril 2010 est rattachée hiérarchiquement à la Direction du Contrôle Périodique (DCPE), est elle-même rattachée directement au Président-Directeur Général du Groupe SG.

En outre, elle dépend de la direction « Afrique du Nord » qui dépend de la direction FEA (France retail, Europe, Afrique).

Le dispositif de contrôle interne du groupe distingue deux niveaux de contrôle permanent qui constitue les premiers niveaux de contrôle puis le contrôle périodique qui représente un second niveau ce dernier est exercé par la Direction d'Audit Interne.

Les différents contrôles périodiques sont assurés par les équipes de la Direction du Contrôle Périodique (DCPE) qui sont des équipes indépendantes vis-à-vis des entités opérationnelles. Le contrôle périodique englobe l'ensemble des entités et des activités du groupe, il peut se concentrer sans aucune restriction, sur n'importe quel aspect des opérations du Groupe. Les équipes d'audit et d'inspection générale ont la charge de réaliser ces contrôles à partir d'un plan de mission annuel.

Figure n°8 : Système de contrôle interne



Source : société générale Algérie, document interne.

La surveillance permanente est une des composantes de l'organisation du contrôle permanent et est complétée par des dispositifs de contrôle permanent dédiés à la surveillance et à la prévention des risques mis en place par les directions centrales Groupe pour les périmètres de risques qui les concernent .

La responsabilité du contrôle permanent est assurée au niveau du groupe par :

- Le directeur des risques pour les risques de marchés et de crédit et les risques opérationnels hors ceux relevant de la conformité.
- Le directeur financier pour les risques structurels de taux de change et de liquidité et pour l'information financière et comptable.
- Le secrétaire général pour les risques juridiques et fiscaux et les risques de non-conformité.
- Le directeur des systèmes d'information Groupe pour la sécurité des systèmes d'information.

3.1 Présentation de la direction de l'audit –Société Générale Algérie- :

Le département de l'audit de Société Générale Algérie est situé au siège social de la filiale à Alger. Son rôle est d'effectuer des audits indépendants des entités opérationnelles qui ont pour mission de vérifier, dans le cadre d'une approche objective, rigoureuse et impartiale, la conformité des opérations, le niveau de risque effectivement encouru, le

respect des procédures ainsi que l'efficacité et le caractère approprié du dispositif de contrôle permanent de la filiale.

Le département d'audit SGA formule des préconisations pour mieux maitriser ces risques et plus largement pour améliorer le fonctionnement de la filiale en Algérie. En effet, l'équipe couvre l'ensemble des risques sur le périmètre géographique et collabore à la mise en place d'une évaluation annuelle des risques et d'un plan d'intervention. Une fois les missions achevées, les équipes doivent s'assurer de la mise en œuvre des plans d'actions nécessaires par les audités.

3.1.1.Organisation du département t d'Audit :

Le département d'audit au sein de la société générale se compose de :

- **Le Directeur du département d'audit :** qui a pour mission d'élaborer le plan annuel d'audit et le soumet à l'approbation du président directeur général. Il organise et exécute le plan d'audit à travers la programmation des missions et la constitution des équipes d'audit ainsi que l'évaluation des résultats des missions réalisées et

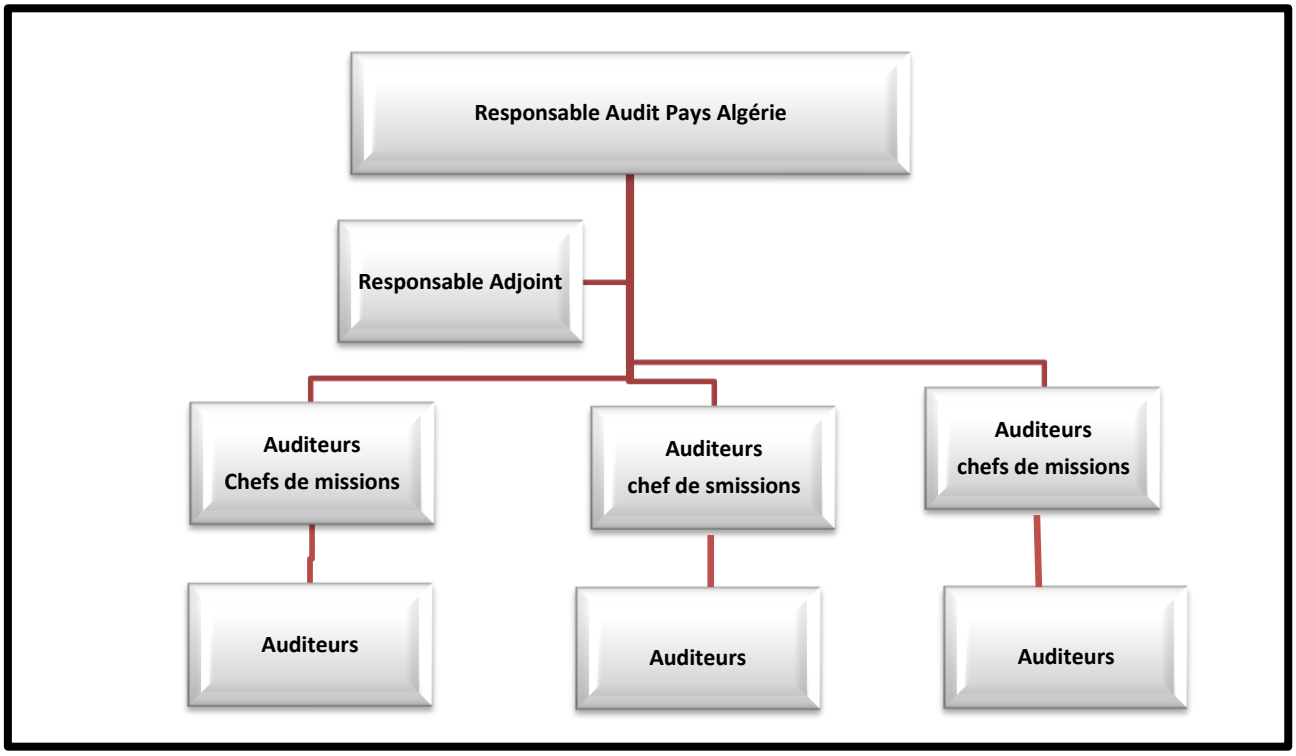
S'assurer de leur qualité. Le directeur veille également au respect du cadre de référence pour la pratique professionnelle de l'audit interne ainsi que la gestion des budgets alloués à la structure d'audit interne.

- **L'adjoint d'audit :** qui aident le directeur dans tout ces travaux et prend lui-même des décisions avant de les faire approuver par son supérieur. Il est le lien entre les chefs de mission et le directeur et supervise les missions d'audit sur le terrain .Il est très souvent chef de mission également.
- **Les chefs de mission** : Au sein de la SGA, il en existe 04, ils constituent les commandants de bord de la mission d'audit chargés d'orchestrer l'équipe qui leur est assignée. Ce sont tous des auditeurs ayant acquis une large expérience leur permettant de s'élever au rang de chef de mission. Les chefs de missions possèdent de large qualités de leadership leur permettant de pouvoir diriger des équipes et un grand sens de l'organisation leur permettant de s'acquitter convenablement de la mission confiée dans les délais fixés.
- **Les auditeurs internes :** Les auditeurs internes de la Société Générale Algérie se composent d'auditeurs séniors et auditeurs juniors.

Ils sont très souvent en mission auprès de différentes structures de la banque (les agences, les groupes, les directions) ce qui leur permet d'être en interaction permanente avec d'autres membres du personnel. Ils sont chargés d'effectuer l'ensemble des travaux qui leur sont confiés par le chef de mission notamment : le recueille des informations, la détection des anomalies et leurs causes, la formulation de recommandations adéquates pour leur résolution et la participation à la rédaction des rapports servant à rendre compte à la hiérarchie des travaux réalisés et des résultats obtenus.

Ci-dessous l'organigramme du département de l'audit interne :

Figure N°09 : organigramme de département audit interne SGA 2016



Source : société générale Algérie, document interne.

3.1.2. Mission et travaux :

L'équipe d'audit de la Société Générale Algérie couvrent de façon régulière tout le territoire national et de ce fait porte l'entière responsabilité de vérifier l'efficacité de la gouvernance, de la gestion des risques, du contrôle permanent afin d'assurer un meilleur contrôle des risques. Les collaborateurs d'audit effectuent une évaluation annuelle des risques qui mène à l'élaboration d'un plan d'audit. Ils conduisent ensuite des missions d'audit visant à s'assurer de l'efficacité du système de contrôle interne, à suivre l'application des procédures et réglementations internes ou externes, à évaluer la sécurité des traitements, la qualité de la comptabilité et des informations financières et l'alignement des systèmes d'information avec les besoins de l'entité.

Ces missions d'audit donnent lieu à l'émission de préconisations.

Enfin les équipes d'audit sont responsables du suivi de la mise en œuvre de ces Préconisations. [1]

Pour bien mener ses missions, l'audit doit :

- se doter de moyens humains suffisants en qualité et quantité et mettre au point les procédures de contrôles, états de reporting, méthodes et outils appropriés.

[1] Charte d'audit Interne, Société Générale Algérie, 2014

- identifier et suivre méthodiquement et sur une base régulière les zones de risques de son périmètre en tenant compte de l'évolution des métiers, activités, opérations et documenter ce processus.
- établir sur cette base un plan d'audit annuel permettant une couverture régulière de l'ensemble du périmètre.
- mener dans le cadre du plan d'audit des contrôles de sécurité , de conformité et d'efficacité (examen des procédures , de la régularité des opérations , de l'efficacité de la surveillance permanente , de la maitrise des risques , de la sécurité des systèmes d'information , de la fiabilité de l'information financière et comptable et de l'exactitude des reporting internes) selon un protocole d'audit rigoureux et audit able.

3.1.3. Les comités d 'Audit Interne :

Lieu d'échange privilégié entre l'audit et les instances de gouvernance des entités du périmètre, le comité d'audit interne est un rouage majeur du dispositif de contrôle périodique qui permet d'examiner à intervalle régulier ses conditions d'exercice et son activité.

A cet effet, une fois par an, un comité d'audit interne se tient en présence du responsable du pole d'activités ou de la direction concernée, de l'inspecteur général et du directeur d'audit. Egalement des comités de même nature se tiennent au niveau des lignes-métiers. A chaque réunion, il est rendu compte :

- des évolutions significatives et des prévisions ou projets concernant l'organisation, les moyens et les méthodes de travail ainsi que les différents aspects du fonctionnement et de l'activité de l'audit.
- des missions de contrôle périodique en cours ou conclues depuis le précédent comité dont sont dégagés les constats et enseignements significatives.
- des enquêtes relatives à des irrégularités conduites sur la période, en pointant d'éventuelles circonstances récurrentes.
- du suivi des préconisations formulées par le contrôle périodique.

Le programme de travail défini pour la période à venir est par ailleurs présenté au comité d'audit interne SGA en le reliant aux éléments ressortant de l'exercice d'identification et de suivi des zones de risques.

Des comités d'audit interne sont également réunis conformément aux dispositions applicables à la filiale en présence du responsable de la filiale, de l'inspecteur général et responsable de l'audit interne.

Section 2 : La gestion du risque opérationnel au sein de la SGA

Au cours des dernières années, Société Générale a développé des processus, des outils de gestion et une infrastructure de contrôle pour renforcer la maîtrise et le pilotage des risques opérationnels dans l'ensemble du Groupe. Ces dispositifs comprennent, entre autres, des procédures générales et spécifiques, une surveillance permanente, des plans de continuité d'activité, des Comités nouveaux produits et des fonctions dédiées à la surveillance et la gestion de certains types de risques opérationnels tels que la fraude, les risques liés aux systèmes de paiement, les risques juridiques, les risques liés à la sécurité des systèmes d'informations et les risques de non conformité.

Pour analyser les principaux outils du risque opérationnel au niveau de la SGA, nous avons établi un questionnaire (copie en jointe en annexe n°02).

D'après les constats de notre stage pratique et les questions que nous avons posées aux Opérationnels, Les réponses à ces questions seront détaillées ci après.

1 .Définition des risques opérationnels à la SGA :

Le risque opérationnel (RO) est Défini par le Groupe comme étant " le risque de perte résultant d'une inadaptation ou d'une défaillance imputable à des procédures, personnels et systèmes internes, ou à des événements extérieurs, y compris les risque de non-conformité*, dont le risque d'atteinte à la réputation. Est également inclus le risque juridique."[1]

Cette définition rejoint celle donnée par le Comité de Bâle dans son premier document consultatif, mais à l'instar de cette dernière, la définition donnée par le groupe inclus le risque d'image et met l'accent sur l'importance des événements rares, et des répercussions désastreuses qu'ils peuvent avoir.

2- Mesure des risques opérationnels[2]

Société Générale a opté, dès 2004, pour l'approche de mesure avancée des risques opérationnels (AMA ou Advanced Measurement Approach) proposée par la Directive Européenne sur l'adéquation des fonds propres. Cette approche permet notamment :

- d'identifier les métiers les plus exposés aux risques et les types de risque qui ont l'impact le plus fort sur le profil de risque du Groupe et sur ses besoins totaux en fonds propres ;

---

* Agir en conformité consiste à inscrire son action au quotidien dans le respect des lois et des règlements spécifiques aux activités bancaires et financières, avec les principes d'éthique professionnelle. Le non respect de la conformité induit un risque dit de non-conformité, vecteur de pertes financières, de sanction judiciaire ou disciplinaire ainsi que de dégradation de l'image.

[1] Société générale, document interne, Direction risque opérationnel et conformité, AOUT 2013.

[2] https:// www.societegenerele.dz Document de référence, rapport financier annuel 2013.société générale

- d'améliorer la culture et la gestion des risques opérationnels du Groupe en créant un cercle vertueux dans lequel les risques sont identifiés, leur gestion est améliorée et des stratégies appropriées sont mises en œuvre afin de les atténuer et les réduire.
- L'Autorité de Contrôle Prudentiel a effectué en 2007 une revue approfondie du dispositif élaboré par Société Générale et a autorisé, en conséquence, le Groupe à utiliser la méthode la plus avancée prévue par l'accord dit de Bâle 2 (c'est-à-dire, la méthode AMA), pour le calcul de son exigence de fonds propres au titre des risques opérationnels à compter du 1er janvier 2008, pour un périmètre représentant plus de 90 % du produit net bancaire total du groupe Société Générale.

Quelques filiales utilisent encore l'approche standard ; un plan de déploiement progressif de l'approche avancée est mis en place pour certaines d'entre elles.

3 .Classification des risques opérationnels à la SGA :

La classification par Société Générale des risques opérationnels en huit catégories d'événements et quarante-neuf sous-catégories(copie en jointe en annexe n°) mutuellement exclusives est la pierre angulaire de sa modélisation des risques. Elle garantit la cohérence d'ensemble du dispositif et permet de réaliser des analyses transversales.

Les huit catégories d'événements sont rappelées ci-après :

3.1. Litiges commerciaux :

Litiges sur activités de conseil, pratiques commerciales inappropriées inadéquation des produits proposés, insuffisance du service au client, autres litiges avec un tiers, contrat ou clauses contractuelles inapplicables.

3.2. Litiges avec les autorités :

Comprend le non-respect de la loi bancaire, des lois contre la discrimination, de la réglementation du travail, des lois sur l'environnement, des règles de fonctionnement des marchés organisés, des normes de sécurité et de santé, d'autres lois, des exigences réglementaires locales, des exigences comptables ou de la communication financière de la législation fiscale, ainsi que le blanchiment d'argent et financement du terrorisme. Autrement dit, tout manquement à une réglementation ou loi commune.

3.3. Erreurs de "Pricing" ou d'évaluation du risque:

Défaillance dans le dispositif de gestion et de suivi des autorisations et des limites, évaluation incorrecte ou inexistante de la position, données de marché et informations publiques fausses ou insuffisantes, modèle de calcul de prix ou de valorisation erroné.

3.4. Erreurs d'exécution :

Défaillance dans le processus de livraison et/ou de règlement de la banque, dans les processus de gestion des confirmations d'opérations, dans la gestion administrative d'une

opération jusqu'à son échéance, erreurs dans la transmission, la saisie ou la compréhension d'une instruction, absence ou inexactitude des données nécessaires à la gestion des activités, absence ou inexactitude des rapports d'erreur dans les chaînes informatiques, structure organisationnelle inadéquate ou faiblesse de l'environnement de contrôle, défaillance dans la conservation pour compte de tiers de documents ou valeurs, défaillances sur services rendus par des sous-traitants, défauts de rapprochement, ainsi que l'accès laissé par la banque aux comptes d'un client sans l'accord de ce dernier.

3.5. Fraude et autres activités criminelles :

Piratage informatique et autres attaques malveillantes des systèmes d'information de la banque par des tiers, autre forme d'actes criminels contre les actifs de la banque, vols/escroqueries /fraudes commis par des tiers, vols par le personnel ou des prestataires internes, fraude sur des transactions par le personnel ou avec sa complicité, utilisation non autorisée ou à mauvais escient d'information privilégiée et confidentielle par le personnel.

3.6. Activités non autorisées sur les marchés (Rogue trading):

Activités non autorisées sur les marchés par le personnel.

3.7. Pertes des moyens d'exploitation:

Défaut de personnel, pertes des donnés, pertes des moyens d'exploitation, et la perte de services.

3.8. Défaillance des systèmes d'information:

Défaillance de matériel, données incohérentes ou incompatibles, mauvaise gestion de projet, défaillance des softwares, faiblesse de la sécurité *logique* (informatique), et enfin la faiblesse de la sécurité physique.

La SGA dispose d'un historique et d'une base de données des pertes internes. Cette base de données permet d'analyser les pertes (par catégorie d'événement, cause, ligne d'activité…) et de suivre leur évolution ainsi que les plans d'actions correctrices proposés.

4. Dispositifs de pilotage des risques opérationnels au SGA

Les différents dispositifs sont :

- la collecte des données internes relatives aux pertes de risques opérationnels ;
- le dispositif d'auto-évaluation des risques et des contrôles (Risk & Control Self-Assessment ou RCSA) ;
- les indicateurs clés de risques (Key Risk Indicators ou KRI) ;
- les analyses de scenarii ;

4.1 Collecte des pertes internes (PI)

La collecte des pertes internes concerne l'ensemble du Groupe depuis 2003. Ce processus a permis aux opérationnels :

- de définir et mettre en œuvre les actions correctrices appropriées (évolution des activités ou des processus, renforcement des contrôles, etc.) ;
- de s'approprier de nouveaux concepts et outils de gestion des risques opérationnels;
- d'acquérir une meilleure connaissance de leurs zones de risques ;
- de mieux diffuser une culture du risque opérationnel au sein du Groupe.

Le seuil minimum à partir duquel une perte est enregistrée est de 10 000 EUR dans l'ensemble du Groupe, sauf dans la Banque de Financement et d'Investissement, où ce seuil est fixé à 20 000 EUR en raison du périmètre de ses activités, des volumes concernés et de la pertinence des points pour la modélisation de l'exigence de fonds propres réglementaires. En deçà de ces seuils, les pertes sont collectées par les différents pôles du Groupe mais elles ne sont pas recensées par le Département des risques opérationnels.

4.2. Auto-évaluation des risques et des contrôles *(Risk & control self assessment* ou RCSA*)*

Le principe du RCSA a été défini dès les années 2001 et 2002, lors de la mise en place de la cellule PRES/BA2/OPE. Fin 2004, comme le dit un des collaborateurs de cette cellule, *« nous avions la beauté d'un dispositif d'identification des zones de risque, quelque chose de superbe en théorie* ». Le RCSA joue le rôle de cartographie des risques. Il vise à apprécier le risque résiduel d'une activité du Groupe en évaluant l'exposition au risque opérationnel, en estimant la qualité des dispositifs de prévention et de contrôle afin d'en déduire l'exposition résiduelle. L'évaluation du risque résiduel doit permettre d'engager les actions correctrices nécessaires.

L'exercice d'auto-évaluation des risques et des contrôles (RCSA) a pour objet d'apprécier l'exposition du Groupe aux risques opérationnels afin d'en améliorer le pilotage. Sur la base des résultats des autres dispositifs de gestion du risque opérationnel (pertes internes), des zones de risques identifiées par les filières sur leurs domaines de compétences respectifs, et d'entretiens menés avec des experts du Groupe, il a pour objectifs :

- d'identifier et d'évaluer les risques opérationnels majeurs auxquels est exposée chaque activité (risques intrinsèques, c'est-à-dire les risques inhérents à la nature d'une activité, en faisant abstraction de ses dispositifs de prévention et de contrôle) ; le cas échéant, les cartographies des risques établies par les filières (par exemple, conformité, sécurité des systèmes d'information…) contribuent à cette évaluation des risques intrinsèques ;
- d'évaluer la qualité des dispositifs de prévention et de contrôle en place, permettant de réduire ces risques majeurs (existence et efficacité de ces dispositifs en termes de détection et de prévention des risques et/ou de leur capacité à en diminuer les impacts financiers) ;

- d'évaluer l'exposition aux risques majeurs résiduels de chaque activité (après prise en compte de l'environnement de prévention et de contrôle, mais abstraction faite de la protection fournie par les polices d'assurance auxquelles le Groupe a souscrit);
- de remédier aux déficiences éventuelles des dispositifs de prévention et de contrôle, et de mettre en œuvre des plans d'actions correctrices ;
- de faciliter et/ou d'accompagner la mise en place d'indicateurs clés de risque ;
- d'adapter, si nécessaire, la politique d'assurance.

Dans le cadre de cet exercice, les risques majeurs d'un périmètre donné sont qualifiés selon une double échelle de sévérité et de fréquence.

4.3 Indicateurs clés de risque *(*key risk indicators ou KRI*)*

Les KRI complètent le dispositif de pilotage des risques opérationnels en fournissant une vision dynamique (système d'alerte) de l'évolution du profil de risque des métiers. Le suivi régulier des KRI complète ainsi l'évaluation de l'exposition du Groupe aux risques opérationnels effectuée *via* l'exercice d'auto- évaluation des risques et des dispositifs de prévention et de contrôle (RCSA), l'analyse des pertes internes et les analyses de *scenarii,* en apportant aux responsables d'entités :

- une mesure quantitative et vérifiable du risque ;
- une évaluation régulière des améliorations ou des détériorations du profil de risque et de l'environnement de prévention et de contrôle, nécessitant une attention particulière ou un plan d'actions.

Les KRI susceptibles d'avoir une incidence notable sur l'ensemble du Groupe sont transmis à la Direction générale du Groupe *via* un tableau de bord dédié.

Le tableau suivant reprend quelques exemples de KRI relatifs aux deux premières catégories de risques SG : « litiges commerciaux » et « litiges avec les autorités » :

Tableau n° 05 : Exemples de KRI pour les deux premières lignes de métier

Catégorie d'événement	**Sous-catégorie d'événement SG**		**Exemples de KRI**
Litiges commerciaux	1	Litiges sur activités de conseil	Nombre de litiges juridiques en cours Nombre de plaintes reçues (demandes de compensation) Nombre de réclamations clientèle ayant débouché sur un litige
	2	Pratiques commerciales inappropriées	
	3	Inadéquation des produits proposés	
	4	Insuffisance du service au client	
	5	Autres litiges avec un tiers (fournisseur, prestataire…)	

	6	Contrat ou clauses contractuelles inapplicables	commercial
Litiges avec les autorités	11	Non respect de règles de fonctionnement des marchés organisés (actions, futures, marchandises, obligations, etc.)	Nombre de réclamations reçues Amendes liées au non respect des normes de marchés organisés
	13	Non respect d'autres lois (non citées dans cette catégorie d'événement)	Cas de litiges ou non-conformité aux règles ou lois
	14	Non respect des exigences réglementaires locales ou françaises	Sanctions imposées et actions juridiques associées
	17	Blanchiment (interne et externe) et financement du terrorisme	Nombre de transactions suspectes

Source : Société Générale Algérie

Un reporting régulier des KRI est effectué par la SGA, le niveau des indicateurs (obligatoires), ainsi que celui de quelques indicateurs facultatifs est transmis trimestriellement à la BHFM pour appréciation et recommandations.

Pour conclure cette section, nous pouvons dire que les différents dispositifs de mesure doivent permettre de:

- Identifier les lacunes existantes (insuffisances de contrôle interne, nature de pertes récurrentes, scénarios de sinistre exposant la banque à un risque excessif et non couvert, etc.).
- Elaborer, face à ces lacunes, des plans d'actions palliatifs.
- Suivre la mise en œuvre effective des actions correspondantes.

4.4. Analyses de scenarii (AS)

Les analyses de scenarii ont pour double objectif d'identifier les zones de risques potentiels importants du Groupe et de contribuer au calcul des fonds propres exigés au titre des risques opérationnels.

Concernant le calcul de l'exigence de fonds propres, le Groupe utilise les analyses de scenarii pour :

- mesurer son exposition à des pertes potentielles rares mais de très forte sévérité ;
- disposer, pour les catégories d'événements où l'historique de pertes internes est insuffisant, d'une estimation de distribution de pertes à dire d'expert.

Section 3 : La cartographie des risques opérationnels liée a la banque de détail.

La banque est confrontée à la nécessité de gérer les risques inhérents à ses activités et sous-jacent aux processus d'exécution. Les établissements bancaires se doivent d'élaborer un bon dispositif afin de gérer les risques. Plus spécifiquement, la cartographie des risques constitue la pierre angulaire dans tout dispositif de gestion des risques ainsi qu'une hiérarchisation de ces derniers.

Dans le but de répondre à notre problématique de départ, nous allons essayer de décrire les étapes à suivre pour la réalisation de notre projet de cartographie des risques opérationnels en faisant une projection sur la méthodologie précédemment présentée dans la partie théorique, et ce pour rester dans le cadre méthodologique universel et pouvoir déceler les anomalies et les insuffisances à la fin de notre travail.

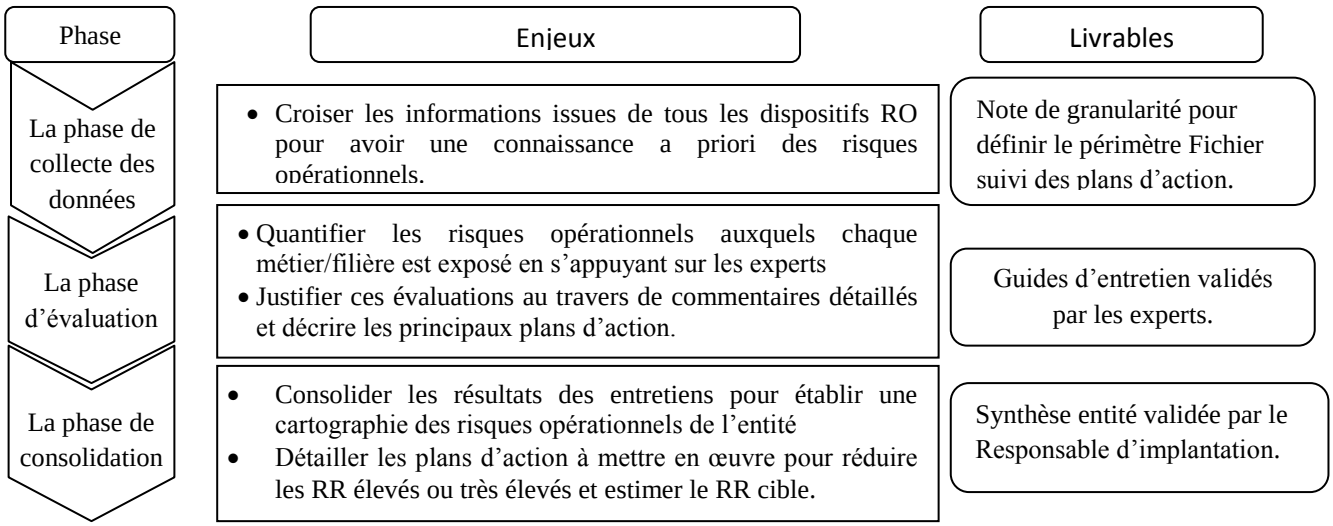
1. Vers la réalisation de la cartographie des risques : analyse descriptive et cadre méthodologique.

Le RCSA joue un rôle important dans le dispositif de gestion des risques opérationnels de la SGA ; il permet d'élaborer la cartographie des risques opérationnels de la banque.

1.1 Méthodologie RCSA :

La méthode d'auto évaluation des risques et des contrôles (RCSA) développée par le groupe consiste en une approche commune d'identification et d'évaluation des risques opérationnels et un processus d'évaluation homogène des dispositifs de prévention et de contrôle afin de garantir la cohérence de la banque et rendre possible une comparaison des évaluations des entités entre elles.

Figure N°10 : Les trois phases de la réalisation du RCSA dans les entités

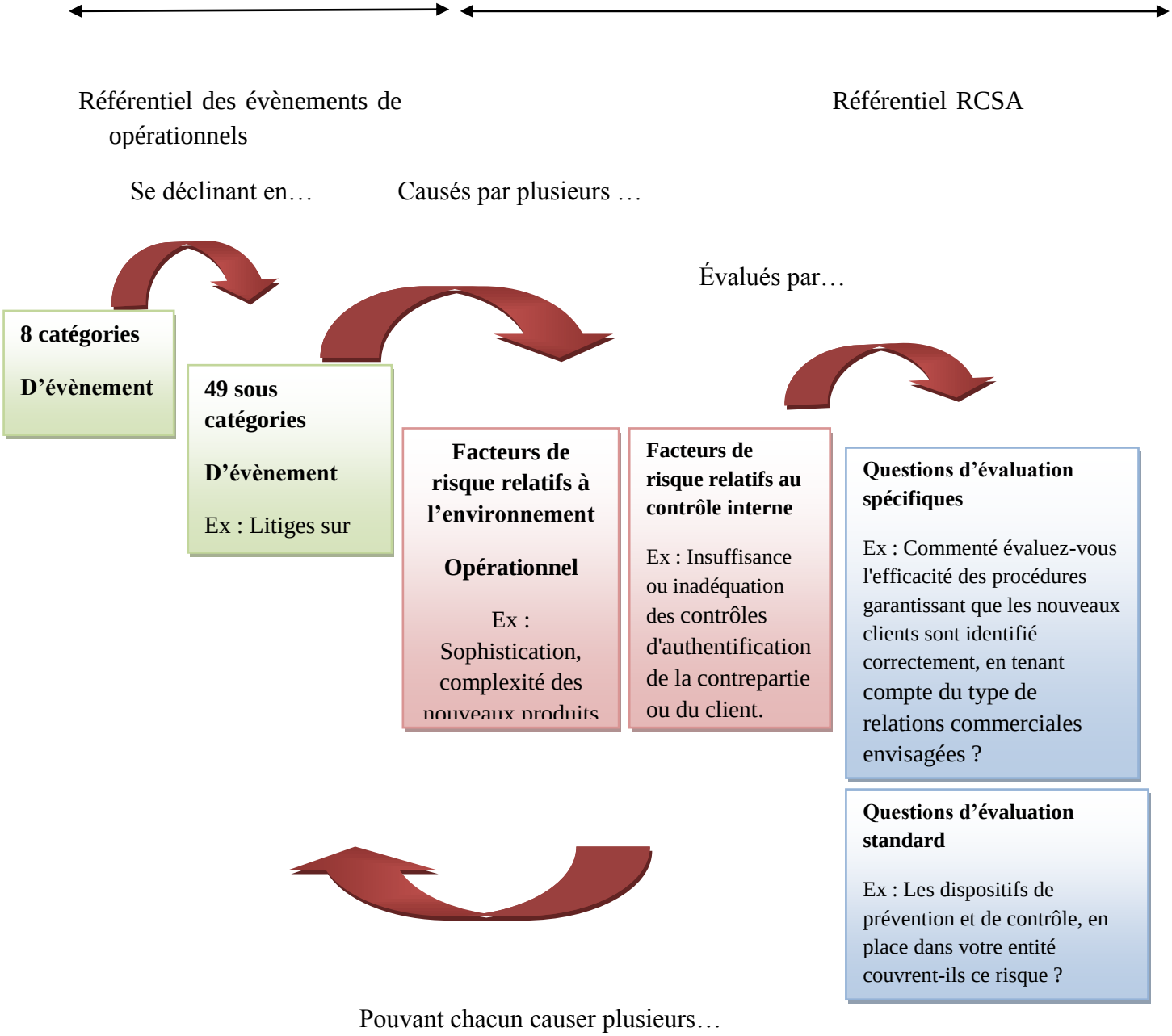


Source : Document Société Générale Algérie

1.2. Démarche de la cartographies (RCSA)

La méthode d'auto évaluation des risques et des contrôles (RCSA) développée par le Groupe SG consiste en une approche commune d'identification et d'évaluation des risques opérationnels. C'est un processus d'évaluation homogène des dispositifs de prévention et de contrôle.

Figure 11 N° : Processus d'élaboration de la cartographie (RCSA)



Source : Document Société Générale Algérie

Pour ce faire, l'exercice RCSA s'appuie sur les étapes suivantes :

Tableau N° 6 : Tableau du livrable RCSA

Évaluation	**Livrables par les métiers**
1. Risques opérationnels intrinsèques (RI) . ⇒	Cartographie des risques Intrinsèques.
2. Dispositifs de prévention de contrôle existants. ⇒	Questionnaires entité notés (ou scorecards entité.
3. Risques opérationnels Résiduels. ⇒	Cartographie des risques résiduels.

Source : élaboré par nos soins

1.3. Réalisation de la cartographie des risques intrinsèques :

Il s'agit d'identifier et évaluer les risques intrinsèques en effectuant une classification des évènements de risques opérationnels en catégories et en sous catégories déjà mise en œuvre par le Groupe pour la collecte des pertes internes. Cette étape nécessite un référentiel de facteurs de risques relatifs à l'environnement dans le quel opère la SGA.

Ces facteurs d'environnement évaluent le niveau d'exposition des risques en tenant compte uniquement de l'environnement dans lequel la banque exerce son activité, sans prendre en compte un quelconque dispositif de prévention et d'atténuation, autrement dit, l'appréciation de la sécurité de l'environnement auquel appartient la banque.

A cet effet, une cartographie des risques intrinsèques s'effectue par catégories ou sous catégories d'évènement prenant en compte les facteurs d'environnement[1] qui ne sont pas notés mais qui soutiennent l'évaluation du risque intrinsèque. Leur prise en compte est dûment documentée et fait l'objet de contrôles périodiques.

Exemples :

- une entité exerçant un service dans le cadre d'un mandat rémunéré est exposée à la catégorie d'évènement « litiges commerciaux ».
- de même, une entité ayant des activités de marché est exposée à la catégorie d'évènement « rogue trading » *

L'exposition à chaque sous-catégorie de risque est appréciée par une note allant de « 0 » jusqu'à
« 4 » comme l'indique le tableau suivant :

[1] Pour ce qui concerne la filiale SGA, il existe 16 facteurs d'environnements.

*activités non autorisée sur les marchés

Tableau n° 07 : L'échelle d'évaluation des risques intrinsèques

	Niveau de criticité	Valeur numérique associée
Echelle d'évaluation du RI	Très élevé	4
	Elevé	3
	Modéré	2
	Faible	1
	Non exposé	0

Source : Document Société Générale Algérie.

1.4. Evaluation des dispositifs de prévention et de contrôle :

Après l'identification des risques intrinsèques, la banque doit mettre en place des dispositifs de prévention et de contrôle visant à réduire les risques opérationnels à un niveau jugé acceptable.

A cet effet, un référentiel de questionnaires métiers appelés « scorecard métier » est mis en place. Il est conçu sous forme de questions élaborées par les responsables des structures en coordination avec les responsables du risque opérationnel au niveau de la banque mère.

C'est le responsable de chaque département de la banque qui doit répondre à ces questionnaires, lesquels concernent plusieurs critères: la continuité d'activité, la sécurité, les systèmes d'information de l'activité des agences, les ressources humaines…etc. A la fin, chaque question sera notée.

Pour chaque risque, la scorecard contient les informations suivantes :

- **Les catégories d'évènement :** présentent les manifestations concrètes possibles des risques opérationnels d'une banque.
- **Les facteurs de risque :** ils sont essentiels pour l'identification des principales causes internes ou externes de ces manifestations. Exemple : insuffisances de procédures de gestion des réclamations de la clientèle.
- **Des questions d'évaluation :** pour chaque facteur de risque, on évalue le dispositif de prévention et de contrôle à l'aide de ces questions. Cette démarche d'auto évaluation permet de mettre en évidence l'efficacité des processus de contrôle interne.

Ces questions sont notées selon le barème ci-après :

Tableau n° 08: Evaluation des dispositifs de prévention et de contrôle.

	Evaluation	Valeurs associées	
Qualité des dispositifs de prévention et de contrôle	Satisfaisant	4	Le dispositif est pertinent et efficace, testé et auditable à tout moment
	Assez bon	3	Le dispositif compte quelques imperfections / omissions mineures
	Faible	2	Le dispositif compte quelques imperfections / omissions importantes
	Quasi-inexistant	1	Le dispositif n'est pas adapté (pertinence) ou est inexistant

Source : Document Société Générale Algérie.

1.4.1. Notation et justification du risque :

Les noteurs sont les responsables en charge de noter les scorecards métiers élaborées par le modélisateur. Ils ont comme objectif l'évaluation du dispositif de prévention et de contrôle en répondant aux questions d'évaluation associées aux facteurs de risque. Il justifie sa note par l'existence de procédures de prévention et de contrôle.
Soulignons que, un facteur de risque est un élément de l'environnement et/ou de l'organisation qui contribue à la survenance d'un risque opérationnel. Il doit toujours être considéré en fonction de la sous-catégorie/ catégorie d'événement à laquelle il se rapporte.

1.4.2. Validation des scorecards entité :

Les notes attribuées aux « scorecards entité » seront transmises par les noteurs à leur hiérarchie pour validation. Le valideur est la personne en mesure de valider les notes et les justifications associées avant la consolidation en vérifiant notamment la cohérence des notes pour l'ensemble des entités de son périmètre.
Afin de finaliser cette étape, nous avons jugé utile de citer cet exemple de facteur de risque évalué dans la scorecard entité: Il s'agit du facteur de risque "sécurité des équipements" et concerne le métier de "Sécurité des systèmes d'information". Il a été repris tel qu'il a été renseigné à la Scorecard.

Afin de finaliser cette étape, nous avons jugé utile de citer cet exemple de facteur de risque évalué dans la scorecard entité: Il s'agit du facteur de risque *"sécurité des équipements"* et concerne le métier de *"Sécurité des systèmes d'information"*. Il a été repris tel qu'il a été renseigné à la Scorecard.

Tableau N°09: Exemple de risque évalué à la Scorecard Métier "Sécurité des systèmes d'information" SGA.

Catégorie d'événement	**Sous-catégorie d'événement**	**Question**	**Note***	**Justification**
Fraude et autres activités criminelles	Piratage informatique et autres attaques malveillantes des systèmes informatiques de la banque par des tiers	Les équipements critiques sont-ils équipés d'onduleurs pour faire face aux coupures d'énergie électrique ?	**4**	Chaque site est doté d'un onduleur et d'un générateur électrique

* la note 4 correspond à l'appréciation "satisfaisant"

Source : Document Société Générale Algérie

1.5. Elaboration de la cartographie des risques résiduels :

Dans cette étape, il s'agira d'estimer les risques par catégorie d'événements et par ligne métier au sein des branches ou par Direction Fonctionnelle, tout en prenant en compte les différents dispositifs de prévention et d'atténuation des risques mis en place par chaque entité évaluée. Cependant, La cartographie des risques résiduels résulte des notes consolidées des risques intrinsèques et de celles du dispositif de prévention et de contrôle.

Au niveau Hiérarchique, la cartographie des risques intrinsèques est généralement établie à un niveau plus élevé que les Scorecards de l'entité. La cartographie des risques résiduels des lignes métier, quant à elle, est établie au sein des Branches et Directions Fonctionnelles, et doit être validée par leur Direction respective. Les risques résiduels doivent être quantifiés par le responsable de la ligne métier selon l'échelle de quantification fixée par la Direction de l'entité. Cette échelle est identique pour les risques résiduels et pour les risques intrinsèques.

Comme les risques intrinsèques et le niveau de contrôle, une note est attribuée au risque résiduel. Cette note est obtenue par division de la note du risque intrinsèque par la note du dispositif de contrôle consolidée pour chaque catégorie d'événements (ou chaque sous catégorie d'événements si la Branche ou l'entité le souhaite). Un paramètre d'ajustement est parfois ajouté à la note obtenue afin de consolider le poids de certains risques.

Note du niveau de risque résiduel (score)	$= \frac{\textbf{Note du niveau de risque intrinsèque}}{\textbf{Note du niveau du dispositif de contrôle}} + \textbf{paramètre d'ajustement}$

Le paramètre d'ajustement peut être de « 1 » ou de « 2 », il est ajouté quand les notes du dispositif de prévention sont « assez bonnes ». En effet, la note attribuée au risque résiduel se fait de la manière illustrée dans le tableau suivant :

Tableau N° 10 : Paramètre d'ajustement.

Evaluation du risque intrinsèque	**Evaluation du contrôle**	**Paramètre d'ajustement**
Elevé	Assez bon	+ 1
Modéré	Assez bon	+ 1
Très élevé	Assez bon	+ 2

Source : Document Société Générale Algérie

De ce fait, la note obtenue correspond à une évaluation du risque résiduel comme suit :

Tableau N° 11 : Evaluation du risque résiduel.

	Niveau de criticité	Valeur numérique associée
Echelle d'évaluation du RI	Très élevé	4
	Elevé	3
	Modéré	2
	Faible	1
	Non exposé	0

Source : Document Société Générale Algérie

Le score ainsi obtenu permettra d'identifier les zones de faiblesses de mesure de prévention et de contrôle et de mettre en œuvre des plans d'actions adéquats.

Les risques considérés comme insuffisamment contrôlée devront être soumis à des mesures correctives pour ramener le risque résiduel à niveau tolérable. D'autre part, s'il ya des risques qui sont identifiés comme étant plus contrôlés, alors il faudrait envisager de réaffecter les ressources dans les zones de contrôle des risques qui sont mal gérées.

1.6. Mise en place de plans d'actions :

Les résultats et les conclusions de l'exercice RCSA peuvent être utilisés en conjonction avec d'autres outils de gestion du risque opérationnel, par exemple : les données de pertes internes et externe et analyse de scénarios. Cela permettra d'avoir un aperçu renforcé du profil du risque opérationnel.

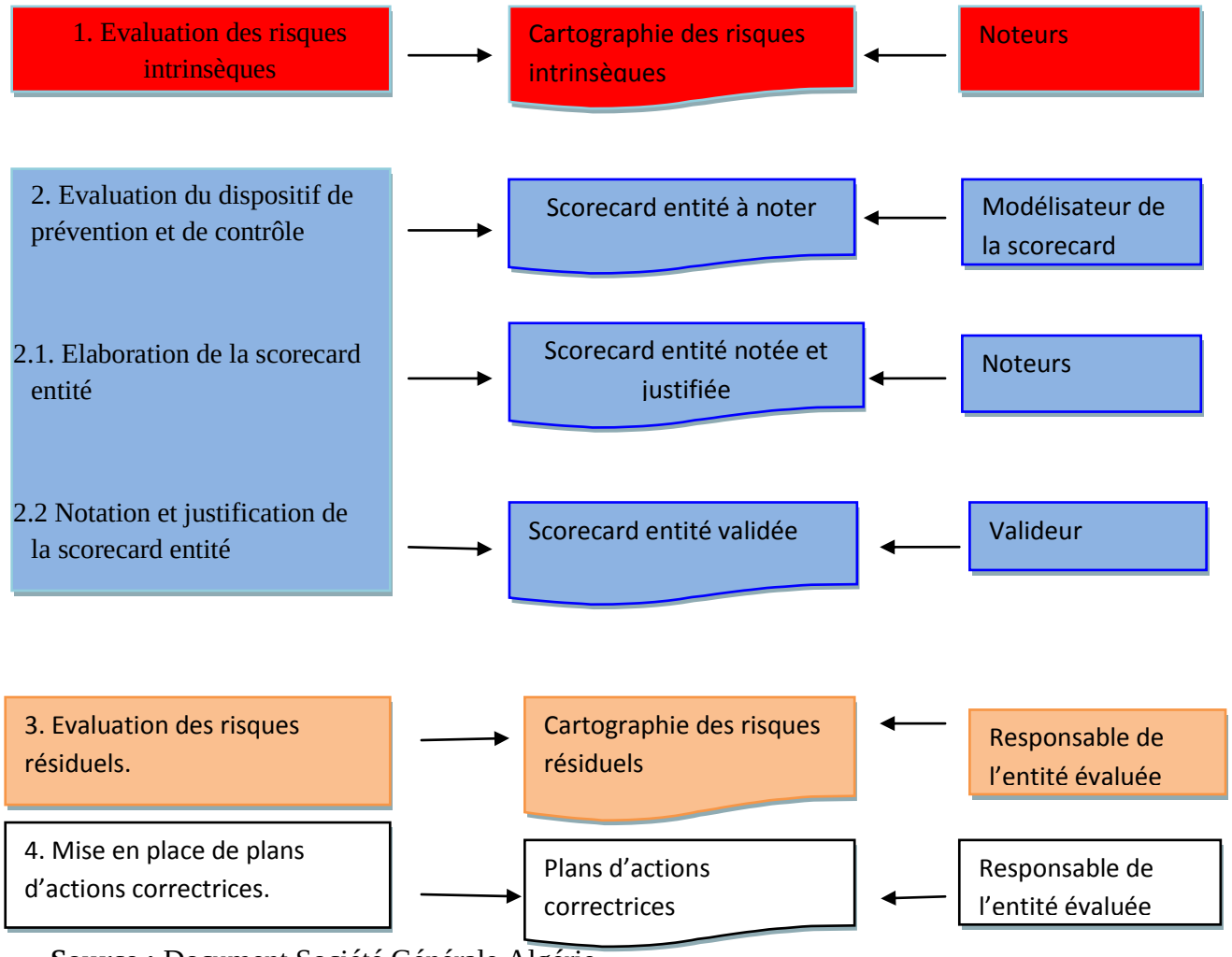
Une fois les risques résiduels connus, ils sont exploités pour renforcer la maîtrise des risques opérationnels auxquelles la SGA est exposée, par les dispositifs de contrôle permanents comme la Surveillance Permanente.
Des plans d'actions seront mis en œuvre par les Responsables métiers au sein des zones de faiblesses, de prévention et de contrôle identifiés. Ils peuvent être éventuellement accompagnés d'une mise en place d'indicateurs clés de risque. En cas de nécessité, ils adaptent la politique d'assurance de la banque.

Lors de son initiation, un plan d'action doit contenir certaines données primordiales qui conditionneront son succès :

- Départements impliqués dans le plan d'action ;
- Description détaillée des actions à entreprendre ;
- Résultats et améliorations attendues (en termes de profil de risque) ;
- Date d'échéance des actions.

Les étapes de l'exercice RCSA peuvent être résumées par le schéma suivant :

Figure N12 : détail des trois étapes et acteurs concernés

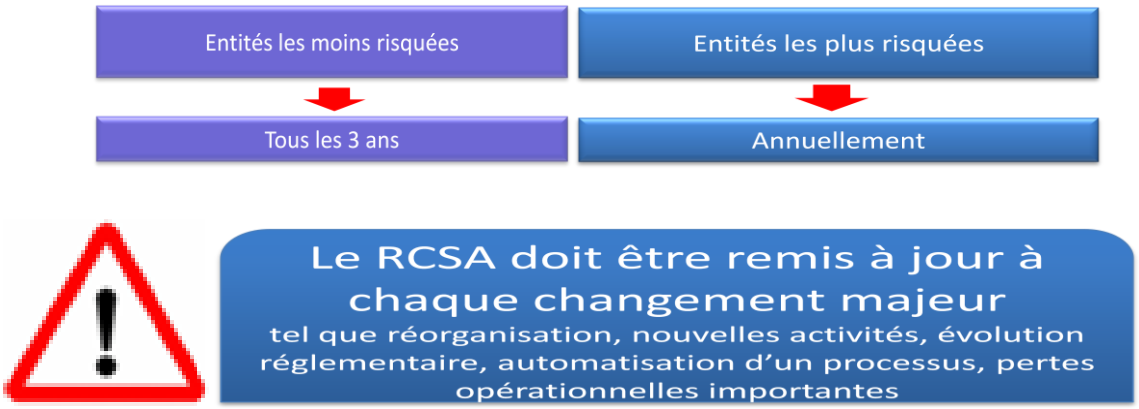


Source : Document Société Générale Algérie

1.7. La mise à jour

- La date de mise à jour est à décider entre la direction des risques et les managers opérationnels
- Bonnes pratiques constatées ➔ au moins tous les deux ans.

Figure N13 : mise à jour RCSA



Source : Document Société Générale Algérie**.**

2 .Mise en place d'une cartographie des risques opérationnels liée a la banque de détail.

Pour cette étape, nous avons procédé au départ par un questionnaire avec questions ouvertes (copie en jointe en annexe n°3).

Au même temps, nous avons essayé de compléter et enrichir ce questionnaire, par l'exploration des diffèrent données collecter durant notre stage, quelles soit des :

- **Données orales :** résultantes des enregistrements effectues au cours des assistance et le recours aux entretiens avec les intervenants.
- **Données écrites :** l'exploitation de la documentation interne et la nomenclature des risques permettent de bien assimiler l'organisation et de diagnostiquer les risques auxquels elle est exposée.

2.1. Le métier de la banque de détail et les risques opérationnels

Selon les métiers, la typologie des risques opérationnels peut être différente.

Les opérationnels de la banque de détail sont sensibilisés depuis de nombreuses années au risque opérationnel « *la banque de détail a une logique de risque opérationnel* », Dans le cadre de sa relation client, l'opérationnel est confronté au risque opérationnel. La plupart des erreurs se traduisent soit par un appel du client car l'erreur est en sa défaveur, soit par une incidence sur le résultat d'exploitation, ce qui génère une réaction de la banque.

Au sein de la Banque de détail, les principaux risques opérationnels identifiés au sein du Groupe Société Générale sont les suivants :

- **Litiges commerciaux** : plus de 40 % des pertes sur 2003-2007. Principalement les litiges avec les tiers liés à l'insuffisance du service au client compte tenu de l'importance de la relation client dans le métier de banque de détail.
- **Erreurs de pricing ou d'évaluation des risques** : principalement pour Etoile Gestion et Gilbert Dupont. Il peut s'agir de la mauvaise évaluation d'une position ou d'une défaillance du suivi des autorisations et des limites.
- **Erreurs d'exécution** : risque inhérent aux flux importants d'opérations à traiter (exemple : erreurs de saisie ou de transmission des ordres).
- **Escroqueries et fraudes commises par des tiers** : cela représente le plus grand nombre d'incidents depuis 2002. Les raisons majeures sont liées à la difficulté de contrôle face à la forte volumétrie et à la crise 2007-08. Importance des fraudes externes (notamment les fraudes monétiques).
- **Pertes des moyens d'exploitation** : risque intrinsèquement élevé (défaut de personnel, pertes de données, pertes des moyens d'exploitation et pertes de services).
- **Défaillance des systèmes d'information** : fréquence faible mais possibilité de forte sévérité

2.2. L'identification des risques opérationnels:

C'est une étape primordiale pour l'élaboration de la cartographie des risques du fait qu'elle conditionne les autres étapes. Son but est répertorier, de manière exhaustive tous les risques opérationnels liés à l'ensemble des activités, produits, processus et systèmes doivent être identifiés.

Pour ce faire, plusieurs techniques peuvent être utilisées, parmi lesquelles le tableau d'identification des risques qui sera utilisé dans cette étude, ce tableau a été établis a partir d'un guide de classification des événements (annexe n°4).

Tableau n°12 : Identification des Risques Opérationnels liée a la banque de détail

Catégorie/Sous-catégorie d'évènement	**Description des risques majeurs et des facteurs d'environnement associés**
Litiges commerciaux	
01. Litige sur activité de conseil.	N/A
02. pratiques commerciales inappropriées.	• Un client nous attaque pour une manière de procéder déloyale vis-à vis de lui : vente forcée suite à la mise en œuvre de campagnes commerciales agressives.
03. inadéquation des produits proposés.	Les demandes de fermeture de compte ne sont pas traitées dans les temps, la banque continue à facturer des frais de tenue de

	compte: les clients déposent plainte pour non respect des instructions. • Habilitation systématique de tous les clients (et facturation) au service de banque en ligne sans vérifier que les clients ont un accès internet. • Le chargé de clientèle vend des produits d'épargne sans se préoccuper des besoins des clients (ex. produits à moyen terme à des personnes âgées)
04. insuffisance au service du client.	• Les relevés compte client sont incomplets et arrêtés à des dates ne correspondant aux clauses contractuelles => litige avec association de défense des consommateurs. • Suite à des débits en compte courant, aucun courrier/information n'a été transmis aux clients qui se retrouvent interdits bancaires et nous attaquent. • Le chargé de clientèle ne transmet pas des ordres de ventes au Bo ou ne les saisit pas directement dans le Core banking system. • Un chargé de clientèle remet un moyen de paiement à un tiers sans procuration sur le compte (conjoint, personne de la famille, associé, coursier). • Un chargé de clientèle traite une demande de virement sur le compte d'une personne protégée (sous tutelle) sans respecter les décisions judiciares le concernant.
05. autres litige avec un tiers (fournisseurs, prestataires…).	• Les comptes d'un client sous administration judiciaire ne sont pas bloqués et le commercial procède à des virements sans l'accord de l'administrateur judiciaire. • Succession: Les héritiers d'un client décédé attaquent la banque car l'agence a viré les avoirs du client à un seul des héritiers sans justificatif. • Apporteur d'affaires : La banque accepte des opérations d'un apporteur d'affaires douteux. • Un client occasionnel fait une remise de cash en faveur d'un client de l'agence et conteste le montant crédité sur le compte du client. • Avocats : conseils inadaptés et/ou honoraires non maîtrisés. • Perte de documents contractuels ou pièces à valeur probatoire. • Signature de document par une personne non habilitée (Représentant de personne morale, personne physique incapable).
06. contrats ou clauses contractuelle inapplicables.	• Les conventions d'ouverture de comptes ou de souscription de produits d'épargne comportent des clauses

	illégales ou des clauses obligatoires n'y figurent pas. • Les clients souscrivent à des produits (yc compris comptes d'épargne) sans signer de formulaire.
Litiges avec les autorités	
07. non respect de la loi bancaire (locale ou française).	• Ouverture de comptes encadrés/réglementés sans respect de la réglementation (comptes d'épargne reglementés, comptes de mineurs, etc). • Comptes dormants/ sans maître non suivis. • Vente de produit d'épargne sans repecter la réglementation bancaire. • Perte de documents officiels administratifs, juridiques ou destruction de documents avant l'extinction du délai légal réglementaire de conservation (autorisation, licence détenue par la banque, garantie reçue, garantie émise, ...).
08. non respect des lois contre la discrimination raciale, sociale et sexuelle…etc.	N/A
09. non respect de la réglementation de travail.	N/A
10. non respect des lois sur l'environnement.	N/A.
11. Non respect des règles de fonctionnement des marchés organisés (actions, futures, marchandises, obligations, etc).	• Un commercial est informé par un de ses clients d'une opération sensible sur le capital de la société où il travaille et tire profit de cette information.
12. non respect des normes de sécurité et de santé.	N/A
13. non respect d'autres lois (non citées dans cette catégorie d'évènement).	• Un employé transmet aux médias des données relatives à certains clients.
14. non respect des exigences réglementaires locales.	• L'entité commercialise des produits non conformes à sa licence : assurance, leasing… • Un chargé de clientèle ouvre un compte à un client présent sur les listes de sanction.
15. non respect des exigences comptables et communication financières.	N/A

16* non respect de la législation fiscale.	N/A
17* blanchiment (interne et externe) et financement du terrorisme.	• Ouverture de comptes sans connaissance client (KYC, embargos etc). • Ouvertures de comptes en courrier guichet sans vérification d'adresse/ sans justificatif. • Défaut de surveillance des comptes (flux exceptionnels, alertes, etc). • Des clients font de grosses remises de cash à la caisse sans que les registres obligatoires soient alimentés. • Souscription de produits 'anonymes' sans vérification de l'origine des fonds (ex. bons de caisse). • Ouverture de compte à un natif américain l'espèce.
Erreurs de « Pricing » ou d'évaluation du risque	
18* défaillance dans le dispositif de gestion et de suivi des autorisations et limites	• Le client dépasse son autorisation de débit et s'engage à couvrir les sommes en question. Le chargé de compte /le responsable d'agence/de DR accepte et force les montants en question. Le déficit s'accroît et finalement le client fait défaut. • Un chargé de comptes procède à une commande de moyens de paiement sans avoir vérifié le statut du client dans le fichier Interdit bancaire/crédit bureau
19* évaluation incorrecte ou inexistante de la position	N/A
20* données de marché et informations publiques fausses ou insuffisantes	N/A
21* modèle de calcul de prix et valorisation erronée	N/A
Erreurs d'exécution	
22* défaillance dans le processus de livraison/règlement de la banque	Défaillance interne dans un processus d'encaissement de chèque. Transfert mal dirigé ou retardé ou inexécuté.
23* défaillance dans les processus de gestion des confirmations d'opérations	N/A

24* défaillance dans la gestion administrative d'une opération jusqu'à son échéance	Un tiers se présente à l'agence et veut réaliser une opération sur le compte du client- ce tiers indique qu'il est le conjoint du client et qu'il a procuration sur le compte et l'opération est traitée par l'agence mais la procuration n'existe pas . Un chargé de clientèle remet un moyen de paiement à un tiers sans procuration sur le compte (conjoint, personne de la famille, associé, coursier) Demande de fermeture de compte non correctement traitée Gestion des avis à tiers détenteurs/saisie-arrêt non faite Successions: suite au décès d'un client les montants arrêtés sont erronés et transmis tels quels au notaire Dossier client perdu Les contrôles obligatoires relatifs à l'inscription des clients sur le fichier crédit bureau/ fichier interdit bancaire ne sont pas effectués lors de l'ouverture de compte et aucune limite dans la commercialisation d'autres produits/moyen de paiement ne peut être appliquée
25* erreurs dans la transmission, la saisie ou la compréhension d'une instruction	La banque facture des commissions de tenue de compte à tort et le PNB s'en trouve artificiellement surévalué. Le chargé de compte omet de transmettre au back office ou d'encoder -s'il doit le faire lui- même les commissions/frais etc liés à la vente de produits ou de services Un caissier inverse les taux acheteurs et vendeurs sur les opérations de change Lors des remises de moyens de paiement aux clients, aucune saisie n'est effectuée dans le CBS ce qui empêche les inventaires réguliers Les dossiers d'ouverture de compte sont partiellement ou mal saisis dans le CBS et ceci provoque des dysfontionnements (adresse d'envoi de relevés, incidents sur virements, commissions de tenue etc).
26* absence ou inexactitude des données nécessaires à la gestion des activités	N/A

27* absence ou inexactitude des rapports d'erreurs dans les chaînes informatiques	N/A
28* structure organisationnelle inadéquate/ faiblesse de l'environnement de contrôle	Inefficience de la surveillance au quotidien et de la supervision managériale.
29* défaillance dans la conservation pour de compte de tiers de document/valeurs	L'accès au coffre d'un client est laissé à une personne non autorisée.
30* défaillance sur services rendus par des sous traitants	Un prestataire essentiel est défaillant (personnalisation CB, fabrication de chéquier, archivage…).
31* défaut de rapprochement	
32* accès laissés par la banque au compte d'un client sans l'accord de ce dernier	N/A
Fraudes et autres activités criminelles	
33* piratage informatique et autres attaques malveillantes des systèmes informatiques de la banque par des tiers	Tous les collaborateurs reçoivent un mail avec un lien. L'und'eux clique sur le lien. C'est uin crypto locker qui bloque tous les postes de travail.
34* autres actes criminelles contre les actifs la banque	N/A
35* vols/escroquerie et fraudes commis par des tiers	Les cartons de signatures sont mal gérés et non numérisés. Lors de demandes de virement, l'agence ne peut vérifier les signatures et des virements frauduleux sont acceptés et traités Les cartes et les codes de CB et les chéquiers clients ne sont pas conservés de manière séparés et dans des armoires fortes. Ces données sont dérobées par un tiers. Le client demande la fermeture de son compte et les moyens de paiements liés ne sont pas récupérés. Des débits en compte surviennent
36* vols par le personnel	Le personnel de caisse dérobe des espèces dans la caisse.

	Des chargés de clientèle dérobent des PC Le personnel de la caisse dérobe le matériel de détection des faux billets et fausses pièces d'identité
37* fraudes sur des transactions par le personnel ou avec complicité	Des clients en courrier guichet ne viennent pas récupérer leurs relevés et n'ont pas d'autres moyens d'accéder à leur compte et le chargé de clientèle fait des retraits/virements non autorisés sur les comptes des clients Aucun suivi des comptes sans mouvement n'est réalisé et un chargé de clientèle ou le responsable d'agence s'approprie les fonds des clients ne se manifestant plus. Les comptes d'épargne ne sont pas rattachés au compte à vue du client et sont rattachés aux comptes de complices qui détournent les fonds. Les clauses bénéficiaires d'un produit d'assurance ne sont pas complétées par le client lors de la signature du contrat et le commercial les détournent à son profit ou ceux de ses proches. Les cartes 'capturées' par le DAB ne sont pas renvoyées vers le BO et sont dérobées par le personnel Un chargé de comptes met en place des faux crédits à partir de comptes clients existants Un informaticien utilise ses privilèges d'accès aux bases de données et aux fichiers de factures CB reçus de l'opérateur monétique pour modifier sur quelques ordres à des fins malveillantes, la domiciliation bancaire des bénéficiaires..
38* utilisation non autorisée / à mauvais escient d'information privilégiée et confidentielle par le personnel	Comportements des utilisateurs non conformes aux principes de prudence liée à la sensibilité des informations manipulées.
Activités non autorisées sur les marchés	
39* activités non autorisées sur les marchés par le personnel	N/A

Pertes de moyens d'exploitation	
40* défaut de personnel	Le caissier est malade et la caisse ne peut être ouverte.
41* perte des données	L'agence brûle: les dossiers clients sont détruits et doivent être reconstitués Les agences sont physiquement indisponibles car des piquets de grèves se tiennent devant chacune d'elles suite à des mouvements socio-politiques
42* pertes des moyens d'exploitation	Les agences sont détruites à cause de mouvements socio-politiques ou une catastrophe naturelle.
43* pertes de services	N/A
8* Défaillance des systèmes d'information	
44* défaut de matériel	N/A
45* données incohérentes ou incompatibles	Des clients viennent à l'agence mais le CBS ne fournit pas le reflet des dernières opérations réalisées par ces derniers => les soldes sont erronés
46* mauvaise gestion de projet	N/A
47* défaillance des softwares	Le Core Banking system est tombé depuis deux jours , dans quelle mesure êtes vous impactés? La fonction d'impression du poste de travail est indisponible pendant 2 jours
48* faiblesse de la sécurité logique.	Le système informatique ne permet pas de ségréguer les droits
49* faiblesse de la sécurité physique.	N/A

Source : élaboré par nos soins

2.3. L'évaluation des risques opérationnels :

Une fois les différents évènements de risque identifiés au niveau chaque activité, l'objectif de la cartographie des risques opérationnels, consiste à procéder à leur évaluation.

Cette étape, aussi, appelée « cotation » s'articule autour de deux informations principales : la fréquence du risque et les pertes financières correspondantes.

Une gestion efficace des risques opérationnels suppose une méthode d'évaluation des risques homogène de façon à pouvoir les comparer les uns par rapport aux autres et être capable d'arrêter les différentes actions à entreprendre au niveau de la banque.
L'approche d'évaluation est découpée en deux niveaux : l'évaluation de la fréquence et celle de l'impact.

L'évaluation de la probabilité et celle de la gravité sont réalisées sur une échelle que présentée ci-dessous :

Tableau n°13 : L'échelle d'évaluation des risques intrinsèques liée à la banque de détail.

Echelle de fréquence / Impact	max perte > 1M €	0,5 < max perte < 1M €	0,05 < max perte <0,5 M €	max perte < 0,05 M €
Mois	4	4	4	3
Année	4	4	3	2
Décennie	3	3	2	1
Au-delà de 10 ans	3	2	1	1
De 1 fois tous les 5 ans à 1 fois tous les 20 ans	4	3	2	2

Source : document société générale

Tableau n°14 : **Cartographie des risques intrinsèques liée à la banque de détail**

Catégorie/Sous-catégorie d'évènement	Evaluation	Barème	Observation
Litiges commerciaux			
02* pratiques commerciales inappropriées	Elevé	3	Non respect de la déontologie bancaire
03* inadéquation des produits proposés	Modéré	2	les produits proposés sont simples.
04* insuffisance au service du client	Elevé	3	Mauvaise qualité du Service fourni
05* autres litige avec un tiers (fournisseurs, prestataires…)	Elevé	3	Les pertes occasionnées par la mise en cause de la responsabilité de la Banque
06* contrats ou clauses contractuelle inapplicables	Modéré	2	Non respect des clauses contractuelles
Litiges avec les autorités			
07* non respect de la loi bancaire (locale ou française)	Elevé	3	Risque d'infraction des lois portant sur

			l'exercice d'une activité bancaire
11* non respect des règles de fonctionnement des marchés organisés	Modéré	2	
13* non respect d'autres lois (non citées dans cette catégorie d'évènement)	Elevé	3	Transgression de décrets, loi de finance…
14* non respect des exigences réglementaires locales	Elevé	3	
17* blanchiment (interne et externe) et financement du terrorisme	Elevé	3	Le marché informel est prépondérant. La manipulation excessive de l'espèce.
Erreurs de « Pricing » ou d'évaluation du risque			
18* défaillance dans le dispositif de gestion et de suivi des autorisations et limites	Elevé	3	Déficience dans une procédure d'autorisation de dossier de crédit.
Erreurs d'exécution			
22* défaillance dans le processus de livraison/règlement de la banque	Très élevé	4	Retard accusé dans livraison/règlement
24* défaillance dans la gestion administrative d'une opération jusqu'à son échéance	Elevé	3	Insuffisance constatée dans la gestion administrative
25* erreurs dans la transmission, la saisie ou la compréhension d'une instruction	Elevé	3	Erreur de saisie. Retard dans l'exécution de l'instruction. Transaction exécutée à tort.
28* structure organisationnelle inadéquate/ faiblesse de l'environnement de contrôle	Elevé	3	Non séparation des tâches (organisation en Front et Back Office). Règle interne et procédure inappropriée.
29* défaillance dans la conservation pour de compte de tiers de document/valeurs	Modéré	2	Perte de documents ou de biens confiés à la banque.
30* défaillance sur services rendus par des sous traitants	Elevé	3	Retard, négligences dans l'exécution de prestations par le sous-traitant.
Fraudes et autres activités criminelles			
33* piratage informatique et autres attaques malveillantes	Modéré	2	Attaque des systèmes Introduction de codes malveillants : (virus, cheval de

des systèmes informatiques de la banque par des tiers			Troie)
35* vols/escroquerie et fraudes commis par des tiers	Elevé	3	Risque de : Hold-up
36* vols par le personnel	Elevé	3	Vols par le personnel de biens propriété de la Banque
37* fraudes sur des transactions par le personnel ou avec complicité	Elevé	3	Transactions fictives sur des comptes client. Non respect délibéré des limites de crédits comme moyen de fraude.
38* utilisation non autorisée / à mauvais escient d'information privilégiée et confidentielle par le personnel	Elevé	3	Utilisation d'informations confidentielles. Délit d'initié.
Pertes de moyens d'exploitation			
40* défaut de personnel	Elevé	3	Risque d'indisponibilité du personnel
41* perte des données	Elevé	3	Risque de détérioration, destruction ou l'indisponibilité des données de référence ou de transaction
42* pertes des moyens d'exploitation	Modéré	2	Risque d'incendie (non criminel). Catastrophes naturelles.
Défaillance des systèmes d'information			
45* données incohérentes ou incompatibles	Elevé	3	Absence ou insuffisance de standard en matière de données. Maintenance insuffisante.
47* défaillance des softwares	Très élevé	4	Dysfonctionnement d'un programme ou toute autre défaillance d'un système informatique
48* faiblesse de la sécurité logique	Elevé	3	Défaillance dans : le contrôle des accès utilisateurs, contrôle des accès au système, aux applications…

Source : élaboré par nos soins

2.4.Représentation graphique de la cartographie

L'identification et l'évaluation détaillée correspondant à chaque tâche dans les processus, sont présentées dans la cartographie des risques suivante.

NB : les notes de qualité des contrôles (QC) ont été établies par rapport aux réponses du questionnaire relatif à l'évaluation des dispositifs de prévention et de contrôle.(annexe 05)

Tableau n°15 : **Cartographie des risques par catégorie d'événement**

Catégories/sous catégories d'évènement	Risques intrinsèques notés	Contrôles notés	Risques résiduels notés	Evaluation des risques résiduels
01 * Litiges commerciaux	**2,8**	**3,00**	**1,86**	**modéré**
02 * Pratiques commerciales inappropriées	3,00	3,00	2 ,00	modéré
03 * Inadéquation des produits proposés	2,00	3,00	1,66	modéré
04 * Insuffisance du service au client	3,00	3,00	2,00	modéré
05 * Autres litiges avec un tiers (fournisseur, prestataire…)	3,00	3,00	2,00	modéré
06 * Contrat ou clauses contractuelles inapplicables	2,00	3,00	1,66	modéré
02 * Litiges avec les autorités	**2 ,8**	**3,00**	**1,58**	**modéré**
07 * Non respect de la loi bancaire (locale ou française)	3,00	3,00	2,00	modéré
11 * Non respect des règles de fonctionnement des marchés organisés (actions, futures, marchandises, obligations, etc.)	2,00	3,00	1,66	modéré
13 * Non respect d'autres lois (non citées dans cette catégorie d'événement)	3,00	3,00	2,00	Modéré
14 * Non respect des exigences réglementaires locales ou françaises	3,00	4,00	0,75	Faible
17 * Blanchiment et financement du terrorisme	3,00	2,00	**1,5**	modéré

03 * Erreurs de "Pricing" ou d'évaluation du risque	**3,00**	**3,00**	**2,00**	modéré
18 * Défaillance dans le dispositif de gestion et de suivi des autorisations et des limites	3,00	3,00	2,00	modéré
04 * Erreurs d'exécution	**3,00**	**2,5**	**2,27**	élevé
22 * Défaillance dans le processus de livraison/règlement de la banque	4	1	4	**très élevé**
24 * Défaillance dans la gestion administrative d'une opération jusqu'à son échéance	3,00	3,00	2,00	modéré
25 * Erreurs dans la transmission, la saisie ou la compréhension d'une instruction	3,00	2,00	2,00	modéré
28 * Structure organisationnelle inadéquate / faiblesse de l'environnement de contrôle	3,00	3,00	2,00	modéré
29 * Défaillance dans la conservation pour compte de tiers de documents / valeurs	2,00	3,00	1,66	modéré
30 * Défaillance sur services rendus par des sous-traitants	3,00	3,00	2,00	modéré
05 * Fraudes et autres activités criminelles	**2,8**	**2,81**	**1,42**	**modéré**
33 * Piratage informatique et autres attaques malveillantes des systèmes informatiques de la banque par des tiers	2,00	1,00	2,00	modéré
35 * Vols / escroqueries / fraudes commis par des tiers	3,00	4,00	0,75	Faible
36 * Vols par le personnel	3,00	3,33	1,90	modéré
37 * Fraude sur des transactions par le personnel ou avec sa complicité	3,00	1,75	1,71	modéré
38 * Utilisation non autorisée / à mauvais escient d'information privilégiée et confidentielle par le personnel	3,00	4,00	0,75	modéré
06 * Activités non autorisées sur les marchés (Rogue Trading)	**0,00**	**0,00**	**0,00**	**Non exposé**
07 * Pertes de moyens d'exploitation	**2,66**	**3,00**	**1,88**	**modéré**

40 * Défaut de personnel	3,00	3,00	2,00	modéré
41 * Perte des données	3,00	3,00	2,00	modéré
42 * Pertes des moyens d'exploitation	2,00	3,00	1,66	modéré
08 * Défaillance des systèmes d'information	**3,33**	**3 ,00**	**2,15**	**élevé**
45 * Données incohérentes ou incompatibles	3,00	3,00	2,00	modéré
47 * Défaillance des softwares	4,00	2,5	2,6	élevé
48 * Faiblesse de la sécurité logique	3,00	3,5	1,85	modéré

Source : élaboré par nos soins

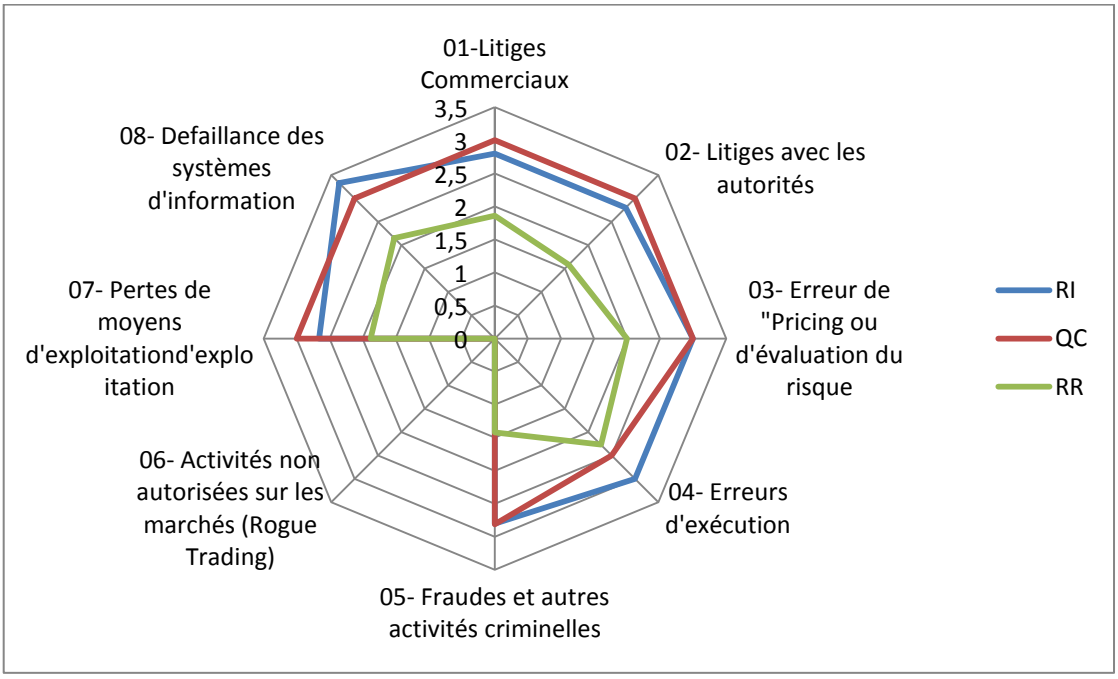
3. Discutions des résultats

Analyse de notre étude de cas est comme suite :

3.1. Analyse des Résultats

La lecture de cette cartographie permet d'apprécier les risques opérationnels identifiés.

Figure N°14 Synthèse des résultats



Source : élaboré par nos soins

A. Erreurs d'exécution (Risque élevé)**:**

- Car possibilités de valorisation erronée des fonds en raison d'un défaut d'information sur le mode de comptabilisation des produits composant les fonds et nombre important de transactions non automatisées.

- La majorité des incidents des RO font partie de la catégorie d'erreur d'exécution liée à la sous catégorie défaillance dans le processus de livraison/ règlement de la banque cette dernière est la plus dominante et elle contient un nombre d'opérations :
  Exécution, livraison et gestion des processus.

- Une défaillance dans le processus de règlement de la banque peut engendrer des pertes directes pour la banque, si ces événements sont répétitifs sur les processus concernés, ils peuvent pénaliser l'activité de la banque et retarder l'exécution de ses engagements vis-à-vis de ses clients et vis-à-vis des correspondants.

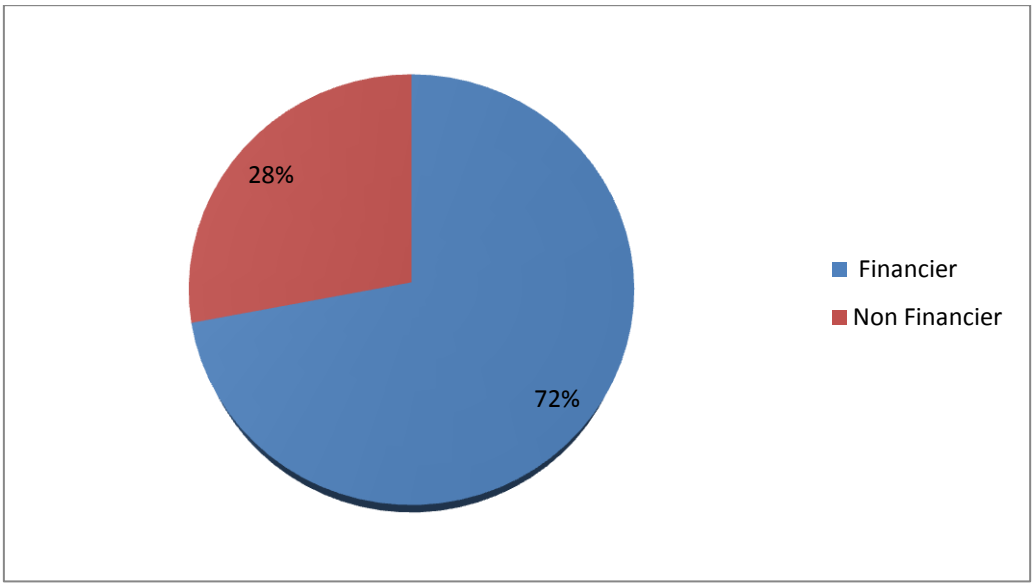
B. Défaillance des systèmes d'information (Risque élevé)**:**

- les activités étant largement dépendantes des systèmes informatiques.
- Une défaillance dans le système d'information : tout problème, fonctionnel ou technique, aussi bien dans les installations des logiciels ou applications (software) ou les équipements de communication : mauvaise adaptation aux besoins, manque de maintenances, introduction non intentionnelle de virus informatique, environnement physique insuffisamment sécurisé, procédures d'accès/ habilitations inadaptées.

C. **Fraudes et autres activités criminelles et Litiges avec les autorités** (Risque modéré) :

Viennent en dernière position et correspondent à des tentatives de fraudes détectées à l'avance.

Figure N°15 Types d'impact des pertes opérationnelles :



Source : élaboré par nos soins

Plus du deux tiers des incidents RO constatés (15 MILLIONS DA) Peuvent potentiellement engendrer un impact financier pour la banque (ne le génère pas systématiquement) dans le sens ou elle concerne des erreurs d'exécutions sur des opérations bancaires aux quotidiens.

3 .2 La mise en place de plans d'actions :

La dernière étape consiste en l'élaboration de plans d'actions correctrices. Le suivi de ces plans est fondamental dans le dispositif global de gestion des risques opérationnels.

Le facteur humain (erreur humaine) représente la cause principale des incidents de type risques opérationnels suite à cela et additivement aux mesures correctrices entreprises pour corriger ces incidents, des plans d'actions transverses ont été arrêté au niveau de siège central de la SGA et correspondant principalement à :

- Un plan de formation pour les collaborateurs non expérimentés sur l'activité bancaire au quotidiens (population cible, agents du guichet et caissiers).
- Une compagne de sensibilisation sur l'importance d'une bonne gestion des risques opérationnels.
- Une communication plus ciblé mise en place lors de la diffusion de nouvelles procédures opérationnelles.
- L'automatisation de certain processus agence et certaines opérations dans le système informatique est une nécessité pour réduire les risque opérationnels.

3.3 Forces des outils du dispositif des gestions des risques opérationnels

Durant notre stage, nous avons eu à relever certaines forces du dispositif de gestion du risque opérationnel de la SGA.

- La SGA est conforme aux normes du groupe SG qui est en conformité avec le comité de bale.
- Le dispositif de gestion des risques opérationnels de la banque concerne tous les acteurs de la banque bien qu'il y ait un département risque opérationnel ce qui permet d'intégrer tout le personnel à la maitrise de ce risque.
- La méthodologie de la SGA en matière de gestion des RO respecte les étapes générales d'un processus de gestion des RO selon les saines pratiques du comité de Bale.
- la politique du groupe inclut des acteurs dont les responsabilités sont clairement définies dans le processus de gestion de chaque filiale dont la SGA.
- **Auto-évaluation des risques et contrôles (RCSA)** :
  - La pertinence de commencer toute démarche ou tout processus de gestion des risques opérationnels par une première évaluation des risque et contrôles.
  - cet outil permet à la banque de déceler les faille des procédures ce qui permet au RRO d'anticiper ou de minimiser la survenance des RO.

- **KRI :**
  - pour chaque KRI il existe une fiche d'identité permettant de diffuser l'intérêt de l'indicateur et l'objectif de la mesure.
  - les indicateurs sont fiables et utiles cela s'explique par les seuils et les limites d'alertes qui ont été fixés par BHFM pour résoudre les incidents.
- **Collecte des pertes internes :**
  -Permet au groupe de connaitre et de suivre le cout de ses risques opérationnels liés soit aux défaillances opérationnels.
  -l'analyse des causes de pertes permet d'identifier et de mettre en place les actions correctrices nécessaires.

3 .4 Insuffisances observées :

Durant notre étude concernant l'élaboration de la cartographie des risques, on a rencontré des difficultés et des insuffisances auxquels il faut pallier.
La défaillance concerne notamment :

- La cartographie est formalisée par l'auto-évaluation des risques et du contrôle, ce qui rend l'outil difficile à utiliser.
- le reporting RCSA est transmis tous les 2 ans à BHFM ce qui est très lent.
- **Lourdeur du dispositif**
  Des termes tels 'lourd', 'prend beaucoup de temps', 'fastidieux' reviennent régulièrement chez les correspondants risques opérationnels.
  Le RCSA est un outil complet mais lourd en termes d'utilisation et complexe pour le personnel de la banque.
- **Rôle du langage**
  La difficulté du langage a été soulevée dans le cadre du RCSA.
  Néanmoins, Le formalisme du RCSA suppose l'utilisation d'un langage spécifique, issu d'une culture de risque et de contrôle. Il a été élaboré au sein de la direction des risques et a rapidement suscité, les questions qui sont parfois difficiles à comprendre. C'est assez théorique pour un expert terrain. Certaines questions font plusieurs lignes et entre ces lignes vous avez également plusieurs questions qui sont regroupées. Il faut répondre aux questions des questions.
  Les difficultés de compréhension se retrouvent dans les réponses et leur pertinence. Pour une même approche du risque, des opérationnels ne répondront pas de la même façon aux questions.

3.5 Pistes d'amélioration.

Afin de remédier à ces insuffisances, nous avons émis les recommandations suivantes :

- L'application de toutes les procédures, pourrait contribuer à l'optimisation de la gestion des risques, en ce qui concerne ce point nous suggérons à la banque de veiller au renforcement de la connaissance des procédures de celle-ci du personnel.

- Lancement de nouveau projet visant à atteindre une qualité opérationnelle acceptable.
- L'auto-évaluation de risque et contrôle étant formalisée par un ensemble de cartographie des risques, rend son utilisation complexe, donc nous suggérons à la banque de mettre à la disposition un fichier RCSA à chaque agent opérationnel pour qu'il le remplisse de manière régulière.
- en ce qui concerne le reporting RCSA fait à BHFM, nous pensons qu'il serait mieux de le transmettre chaque année voire semestriellement pour que la société mère et sa filiale sachent les procédures manquantes.
- dialogue, échange, communication, sont autant d'éléments qui ont été mis en avant comme essentiel au déploiement et à la compréhension du dispositif du risque opérationnel. cette communication ne se caractérise pas par sa fréquence mais par la qualité des échanges.
- Renforcer d'autres dispositifs de pilotage de risque, en procédant par exemple à la mise en place de nouveaux KRI qui permettront de suivre les processus à risque avec d'avantage de précision.
- **Constitution d'un langage commun :**

  La communication suppose la compréhension de la terminologie utilisée. La définition des catégories de risque, le vocabulaire porté par le RCSA a constitué la base de la communication. La répétition des mêmes termes, tant dans la communication écrite qu'orale, facilite le partage d'un langage commun.

  Le langage a du s'adapter aux exigences du métier afin d'en faciliter la compréhension. Par delà le langage en tant que moyen de communication, la question du sens a été prise en compte rapidement par nos interlocuteurs de la ligne métier risque opérationnel.

- **Formation et sensibilisation**

La dimension pédagogique de la cartographie est importante. La spécificité de l'exercice, les concepts utilisés et le passage obligatoire par l'outil ont nécessité de la part de RISQ/OPE d'effectuer de nombreuses formations vis-à-vis des correspondants risque opérationnel, ceux-ci devant alors maîtriser l'exercice pour pouvoir le faire de manière autonome avec les interlocuteurs du métier. Il s'agit alors de sensibiliser, de former et de faire comprendre.

Conclusion

Le but de cette deuxième partie, a été de connaitre de manière générale l'application des outils du dispositif de gestion des risques opérationnels mise en place par la SGA.

Cette partie nous a permis également de présenter l'exercice RCSA.

Ce dernier, sert à repérer les risques auxquels l'activité bancaire est exposée. Il se résume en quatre étapes : La réalisation de la cartographie des risques intrinsèques, l'évaluation du dispositif de prévention et de contrôle, l'élaboration d'une cartographie des risques résiduels et enfin la proposition de plans d'actions correctrices. Le principal but revient à minimiser l'impact des risques opérationnels sur l'activité de la banque et à diminuer le montant des pertes en cas de survenance.

Par la suite, nous avons mis en application la méthode d'élaboration de la cartographie des risques opérationnels, ou nous avons précisé nos choix quant à la portée de nos travaux (cartographie thématique liée a la banque de détail). Ainsi, nous avons identifié les risques inhérents et évalué ces risques. En effet, ces derniers ont fait l'objet de plusieurs représentations suivant les différents axes d'analyse. De plus, les résultats de tout ce que nous venons d'avancer ont été présentés et commentés.

L'étude de ce cas pratique a été intéressante et surtout très enrichissante pour nous. Nous avons, dans un premier temps, pu voir, sur le terrain, la déclinaison de différentes réflexions faites par les théoriciens au sujet de la cartographie des risques, et dans un second temps, nous avons essayé de répondre aux différentes interrogations.

CONCLUSION GENERALE

Conclusion Générale

L'activité bancaire est une activité complexe, du fait de la diversification des produits et services qu'elle propose. Cette complexité rend le système bancaire vulnérable envers une multitude de risques en général, et plus particulièrement le risque opérationnel.

Il y a lieu de noter que pour assurer une gestion optimale, les banques algériennes doivent impérativement se conformer aux nouvelles dispositions de Bâle (notamment Bâle II portant ratio de solvabilité Mc DONOUGH), et cela ne peut se faire qu'à travers la mise en place d'un dispositif efficace de maitrise du risque précité.

Il y a lieu de rappeler qu'un tel dispositif nécessite au préalable une identification rigoureuse et précise des risques

Pour y parvenir, la cartographie des risques s'impose comme un atout indispensable pour une gestion saine dans la mesure où cette dernière permet d'identifier, d'évaluer et de classifier l'ensemble des risques y afférents.

A la lumière de ces propos et dans le cadre de notre mémoire, nous avons opté pour la cartographie des risques opérationnels comme sujet de notre étude, et nous avons choisi la banque de détail comme une application pratique de la cartographie des risques, au sein de la société générale Algérie.

Afin d'atteindre l'objectif de la recherche, la problématique suivante a été le socle de cette étude : **quelle méthodologie de cartographie des risques est la plus appropriée pour la maîtrise des risques opérationnels au sein de la Société Générale Algérie?**

Et afin de répondre à cette dernière, elle a été scindée en les questions subsidiaires suivantes :

1. Comment la cartographie des risques opérationnels contribue à la maitrise des risques afférents aux processus métier ?
2. Quel sont les dispositifs mis en place pour la gestion du risque opérationnel au sein de la banque Société Générale Algérie?
3. Dans quelle optique s'inscrit la démarche de la Société Générale Algérie pour pouvoir gérer efficacement le risque opérationnel

La recherche a été axée sur une réponse anticipée à affirmer ou à nier, en effet, les hypothèses suivante a été avancée :

- Elaborer une cartographie des risques est une impérieuse nécessité. D'une part, c'est une aide précieuse à la prise de décision. D'autre part, c'est un moyen efficace permet aux banque d'avoir une bonne anticipation des risque liés à l'activité bancaire auxquels elles doivent faire face pour mettre en place les contrôles indispensables.
- Les dispositifs de gestion des risques opérationnels mis en place par la SGA conformément aux exigences du comité de Bale.

- pour assurer une gestion efficace du risque opérationnel, la banque doit tout d'abord procéder à une décomposition de son activité en lignes de métiers reflétant les différentes composantes de ce risque.

A fin d'apporter des éléments de réponses aux questions posées. Une recherche sur la littérature du sujet a été effectuée, afin de ressortir les fondements de bases du secteur bancaire, ainsi que les risques opérationnels qui lui sont afférent. Par la suite, l'étude s'est focalisée, avec plus de détails, sur la cartographie des risques et sur la méthodologie de son élaboration.

Cette méthodologie adoptée dans le traitement de ce thème a permis de répondre aux questions posées et de confirmer touts les hypothèses.

En effet, **la première hypothèse** est confirmée, Une cartographie des risques bien conçue et bien menée permet d'apporter des repenses satisfaisantes aux attentes en matière de gestion des risques, ainsi que la collecter les informations nécessaires a la compréhension global des risques et a leurs évaluation. C'est bien le minimum que l'on doit dans le cadre du pilotage des performances opérationnelles.

Tandis que **la seconde** est partiellement confirmée. Concernant le Groupe Société-Générale, le choix a été porté sur l'utilisation des Méthodes Avancées (approche prescrite par les textes bâlois) pour la gestion des risques opérationnels. A cet effet, le Groupe exige à ses filiales de couvrir leurs risques opérationnels (cas de la SGA), de mettre en place et de développer les dispositifs de suivi et outils de mesure constituant la méthode AMA. Les dispositifs mis en place sont importants et dès 2006, ils étaient conformes aux principales exigences réglementaires.

Quant à la **troisième hypothèse** elle aussi confirmée. C'est ainsi que la SGA applique les recommandations de Bâle II en introduisant l'exercice d'auto évaluation des risques et des contrôles (RCSA) qui consiste d'abord à évaluer les risques intrinsèques sans prendre en compte les dispositifs de contrôles en se basant sur les facteurs d'environnement, le référentiel des questionnaires métier, également appelés «scorecards métier», spécifiques à chaque métier ou fonctionnel, regroupant les facteurs de risque pertinents pour le métier considéré et les questions d'évaluation associées, une fois cette étape terminée, on évalue les dispositifs de prévention et de contrôle afin de déduire les risques résiduels.

A travers notre revue de littérature et notre étude pratique, nous pouvons constater que le risque opérationnel est un risque qui se situe non seulement au niveau de chaque activité et transaction effectuée au sein de la banque mais est surtout un risque qui ne prévient pas. En effet, il peut survenir à n'importe quel moment suite à n'importe quelle erreur d'exécution effectué par les agents de la banque et les opérationnels du métier. Il

peut donc faire l'objet de propagation rapide et causer des pertes matérielles et financières considérables à la banque.

L'audit interne ,étant le garant de l'efficacité du contrôle interne de la banque , contribue a l'évaluation et l'amélioration du système de contrôle interne et aide donc à la prévention des risques opérationnels .Cependant , le risques peut être persistant et l'audit ne peut ,à elle seule, le maitriser . C'est pour cela que le groupe Société Générale a mis en place une structure de détection et de gestion du risque spécialisée dans les risques opérationnels et risque de conformité et qui se trouve totalement indépendante de celle qui traite des autres types de risques.
Cette structure, dénommée département ROC « Risques Opérationnels et Conformité », est responsable de concevoir et de mettre en œuvre le dispositif de gestion des risques opérationnels du groupe et d'assurer la supervision fonctionnelle de la filière risque opérationnels. Elle a la lourde tache d'assurer la cohérence, l'intégrité et la conformité de ce dispositif aux dispositions réglementaires et est également en charge de la coordination et de la maitrise des risques opérationnels du groupe et de ses filiales dans le monde.
A cet effet, nous considérons qu'il serait intéressant et consciencieux que toutes les banques créent une structure « ROC » au sein de leur organisation qui non seulement se spécialiserait dans la gestion du risque opérationnel mais collaborerait directement avec la structure d'audit interne pour une meilleure détection, prévention et maitrise de cette catégorie de risque.

Tout travail de recherche comporte **des limites** et nous n'échappons pas à cette règle. S'il ne s'agit pas de remettre en cause nos résultats, la prise de conscience de ces limites suscitera des points d'attention dans le cadre de futures recherches. Notre principale limite nous semble d'ordre méthodologique. Si le choix de l'étude est venu naturellement au regard de la confidentialité perçue du sujet, nombre limité de risques identifiés.

A la fin de ce travail, nous ouvrons quelques **pistes de recherches** du fait que certaines questions ambigües restent en suspens et méritent d'être étudier, parmi lesquelles nous pouvons citer :

- quelle est la performance des outils permettent de mesurer la qualité du dispositif de gestion du risque opérationnel mis en place par la SGA ?

- Quel est l'apport de l'audit interne en matière de maitrise des risques opérationnels au sein d'un établissement bancaire ?

Bibliographie

1. les ouvrages

- VERBOOMEN Alain, Louis DE BEL, « Bâle II et le risque de crédit », ED Larcier, Belgique 2011.
- COHEN Elie, « Dictionnaire de gestion », Ed La découverte, Paris, 1997.
- COUCHOUD Christian, « risques opérationnels, chronique d'une mise en place commune d'intérêt », horizons bancaire, 2004.
- CARON Pierre « investir et gérer le risque »ED presses de l'université du Québec, CANADA ,2014.
- GILBERT de Marshal, « La Cartographie Des Risques », ED. AFNOR, 2003.
- IFACI et Price Water House Coopers, « Le Management Des Risques De L'entreprise : cadre de référence et techniques d'application», édition d'organisation, Paris, 2005.
- JEAN le Ray, « organiser une démarche de cartographie des risques », AFNOR, 2008.
- KERBEL Pascal, « mise en oeuvre d'un contrôle interne efficace », Edition AFNOR, 2007.
- LEMARQUE Eric, «Management de la banque : Risque, relation client, organisation », 2éme édition, ED PEARSON, France, paris, 2008.
- LOUISO Jean-Paul, « Gestion des risques, 100 question pour comprendre et agir », 2eme édition, édition AFNOR, paris 2014.
- METAYER Y, HIRSCH L, « Premiers pas dans le management des risques », Edition afnor, Paris, 2007.
- MOREAU Franck, « Comprendre Et Gérer Les Risque », Edition d'organisation, Paris, 2002.
- MOUGIN Yvon, la cartographie des processus, édition d'organisation, paris 2004, P 37.
- Renard Jacques, « théorie et pratique de l'audit interne, éditions d'organisation », 7ème édition, paris, 2010.
- SARDI Antoine, « Audit et contrôle interne bancaire », ED AFGES, France, Paris 2002.

2. Articles et revues

- ALBRAND Guy, « le risk assessement : quelques bonnes pratiques », revue française d'audit interne, 2003.
- DENIAU Philippe and RENOUX, Etienne **«** la cartographie du risque opérationnel : outil réglementaire ou outile de pilotage ?; » revue d'économie financière, NO 84 ;le risque opérationnel ; juin 2006 .
- DUMONTIER Pascal & DUPRE Denis, « Pilotage bancaire : les normes IAS et la réglementation Bâle II », Edition Revue Banque, 2005
- EUROGROUP consulting, Bale 3 quel impact sur les métiers de la banque, Avril 2011
- FORTUGUE & al, « cartographie des risques : quelle valeur ajoutée ? Quel processus ? », 2001
- IFACI « Cahiers de la recherche, la cartographie des risques », 2013.
- IFACI, « guide d'audit cartographie des risques », Edition Les Cahiers de la Recherche, 2006.
- JIMENEZ .C & P.MERLIER, « prévention et gestion des risques opérationnels », ED REVUE-BANQUE, Paris, 2004.
- JIMENEZ .C & P.MERLIER & D.CHELLY, « Risques Opérationnels : de la mise en place du dispositif à son audit», Éd. Revue Banque 2008.
- NICOLET Marie-Agnès, Michel Maignan**,** « Méthodologie Contrôle interne et gestion des risques opérationnels », Revue Banque, nº668, Avril 2005.
- MOULAIRE M, « la cartographie des risques , un outil de management des risques en établissement de santé », risque et qualité , N°4 ,2007 .

3. Texte réglementaires

- Le comité de Bale sur le contrôle bancaire, « nouvelle accord de Bale sur les fond propres » (document soumis à consultation), avril 2003.
- le règlement banque d'Algérie n ° 11/08 du 28 novembre 2011.
- le règlement banque d'Algérie n ° 14/01 du 16 février 2014.

4. Thèse et mémoires

- FRITCH Henri, « La maitrise des risques lié aux processus de gestion des réclamations clients », Thèse professionnelle présentée et soutenue en vue de l'obtention du Mastère spécialisé « Audit Interne et Contrôle de Gestion **»,** Paris, 2012.
- NDIAYE Serigne « Elaboration d'une cartographie des risques opérationnels du cycle personnel /organismes sociaux : cas de la fondation agir pour la santé(FAES) »institut supérieur de comptabilité, de banque et de finance, ISCBF, promotion 19 (2007-2008).
- SAHLI EL-HACHEMI Aniss, « le role de l'audit interne dans la maitrise des risques opérationnels au sein du secteur bancaire », master 2 en sciences de gestion .option : audit comptable et financier, MDI, promotion 2014 -2015.
- SAIDANI Zahir, « analyse du processus de gestion du risque opérationnel par les banques » , mémoire en vue de l'obtention du diplôme de magistère en sciences économiques, option : monnaie-finance-banque, université mouloud MAMMERI. TIZI OUZOU, 2011/2012.
- TANTAN Kawtar, « Le processus de gestion et de mesure du risque opérationnel dans le cadre des règles et des saines pratiques prévues par le comité de Bâle », université TIME , Tunisie, 2007/2008.

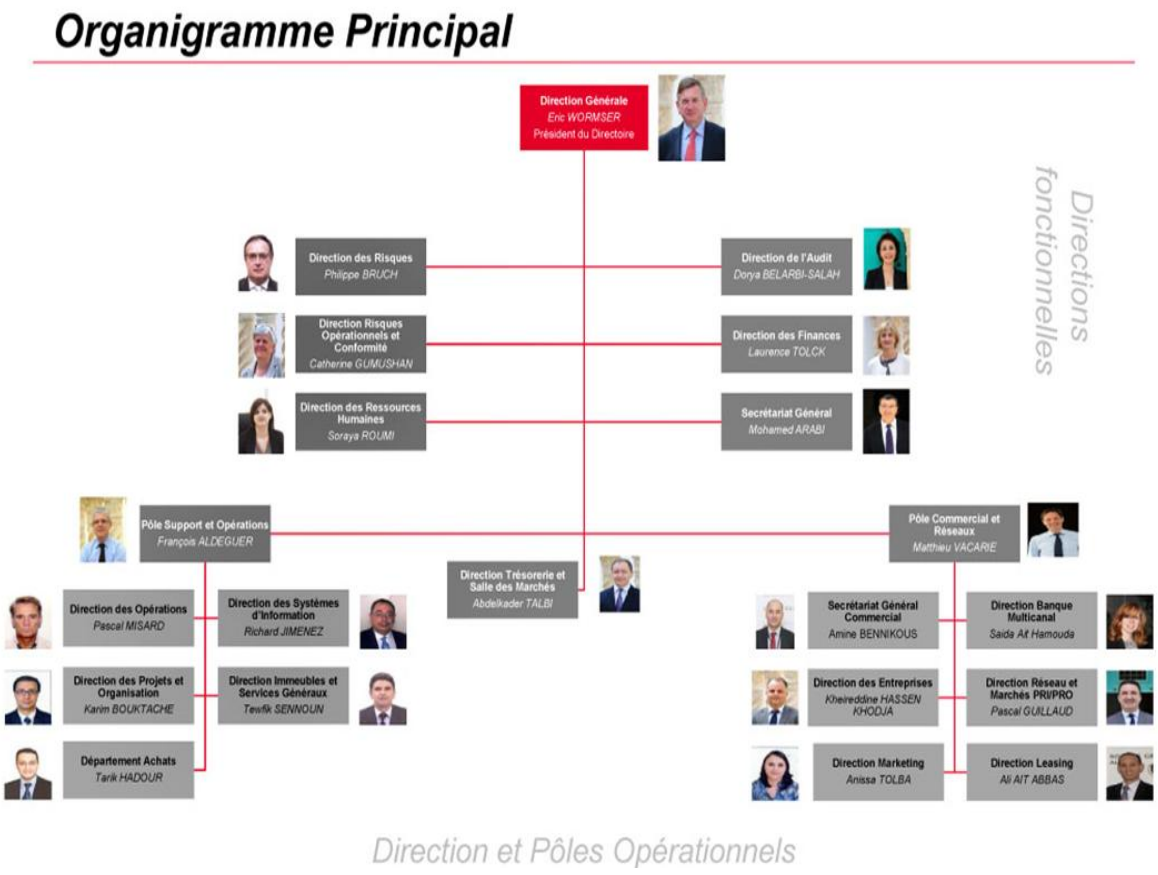
5. Autres

- Document groupe société générale, document de référence ; 2015
- Document groupe société générale, dispositif d'auto évaluation des risques RCSA ,2014
- KPMG. Bale III : les impacts à anticiper , , Mars 2011.

6. Webographie

- www.bis.org
- Http://www.bank-of-algeria.dz/html/legist014.htm
- http://www.memoireonline.com
- http://www.societegenerale.dz/nous_connaitre.html
- http://www.eurogroupconsulting.fr
- http://www.kpmg.com
- https:// www.societegenerele.dz

<u>Annexe n° 1</u> : Organigramme société générale.



Annexe n° 2 :Questions relatives à l'environnement de gestion du risque opérationnel.

		Oui	Non	En cours de réflexion	En cours de mise en place	Sans objet
	1. Environnement de gestion du risque opérationnel					
1	L'organe délibérant de votre établissement a-t-il approuvé la **mise en place** d'un dispositif de surveillance dédié au risque opérationnel ?	X				
2	Ce dispositif couvre-t-il **l'ensemble** de l'activité de votre établissement ?	X				
3	La Direction générale a-t-elle établi des lignes claires de **responsabilité** en matière de risque opérationnel ?	X				
4	Dispose-t-elle **d'états de synthèse** adaptés permettant la surveillance du risque opérationnel ?	X				
5	Votre établissement définit-il clairement les **types** de risques opérationnels auxquels il est exposé?	X				
6	Le dispositif de surveillance du risque opérationnel de votre établissement est-il **proportionné** à son profil de risque ?	X				
7	L'organe délibérant **examine-t-il régulièrement** l'adéquation du dispositif à l'exposition de votre établissement aux risques opérationnels ?	X				
8	La Direction générale s'assure-t-elle de la mise à niveau du dispositif de surveillance du risque opérationnel au sein de **toutes les activités, et de toutes les implantations** ?	X				
9	La Direction générale s'assure-t-elle de la mise à niveau du dispositif de surveillance du risque opérationnel à **tous les échelons de l'encadrement** ?	X				
10	La fonction de gestion de risque opérationnel est elle **séparée** de la fonction de contrôle interne ?		X			
11	La gestion des risques fait elle partie du domaine **suivi** par le contrôle interne ?	X				
12	Votre établissement a-t-il mis en place un **programme d'audit** adéquat pour vérifier que les règles et procédures en matière de risque opérationnel ont été mises en place efficacement ?	X				
13	La Direction générale s'assure-t-elle que **l'indépendance de l'Audit** est maintenue ?	X				
14	La Direction générale **transfère-t-elle effectivement à l'encadrement la responsabilité et l'autorité** en matière de gestion du risque opérationnel ?	X				
15	La Direction générale **transfère-t-elle effectivement à l'encadrement les moyens et ressources** nécessaires en matière de gestion du risque opérationnel ?	X				
16	L'encadrement traduit-il les principes de la gestion de risque opérationnel en **procédures** au niveau de chaque unité ?	X				
17	La Direction générale s'assure-t-elle que les procédures en matière de risque opérationnel ont été clairement **communiquées à l'ensemble du personnel** ?	X				
18	La Direction générale s'assure-t-elle que le dispositif de gestion du risque opérationnel est **conforme** aux règles qu'elle a établi en la matière ?	X				
19	La Direction générale s'assure-t-elle que les différentes équipes responsables de la gestion des risques (marché, crédit, opérationnel) **communiquent efficacement** entre elles ?	X				

20	La Direction générale s'assure-t-elle que sa **politique de rémunération du personnel** n'est pas susceptible d'entrainer des comportements à risque ?	X				

2. Identification et évaluation du risque opérationnel

21	Votre établissement a-t-il mené une analyse **historique** sur le risque opérationnel (analyse des causes et pertes subies par l'établissement) ?	X				
22	Votre établissement a-t-il mené une analyse **prospective** sur le risque opérationnel (inventaire des différents facteurs de risque auxquels l'établissement est exposé) ?	X				
23	Ces analyses ont-elles conduit à l'élaboration d'une typologie du risque opérationnel **conforme aux 7 facteurs de risques** définis par le Comité de Bâle ?	X				
24	Les 8 **lignes de métiers** définies par le Comité de Bâle ont-elles été identifiées au sein de votre établissement ?	X				
25	Quelles sont cellescorrespondant aux **activités exercées** par votre établissement ?					
	Financement des entreprises					
	Négociation et vente					
	Banque de détail	X				
	Banque commerciale					
	Paiement et règlement					
	Fonctions d'agent (et conservation)					
	Gestion d'actifs					
	Courtage de détail					
26	Les **facteurs internes** (nature des activités, qualité de l'organisation, des procédures et des ressources humaines) sont-ils pris en compte dans votre évaluation du risque opérationnel ?	X				
27	Les **facteurs externes** (progrès technologiques, mutations sectorielles, cadre réglementaire) sont-ils pris en compte dans votre évaluation du risque opérationnel ?	X				
28	Une étude d'impact sur l'exposition au risque opérationnel est-elle réalisée **préalablement à tout changement** intervenant dans l'organisation et l'activité de votre établissement ?	X				
29	Votre établissement utilise-t-il un de ces **types d'outils** pour évaluer les risque opérationnel :					
	Evaluation qualitative (scorecards) ?		X			
	Cartographie de risques ?	X				
	Indicateurs-clés de risques ?	X				
	Modèle interne ?		X			
	Autre ?					
30	Ces outils sont-ils **mis en place** dans vos différentes lignes de métiers ?					
	Financement des entreprises					
	Négociation et vente					
	Banque de détail	X				
	Banque commerciale					
	Paiement et règlement					
	Fonctions d'agent (et conservation)					
	Gestion d'actifs					
	Courtage de détail					

31	Votre établissement dispose-t-il d'une **base de données historique** recensant les pertes et incidents ?	X					
32	Avez-vous **mis en place** la collecte de ces données historiques pour vos différentes lignes de métiers ?						
	Financement des entreprises						
	Négociation et vente						
	Banque de détail	X					
	Banque commerciale						
	Paiement et règlement						
	Fonctions d'agent (et conservation)						
	Gestion d'actifs						
	Courtage de détail						

3. Reporting interne relatif au risque opérationnel

33	Votre établissement a-t-il **mis en place** un reporting interne sur le risque opérationnel ?	X					
34	**Une unité dédiée** est-elle responsable de la production de ce reporting ?	X					
35	Ce reporting **reflète-t-il et identifie-t-il** tous les domaines à risques ?	X					
36	Ce reporting est-il **communiqué** aux responsables opérationnels et au contrôle interne ?	X					
37	Les responsables opérationnels vérifient-ils régulièrement la **justesse et la pertinence** de ce reporting ?	X					
38	Ce reporting comporte-t-il des **indicateurs d'alerte** qui mettraient en évidence toute augmentation du risque ou toute possibilité de pertes futures ?	X					
39	Ce reporting motive-t-il des **actions correctrices** sur les problèmes mis en évidence ?	X					
40	Les informations transmises à la Direction générale lui permettent-elles d'apprécier le profil général d'exposition au risque opérationnel de l'établissement ?	X					

4. Dispositif de réduction du risque opérationnel

41	Les domaines présentant des sources potentielles de **conflit d'intérêt** au sein de votre établissement sont-ils identifiés ?	X					
42	Une **séparation appropriée des tâches** a-t-elle été mise en place sur la base de cette identification ?	X					
43	Ces domaines, sources potentielles de conflit d'intérêt, font-ils l'objet d'un **suivi et d'un contrôle indépendant et attentif** ?	X					
44	Votre dispositif de **contrôle interne** prévoit-il la surveillance du respect d' un **système de limites** formalisé encadrant les engagements et les opérations ?	X					
45	Votre dispositif de **contrôle des systèmes d'information s'assure-t-il dela maintenance** d'**accès sécurisés aux actifset aux données** ainsi que des procédures permettant leurs sauvegardes ?	X					
46	Votre dispositif de **contrôle interne** permet-il d'identifier les lignes de métiers ou produits dont la **rentabilité est atypique** ?	X					
47	Votre dispositif de **contrôle interne** inclut-il des **vérifications de transactions et des rapprochements de compte** en vue de réduire l'exposition au risque	X					

	opérationnel ?					
48	Votre dispositif de **contrôle interne** couvre-t-il le développement de **nouvelles activités** pour lesquelles le risque opérationnel peut-être plus prononcé ?	X				
49	Votre établissement procède-t-il à la vérification de l'**adéquation des compétences et de l'expérience des employés** aux fonctions exercées ?	X				
50	Lors de l'**automatisation des processus** et des traitements de données, des mesures sont-elles prises pour éviter que les pertes opérationnelles de "haute fréquence et faible sévérité" ne se transforment en pertes opérationnelles de "faible fréquence et de grande sévérité" ?	X				
51	Votre établissement a-t-il recours à l'**externalisation** de certaines de ses activités ou fonctions ?		X			
52	Si oui, des **règles internes de gestion des risques liés à l'externalisation** ont-elles été établies ?					X
53	Vos **accords d'externalisation** assurent-ils un **partage clair des responsabilités** entre les prestataires externes et votre établissement ?					X
54	Votre établissement s'assure-t-il que les prestataires externes disposent d'une **capacité financière** leur permettant de faire face à leurs responsabilités ?	X				
55	Votre établissement s'assure-t-il que l'activité des prestataires externes est conduite **en accord avec les lois et les réglementations** applicables ?	X				
56	Votre établissement s'assure-t-il que l'activité des prestataires externesest conduite d'une manière **sûre et de qualité** ?	X				
57	Votre établissement évalue-t-il l'**impact** sur ses opérations et ses clients d'une **déficience potentielle** de ses prestataires externes (interruption de service ou défaillance plus grave) ?	X				
58	Votre établissement mène-t-il des **audits** des prestataires externes et suit-il leurs activités sur une base régulière ?				X	
59	Votre établissement a-t-il évalué les coûts et les ressources nécessaires pour **changer de prestataires externes** dans le cadre de la mise en oeuvre d'un plan de secours ou d'un plan de continuité de l'activité ?	X				
60	Votre établissement a-t-il **décidé de ne pas réduire** certains risques opérationnels ?		X			
61	Ces risques opérationnels qui ne font pas l'objet d'une réduction sont-ils **couverts par une assurance** ?				X	
62	Votre établissement a-t-il fait la cartographie des risques **couverts par une police d'assurance** ?				X	
63	Votre établissement s'assure-t-il régulièrement que les contrats d'assurance n'ont pas **d'échéance résiduelle inférieure à 3 mois** ?				X	
64	Ces décisions (questions 59 et 60) font elles l'objet d'une **information de l'organe délibérant** ?					X
65	Disposez-vous d'un **outil desuivi des risques que votre établissement a décidé de ne pas réduire ou assurer** ?					X

5. Plans de secours et de continuité de l'activité

66	Votre établissement **dispose-t-il de plans de secours et de continuité de l'activité** ?	X				

67	Ces plans s'appuient-ils sur des **scénarios en adéquation avec la taille et la complexité des opérations** de votre établissement ?	X				
68	Votre plan de continuité de l'activité comprend-il des mesures permettant un **redémarrage planifié** de l'ensemble des activités ?	X				
69	Votre établissement s'assure-t-il de la **conformité du plan de continuité de l'activité avec les lois et les réglementations** applicables ?	X				
70	Votre établissement s'assure-t-il de l'**efficacité** du plan de continuité de l'activité ?	X				
71	Votre plan de continuité de l'activité couvre-t-il les **processus critiques qui dépendent de prestataires externes ou d'autres tiers,** et pour lesquels une reprise rapide des services est essentielle ?	X				
72	Votre établissement dispose-t-il de **sites de stockage** pour y sauvegarder des données essentielles ?	X				
73	Votre établissement dispose-t-il de **sites de secours** pour y poursuivre certaines de ses activités essentielles ?	X				
74	Vos sites de stockage et de secours sont-ils éloignés d'une **distance suffisante** de votre site principal ?	X				
75	L'**intégrité des données** qui sont restituées à partir du site de secours est-elle **régulièrement testée** ?	X				
76	Vos plans de continuité d'activité sont-ils **régulièrement mis à jour** afin de demeurer cohérents avec l'activité courante et les orientations stratégiques de votre établissement ?	X				
77	Ces plans sont-ils **périodiquement testés** pour s'assurer que votre établissement sera capable de les exécuter dans le cas d'une interruption de l'activité ?	X				

Annexe n° 3 : Catégories/Sous-catégories d'événements

LITIGES COMMERCIAUX	LITIGES AVEC LES AUTORITES	ERREURS DE « PRICING » OU D'EVALUATION DU RISQUE	ERREURS D'EXECUTION	FRAUDE ET AUTRES ACTIVITES CRIMINELLES	ACTIVITES NON AUTORISEES SUR LES MARCHES (ROGUE TRADING)	PERTES DES MOYENS D'EXPLOITATION	DEFAILLANCE DES SYSTEMES D'INFORMATION
1. Litiges sur activités de conseil	7. Non respect de la loi bancaire	18. Défaillance dans le dispositif de gestion et de suivi des autorisations et des limites	22. Défaillance dans le processus de livraison et/ou de règlement de la banque	33. Piratage informatique et autres attaques malveillantes des systèmes informatiques de la banque par des tiers	39. Activités non autorisées sur les marchés par le personnel	40. Défaut de personnel	44. Défaillance de matériel
2. Pratiques commerciales inappropriées	8. Non respect des lois contre la discrimination	19. Evaluation incorrecte ou inexistante de la position	23. Défaillance dans les processus de gestion des confirmations d'opérations	34. Autres formes d'actes criminels contre les actifs de la banque		41. Pertes de données	45. Données incohérentes ou incompatibles
3. Inadéquation des produits proposés	9. Non respect de la réglementation du travail	20. Données de marché et informations publiques fausses ou insuffisantes	24. Défaillance dans la gestion administrative d'une opération jusqu'à son échéance	35. Vols/escroqueries /fraudes commis par des tiers		42. Pertes de moyens d'exploitation	46. Mauvaise gestion de projet
4. Insuffisance du service au client	10. Non respect des lois sur l'environnement	21. Modèle de calcul de prix ou de valorisation erroné	25. Erreurs dans la transmission, la saisie ou la compréhension d'une instruction	36. Vols par le personnel (induant les prestataires de services, stagiaires)		43. Perte de services	47. Défaillance de software
5. Autres litiges avec un tiers	11. Non respect des règles de fonctionnement des marchés organisés		26. Absence ou inexactitude des données nécessaires à la gestion des activités	37. Fraude sur des transactions par le personnel ou avec sa complicité			48. Faiblesse de la sécurité logique
6. Contrat ou clauses contractuelles inapplicables	12. Non respect des normes de sécurité et de santé		27. Absence ou inexactitude des rapports d'erreur dans les chaînes informatiques	38. Utilisation non autorisée/à mauvais escient d'information privilégiée et confidentielle par le personnel			49. Faiblesse de la sécurité physique
	13. Non respect d'autres lois		28. Structure organisationnelle inadéquate/faiblesse de l'environnement de contrôle				
	14. Non respect des exigences réglementaires locales		29. Défaillance dans la conservation pour compte de tiers de documents/valeurs				
	15. Non respect des exigences comptables ou de la communication financière		30. Défaillances sur services rendus par des sous-traitants				
	16. Non respect de la législation fiscale		31. Défauts de rapprochement				
	17. Blanchiment d'argent et financement du terrorisme		32. Accès laissé par la banque aux comptes d'un client sans l'accord de ce dernier				

<u>Annexe 04</u> : Questions relatives à l'identification et l'évaluation du risque opérationnel.

1- Quels sont les risques opérationnels inhérents a votre activité?

2- Où se trouve le risque ? (dans le processus, vis-à-vis de qui, localisation)

3- Pour chaque risque :

   - Au cours de cette années, ce risque s'est il réalisé ?
   - Si oui, combien de fois ?

4- Quels contrôles sont en place aujourd'hui ? Qui en a la charge? Quelle qualité ?

5- Estimation des pertes max./ attendues et des fréquences

6- Quels Plans d'Actions sont –ils nécessaires ?

<u>Annexe 06</u> : Questionnaire pour évaluation des dispositifs de prévention et de contrôle.

	Oui			Non
	Satisfaisant	**Assez bon**	**Faible**	
2 Pratique commerciales inappropriées : 1-Existe-t-il des dispositions permettant de faciliter la connaissance du client et précisant les bonnes conditions d'entrée en relation avec le client ? 2- Existe-t-il un dispositif qui permet de réaliser l'adéquation des produits avec les besoins des clients ?		**X** **X**		
3 Inadéquation des produits proposés Les dispositions en vigueur afin de faciliter le partage d'informations sur les clients au sein de l'entité sont-elles efficaces?		**X**		
4 Insuffisance du service au client - Existe-t-il des procédures ou des systèmes qui permettent de centraliser les réclamations des clients, ensuite de les suivre afin de répondre dans les meilleurs délais ? -Des mesures efficaces sont-elles en vigueur afin de s'assurer que toutes les communications écrites sensibles aux clients ou contre partie soient soumises à supervision/ vérification de leur exactitude avant leur envoi ?		**X** **X**		
5 Autres litiges avec un tiers (fournisseur, prestataire, ...) -Existe-t-il des dispositifs qui permettent une coordination entre les décisions judiciaires et les opérations BO, FO ? - y a-t-il un respect des dispositifs incitant les collaborateurs à mieux connaitre les clients dans le cadre du KYC ?	**X**		**X**	

6 Contrat ou clauses contractuelles inapplicables - Les conventions ainsi que les formulaires comportent des clauses indispensables, sont-elles prises en considération ?		**X**		
7 Non-respect de la loi bancaire -Les dispositions réglementaires dans le cadre d'ouverture et de gestion des comptes sont-elles respectées ? - Existe-t-il une mise à jour régulière des contrats-standards utilisés dans les relations banque-client par le service juridique dans le cadre de ses missions de veille juridique ? -Les caissiers et responsables d'agence ont-ils connaissance de la réglementation en matière d'affichage des tarifs, commissions et mentions obligatoires à faire figurer sur les chèques ou effets de commerce ?	**X**	**X**	**X**	
13 * Non respect d'autres lois (non citées dans cette catégorie d'événement) Les équipes commerciales sont-elles formées et régulièrement sensibilisées à la protection des données personnelles (données clients)?		**x**		
14 * Non respect des exigences règlementaires locales -Lors du lancement de nouvelles activités y-a-t-il systématiquement une vérification de la conformité des produits avec la licence?	**x**			

17 * Blanchiment (interne et externe) et financement du terrorisme - Existe-t-il un programme régulier de formation couvrant tous les aspects pertinents de la législation de lutte contre le blanchiment d'argent et le financement du terrorisme qui doit être suivi par le personnel, priorisant les formations selon la nature des fonctions exercées ? - Existe-t-il un comité d'ouverture de compte (personnes politiquement exposées, spécifique.) ? - Les adresses physiques des clients en courrier guichet sont-elles vérifiées systématiquement?	**X**			**X** **X**
18 * Défaillance dans le dispositif de gestion et de suivi des autorisations et des limites -Est-ce qu'il existe des états d'alertes (seuils à préciser) au niveau de la direction des risques de l'entité avec revue au fil de l'eau (et demande de justification)? -Existe-t-il une check list imposant de procéder à des vérifications a minima en matière solvabilité?	**X** **X**			
22 * Défaillance dans le processus de livraison/règlement de la banque Existe-t-il une automatisation des éditions des chèques de banque				**X**

24- Défaillance dans la gestion administrative d'une opération jusqu'à son échéance Existe-t-il une procédure relative aux saisies arrêts (blocage de la provision liée)? Existe-t-il un contrôle/validation de second niveau sur le dossier transmis au notaire/au service en charge de traiter les successions ?		**X** **X**		
25 .Erreurs dans la transmission, la saisie ou la compréhension d'une instruction - Existe-t-il un double contrôle et double signature pour les opérations de change au-delà d'un certain seuil ? - Existe-t-il un double contrôle et double signature sur les opérations de virement au-delà d'un certain seuil ? - Existe-t-il un double contrôle pour la saisie des données clés ?			**X** **X** **X**	
28. Inefficience de la surveillance au quotidien et de la supervision managériale -Le dispositif de contrôle au quotidien est-il performant ? - le dispositif de contrôle en matière de supervision managériale est-il performant ?		**X** **X**		
30 * Défaillance sur services rendus par des sous-traitants Existe-t-il dispositif de contrôle mis en place pour mesurer la performance de ces prestataires ?			**X**	
33 * Piratage informatique et autres attaques malveillantes des systèmes informatiques de la banque par des tiers Y-a-t-il des formations régulières des collaborateurs sur les risques de piratages?				**X**

35 * Vols / escroqueries / fraudes commis par des tiers -Est-ce que les versions anciennes ou obsolètes des mandats de client (signature, pouvoir) sont retirées et correctement archivées conformément aux conditions de conservation internes/ externes ? - Le compte est-il soumis à des contrôles spécifiques jusqu'à son réapprovisionnement ?	**X** **X**			
36. Vols par le personnel -Existe-t-il un rapprochement entre les encaissements enregistrés dans les dossiers et les encaissements enregistrés en trésorerie? -Existe-t-il un contrôle sur la sortie physique de matériel par les agents? -Existe-t-il des codes barres sur les matériels et des inventaires a minima annuels sont-ils réalisés?	**X**	**X** **X**		
37 * Fraude sur des transactions par le personnel ou avec sa complicité - Existe-t-il un contrôle sur la récupération des courriers guichets par les clients? - Existe-t-il des contrôles sur les comptes des personnes âgées, sous tutelle et curatelle, handicapées, des clients mineurs? - Existe-t-il une demande de la justification économique pour les opérations de virement au-delà d'un seuil à préciser? - Existe-t-il un contrôle de second niveau par sondage sur les opérations de comptes à comptes?	**X**			**X** **X** **X**

38 * Utilisation non autorisée / à mauvais escient d'information privilégiée et confidentielle par le personnel Les collaborateurs sont t-ils sensibilisés aux informations manipulées ?	**X**			
40 * Défaut de personnel Pour les fonctions sensibles des agences, un plan de recouvrement est-il établé ?		**X**		
41 * Perte des données -Les dossiers clients sont-ils biens conservés ? -existe-t-il une solution de sauvegarde électronique ?		**X** **X**		
42 * Pertes des moyens d'exploitation En cas de problème concernant le réseau, existe-t-il des solutions de contournement ?		**X**		
45 * Données incohérentes ou incompatibles Etes-vous informés rapidement en cas de dysfonctionnement du core banking system .		**X**		
47 * Défaillance des software Le dispositif de contrôle des systèmes d'information s'assure-t-il de la maintenance d'accès sécurisé aux actifs et aux données ainsi que des procédures permettant leur sauvegarde ? Existe-t-il un système de secours ?		**X**	**X**	
48. Faiblesse de la sécurité logique Le système d'informations est-il paramétré et sécurisé ?	**X**			

Les habilitations des personnes sont-elles revues régulièrement ?		**X**		

Résumé

Ces dernières années, l'environnement bancaire s'est caractérisé par une sophistication de l'activité et des produits pour répondre aux besoins d'une clientèle de plus en plus exigeante.
L'activité est focalisée sur une innovation et une croissance débridée au détriment de la fiabilité, ce qui a rendu les banques de plus en plus exposées aux risques, notamment les risques opérationnels.
Les pertes ayant pour origine des dysfonctionnements opérationnels témoignent de la gravité de ces risques. C'est ainsi que la gestion des risques opérationnels est devenue un enjeu majeur pour les banques et établissements financiers.

Le présent mémoire s'intéresse à l'un des outils les plus recommandés en la matière de nos jours, à savoir la cartographie des risques opérationnels qui apparaît comme un outil permettant l'identification, l'évaluation et la hiérarchisation de risques opérationnels grevant l'activité bancaire. La cartographie favorise aussi l'émergence d'une culture partagée du risque, source d'une meilleure performance et d'une plus grande prévention des défaillances.

Mots clé : gestion des risques, cartographie des risques, risques opérationnels.

In recent years, the banking environment has been characterized by sophistication of the activity and products in order meet with the needs of increasingly demanding customers.
The activity is focused on an innovation and in controlled growth at the detriment of reliability, the fact of which has made the banks more and more exposed to risks, namely the operating risks.

Losses originating from operational malfunctions reflect the seriousness of those risks. Thus the management of operating risks has become a major challenge for banks and financial establishment.

The present thesis is interested in one of the most recommended tools in this nowadays field, namely the mapping of operating risks which appears as a tool for the identification, assessment and prioritization of operating risks encumbering the banking activity. The mapping encourages alike the emergence of a shared risk culture, source of an improved performance and greater failure prevention.

Keywords: Management of risks, mapping of risks, operating risks.