A ma mère, pour ses prières sincères,

A mon père, pour toute goutte de sueur …

REMERCIEMENTS

Je tiens tout d'abord à remercier Dieu le tout puissant et miséricordieux, qui m'a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, je tiens à exprimer ma profonde gratitude à mon encadrant, Monsieur. Chiheb GHANMI pour ses précieux conseils et son aide.

Je tiens à présenter mes vifs remerciements à mon tuteur, Monsieur. Zied BOUDRIGA pour les apprentissages qu'il a su me faire transférer pendant la période de stage et pour sa grande disponibilité.

Mes remerciements sont aussi adressés à toutes les personnes qui ont collaboré avec moi au sein de l'ATB.

Je tiens à exprimer ma profonde gratitude et mes vifs remerciements à l'administration et à l'ensemble du corps enseignant de l'I.F.I.D d' avoir assuré le bon déroulement de notre formation.

Je remercie également, mes deux frères Hazem et Atef pour leur soutien inconditionnel.

Un remerciement spécial à Nidhal pour son écoute et son affectation.

Un grand Merci à mes chers amis Malak, Molka, Ghazi, Mahmoud, Molka et Jihen pour leur soutien et leur encouragement tout au long de la formation.

Mes vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à mon recherche en acceptant d'examiner mon travail et de l'enrichir par leurs propositions.

Enfin, je tiens également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

LISTE DES ABREVIATIONS

ALCO: Asset and Liability Committee

AMA: Approche Avancée de Mesure

ATB: Arab Tunisian Bank

BCT: Banque Centrale de Tunisie

C: Criticité

C': Criticité modifiée

CEC: Comité Exécutif de Crédit

COU: Direction Centrale des Opérations

CSC: Comité Supérieur de crédit

DACE: Direction Administrative et Contrôle des Engagements

DCAJR: Direction Centrale des affaires juridiques et du Recouvrement

DCC : Direction Centrale des Crédits

DCCOR: Direction Centrale Corporate

DMR: Dispositif de Maîtrise des Risques

I: Impact

IFACI: Institut Français de l'Audit et du Contrôle Interne

ISO: Organisation Internationale de Normalisation

NPC: Notification Provisoire de Crédit

OCDE: Organisation de Coopération et de Développement Economiques

SED: Système d'Echange de Données

V: Vraisemblance

SOMMAIRE

LISTE DES TABLEAUX

LISTE DES FIGURES

INTRODUCTION GÉNÉRALE

Quel est le point commun entre une épidémie de grippe A, un braquage armé, un piratage de données, une erreur de saisie, une catastrophe naturelle ou encore une fraude engageant des pertes de trading de plus de 5 milliard d'euros ?

Tous ces événements font partie de ce que l'on appelle le risque opérationnel !

Au-delà de la vision financière traditionnelle évoquant les risques de marché ou le risque de crédit comme facteur de défaillance principal des banques. Les nombreux scandales observés depuis le début des années 2000 (affaire Enron, Worldcom, Parmalat ou les attentats de septembre 2001) sont venus rappeler qu'une autre source de pertes financières significatives pouvait provenir du fonctionnement opérationnel : fraudes, détournements, condamnations, dysfonctionnements…

Outre ces pertes importantes, le risque opérationnel touche toutes les activités et les opérations des institutions financières de différentes manières. En effet, nous trouverons des événements opérationnels attribuables « à une inadéquation ou à une défaillance des procédures, des personnels, des systèmes internes ou à des événements extérieurs[1] » .En revanche, les unités ne sont pas touchées de la même façon par le risque opérationnel. L'impact varie selon la nature des activités et les différents intervenants.

Conscientes de ce grand risque, les autorités réglementaires ont lancé le débat sur la définition, l'identification, la mesure et la gestion du risque opérationnel à partir de juin 1999. Ainsi, avec la réforme de Bâle II en 2004, cette catégorie de risque est devenue prise en compte dans l'évaluation des fonds propres des établissements financiers. Une façon de couvrir l'exposition au risque opérationnel est de détenir un capital permettant de couvrir les pertes non anticipées, comme c'est le cas pour le risque de marché et de crédit.

Leur évaluation quantitative est donc la première démarche qui ait été entreprise. Cependant cette approche apparait comme insuffisante pour maîtriser ces risques et la gravité des événements exceptionnels est extrêmement difficile à évaluer. Il faut donc combiner ces approches quantitatives à des démarches plus qualitatives.

Il importe, ainsi, pour les banques de mettre en place un dispositif de gestion des risques opérationnels qui comprend un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque institution. Ce qui permettra

[1]Ce passage est pris de la définition du risque opérationnel par le comité de Bâle.

aux dirigeants de maintenir les risques à un niveau acceptable, de maximiser la valeur de l'institution en réduisant les coûts associés à la volatilité de ses flux d'entrée et de sortie de fonds et aussi de garder l'entreprise performante. La mise en œuvre du dispositif de gestion des risques va permettre de couvrir de manière intégrée et transversale l'ensemble des risques opérationnels auxquels l'institution peut être confrontés. Il est donc important pour chaque institution de mettre en place un dispositif pertinent de gestion et de suivi du risque opérationnel.

A ce titre, la cartographie des risques se présente comme une démarche bien structurée et très efficace pour la gestion des risques opérationnels. Elle consiste en une démarche participative (entretiens avec les différents directeurs, responsables de services ou collaborateurs de la banque), et progressive (description des processus, cotation, fréquence/impact et hiérarchisation des risques opérationnels). Cette démarche a pour finalité d'appréhender le niveau d'exposition aux risques opérationnels d'une entité dans l'ensemble de ses activités ainsi que leur niveau de maitrise perçus, de manière à aider les dirigeants dans la mise en place d'un plan d'actions visant à traiter ces risques.

Les développements qu'a subis le risque opérationnel à l'échelle internationale sous l'effet des accords de Bâle, n'ont pas été sans conséquences sur le système bancaire tunisien. Plusieurs réformes ont été entreprises par les autorités publiques tunisiennes dans le but de préparer un cadre adéquat pour prendre en considération le risque opérationnel.

Comme toute institution bancaire consciente du danger du risque opérationnel et soucieuse de se conformer à la réglementation en vigueur, l'ATB a décidé de mettre en place le projet de cartographie des risques opérationnels. C'est dans cette logique que nous présentons notre travail et ceci afin de trouver une réponse à notre problématique principale qui n'est autre que :

« L'identification, l'évaluation et la gestion des risques opérationnels liés au processus crédits Corporate au sein de l'ATB au regard des contrôles existants »

En vue de trouver une solution à notre problématique, nous posons les questions suivantes :

- Quels sont les risques opérationnels qui menacent le processus crédits Corporate au sein de l'ATB ?
- Quels sont les éléments de maitrise interne ? Et sont-ils efficaces ?

- Quel plan d'actions à adopter pour arriver à maitriser et réduire ces risques ?

Afin de répondre à ces questions, notre mémoire sera alors structuré autour de 3 chapitres :

A travers le premier chapitre intitulé « Le risque opérationnel dans l'activité bancaire », nous exposerons le cadre conceptuel du risque opérationnel tout en commençant par présenter la spécificité de l'activité bancaire et les risques qui y sont associés, pour passer ensuite à la définition du risque opérationnel et ses spécificités et finir avec le cadre réglementaire du risque opérationnel.

Dans le second chapitre intitulé «La démarche d'élaboration d'une cartographie des risques opérationnels », nous proposons de présenter la démarche d'élaboration d'une cartographie des risques opérationnels. Nous allons commencer par le cadre conceptuel relatif à la cartographie des risques. Ensuite nous allons mettre l'accent sur les différentes étapes de cette démarche.

Le troisième chapitre sera consacré à la partie empirique, où nous allons suivre la démarche décrite dans le chapitre précédent pour « l'élaboration d'une cartographie des risques opérationnels liés au processus Crédits Corporate au sein de l'ATB ».

CHAPITRE 1 :LE RISQUE OPÉRATIONNEL DANS L'ACTIVITÉ BANCAIRE

INTRODUCTION

Le risque opérationnel est inhérent à tous les produits, les services et les activités et concerne tous les employés de toutes les firmes, aussi différentes soient-elles (Thirlwell, 2011). Il n'est donc pas spécifique à l'activité bancaire, mais étant données les caractéristiques de cette dernière, un tel risque peut avoir une dimension particulière.

Ce risque, longtemps considéré comme moins fréquent que les autres types de risques bancaires, n'a pas cessé de prendre de l'importance ces dernières années, aussi bien pour les autorités de régulation que pour les banquiers et les chercheurs académiques. Un tel intérêt est notamment motivé par la multiplication des scandales financiers liés aux risques opérationnels, ayant entraîné des pertes financières substantielles.

En effet, l'environnement nouveau des banques accentue considérablement leur exposition aux risques (dont le risque opérationnel) avec notamment : une internationalisation des activités et une multiplication des interconnexions, une sophistication des techniques financières, une sensibilité plus grande aux systèmes d'information ainsi qu'une inventivité des fraudes.

Face à cette matérialisation croissante des risques opérationnels, le Comité de Bâle a jugé nécessaire d'en assurer une couverture non seulement par le développement de meilleures pratiques au sein des banques, mais également par la mise en place d'exigences de fonds propres (Bâle II, 2004).

Toutes ces idées que nous venons d'avancer et autres, seront détaillées davantage dans ce premier chapitre, scindé en trois sections :
Section 1 :Activités bancaires et risques ;
Section 2 : Définitions, spécificités et typologie du risque opérationnel;
Section 3 : Cadre réglementaire du risque opérationnel.

SECTION 1 : ACTIVITES BANCAIRES ET RISQUES

1. La spécificité de l'activité bancaire

La banque se distingue des autres firmes par un certain nombre de caractéristiques et de fonctions qui lui sont propres. Ces particularités bancaires ont valu à la banque un traitement particulier, notamment en matière de réglementation.

Les banques sont exposées à de nombreux risques notamment le risque de marché, le risque de crédit, le risque de liquidité et le risque opérationnel mais elles sont en particulier exposées au risque systémique. En effet, la liquidité du contrat de dépôt et l'illiquidité du crédit bancaire engendrent une incertitude sur les demandes de remboursement des dépôts pouvant rendre les banques vulnérables aux « ruées bancaires » en période de défiance. En cas de panique bancaire, tous les déposants demandent le retrait de leurs dépôts, puisque ces derniers sont remboursés au pair et dans l'ordre d'arrivée au guichet (premier arrivé, premier servi). Étant donné les spécificités des dépôts et l'asymétrie d'information, la course des déposants aux guichets pour retirer leurs dépôts peut s'avérer rationnelle même si elle se base sur une simple rumeur. Ces comportements peuvent entraîner l'insolvabilité - voire la faillite - de la banque qui n'est plus capable de faire face à ses engagements.

Toutefois, la faillite d'une banque peut provoquer celle d'autres banques, puisque le secteur bancaire est plus vulnérable à l'instabilité que les autres secteurs de l'économie. En effet, les banques sont fortement engagées dans les marchés interbancaires et dans le système des paiements. Étant donné leur exposition aux risques et aux asymétries d'information, les problèmes rencontrés par une banque peuvent se propager aux autres, conduisant à une crise systémique (Diamond et Dybvig, 1983 ; Simpson et al, 2005). Une telle crise a de graves conséquences pour l'économie dans son ensemble, puisqu'elle engendre la destruction du mécanisme des paiements. À cet égard, les banques gèrent l'épargne des personnes physiques et morales et financent la croissance économique. Elles sont indispensables pour le bon fonctionnement de l'économie. L'insolvabilité ou la faillite d'une banque peut donc avoir des conséquences importantes sur l'ensemble de l'économie.

Compte tenu du risque systémique auquel sont exposées les banques, la gestion des risques bancaires s'avère capitale pour la stabilité de l'ensemble du système financier. En particulier, la surveillance du risque opérationnel est spécialement délicate étant donné les difficultés inhérentes à l'évaluation et à la gestion d'un tel risque. Ces particularités bancaires valent à la banque une réglementation prudentielle stricte.

2. Typologie des risques bancaires

Plusieurs définitions du risque ont apparus. Selon l'Organisation Internationale de Normalisation (ISO) le risque est « la possibilité d'occurrence d'un événement ayant un impact sur les objectifs, il se mesure en terme de conséquences et de probabilité ».

L'Institut Français de l'Audit et du Contrôle Interne (IFACI) définit la notion de risque comme étant « un ensemble d'aléas susceptible d'avoir des conséquences négatives sur une entité et dont le contrôle interne et l'audit ont notamment pour mission d'assurer sa maîtrise ».

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

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

A ce niveau, on peut classer les risques confrontés par la banque en 2 catégories : les risques acceptés et les risques subis. En effet, les intérêts rémunèrent les prêts accordés par celle-ci à ses clients. Elle y intègre une prime de risque considérant que certains clients ne rembourseront pas leurs crédits. Dans ce cas, il s'agit donc d'un risque accepté que la banque cherche à encadrer pour éviter toute dérive. A l'inverse, certaines de ses activités peuvent l'exposer à des risques qu'elle ne souhaite pas, par exemple la fraude. Ces risques existent du fait même de son activité. Il s'agit ici de risques subis.

2.1.Les risques acceptés et rémunérés

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

*** Le risque de crédit :** c'est le risque de pertes financières consécutives à l'incapacité des clients ou autres contreparties à honorer leurs engagements financiers.

*** Le risque de marché :** c'est le risque de variation du prix d'une grandeur économique constatée sur un marché, se traduisant par une perte ou comme le risque financier dû à l'incertitude quant à la valeur future d'un portefeuille d'avoirs ou de dettes. On distingue

généralement trois catégories de risques de marché : le risque de taux d'intérêt, le risque de change, le risque de variation de cours.

*** Le risque de liquidité :** c'est le risque qu'un établissement de crédit se trouve dans l'impossibilité de pouvoir faire face, à un instant donné, à ses engagements ou à ses échéances, par la mobilisation de ses actifs.

2.2.Les risques subis

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

*** Les risques stratégiques :** Intimement lié aux grandes lignes stratégiques d'une banque, ce risque stratégique peut être appréhendé comme le risque que les stratégies d'affaires de la banque soient inefficaces, pas bien mises en œuvre ou pas bien adaptées aux changements touchant le contexte commercial.

*** Les risque opérationnels :** Sous-estimé jusqu'à peu, le risque opérationnel a été récemment réintroduit par les autorités de contrôle qui le définissent comme la perte découlant de l'erreur d'un opérateur, d'un sinistre informatique, d'une non-conformité à la réglementation ou d'un sinistre physique (vol, incendie, inondation, …). Plus d'approfondissement concernant ce risque spécifique sera présenté lors de notre étude et au cours des prochains chapitres.

3. Le risk management

Le pilotage bancaire repose sur une estimation exhaustive des risques, qui nécessite de recourir à des modèles de plus en plus complexes et sophistiqués. Dans ce contexte, l'activité de Risk management devient un véritable pôle stratégique au sein de l'organisation bancaire. Au sein des banques, les risques ont toujours fait l'objet d'une attention particulière. La nouveauté dans ce domaine réside dans la détermination et l'obligation d'une gestion plus active des risques. Ces objectifs modifient radicalement les dispositifs traditionnels de suivi des risques de plusieurs manières : une meilleure définition des différentes dimensions des risques bancaires, l'apparition d'une gestion quantitative et planifiée de ces risques, un pilotage plus actif des risques, des mesures plus précises, des outils et des dispositifs nouveaux. Bref, il s'agit de mettre en place une gestion calculée des risques dans le but de

faciliter et d'améliorer l'efficience dans la prise de risque. Le risque n'est plus un élément intangible dont l'appréciation est essentiellement qualitative. Il devient un objet spécifique, mesurable et quantifiable, et un facteur de performance. La gestion des risques n'est autre que l'ensemble des outils, des techniques et des dispositifs organisationnels nécessaires pour y parvenir. Elle n'est nullement figée mais, au contraire, en évolution constante.

SECTION 2 : DEFINITION, SPECIFICITES ET TYPOLOGIE DU RISQUE OPERATIONNEL

1. Définition du risque opérationnel

Pour être appréhendé et géré, un risque doit être connu et identifié. La première étape dans la mise en œuvre d'une stratégie de gestion des risques opérationnels est donc de définir avec assez de précision quels sont les risques que l'on souhaite suivre.

La définition du risque opérationnel est la clé primordiale d'une gestion efficace. Jusqu'à maintenant, il n'y a pas une définition unanime permettant d'adopter une approche commune et une méthodologie unique de gestion par toutes les banques. Le débat sur la définition a commencé avec le comité de Bâle. Les risques opérationnels correspondaient, pour lui, aux risques de pertes directes et indirectes résultant de l'inadéquation ou de la défaillance de procédures, de personnes et de systèmes ou résultant d'événements extérieurs. Cette définition a été critiquée, car il est difficile de calculer certaines pertes indirectes.

Ensuite et avec les accords de Bâle II, le risque opérationnel est désormais défini comme étant « le risque de pertes dues à une inadéquation ou à une défaillance des procédures, des personnels, des systèmes internes ou à des événements extérieurs ». Cette définition inclut le risque juridique, mais ne prend pas en compte les risques stratégique et de réputation.

Vanini (2004) critique la définition de Bâle, selon lui, l'utilisation de cette définition sans aucune extension amène à des difficultés d'application dans les banques, telles que le risque opérationnel représente seulement une possibilité de perte, le potentiel de gain est négligé. La définition indique que les personnels et les systèmes sont les causes de pertes, mais elle ne prend pas en compte le fait qu'ils soient les mieux placés pour détecter les sources de pertes potentielles et lancer des avertissements. De plus, le document de travail de Bâle centré sur la perte, ne permet pas de représenter les anciennes pertes des banques, ni les

éventuelles à venir. Et enfin, Vanini ajoute que cette définition sous-entend que les pertes sont seulement directes, alors qu'en réalité, les pertes indirectes sont comparativement plus importantes.

Vanini définit le risque opérationnel comme le risque de déviation entre le profit associé à la production d'un service et les attentes de la planification managériale. Le risque opérationnel correspond à l'écart enregistré, positif ou négatif, par rapport au profit attendu. La gestion du risque opérationnel doit être basée sur trois facteurs : le gain, les coûts et le risque de production des services.

A la recherche d'une relation causale entre les différents risques bancaires et une représentation plus significative des pertes, les gestionnaires ont défini le risque opérationnel selon leurs propres points de vue. Le « Wild West Semantico » donne une définition plus vaste du risque opérationnel : « tout risque autre que les risques de crédit et de marché ». Le risque opérationnel présente au moins deux caractères distincts du risque de crédit et du risque de marché. Tout d'abord, l'exposition au risque opérationnel n'est pas la contrepartie d'un gain potentiel. Ce qui conduit au second point : le risque opérationnel doit être obligatoirement contrôlé et éliminé autant que possible.

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

Une autre approche de la définition du risque opérationnel s'appuie sur la décomposition des risques bancaires en deux grandes catégories : financiers et non financiers. Kuritzkes (Wharton, 2002) définit le risque opérationnel comme un risque non financier ayant 3 sources : le risque interne (ex : « rogue trader »), le risque externe c'est à dire tout événement extérieur incontrôlable (ex : une attaque terroriste) et le risque stratégique (ex : un affrontement dans une guerre de prix). Pour Kuritzkes, le risque stratégique est le plus important. Il est cependant ignoré par l'accord de Bâle.

Enfin, Harris (2002) classe les bénéfices de gestion du risque opérationnel en trois cas: a) une gestion saine réduit les pertes de basse fréquence et forte sévérité, b) elle peut réduire la prime de l'assurance et c) baisser les charges en capital. Rosengen (2002) soutient Harris

par son étude dans laquelle il incite les organisations financières à gérer le risque opérationnel en raison du coût potentiellement significatif des pertes opérationnelles.

Jusqu'à présent, le risque opérationnel souffre d'un problème de définition. La méthodologie unique d'action face au risque n'existe pas. Selon leurs buts de gestion et leurs modes d'organisation, les entreprises adoptent la définition du risque opérationnel qui représente mieux leurs distributions de perte.

2. Spécificités du risque opérationnel

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

Le risque opérationnel est réputé **moins fréquent** que les autres risques, même si la complexité et la grande taille des institutions financières, ainsi que la sophistication des produits financiers augmentent sa probabilité d'occurrence ;

Le risque opérationnel est considéré comme **très grave**. Il engendre des pertes financières désastreuses. Contrairement aux autres types de risques, l'exposition au risque opérationnel ne peut être ni plafonnée, ni échangée(Thirlwell, 2010). De surcroît, étant donné son caractère imprévisible, son impact financier ne peut être limité ni couvert par des contrats de couverture;

Le risque opérationnel est un risque **diffus**, présent dans tous les départements d'une banque, y compris ceux n'ayant pas une activité commerciale. Il concerne toutes les personnes employées par la banque sans distinction(Blunden et Thirlwell, 2010). À cet égard, ce risque est encore plus difficile à gérer et à évaluer ;

Le risque opérationnel est un risque **multiforme**. Il regroupe un ensemble de risques variés, tels que :

- Des risques de nature qualitative : les risques stratégiques, juridiques, administratifs …
- Des risques d'ordre technique : les risques associés aux systèmes d'information, aux procédures …
- Des risques environnementaux : les risques économiques, politiques, climatiques …

L'identification précise du risque opérationnel est délicate. De plus, ses manifestations sont souvent difficiles à isoler. Par exemple, un événement, comme une

position non autorisée d'un trader, peut résulter de plusieurs causes, à savoir une fraude interne (dépassements de limites autorisée) et/ou des carences du contrôle interne et/ou d'un système informatique inadapté. D'autant plus, ce même événement peut avoir plusieurs effets tels que des pertes financières, atteinte à la réputation, baisse du cours des titres ;

Le risque opérationnel **peut engendrer des pertes financières élevées** pour les institutions financières. Parmi les types d'incidents de nature opérationnelle susceptibles d'occasionner de lourdes pertes, il existe notamment le risque de fraude interne (vol commis par un employé), de fraude externe (piratage informatique) ou la panne de systèmes informatiques.

3. Typologie du risque opérationnel

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

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

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

Chacune de ces sources du risque opérationnel est à l'origine des sous-catégories de ce risque, qui sont à l'ordre de sept selon l'accord de Bâle II :

- **Fraude interne :** pertes dues à des actes visant à frauder, détourner des biens ou à contourner les règlements, la législation ou la politiques de l'entreprise impliquant au moins une partie interne à l'entreprise. Exemples : le vol commis par un employé, la falsification de documents, le délit d'initié d'un employé opérant pour son propre compte ;

- Fraude externe : pertes dues à des actions visant à frauder, à détourner des biens ou à contourner des règlements, la législation de la part d'une partie extérieure à la banque. Exemples : le détournement de fonds, le vol de données, les dommages dus au piratage informatique, les chèques de cavalerie ;

- Pratiques en matière d'emploi et de sécurité sur le lieu de travail : pertes résultant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou 1a sécurité, de demandes d'indemnisation ou d'attente à l'égalité ou actes de discrimination. Exemples : la violation des règles de santé et de sécurité des employés, les activités syndicales, les plaintes pour discrimination à l'embauche ;

- Clients, produits et pratiques commerciales : pertes résultant d'un manquement non intentionnel ou du à la négligence, à une obligation professionnelle envers les clients spécifiques ou de la nature ou conception d'un produit. Exemples : le défaut de conseil, le défaut d'information, l'utilisation frauduleuse d'informations confidentielles sur la clientèle, la vente agressive et le blanchiment d'argent ;

- Dommages aux actifs corporels : destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres. Exemples : actes de terrorisme, vandalisme, séisme, incendies et inondation ;

- Interruption de l'activité dysfonctionnement des systèmes : cette composante couvre les interruptions et dysfonctionnements des systèmes informatiques et de télécommunications. Exemples : les pannes de matériel et de logiciel informatiques, problèmes de télécommunications et pannes d'électricité ;

- Exécution, livraison et gestion des processus : pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties commerciales et fournisseurs. Exemples : erreur de saisie de données, défaillance dans la gestion des sûretés, lacunes dans la documentation juridique, erreur d'accès aux comptes de la clientèle et défaillances des fournisseurs ou conflits avec eux.

Outre la nature de l'événement, le type d'activité où cet événement s'est produit la perte a de l'importance également. Ainsi, le comité de Bâle a défini huit lignes de métier qui sont les suivantes :

Tableau 1 : La classification des lignes de métier

Niveau 1	Niveau 2	Activités
Ingénierie financière	Financement des entreprises	Fusions/acquisitions, engagements, privatisations, titrisations, recherche, titres de dette, actions, prêts consortiaux, introduction en bourse, placement sur le marché secondaire.
	Financement des collectivités locales et administrations publiques	
	Banque d'affaires	
	Service conseil	
Négociation et vente	Ventes	Valeur à revenu fixe, actions, change, matières premières, crédit financement, titres sur positions propres, prêts et pensions, courtage, titre sur dette, courtage de premier rang
	Tenue de marché	
	Positions pour compte propres	
	Trésorerie	
Banque de détail	Banque de détail	Prêts et dépôts, services bancaires, fiducie, gestion de patrimoine, conseil en placement, cartes commerçants/ commerciales, cartes d'entreprises/ de clientèle
	Banque privée	
	Cartes	
Banque de gros	Banque commerciale	Financement de projets, immobilier, exportations, commerce, crédit bail, prêt, garanties, lettres de changes
Paiements et règlements	Clientèle extérieure	Paiements et recouvrements, transferts de fonds, compensation et règlements
Fonction d'agent	Conservation	Dépôts, certificats, prêts de titre, opérations de sociétés
	Prestation d'agent aux entreprises	Agents émetteurs et payeurs
	Service fiducie aux entreprises	
Gestion d'actifs	Gestion de portefeuille Discrétionnaire	Gestion centralisée, séparée, de détail, institutionnelle, fermée, ouverte, capital investissement
	Gestion de portefeuille non discrétionnaire	
Courtage	Courtage de détail	Exécution et service complet

Source : Comité de Bâle sur le contrôle bancaire 2004[2]

4. Exemples de pertes inhérentes aux risques opérationnels

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

[2]Comité de Bâle sur le contrôle bancaire. 2004. Convergence internationale de la mesure et des normes de fonds propres (dispositif révisé). Bâle : Banque des règlements internationaux. 216 pages. Annexe 8.

- Fraude interne : Allied Irish Bank, Barings, Daiwa et la Société Générale ont perdu 700 millions de dollars, 1 milliard de dollars, 1.4 milliard de dollars et 4,82 milliards d'euros respectivement sur la base de transactions frauduleuses.

- Fraude externe : Republic New York Corporation a perdu 611 millions de dollars en raison de fraudes commises par un client.

- Pratiques en matière d'emploi et de sécurité sur le lieu de travail : Menin Lynch a perdu 250 millions de dollars suite à une décision de juste dans une affaire de discrimination à l'embauche.

- Pratiques concernant les clients, les produits et l'activité commerciale : Household International a perdu 484 millions de dollars à cause de prêts frauduleux.

- Dommages aux biens : Bank of New York a perdu 140 millions de dollars à cause des attaques terroristes du 11 septembre 2001.

- Interruption d'activité et pannes de systèmes : Salomon Brothers a perdu 303 millions de dollars en raison d'une modification du système informatique.

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

En réalité, il est beaucoup plus difficile de quantifier et de gérer le risque opérationnel que les risques de crédit ou de marché. Les banques prennent des décisions d'octroi de prêts ou de prise de risque de marché de façon consciencieuse. Alors que, de nombreux produits de marché existent pour réduire ces risques, le risque opérationnel fait partie intégrante de l'activité quotidienne. A cet égard, le risque opérationnel fait l'objet d'un encadrement législatif et réglementaire et d'une surveillance accrue de la part des banques.

SECTION 3 : CADRE REGLEMENTAIRE DU RISQUE OPERATIONNEL

1. Accord de Bâle II : l'entrée en scène du risque opérationnel

Par rapport à l'accord de Bâle I qui repose uniquement sur l'exigence quantitative de fonds propres calculée selon une méthode standard, la réforme de Bâle II comporte un certain nombre de nouveautés. Ainsi, les nouvelles exigences en fonds propres tiennent compte des

risques de crédit, des risques de marché mais également des risques opérationnels. Ces derniers sont pour la première fois pris en compte dans le calcul du capital réglementaire. Aussi s'avère-il important de présenter les principaux apports de cette réforme, en portant un intérêt particulier aux mesures prises pour la surveillance du risque opérationnel.

Le ratio de fonds propres proposé dans le cadre des accords de Bâle II intègre davantage la réalité des risques. Pour le calcul du minimum de fonds propres exigés, les banques ont le choix entre l'utilisation des méthodes standard et des méthodes fondées sur des notations internes IRB. Le dispositif de Bâle II repose sur trois piliers :

Pilier I -« Exigences en fonds propres » : le tableau ci-dessous résume les principaux changements concernant le calcul du ratio de solvabilité.

Tableau 2 : Exigences en fonds propres, Bâle I versus Bâle II

	Bâle I	Bâle II
Ratio de fonds propres	$\text{Ratio Cooke} = \frac{\text{Fonds propres}}{\text{Risque de crédit + Risque de marché}} \geq 8\%$	$\text{Ratio Mac Donough} = \frac{\text{Fonds propres}}{\text{Risque de crédit + Risque de marché + Risque opérationnel}} \geq 8\%$
Méthode de calcul des risques	Méthode de calcul uniforme.	Choix entre une méthode standard et des méthodes fondées sur des notations ou des mesures internes.
Le risque de crédit	Méthode standard : - Catégories d'emprunteurs : Etat OCDE, banque, hypothécaire et « normal » (entreprises, particuliers, Etats hors OCDE). - Pondérations respectives : 0%, 20%, 50% et 100%.	Méthode standard révisée : - Catégories d'emprunteurs : souverains (abandon du critère d'appartenance à l'OCDE), autres entités du secteur public, banques multilatérales de développement, banques, entreprises, détails, crédits hypothécaires, risques élevés, hors bilan. Pondérations (plus différenciées en fonction du risque) : 0%, 20%, 40%, 50%, 100% ou même 150%.
Le risque de marché	Risque de marché mesuré par une approche standard ou une approche de modèle interne.	Pas de changement pour le calcul du risque de marché entre l'accord de Bâle I et l'accord de Bâle II.
Le risque opérationnel	Pas de prise en compte du risque opérationnel.	Le risque opérationnel par l'approche standard, l'approche de base ou par l'approche avancée.

Source : Article de recherche[3]

[3]Meriem Haouat Asli, « Risque opérationnel bancaire : le point sur la réglementation prudentielle », Management & Avenir 2011/8 (n° 48), p. 232.

Pilier II - « Processus de surveillance prudentielle » : les autorités de contrôle peuvent imposer des exigences individuelles supérieures à celles calculées par les méthodes proposées par le premier pilier ;

Pilier III - « Discipline de marché » : les établissements bancaires sont tenus de publier des informations complètes sur la nature, le volume et les méthodes de gestion de leurs risques.

En particulier, le comité de Bâle exige des banques l'allocation de capital permettant de couvrir leur risque opérationnel. Il propose à celles-ci trois méthodes de calcul, sans imposer aucune d'entre-elles :

- L'indicateur de base (méthode la plus simple) permet d'appliquer un taux forfaitaire de 15% au produit net bancaire des trois derniers exercices ;
- L'approche standard consiste à retenir des coefficients de pondérations différents (allant de 12% à 18%) selon les lignes de métiers ;
- L'approche avancée « Advanced Measurement Approach » (AMA) laisse à la banque le soin de mettre en place une méthode interne d'évaluation des risques opérationnels.

Dans le cadre de cette dernière approche, différentes méthodes d'évaluation du risque opérationnel peuvent être retenues. Elles peuvent être classées en 3 grandes familles : les méthodes statistiques, les approches par scénario et les approches par « scorecard ».

L'approche actuarielle ou « Loss Distribution Approach » (LDA), basée sur les données collectées concernant les évènements passés de pertes tout en combinant des sources internes et externes d'informations, est la principale approche retenue dans le cadre des méthodes statistiques.

L'approche par scénario est basée sur les opinions subjectives des experts comme point de départ pour la détermination des exigences en capital et la couverture du risque opérationnel.

Plusieurs tentatives de modélisation ont été faites afin de combiner l'approche actuarielle et l'approche par scénario pour satisfaire les exigences de la réglementation prudentielle (Peters et Hübner, 2009). Il s'agit d'un vrai défi méthodologique permettant de pallier les insuffisances des deux méthodes.

Quant à l'approche par « scorecard » ou Risk Drivers and Controls Approach (RDCA), elle est basée sur des indicateurs de risque reflétant les risques opérationnels plutôt que sur des données statistiques. À partir de questionnaires, préparés par des experts en risques bancaires, un score est établi pour chaque ligne de métier et pour chaque type de risque opérationnel afin d'évaluer la quantité de capital requise pour couvrir un tel risque. Le score est recalculé régulièrement, permettant d'ajuster le montant du capital en fonction de l'évolution des risques.

La diversité des méthodes d'évaluation ainsi que les problèmes techniques liés à leur application nécessitent davantage de réglementations prudentielles, pour une homogénéité des calculs, ainsi qu'une meilleure évaluation du risque opérationnel. Toutefois, contrairement à ces attentes, la réforme de Bâle III ne s'est pas focalisée sur ce risque en particulier : la surveillance du risque de liquidité et du risque systémique a été largement privilégiée.

2. Saines pratiques de gestion des risques opérationnels [4]

Dans le but de mieux définir les pratiques qui doivent être appliquées, le régulateur a lui- même défini, dans un document intitulé « Sound Practices for the Management and Supervision of Operational Risk », un code de saines pratiques à utiliser par les banques et leurs superviseurs. Au nombre de dix, ces principes sont regroupés en quatre points :

- **Développement d'un environnement de gestion des risques adapté :**

Principe 1 : La direction doit considérer les principaux aspects du risque opérationnel de la banque comme une catégorie distincte de risque à gérer, et elle doit approuver et réexaminer périodiquement le dispositif de gestion de ce risque. Ce dispositif doit fournir une définition du risque opérationnel valable pour la banque tout entière et poser les principes servant à identifier, évaluer, suivre et maîtriser/atténuer ce risque.

Principe 2 : La direction doit garantir que le dispositif de gestion du risque opérationnel de la banque est soumis à un audit interne efficace et complet, effectué par un personnel fonctionnellement indépendant, doté d'une formation appropriée et compétent. La fonction d'audit interne ne doit pas être directement responsable de la gestion du risque opérationnel.

[4]Comité de Bâle sur le contrôle bancaire. 2003. Saines pratiques pour la gestion et la surveillance du risque opérationnel. Bâle : Banque des règlements internationaux, 12pages.

Principe 3 : La direction générale doit avoir pour mission de mettre en œuvre le dispositif de gestion du risque opérationnel approuvé par le conseil d'administration. Ce dispositif doit être appliqué de façon cohérente dans l'ensemble de l'organisation bancaire, et les membres du personnel, à tous les niveaux, devraient bien comprendre leurs responsabilités dans la gestion du risque opérationnel. La direction générale doit aussi être chargée d'élaborer des politiques, processus et procédures de gestion du risque opérationnel pour tous les produits, activités, processus et systèmes importants.

- **Gestion des risques :**

Principe 4 : Les banques doivent identifier et évaluer le risque opérationnel inhérent à tous les produits, activités, processus et systèmes importants. Elles doivent aussi, avant de lancer ou d'exploiter des produits, activités, processus et systèmes nouveaux, soumettre à une procédure adéquate d'évaluation le risque opérationnel qui leur est inhérent.

Principe 5 : Les banques doivent mettre en œuvre un processus de suivi régulier des profils de risque opérationnel et des expositions importantes à des pertes. Les informations utiles à une gestion dynamique du risque opérationnel doivent être régulièrement communiquées à la direction générale et au conseil d'administration.

Principe 6 : Les banques doivent adopter des politiques, processus et procédures pour maîtriser et/ou atténuer les sources importantes de risque opérationnel. Elles doivent réexaminer périodiquement leurs stratégies de limitation et de maîtrise du risque et ajuster leur profil de risque opérationnel en conséquence par l'utilisation de stratégies appropriées, compte tenu de leur appétit pour le risque et de leur profil de risque globaux.

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

- **Rôle des superviseurs :**

Principe 8 : Les autorités de contrôle bancaire doivent exiger que toutes les banques, quelle que soit leur taille, aient mis en place un dispositif efficace pour identifier, évaluer, suivre et maîtriser/atténuer les risques opérationnels importants, dans le cadre d'une approche globale de la gestion du risque.

Principe 9 : Les superviseurs devraient procéder régulièrement, de manière directe ou indirecte, à une évaluation indépendante des politiques, procédures et pratiques des banques en matière de risque opérationnel. Les superviseurs doivent veiller à ce qu'il existe des mécanismes appropriés leur permettant de se tenir informés de l'évolution dans les banques.

- **Rôle de la communication financière :**

Principe 10 : La communication financière des banques doit être suffisamment étoffée pour permettre aux intervenants du marché d'évaluer leur méthodologie de gestion du risque opérationnel.

3. Réglementation tunisienne

Les risques opérationnels sont considérés par le comité de Bâle comme une catégorie spécifique de risque qui nécessite, au même titre que les risques de crédit ou de marché, la définition d'un dispositif de gestion particulier. La maîtrise de ces risques est associée alors au contrôle interne chargé de la mise en place d'un dispositif de contrôle des opérations et des procédures internes. Dès lors, la réglementation tunisienne n'a pas ignoré cet aspect très important à travers différents textes réglementaires :

La question du contrôle interne a été abordée alors par la réglementation comptable tunisienne à travers les normes comptables générale et qui ont apporté de nouvelles idées résumées en un meilleur environnement de contrôle imposant discipline et organisation, une évaluation des risques, une application des normes et procédures facilitant les activités de contrôle, la collecte d'information pertinente à travers des systèmes d'information efficients ainsi qu'un système de suivi et de pilotage permanent.

De plus, la circulaire 2006-06[5] a instauré pour les établissements de crédit l'obligation de mettre en place un système de contrôle de la conformité. Ce système comporte les principes fondamentaux, les mécanismes et procédures adéquats pour garantir le respect par l'établissement des lois et règlements en vigueur, des bonnes pratiques et des règles professionnelles et déontologiques.

[5] Circulaire aux établissements de crédit n° 2006-06, «Mise en place d'un système de contrôle de la conformité au sein des établissements de crédit ».

Encore, la circulaire aux établissements de crédit 2006-19[6] de la BCT désigne le système de contrôle interne par « l'ensemble des processus, méthodes et mesures visant à assurer en permanence la sécurité, l'efficacité et l'efficience des opérations, la protection des actifs de l'établissement de crédit ou de la banque non résidente, la fiabilité de l'information financière et la conformité de ces opérations avec les lois et les règlements en vigueur ».

Une autre innovation de taille a été apportée par la circulaire 2006-19 : Il s'agit de l'obligation par les établissements de crédit de mettre en place un système de mesure, de surveillance et de maîtrise des risques de crédit, de marché, de taux d'intérêt, de liquidité, de règlement et opérationnel.

Malgré l'apport de la circulaire (surtout au niveau des articles 46 et 47 exigeant des mesures d'identification, d'évaluation, de suivi et d'atténuation du risque opérationnel), certaines critiques peuvent lui être adressées dont notamment : la non spécification des composantes et des systèmes de gestion du risque opérationnel à mette en place, le libre choix des méthodes voire du « mix » des méthodes d'évaluation et l'absence d'obligation au niveau de reporting (la seule obligation incombant aux établissements de crédit est la communication à la BCT d'un rapport annuel sur la mesure et la surveillance des risques auxquels ils sont exposés).

La circulaire 2011-06[7] est venue renforcer la gouvernante des établissements de crédit par le biais de règles que ces derniers sont tenus de respecter. La circulaire s'articule autour des quatre axes en étroite relation avec la gestion du risque notamment le risque opérationnel (le conseil d'administration, les comités ; la nomination et rémunération ainsi que la politique de communication) permettant aux établissements de crédit d'assurer une bonne gestion (une gestion prudente), de garantir la pérennité de l'établissement et de préserver les intérêts des actionnaires, des déposants et du personnel.

CONCLUSION

Ces dernières années, les problèmes bancaires dont les conséquences financières étaient substantielles, n'étaient pas dus aux mauvaises décisions de crédit mais principalement aux fraudes humaines, au manque de contrôle interne ou aux menaces technologiques. Le

[6] Circulaire aux établissements de crédit n° 2006 - 19 « Contrôle Interne ».
[7] Circulaire aux établissements de crédit n° 2011 -06, « Renforcement des règles de bonne gouvernance dans les établissements de crédit ».

risque opérationnel se retrouve ainsi au cœur de la réglementation prudentielle et des recherches académiques.

Dans ce premier chapitre, nous avons présenté brièvement la spécificité de l'activité de la banque ainsi que les risques qui y sont inhérents. Ensuite, nous avons mis l'accent sur la définition et les particularités du risque opérationnel bancaire. La dernière section du présent chapitre est consacrée au cadre réglementaire du risque opérationnel pour les établissements bancaires. Pour cela, nous avons mis en exergue les réglementations nationales et prudentielles relatives à ce sujet.

Même si la gestion des risques n'est pas un nouveau débat, la problématique actuelle pour une banque, est de disposer de meilleurs outils d'identification et d'analyse des risques opérationnels. Une fois identifiés, il est possible de les mesurer, de mettre en place des mesures destinées à les atténuer et de prévoir les fonds propres nécessaires pour faire face aux pertes potentielles. On parle ainsi de la cartographie des risques opérationnels qui fera l'objet du chapitre suivant.

CHAPITRE 2 :LA DÉMARCHE D'ÉLABORATION D'UNE CARTOGRAPHIE DES RISQUES OPÉRATIONNELS

INTRODUCTION

Les évolutions de la règlementation prudentielle bancaire (Bâle II) ont incité les banques à gérer de manière explicite le risque opérationnel afin de lui affecter un montant en fonds propres. L'évaluation du risque opérationnel se distingue des risques traditionnels de la banque notamment par l'absence d'encours connus. Il est diffus, multiforme et ambigu (Power, 2005). Comme le soulignent Lamarque et Maurer (2009), l'approche quantitative du risque opérationnel, compte tenu de sa difficile prévisibilité, est « insuffisante pour maîtriser ces risques et la gravité des évènements exceptionnels est extrêmement difficile à évaluer ».

C'est pourquoi, en complément de l'analyse des pertes internes au travers de leur collecte, le régulateur impose aux établissements de crédit d'intégrer dans leur démarche des éléments prospectifs liés à l'environnement opérationnel et au contrôle interne : c'est ainsi que la démarche de cartographie des risques s'est progressivement imposée aux banques. Cette démarche s'inscrit dans une volonté de rationaliser la complexité dans un univers incertain.

Dans ce deuxième chapitre, nous allons exposer, en premier lieu, les notions de base de la cartographie des risques opérationnels. Ensuite, nous allons mettre en exergue les différentes étapes de son élaboration.

SECTION 1 : CADRE CONCEPTUEL RELATIF A LA CARTOGRAPHIE DES RISQUES

1. Définition de la cartographie des risques

Plusieurs auteurs et groupes professionnelles ont défini la cartographie des risques. La multitude de définitions relatives à ce terme tournent autour du même objectif une représentation visuelle des risques de l'entreprise servant de support à leur maîtrise.

Commençons par la définition de F. Moreau (2002) qui a considéré la cartographie des risques comme étant « le produit essentiel du processus global de gestion des risques qui doit s'appuyer sur une organisation permettant de mettre à jour régulièrement et efficacement cette cartographie en fonction de l'évolution du contexte et des activités de l'entreprise et d'appliquer les actions de transformation du profil des risques qui s'imposent. D'une manière

générale, la cartographie des risques est un outil de pilotage et d'aide à la décision en matière de gestion des risques ».

Pour G. De Mareshal (2004), la cartographie des risques est « un mode de représentation et de hiérarchisation des risques d'une organisation. Cette représentation s'appuie sur une identification des risques effectués sur la base de la définition des risques ». Destinée à offrir une vision globale et synthétique des risques, la cartographie est alors un moyen d'hiérarchiser, suivre et organiser le traitement des risques.

Selon l'Institut Français de l'Audit et du Contrôle Interne IFACI (2003), la cartographie des risques est « le positionnement des risques majeurs selon différents axes, tels que l'impact potentiel, la probabilité de survenance ou le niveau actuel de maîtrise des risques». Encore, l'IFACI (2005) rajoute que cette cartographie est « une représentation graphique de la probabilité d'occurrence et de l'impact d'un ou de plusieurs risques représentés de manière à identifier les risques les plus significatifs et encore les moins significatifs.

Cependant la définition de Bernard et al. (2008), va encore plus loin. En effet, pour eux« la cartographie est un outil de pilotage vivant cul: doit permettre de mesurer régulièrement la progression de l'entité dans son niveau de maîtrise des risques »

De ces définition il en ressort que la cartographie des risques n'est autre qu'un outil de pilotage et d'aide à la décision en matière décision des risques qui permet de recenser les risques majeurs d'une organisation et de les présenter de façon synthétique sous une forme hiérarchisée.

2. Types de cartographie des risques

Avant de mettre en place une cartographie des risques, il est indispensable de définir son type. Selon Mareschal (2003), il existe deux types de cartographies de risques : la cartographie globale et la cartographie thématique. Le choix de l'une ou de l'autre de ces options découle des objectifs de l'étude et de l'arbitrage coût/bénéfices.

2.1.La cartographie globale

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

risques et à les hiérarchiser afin de diffuser une vision globale des risques majeurs au sein de l'organisation concernée.

2.2.La cartographie thématique

A la différence de la cartographie globale, celle thématique se limite à un domaine particulier. DE MARESCHAL (2003) définit la cartographie thématique comme étant un outil de recensement et d'hiérarchisation des risques spécifiques à un domaine bien particulier ou un thème bien précis, pouvant constituer un premier jalon vers une cartographie globale de l'entité.

3. Objectifs de l'établissement de la cartographie des risques

La cartographie des risques constitue un véritable inventaire des risques d'une organisation. Elle permet d'atteindre les objectifs ci-après (Bernard & al, 2010 ; Renard, 2010):

- Inventorier, évaluer et classer les risques de l'organisation ;
- Informer les responsables afin qu'ils puissent adapter le management de ses activités ;
- Intégrer l'analyse approfondie des processus et capitaliser l'expertise professionnelle ;
- Permettre à la hiérarchie d'élaborer une politique de risque ;
- Établir un plan d'audit et un plan d'action ;
- Répondre aux dispositions réglementaires et aux bonnes pratiques en matière de gouvernement d'entreprise.
- Créer un référentiel commun, connu et compris ;
- Promouvoir le contrôle interne ;
- Communiquer sur les résultats.

4. Les motivations de l'établissement d'une cartographie des risques

Plusieurs raisons peuvent motiver une entreprise à envisager l'élaboration d'une cartographie des risques.

Le plan d'audit : la cartographie des risques permet le pilotage de la gestion du risque en identifiant les domaines d'actions prioritaires. En effet, elle oriente le plan d'audit interne en mettant en lumière les processus ou les activités où se concentrent les risques majeurs ;

Un référentiel d'analyse des risques : La cartographie des risques est établie pour

permettre autant aux dirigeants ainsi qu'aux opérationnels d'avoir un référentiel homogène en matière de risques.

La communication en matière des risques : la cartographie est un outil de communication interne. En effet, les dirigeants l'utilisent pour maitriser l'évolution des risques majeurs susceptibles d'affecter gravement leurs activités et pour lesquels des actions préventives et correctives doivent être menées en priorité. La cartographie des risques est aussi un outil de communication externe. Elle vise à rassurer l'ensemble des parties prenantes (Etat, assurance, commissaires aux comptes, marchés financiers) quant à la capacité de l'entreprise à honorer ses engagements en toutes circonstances.

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

5. Les facteurs clés de succès d'une cartographie des risques

Etant un outil essentiel de gestion des risques au sein de l'entreprise, la cartographie des risques exige un certain nombre de facteurs de réussite (FONTUGNE et AL, 2001) qui sont essentiellement les suivants :

- La définition et la diffusion des objectifs clairs ;
- La définition précise du périmètre des risques pertinents ;
- Le caractère opérationnel et concret du projet ;
- La disponibilité des moyens financiers, informatiques et humains nécessaires pour un bouclage rapide du projet;
- La gestion du projet : pour que le projet de la cartographie soit bien mené, il est important de l'encadrer et de transmettre à chacun ce qu'on attend de lui, le format de restitutions attendues et le calendrier ;
- La désignation d'un responsable qui sera chargé de coordonner le travail ;
- Un groupe de travail qualifié : Une telle équipe doit être composée de responsables opérationnels ayant une meilleure vision des processus et activités de la banque, ainsi que des membres de la direction générale ayant à charge d'adapter la stratégie de la

banque et de prendre les décisions en matière de politique de risque. L'intervention des spécialistes outillés tels que les cabinets de conseil externes peut être très bénéfique dans la prise de décisions ;

- L'implication de la hiérarchie : Un tel projet comporte souvent une forte composante de changement et dans ce cas, la résistance au changement dans une organisation peut empêcher le projet de cartographie des risques d'atteindre ses objectifs ;
- La prise en compte de la culture de l'entreprise puisque la gestion des risques dans une entreprise dépend d'une manière significative de la culture de l'entreprise.

6. Les différentes approches d'élaboration d'une cartographie des risques

L'approche de l'élaboration de la cartographie des risques varie en fonction de l'objectif visé. Renard (2002), distingue trois approches d'élaboration de cartographie des risques, à savoir le top-down, le bottom-up et leur combinaison. D'autres auteurs comme AMARE (2002), propose en plus de ces trois méthodes précitées cinq autres. Il s'agit de l'approche par le benchmarking, approche par l'auto-évaluation, approche par analyse et synthèse rationnelle des risques, les points d'entrée, la macro cartographie. Dans ce qui suit, nous allons illustrer les approches les plus utilisées.

6.1.L'approche Bottom-Up

Cette approche dite ascendante consiste à faire identifier les risques par les opérationnels c'est-à-dire ceux chargés d'exécuter quotidiennement les tâches. Les risques recensés sont à l'état brut et font l'objet d'une remontée au niveau de la hiérarchie à charge pour cette dernière de les analyser pour ne retenir que ceux qui sont pertinents. Ce type de recensement des risques se fait généralement par l'intermédiaire des entretiens. L'utilisation d'une grille des risques potentiels, préparée à l'avance, permet de s'assurer que tous les risques ont bien été évoqués. Cette approche est souvent utilisée dans une cartographie globale.

Cependant, cette démarche interactive et participative peut être porteuse de difficultés. Pour BARBIER (1999), « elle est séduisante mais se heurte à d'importantes difficultés de principe et de pratique que l'on peut résumer comme suit : les participants ont-ils la motivation, la disponibilité, l'indépendance d'esprit, le recul et la compétence pour évaluer eux-mêmes l'état de leur contrôle interne ? Et sinon, quelles réponses apporter à ces questions? ».

6.2.L'approche Top-Down

Cette approche dite descendante se présente comme l'inverse de l'approche précédente. Elle consiste à faire détecter les risques par la hiérarchie qui les soumet aux opérationnels pour avis. Cette approche est souvent utilisée dans une cartographie thématique et peut se faire par questionnaire. Elle présente l'avantage de la facilité de mise en œuvre. En effet, le nombre d'entretiens nécessaires est réduit. Cependant, elle présente l'inconvénient d'être mois précise dans l'identification des risques.

6.3.L'approche combinée

Comme son nom l'indique, cette approche combine les deux approches précédentes. Selon cette approche, les risques sont déterminés parallèlement par la hiérarchie et les opérationnels. Elle est considérée comme la plus efficace par rapport aux deux premières approches parce qu'elle permet d'avoir une base assez complète des risques dans l'institution.

6.4.L'approche par le Benchmarking

Selon BRILMAN & al (2006), le benchmarking est le processus qui consiste à identifier, analyser et adopter, en les adaptant, les pratiques des organisations les plus performantes dans le monde en vue d'améliorer les performances de sa propre organisation.

C'est une approche qui consiste à collecter, auprès des entreprises du même secteur, les bonnes pratiques en matière d'identification et de gestion des risques. Les bonnes pratiques en matière d'identification des risques. Cela peut se faire à l'occasion des séjours d'échanges d'expériences dans ces entités, ou lors de conférences et d'ateliers de formations.

SECTION 2 : DEMARCHE D'ELABORATION D'UNE CARTOGRAPHIE DES RISQUES OPERATIONNELS

De prime abord, il y a lieu de préciser, comme le souligne Renard (2002), qu'il n'existe pas de méthode idéale, unique et rigoureuse, adaptable à toutes les entreprises. Ainsi chaque méthode à sa valeur suivant des situations bien définies. Cependant, nous pouvons identifier trois phases primordiales dans chaque démarche à savoir : la phase de préparation, la phase de conception et la phase après cartographie.

1. La phase de préparation

Toute cartographie des risques nécessite une préparation rigoureuse. Selon Moreau (2003), De Marschal (2003), cette phase comprend :

- La constitution d'une équipe de qualité pour les travaux ;
- La préparation des fonds nécessaires à la réalisation de ces travaux ;
- La définition du périmètre de la cartographie ;
- Le choix d'une typologie des risques.
- Le choix de la démarche de conception de la cartographie.
- L'analyse du contexte de l'étude et fixation des objectifs

Par ailleurs, il faudra procéder à une étude documentaire sur les pratiques existantes en matière de cartographie des risques et construire une démarche contenant les meilleures pratiques. Le choix de la démarche de conception de la cartographie des risques doit tenir compte de la spécificité de l'entreprise en termes de choix stratégiques, de son organisation, de son système d'information et de ses activités. Selon Baron (2001), cette phase peut se poursuivre jusqu'à la segmentation de l'organisation en processus, sous processus et tâches élémentaires. Ceci permet de mieux comprendre le processus, d'identifier les principales zones à risques, ce qui facilite la construction du questionnaire de contrôle interne (Renard, 2009).

2. La phase de conception

2.1.Identification des risques opérationnels

Après avoir décomposé les processus en différentes activités ou tâches élémentaires, il s'agit dans cette étape d'identifier tous les événements à risque qui peuvent se produire lors d'un processus et qui pourraient avoir des conséquences sur son déroulement (Jiménez & al 2008). Pour Barthelemy & Courreges (2004), il n'existe pas de méthode sans faille, seule l'expérience et l'humilité des dirigeants sont garanties pour l'identification des risques.

2.1.1. Les techniques d'identification des risques

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

Identification basée sur l'atteinte des objectifs : il s'agit d'identifier d'abord les objectifs et leur affecter les menaces inhérentes. L'efficacité de cette technique se base sur une identification claire et partagée des objectifs en amant ;

Identification basée sur les check-lists : qui s'inspire des check-lists établies à l'avance dans lesquelles on retrouve l'ensemble des risques possibles en rapport avec l'activité et les processus d'après Ohanessian (2004) et Maders & al (2006) ;

Identification par l'analyse des activités (tâches élémentaires) : qui consiste à subdiviser l'activité, la fonction, le processus en tâches élémentaires facilement observables. Par la suite, chaque tâche non effectuée ou mal effectuée sera rattachée à ses risques. Renard (2006) ;

Identification par l'analyse historique : qui consiste à déterminer les lignes des opérations touchées par un événement défavorable dans le passé et d'évaluer l'occurrence d'un tel événement Barroin et al (2002). Pour cela, il faut établir un récapitulatif des différents risques qui ont touché les processus de l'entreprise et qui ont occasionné des pertes. Toutefois cette méthode présente des limites compte tenue de la variation des risques tant en interne qu'en externe ;

Identification basée sur les scénarii : qui est une technique qui part d'événements primaire, pour établir un scenario d'événements redoutés générateurs de risques d'après Ellenberger (2004). Ainsi, la première étape décrit chacune des tâches qui composent l'activité. La seconde imagine collectivement les menaces qui vont permettre de détecter les risques qui vont se réaliser (Bernard et al, 2006) ;

Identification basée sur l'analyse de l'environnement : qui propose de déterminer les risques potentiels par anticipation de l'évolution future de l'environnement externe et interne.

2.1.2. Les outils d'identification des risques

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

L'entretien : C est un outil de collecte des données afin de les analyser. L'objectif de l'entretien est de dégager des interlocuteurs une description détaillée du processus étudié, d'identifier les risques inhérents au processus ainsi que les contrôles y associés.

Le questionnaire : Le questionnaire est un ensemble de questions construites dans le but d'obtenir des réponses structurées. Il combine souvent deux formes de questionnaires à savoir le questionnaire fermé et le questionnaire ouvert. Dans un questionnaire fermé, les questions imposent au répondant une forme précise de réponse et un nombre limité de choix de réponse. Dans un questionnaire ouvert, la personne interrogée développe une réponse que l'enquêteur prend en note. Dans ce cas, l'enquête par questionnaire ouvert ressemble à un entretien individuel de type directif.

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

Tableau 3 : Tableau d'identification des risques

Tâches	Objectifs	Risques	Evaluation	Dispositif du contrôle interne	Constats

Source : RENARD (2010)

2.2.Evaluation des risques inhérents

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

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

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

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

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

L'estimation qualitative des risques : c'est une estimation où la probabilité et l'importance des conséquences sont exprimées en termes qualitatifs. Elle est moins fiable et considérée comme subjective, car elle est basée sur des perceptions subjectives. Cette méthode d'estimation est utilisée lorsque (LANDWELL et al, 2005) :

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

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

Tableau 4 : Echelle d'évaluation de la fréquence des risques

Cotation	Fréquence	Eléments de mesure
1	Exceptionnel	Occurrence quasi nulle (<1%) sur 2 ans
2	Rare	Occurrence possible, mais peu probable (1 à 10%) sur 2 ans)
3	Probable	Occurrence plausible (10 à 50%) sur 2 ans
4	Très probable	Occurrence très probable (>50%) sur 2 ans

Source : IFACI[8]

[8] IFACI. Groupe Professionnel Assurance, La cartographie des risques. 2éme édition, Paris, « cahier de recherche », 2013, 136p, page 36.

L'impact du risque : il représente la sévérité de ces conséquences sur l'entreprise en cas de manifestation. Selon l'IFACI l'impact peut être classé en 3 catégories :

Tableau 5 : Catégories d'impact des risques

Impact financier	Impact juridique	Impact sur l'image
- Hausse des coûts ; - Perte financière ; - Baisse des revenus.	- Responsabilité civile et/ou légale ; - sanctions légales ou professionnelles.	- Dégradation de l'image ; - Réputation remise en cause.

Source : IFACI[9]

Le tableau ci-dessus présente un exemple d'échelle d'évaluation de l'impact des risques.

Tableau 6 : Echelle d'évaluation de la fréquence des risques

Cotation	Impact	Impact financier	Impact image	Impact légal réglementaire
1	Faible	< 10 000 euros	Impact local	Observation des autorités de tutelle
2	Modéré	Entre 10 000 et 100 000 euros	Impact régional	Avertissement des autorités de tutelle Mise en cause juridique devant une juridiction autre que pénale
3	Significatif	Entre 100 000 et 500 000 euros	Impact national limité	Blâme des autorités de tutelle / Mise en cause devant une juridiction pénale
4	Elevé	> 500 000 euros	Impact national large	Sanction des autorités de tutelles Condamnation pénale

Source : IFACI[10]

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

Criticité du Risque = Probabilité * Gravité

[9]IFACI. Groupe Professionnel Assurance, La cartographie des risques. 2éme édition, Paris, « cahier de recherche », 2013, 136p, page 37.

[10]IFACI. Groupe Professionnel Assurance, La cartographie des risques. 2éme édition, Paris, « cahier de recherche », 2013, 136p, page 38.

2.3.Hiérarchisation des risques inhérents

Il s'agit d'un classement en fonction du criticité de chaque risque inhérent en tenant compte du seuil de tolérance aux risques de l'organisation ainsi que son risque intrinsèque (risque maximum possible) RENARD (2004).

Selon Jokung (2008), la hiérarchisation des risques s'effectuera suivant la valeur des paramètres de l'évaluation. Trois cas pourront être présentés :

- Survenance et gravité sont élevées, ce type de risque est qualifié de majeur, il remet en cause les objectifs de l'entreprise ;
- Survenance et gravité sont faibles, le risque est qualifié de mineur, il ne remet pas en cause les objectifs de l'entreprise ;
- Les deux paramètres ne sont pas simultanément faibles ou simultanément élevés, le risque est qualifié d'intermédiaire. Il peut remettre en cause les objectifs de l'entreprise. Au sein des risques intermédiaires, on distingue des risques de fréquence, des risques de gravité et des risques moyens.

La hiérarchisation des risques inhérents devrait être affinée par l'appréciation des contrôles internes ayant déjà été mis en œuvre pour la réduction des effets de ces différents risques.

2.4.Identification et appréciation des contrôles internes existants

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

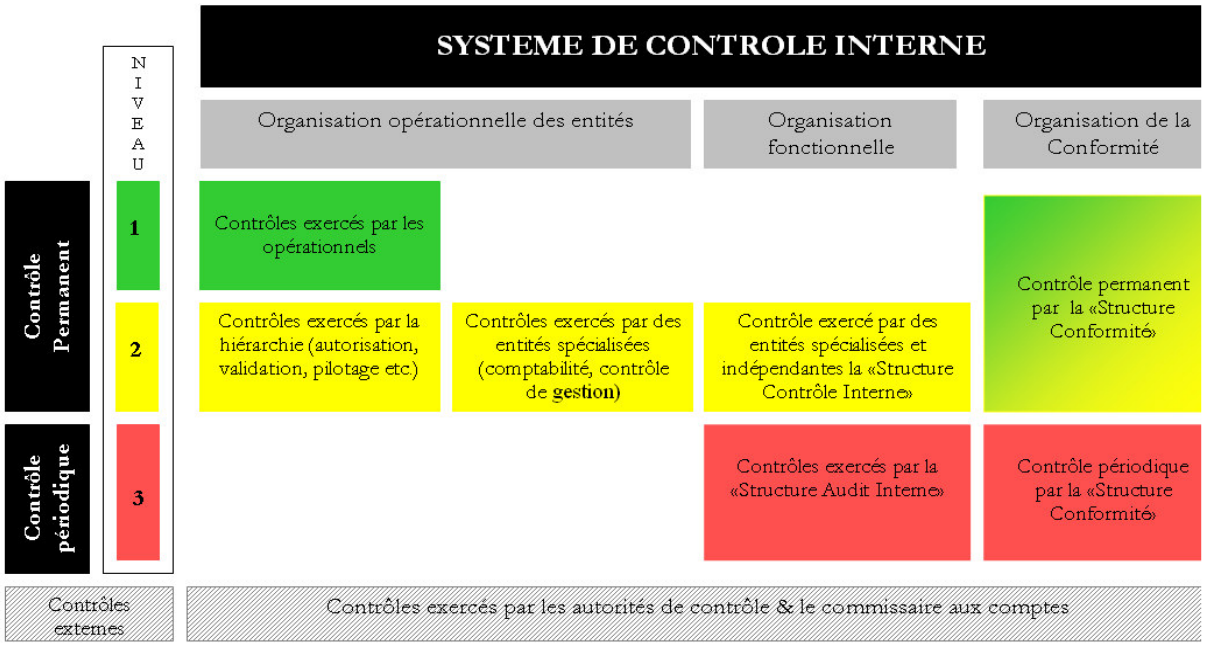
- L'efficacité : l'aptitude du contrôle à atteindre les objectifs pour lesquels il est mis en place ;
- La pertinence : l'utilité du contrôle et rapport coût/utilité ;
- La fiabilité : la capacité du contrôle à fonctionner de façon continue ;

- La qualité de la conception et de la mise en œuvre ;
- L'efficience il s'agit de rapprocher les trois critères à savoir coût, rendement et délai d'obtention des résultats.

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

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

Figure 1 : Hiérarchisation du système de contrôle interne



Source : Cours R.O[11]

2.5.Evaluation des risques résiduels

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

[11] Cours IFID « Risques Opérationnels » de Mr. Chiheb GHANMI.

2.6. Hiérarchisation des risques résiduels et préparation de la cartographie des risques

L'élaboration de la matrice des risques consiste à présenter les risques identifiés de l'entreprise à un moment donné, en fonction de leurs scores. A ce niveau, il est essentiel de prendre en considération le seuil de tolérance aux risques de l'entreprise. Ensuite, les risques seront représentés de manière à identifier les risques les plus significatifs et les moins significatifs (IFACI, 2006).

Selon Jiménez (2008) et Bapst (2003), après les travaux d'identification, d'évaluation, de classement et de hiérarchisation des risques, les risques susceptibles d'impacter l'atteinte des objectifs sont présentés dans un tableau suivant deux axes: impact et probabilité de survenance du risque. La matrice de risque peut être présentée sur la base d'une échelle de trois (3) a dix (10) intervalles en fonction de ce que l'entité veut mette en place, du temps allouer pour l'élaboration et de la complexité du processus étudié. La figure ci-dessous présente une matrice d'évaluation à quatre intervalles (4X4) :

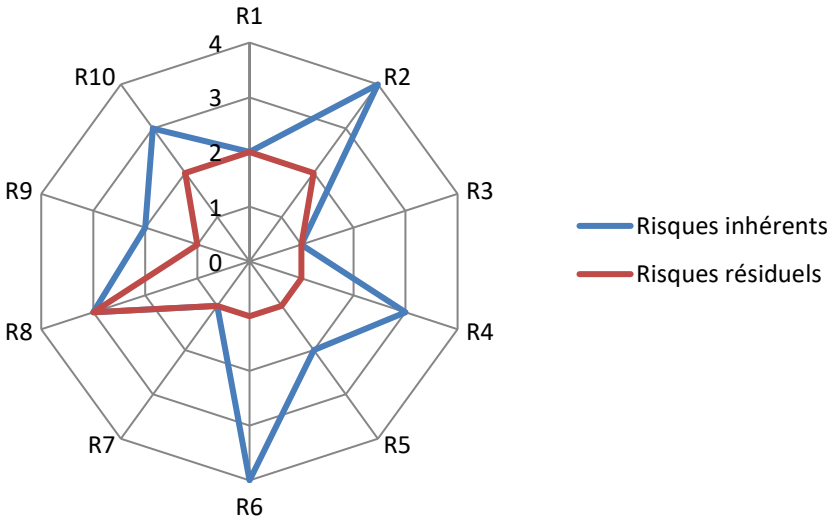
Figure 2 : Matrice d'évaluation des risques résiduels

Probabilité De survenance	**Fréquent**	Sérieux	Sérieux	Elevé	Elevé
	Probable	Faible	Modéré	Sérieux	Elevé
	Possible	Faible	Modéré	Modéré	Sérieux
	Improbable	Faible	Faible	Faible	Modéré
		Négligeable	**Marginal**	**Critique**	**Catastrophique**
	Sévérité des conséquences				

Source : Bonnal & al (2006 : 6)

Les risques inhérents et les risques résiduels peuvent être représentés dans un seul graphique (voir la figure ci-dessous) afin de mettre en valeur le rôle des contrôles internes dans l'atténuation des risques.

Figure 3 : Représentation schématique risques inhérents versus Risques résiduels



Source : Elaborée par nos soins

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

SECTION 3 : PHASE POST-ELABORATION D'UNE CARTOGRAPHIE DES RISQUES OPERATIONNELS

1. La mise en place d'un plan d'actions

Après avoir identifié, évalué et hiérarchisé, tous les risques qu'encoure l'entreprise feront l'objet d'un traitement. Parmi les deux composantes du risque qui sont l'impact et la probabilité, il faut pour chaque risque choisir une stratégie. Ce choix va dépendre largement de deux facteurs :

- La nature du risque ;
- Le rapport cout/bénéfice.

On distingue quatre solutions possibles :

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

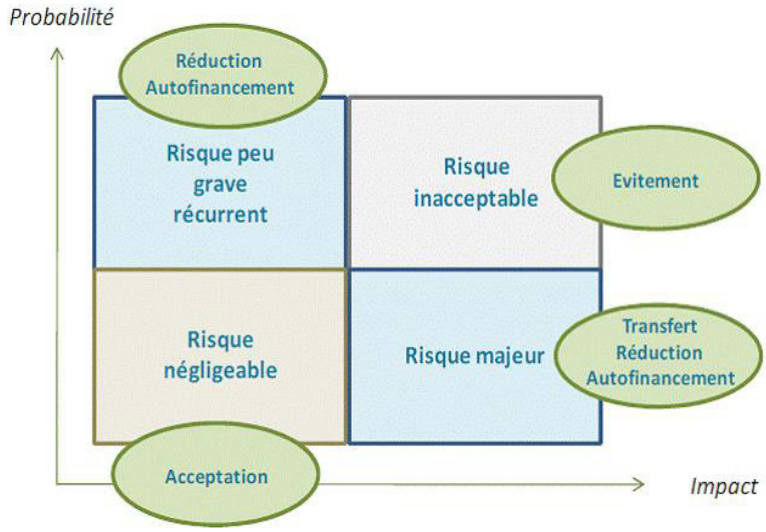
Le transfert : Le risque est déplacé vers une tierce partie soit par le biais de l'assurance soit via la sous-traitance d'une activité risquée.

L'évitement : On fait disparaître le risque en cessant l'activité qui le fait naître. Cette solution peut être envisagée quand le traitement du risque est très coûteux par rapport aux bénéfices rapportés par cette activité.

La réduction : La réduction de risque consiste à prendre des mesures pour réduire sa fréquence (la prévention) ou son impact (la protection) ou les deux à la fois. Le choix des actions à engager est effectué en comparant les coûts de leur mise en œuvre avec les coûts des conséquences du risque.

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

Figure 4 : Plan d'actions selon le résultat de la cartographie des risques résiduels



Source : OTC Conseil[12]

[12]OTC Conseil, lettre n°42 avril 2010.

2. La communication de la cartographie des risques

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

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

3. La phase de suivi

Elle permet de s'assurer de l'efficacité et de l'efficience des objectifs attribués au plan d'actions. Ainsi que de faire des comparaisons entre les résultats réels et ceux attendus. Toutefois, elle permet de se focaliser sur les dysfonctionnements dans le but de révolutionner les actions de progrès suivant Maders et Masselin (2009).

4. La mise à jour de la cartographie des risques

La cartographie des risques étant une photographie des risques de l'entreprise à un moment donné, sa mise à jour s'impose compte tenu de l'évolution rapide de 1 'environnement afin de prendre en considération non seulement 1'avènement des nouveaux facteurs de risques mais aussi de tenir compte des meilleures pratiques dans le domaine d'activité et des nouveautés issues des recherches. En fait, il s'agit de suivre l'évolution du profil de risque de l'entité à travers ses indicateurs et les dispositifs du contrôle interne mis en place grâce aux indicateurs de performance, pour une meilleure gestion des risques.

CONCLUSION

La cartographie des risques est l'un des instruments les plus pertinents pour identifier, évaluer et hiérarchiser les risques opérationnels pouvant impacter de façon significative l'atteinte des objectifs d'un établissement donné. Ainsi, l'analyse des résultats trouvés permet d'élaborer un plan d'actions à entreprendre pour faire face aux défaillances des contrôles existants et sert de base pour la planification d'un plan d'audit fondé sur les risques. Cela signifie que la cartographie des risques doit faire l'objet d'une communication interne et externe. Enfin, il est impératif qu'elle soit mise à jour pour suivre l'évolution de l'activité de la banque et de son environnement.

De ce fait, il importe de l'élaborer selon une démarche claire et rigoureuse, basée sur un modèle bien conçu et une approche appropriée à la nature de l'organisation. Notre prochain chapitre fera l'objet d'élaboration d'une cartographie des risques opérationnels liés au processus crédits Corporate au sein de l'ATB.

CHAPITRE 3 :LA CARTOGRAPHIE DES RISQUES OPÉRATIONNELS LIÉS AU PROCESSUS CRÉDITS CORPORATE AU SEIN DE L'ATB

INTRODUCTION

La gestion des risques est un facteur déterminant pour la conduite des organisations. Dans le domaine bancaire, la gestion des risques constitue l'essence même du secteur. Il importe donc aux dirigeants d'avoir à chaque moment une vue sur les risques encourus. Pour se faire la banque devrait se doter d'un dispositif d'identification, d'évaluation et de hiérarchisation des risques afin de les maitriser et assurer la continuité de ses activités.

L'élaboration de la cartographie des risques opérationnels liés au processus de crédit Corporate au sein de l'ATB s'inscrit dans cette logique. Pour se faire, nous procéderons à appliquer la démarche décrite dans le chapitre « La Démarche d'élaboration d'une cartographie des risques opérationnels ».

Le présent chapitre sera scindé en cinq sections :
Section 1 : Le contexte général du travail ;
Section 2 : Méthodologie de travail ;
Section 3 : La phase de préparation ;
Section 4 : La phase de conception ;
Section 5 : Analyse des résultats et plan d'actions.

SECTION 1 : LE CONTEXTE GENERAL DU TRAVAIL

1. Présentation de l'ATB[13]

L'Arab Tunisian Bank (ATB) est une société anonyme, créée en 1982 par l'intégration de la succursale tunisoise de l'Arab Bank et l'apport de personnes physiques tunisiennes.

Le capital de l'Arab Tunisian Bank s'élève à 100 000 000 de dinars composé de 100 000 000 d'actions d'une valeur nominale de un dinar chacune. Au 31 décembre 2016, le capital est détenu à hauteur de 64,24% par l'Arab Bank PLC, 24,10% par divers groupes privés, 8,38% par diverses personnes physiques et 3,01% par diverses personnes morales.

Actuellement, l'ATB dispose d'un réseau de 130 agences réparties sur tout le territoire tunisien et emploie prés de 1400 employés.

[13] Rapport annuel de l'ATB 2016.

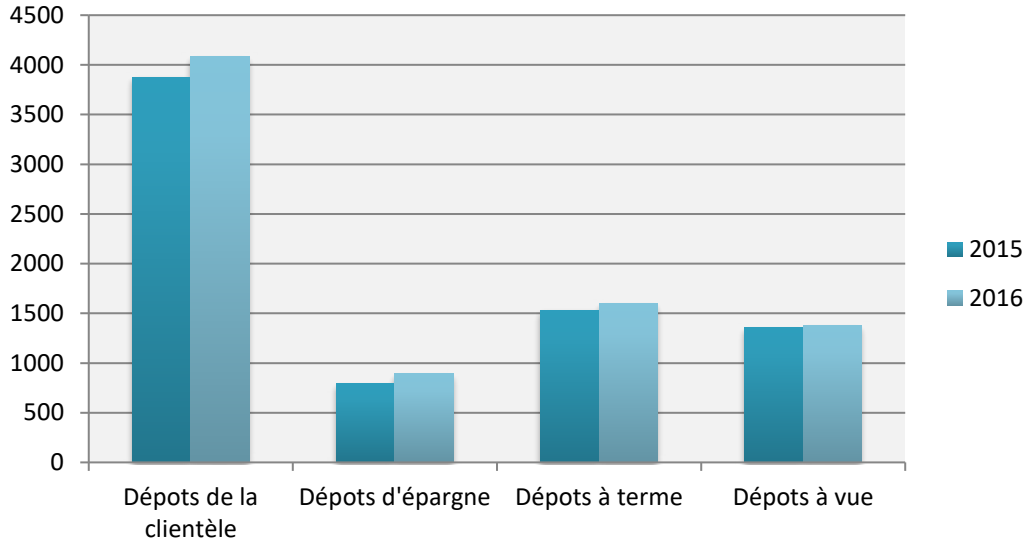
2. Indicateurs d'activité et de performance de l'ATB14

2.1.Les Dépôts

Les dépôts de la clientèle se sont établis au 31-12-2016 à 4 082,8 millions TND contre 3876,9 millions TND à fin décembre 2015, soit une évolution de 205,9 millions TND et une croissance de 5,3%.

Au terme de l'exercice 2016, les dépôts d'épargne ont affiché une variation positive de 12,8% pour s'établir à 891 millions TND contre 790 millions TND en 2015. Les dépôts à terme ont enregistré une hausse de 4,0% pour s'établir à 1 595 millions TND contre 1 533 millions TND au 31/12/2015. Les dépôts à vue ont évolué de 1,1% pour atteindre 1 373 millions TND contre 1 358 millions TND à fin décembre 2015.

Figure 5: Evolution de l'encours des dépôts (en millions de dinars)



Source : Elaborée par nos soins

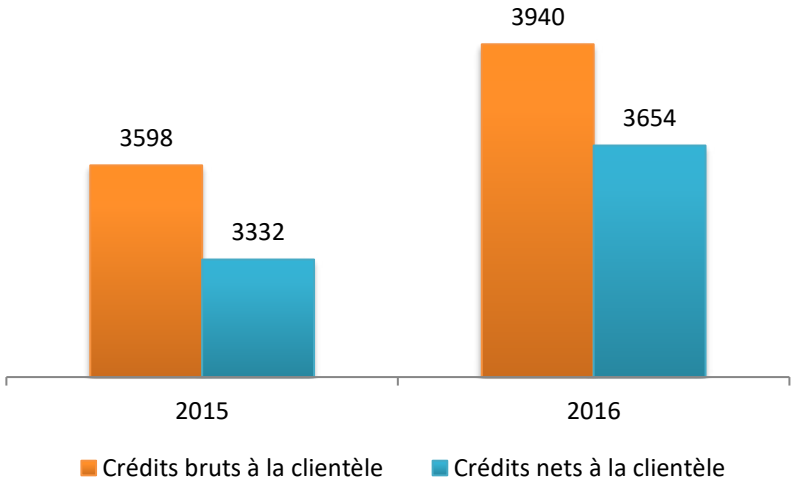
2.2.Les Crédits

Les crédits bruts à la clientèle se sont établis à fin décembre 2016 à 3 940 millions TND contre 3 598 millions TND au terme de l'exercice 2015, soit une hausse de 9,5%.

Les crédits nets à la clientèle se sont élevés à fin décembre 2016 à 3 654 millions TND contre 3 332 millions TND au terme de l'exercice 2015, soit une hausse de 9,7%.

[14] Rapport d'activité de l'ATB pour 2016.

Figure 6 : Evolution du volume des crédits accordés à la clientèle (en millions de dinars)



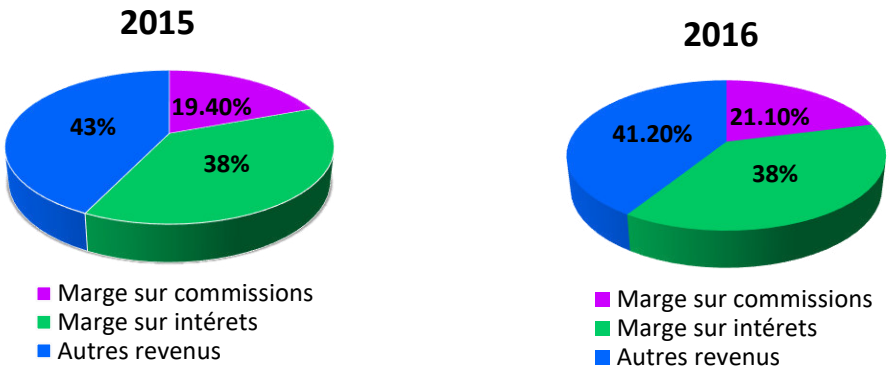
Source : Elaborée par nos soins

2.3.Le Produit Net Bancaire

Le Produit Net Bancaire s'est inscrit à la hausse atteignant 212 millions TND à fin 2016 contre 200 millions TND une année auparavant enregistrant, ainsi une augmentation de 6,1% par rapport à l'exercice 2015.

La structure du PNB de l'ATB a enregistré une hausse au niveau de la marge sur commissions qui a évolué de 19,4% à 21,1% et une stabilité au niveau de la marge sur intérêts de presque 38% entre 2015 et 2016. La part des revenus liés aux opérations financières et d'investissements a enregistré une baisse, son niveau est passé de 43% au 31/12/2015 à 41,2% au 31/12/2016.

Figure 7 : Evolution de la structure du PNB

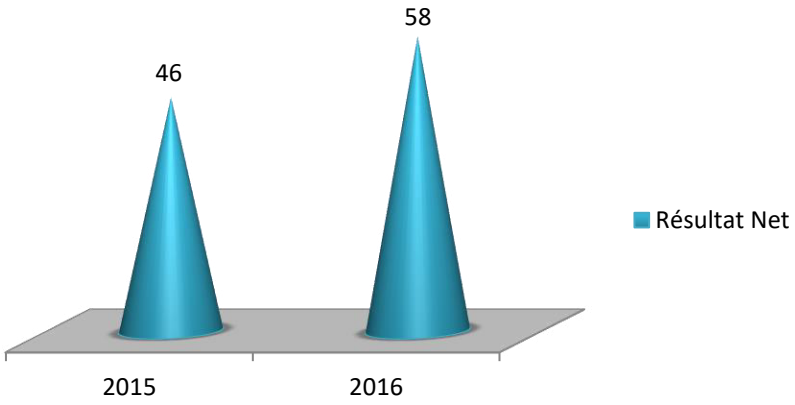


Source : Elaborée par nos soins

2.4.Le Résultat Net

L'exercice 2016 s'est soldé par la réalisation d'un Résultat Net d'un montant de 46 millions TND contre 58 millions TND au 31/12/2015, soit une baisse de 19,9%.

Figure 8 : Evolution du Résultat Net (en millions de dinars)



Source : Elaborée par nos soins

3. La gestion des risques au sein de l'ATB

Afin de se développer et de garantir sa pérennité dans un environnement évolutif de plus en plus réglementé, l'ATB accorde une grande importance à sa gestion des risques qui doit permettre l'identification, la mesure, le contrôle et la gestion de tous les risques auxquels elle fait face, dans les limites de son appétence aux risques. C'est ainsi que la Direction Centrale du Risk Management a été créée en 2013.

La politique générale de gestion des risques est établie conformément aux textes législatifs et réglementaires de la Banque Centrale de Tunisie traitant le sujet de gestion des risques à savoir, les circulaires BCT n°2006-19 et n°2011-06. Elle se base sur les recommandations du comité de Bâle qui sont considérées comme la référence internationale en matière de gestion des risques.

La gouvernance de la maitrise des risques de l'ATB est assurée au travers :

- Le Conseil d'administration, appuyé par 3 comités : Le Comité Exécutif de Crédit, le Comité Permanent d'Audit interne et le Comité des Risques ;
- Et les comités internes à la banque : Le comité Supérieur de crédit, le comité d'orientation de conformité, le comité ALCO le comité de trésorerie.

4. La gestion des risques opérationnels au sein de l'ATB

Pour les risques opérationnels, l'ATB a mis en place une culture d'observation, de quantification et de déclaration des risques opérationnels par le lancement de deux grands projets, à savoir :

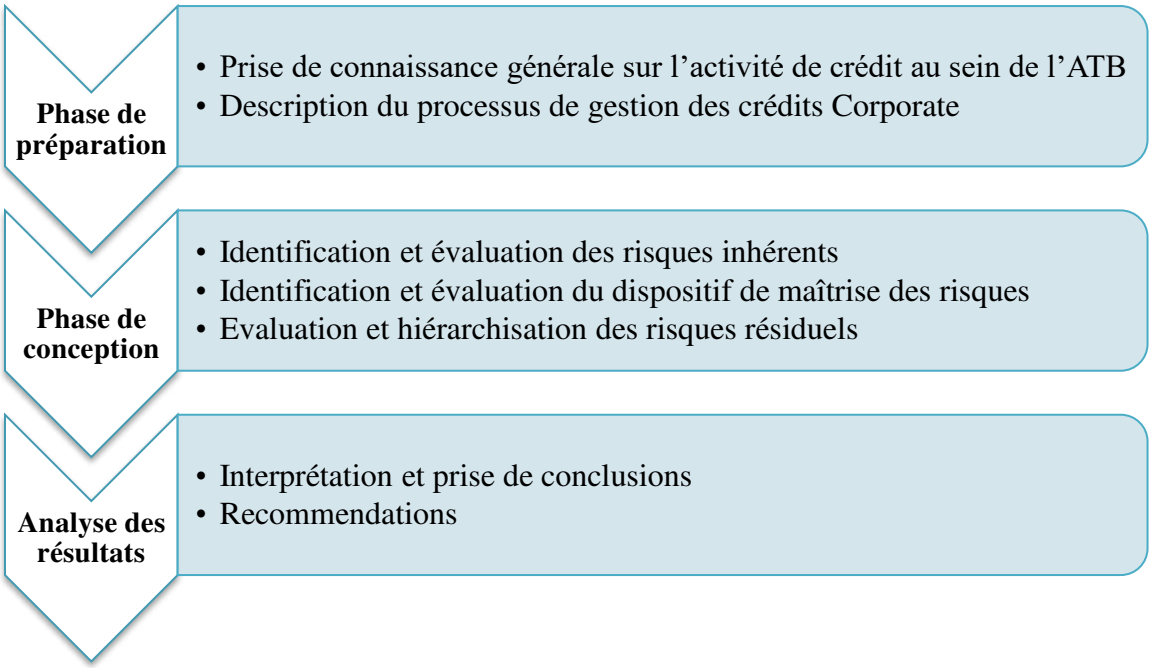
- La mise en place d'une procédure de collecte des incidents liés au risque opérationnel déployé au niveau des directions centrales et des agences. Une sensibilisation et un encadrement rigoureux des diverses entités de la banque sont mis en place en vue de donner l'efficacité nécessaire aux déclarations collectées ;
- Et l'élaboration d'une cartographie des risques opérationnels à partir du quatrième trimestre 2017.

SECTION 2 : METHODOLOGIE DE TRAVAIL

1. Le modèle d'analyse

Dans l'élaboration de notre cartographie des risques opérationnels, nous allons suivre la démarche telle qu'elle est schématisée ci-dessous.

Figure 9 : Modèle d'analyse



Source : Elaborée par nos soins

2. La collecte des données

Les outils de collecte de données utilisés sont les suivants :

Le questionnaire : Nous avons procédé, pendant la période de stage, à des questionnaires avec les collaborateurs intervenants dans la réalisation du processus Crédits Corporate, ainsi qu'avec les collaborateurs à la direction de conformité et à la division des risques opérationnels.

L'observation directe : Cet outil consiste à suivre le traitement d'un dossier de crédit Corporate dés le dépôt de la demande de crédit à l'agence jusqu'au déblocage. L'observation permet également de vérifier l'application des contrôles prévus à chaque étape.

L'analyse documentaire : Les documents consultés sont essentiellement :

- Le manuel de procédure de la banque décrivant le processus de crédit Corporate ;
- Les circulaires internes à la direction de Conformité ;
- Les circulaires internes à la direction Risk management.

3. L'analyse des données

Les outils utilisés dans l'analyse des données sont :

Le tableau d'identification des risques : Ce tableau est utilisé dans le cadre de recensement des risques. Il est construit par l'identification à chaque tâche du processus les risques susceptibles de se manifester et les contrôles internes pour les atténuer.

Le questionnaire du contrôle interne : Le questionnaire du contrôle interne est une grille de questions posées aux intervenants dans le processus du crédit Corporate pour identifier les contrôles existants ainsi que pour apprécier leur efficacité.

Les tests de conformité : Les tests de conformité donnent une réponse au degré d'application des mesures de contrôle interne. Il s'agit d'une analyse des différents documents et autres éléments matériels en vue de valider les réponses recueillies lors des entretiens.

SECTION 3 : LA PHASE DE PREPARATION

La première étape de conception d'une cartographie des risques opérationnels consiste à délimiter l'étude de la recherche par le choix entre une cartographie globale ou une

cartographie thématique selon les objectifs fixés ainsi que les moyens mis en œuvre pour la réalisation des travaux. Dans notre travail, nous avons opté pour la cartographie thématique en choisissant le processus crédits Corporate.

1. Définition du crédit Corporate

L'activité de crédit à l'ATB est devisée en deux lignes : les crédits Retail (les crédits aux particuliers) et les crédits Corporate (les crédits aux entreprises).

Concernant les crédits Corporate, objet de notre étude, ils prennent deux formes : des crédits de gestion et des crédits d'investissement.

Le portefeuille Corporate est composé de trois segments : Corporate Small, Corporate Medium et Corporate Large. La segmentation est effectuée selon deux critères : Le chiffre d'affaires et/ou le total des engagements auprès de l'ATB.

Tableau 7: Segmentation du portefeuille Corporate

	Chiffre d'affaires	Total des engagements
Corporate Small	Inférieur à 2 Md	Inférieur à 500 md
Corporate Medium	Compris entre 2 Md et 5 Md	Compris entre 500 md et 5 Md
Corporate Large	Supérieur à 5 Md	Supérieur à 5 Md

Source : Documents internes ATB

Le tableau ci-dessous indique le nombre annuel de dossiers de crédits Corporate traités au sein de l'ATB sur la période 2015-2017:

Tableau 8 : Statistiques sur les dossiers Corporate

	2015	2016	2017 (10 mois)
Nombre de dossiers de crédits Corporate traités	1270	1371	1144

Source : Données internes ATB

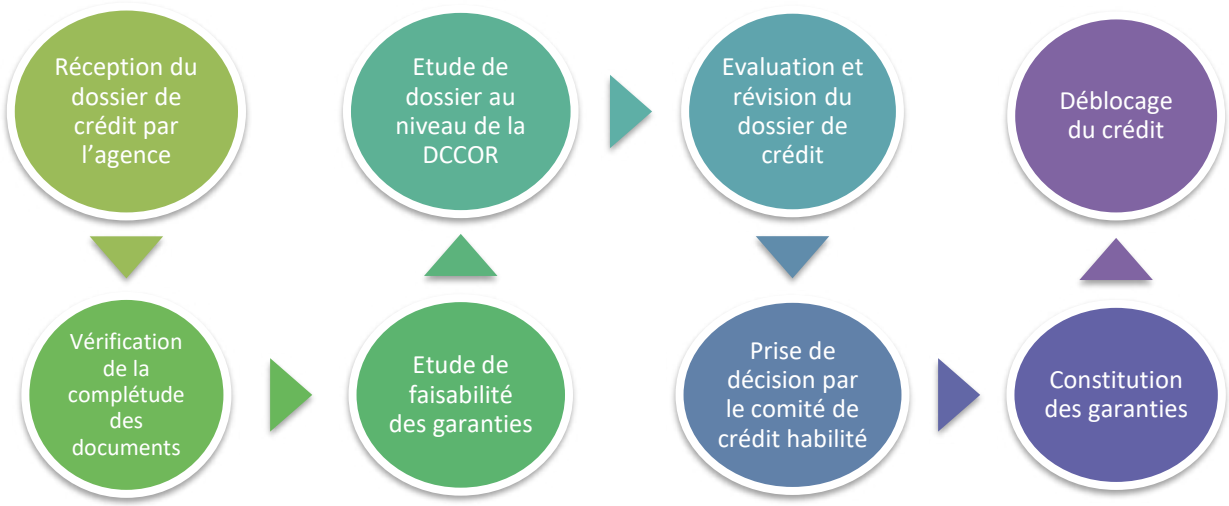
Nous remarquons que le volume des dossiers Corporate traités est en hausse et nous pouvons le qualifier comme relativement élevé (en moyenne 6 dossiers par jour pour 2016). Traiter un tel nombre de dossiers par jour est susceptible d'augmenter la fréquence des risques opérationnels ainsi que leur impact.

De ce fait, élaborer une cartographie des risques opérationnels liés au processus crédits Corporate revêt d'un intérêt particulier. Il s'agit d'un processus métier qui participe avec 31%[15] dans la formation du produit net bancaire.

2. La description du processus Crédits Corporate

La première étape de notre travail consiste à analyser le processus objet de la cartographie des risques. Nous avons donc procédé à la décomposition du processus de crédit Corporate en huit étapes principales qui nous permettent d'entamer l'identification des risques qui leur sont intrinsèques. Ainsi, au niveau de l'ATB six structures interviennent dans le processus crédits Corporate à savoir, l'agence, la direction centrale Corporate DCCOR, la direction des garanties de la DCAJIR, la direction centrale de crédit DCC, la direction administrative et contrôle des engagements DACE et la division portefeuille de la COU.

Figure 10 : Processus de gestion des crédits Corporate au sein de l'ATB[16]



Source : Manuel des procédures ATB

[15] Rapport d'activité de l'ATB pour 2016.
[16] Le schéma détaillé se présente à l'Annexe N°1.

- **1ére Etape : La réception du dossier de crédit par l'agence**

Le chargé de clientèle à l'agence, réceptionne le dossier de crédit présenté par le client. Ensuite, il invite le client à prendre attache avec le Chargé d'Affaires au niveau de la DCCOR qui le prendra en charge. Il scanne les documents financiers et juridiques accompagnés de la demande de crédit et l'envoi par e-mail à la DCCOR et la DCAJR. En suit, il envoi, à la DCCOR, le dossier original du crédit contre décharge le lendemain ouvrable.

Le Chargé d'Affaires DCCOR et le chef de la Division Garanties de la DCAJR récupèrent les documents respectivement financiers et Juridiques et procèdent à leurs traitement chacun en ce qui le concerne.

- **2éme Etape : La vérification de la complétude des documents au niveau de la DCCOR**

Le chargé d'affaires DCCOR entame la complétude des documents. S'il y a des documents absents, le chargé d'affaires doit remplir la note de complément des documents, la faire signer par la personne habilitée et la remettre au client. Sinon il établit un accusé réception de la complétude des documents, le faire signer par les personnes habilitées, et, le remettre au client contre décharge.

- **3éme Etape : L'étude de faisabilité des garanties au niveau de la direction des garanties de la DCAJR**

Au niveau de la direction des garanties, le chef de la Division des Garanties télécharge les documents juridiques, étudie la faisabilité des garanties et transmet par e-mail, ses conclusions, au chargé d'affaires de la DCCOR.

- **4éme Etape : Etude du dossier au niveau de DCCOR**

Après l'étude du risque client (consulter la base de classification ATB, la base des clients black listés et la base SED de la BCT), le chargé d'affaire étudie le dossier de crédit et remplit la fiche de décision du Comité de Crédit habilité. Puis, il le remet accompagné par des analyses financières et une évaluation du risque client, au directeur Centrale Corporate pour discussion, vérification. Suite à cette discussion, un avis motivé doit être précisé sur la fiche de décision.

- **5éme Etape : Evaluation et révision du dossier de crédit au niveau de la DCC**

Suite à la stratégie « BUSINESS-REVIEW » adoptée par l'ATB, l'octroi d'un crédit est une opération conjointe entre les chargés d'affaires de la DCCOR et les instructeurs de crédit de la DCC. Pour cette raison, le dossier doit être contrôlé, en ce qui concerne les données, les analyses et l'avis indiqué dans la fiche de décision de crédit, par DCC.

- **6éme Etape : Prise de décision par le comité de crédit habilité**

Ainsi, le dossier doit être discuté avec le comité supérieur de crédit afin de prendre la décision finale. Si la décision dépasse l'habilitation de ce comité, le dossier devrait être l'objet d'une autre discussion avec l'instance habilité pour avoir la décision finale. En cas d'accord, le chargé de dossier DCC, transmet la fiche de décision à la DACE pour élaboration de la notification provisoire de crédit « NPC» qui sera éditée par la suite et remise à la direction des garanties de la DCAJR.

- **7éme Etape : Constitution des garanties**

A ce niveau, le chef de la division des garanties doit élaborer le contrat de prêt, le faire signer par les personnes habilitées de la banque et l'envoyer pour légalisation des signatures de la banque. Au niveau de la DCCOR, le chargé d'affaires reçoit le contrat de prêt et invite le client à se présenter pour signature, légalisation et enregistrement de son contrat. Le chargé d'affaires, doit assurer un suivi auprès du client pour qu'il ramène le plus rapidement possible son contrat dûment signé, légalisé et enregistré ainsi que les formalités relatives aux garanties. En s'assurant de la bonne constitution des garanties, le chef de division des garanties envoie la NPC avec « bon pour déblocage » à la DACE.

- **8éme Etape : Déblocage du Crédit**

Le Chef de la Division Mise en place des Crédits, reçoit la NPC avec « bon pour déblocage ». Après le contrôle des habilitations et des termes de la NPC, il saisit la décision en NPC. Au niveau de la DCCOR/Agence et après l'édition de la décision de crédit, du titre de crédit et du tableau d'amortissement, le chargé d'affaires/ chargé de clientèle invite le client afin de lui remettre le titre de crédit et le tableau d'amortissement pour signature, lui vendre le timbre fiscal et percevoir les commissions. Puis, il scanne et transmet les documents de déblocage à la division portefeuille de la COU pour déblocage de crédit et conservation des documents.

SECTION 4 : LA PHASE DE CONCEPTION

1. Identification des risques inhérents

Après avoir décortiqué le processus crédits Corporate en huit sous processus, l'étape suivante consiste à identifier les principaux risques qui leur sont inhérents. A ce niveau, en adoptant l'approche combinée, nous avons procédé à des questionnaires (voir Annexe N°2) avec les collaborateurs des différentes unités intervenantes dans la réalisation du processus Crédits Corporate (Agence, DCCOR, Direction des garanties, DCC, DACE et division portefeuille de la COU) ainsi qu'avec les collaborateurs à la direction centrale de conformité et à la division des risques opérationnels.

Pour l'identification des risques, nous nous sommes basés sur la nomenclature des risques opérationnels, élaborée par nos soins, adaptée aux recommandations de Bâle 2 (voir Annexe N°3).

L'analyse des comptes rendus des questionnaires nous a permis de recenser les différentes catégories de risques opérationnels affectées au processus crédits Corporate, qui sont au nombre de cinq :

- Fraude interne ;
- Fraude externe ;
- Interruption de l'activité et dysfonctionnement des systèmes ;
- Exécution, livraison et gestion des processus ;
- Pratiques concernant les clients, les produits et l'activité commerciale.

Les résultats d'inventaire des risques opérationnels inhérents à chaque sous processus se présentent dans l'Annexe N°6.

2. Evaluation des risques inhérents

La quantification des risques bruts s'est avérée difficile à cause de non exhaustivité de la base des incidents de risque opérationnel. A ce stade, nous avons procédé aux questionnaires (voir Annexe N°6) et nous nous sommes basés sur les cotations des risques opérationnels en termes de vraisemblance et d'impact mentionnées dans la déclaration de l'appétence aux risques de l'ATB[17].

[17] Approuvée par le Conseil d'Administration et la Direction Générale.

Tableau 9 : Echelle d'évaluation de la vraisemblance des risques

Niveau de risque	Cotation chiffrée	Critères de vraisemblance
Fréquent	6	Se produit d'une manière fréquente, au moins une fois par semaine
Plausible	5	Probable de se produire une à deux fois au mois prochain
Probable	4	Probable de se produire une à deux fois dans les trois prochain mois
Occasionnel	3	Probable de se produire une à deux fois l'année prochaine
Lointain	2	Probable de se produire une à deux fois dans les trois prochaines années
Improbable/rare	1	Improbable de se produire dans les cinq prochaines années

Source : Déclaration d'appétence aux risques de l'ATB

Tableau 10 : Echelle d'évaluation de l'impact des risques[18]

Niveau de risque	Cotation chiffré	Critères d'impact financier
Catastrophique	6	Perte potentielle ou réelle dépassant les 4 millions de dinars
Majeur	5	Perte potentielle ou réelle dépassant les 2 millions de dinars et inférieur à 4 millions de dinars
Important	4	Perte potentielle ou réelle dépassant les 1 million de dinars et inférieur à 2 millions de dinars
Significatif	3	Perte potentielle ou réelle dépassant les 0.2 million de dinars et inférieur à 1 million de dinars
Modéré	2	Perte potentielle ou réelle dépassant les 0.05 million de dinars et inférieur à 0.2 million de dinars
Mineur	1	Perte potentielle ou réelle est inférieure à 0.05 million de dinars

Source : Déclaration d'appétence aux risques de l'ATB

Les résultats d'évaluation des risques opérationnels inhérents à chaque sous processus se présentent dans l'Annexe N°6.

[18]L'échelle détaillée d'évaluation de l'impact des risques se présente dans l'Annexe N°4.

3. Evaluation de la criticité des risques

La criticité est calculée de la manière suivante : « Fréquence X Gravité ». Les risques inhérents seront donc classés selon l'échelle quantitative suivante :

Tableau 11 : Matrice d'évaluation de la criticité des risques inhérents

		Criticité					
Vraisemblance	**6**	6	12	18	24	30	36
	5	5	10	15	20	25	30
	4	4	8	12	16	20	24
	3	3	6	9	12	15	18
	2	2	4	6	8	10	12
	1	1	2	3	4	5	6
		1	**2**	**3**	**4**	**5**	**6**
		Impact					

Source : Elaborée par nos soins

Afin de mettre en cohérence l'échelle d'évaluation des risques inhérents, nous avons eu recours à une table de correspondance pour la notation, qui aboutit aux conversions suivantes :

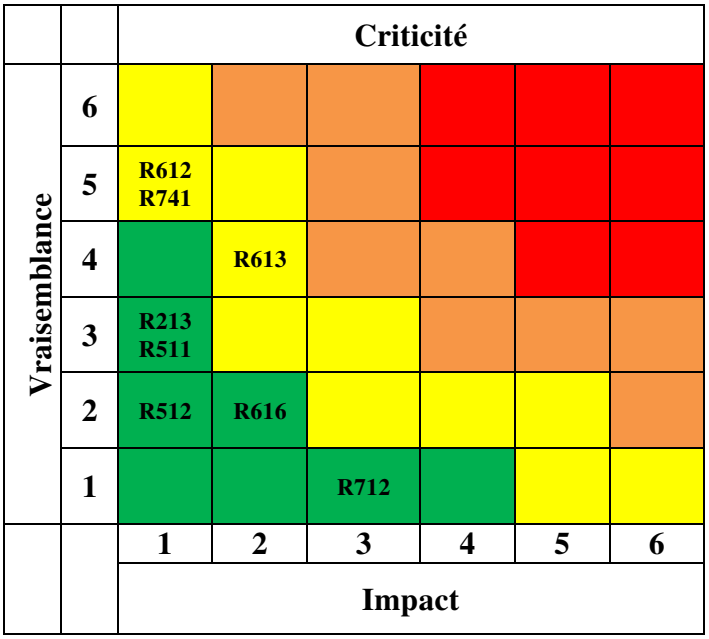
- [1,4]= 1 : **Risque Faible** ;
- [5,10]= 2 ; **Risque Moyen** ;
- [12,18]= 3 : **Risque Elevé** ;
- [20,36]= 4 : **Risque Extrême**.

Les résultats d'évaluation de la criticité des risques opérationnels inhérents à chaque sous processus se présentent dans l'Annexe N°6.

4. Hiérarchisation des risques inhérents

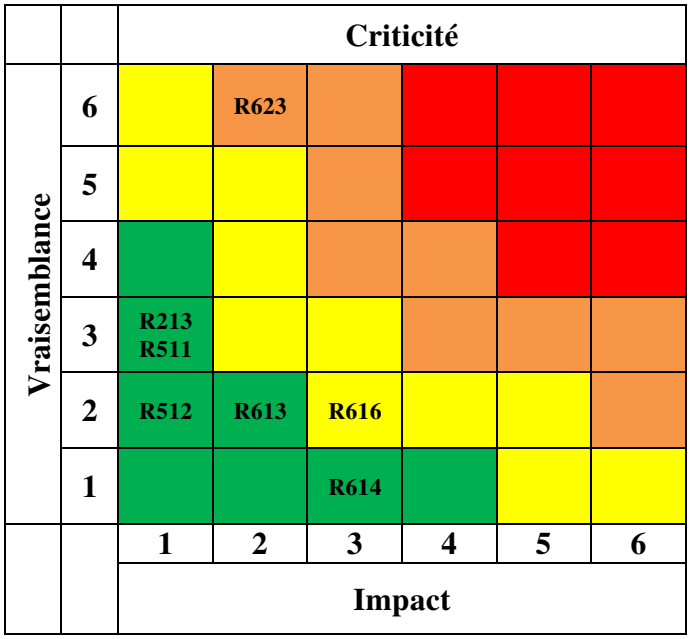
Sur la base des résultats des travaux d'identification et d'évaluation des risques inhérents, nous avons procédé à la hiérarchisation des risques inhérents par sous processus.

Figure 11 : Matrice des risques inhérents au sous processus « Réception du dossier de crédit par l'agence »



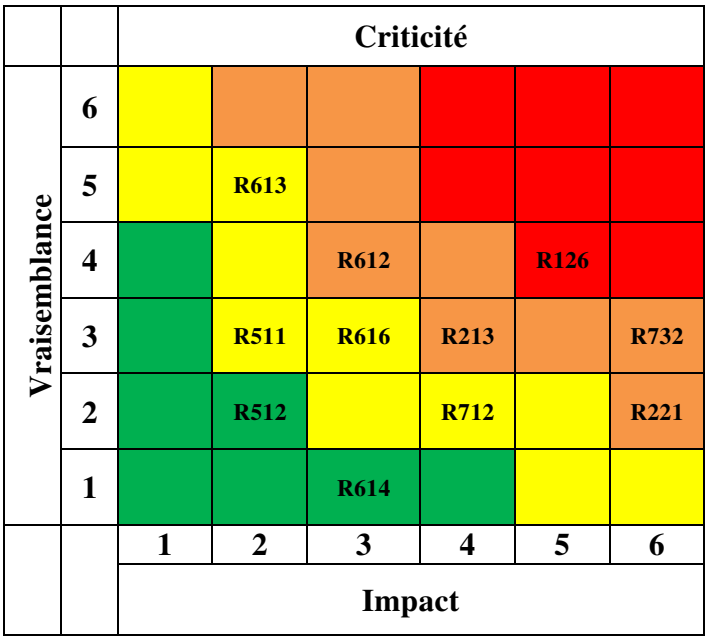
Source : Elaborée par nos soins

Figure 12 : Matrice des risques inhérents au sous processus « Vérification de la complétude des documents »



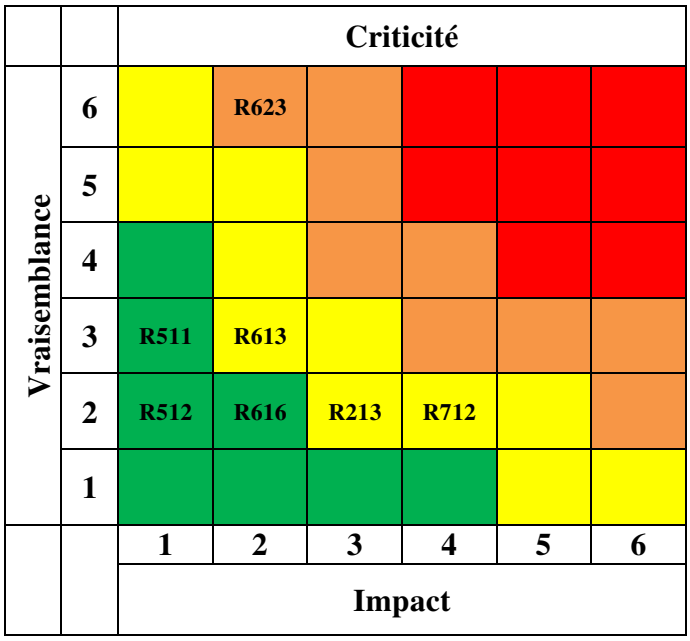
Source : Elaborée par nos soins

Figure 13 : Matrice des risques inhérents au sous processus « Etude de dossier de crédit »



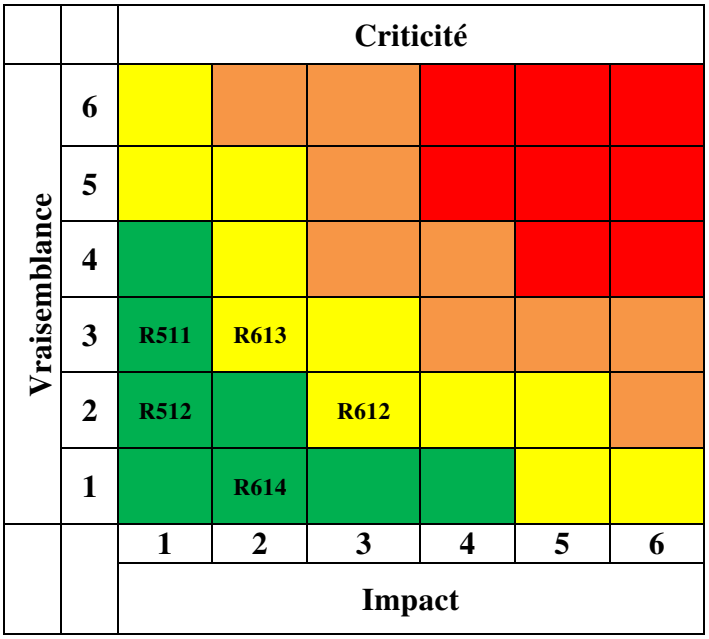
Source : Elaborée par nos soins

Figure 14 : Matrice des risques inhérents au sous processus « Etude de faisabilité des garanties »



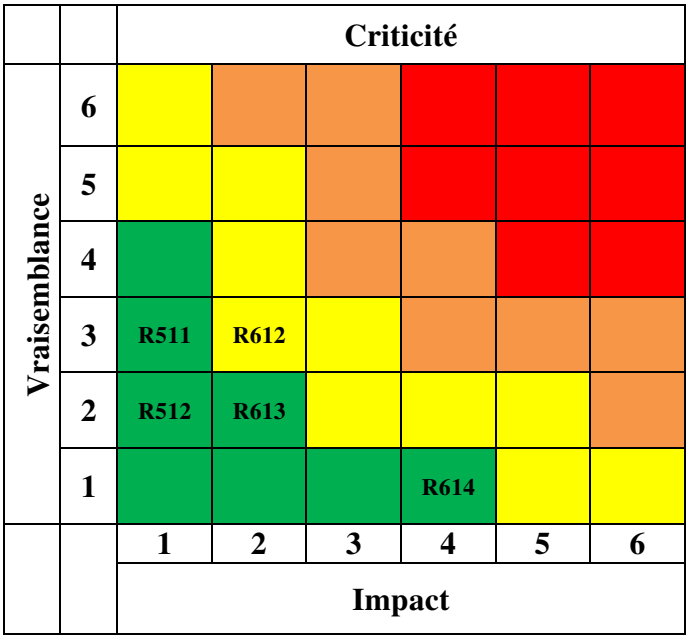
Source : Elaborée par nos soins

Figure 15 : Matrice des risques inhérents au sous processus «Evaluation et révision du dossier de crédit par la DCC »



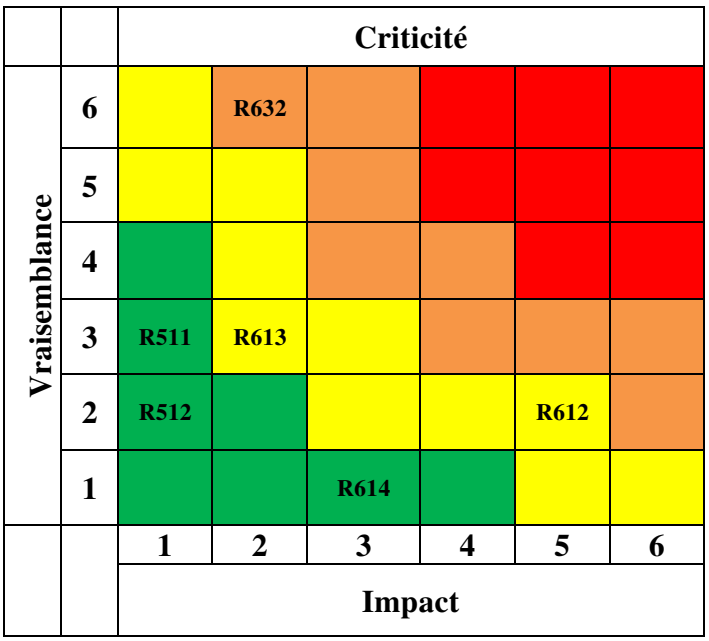
Source : Elaborée par nos soins

Figure 16 : Matrice des risques inhérents au sous processus «Prise de décision par le comité de crédit habilité»



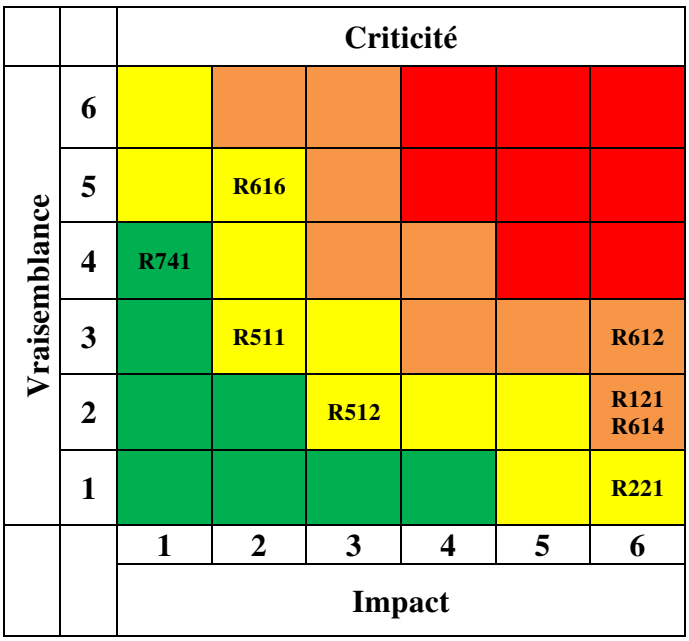
Source : Elaborée par nos soins

Figure 17 : Matrice des risques inhérents au sous processus «Constitution des garanties»



Source : Elaborée par nos soins

Figure 18 : Matrice des risques inhérents au sous processus «Déblocage du crédit»



Source : Elaborée par nos soins

5. Identification et évaluation des mesures de contrôle

L'identification et l'évaluation des mesures de contrôle existantes seront basées sur l'étude des dispositions organisationnelles ainsi que sur les réponses des questionnaires de contrôle interne (voir Annexe N°5). Ainsi, les mesures de contrôle seront cotées comme suit :

Tableau 12 : Echelle d'évaluation des contrôles internes

Efficacité du contrôle	Cotation chiffrée	Description
Inexistant	1	Pas de contrôle
Insuffisant	2	Le contrôle appliqué permet de réduire la criticité du risque inhérent à moins de 30%
Suffisant	3	Le contrôle appliqué permet de déduire entre 30% et 60% de la criticité du risque inhérent
Efficace	4	Le contrôle appliqué permet de déduire plus que 60% de la criticité du risque inhérent

Source : Elaboré par nos soins

Les résultats d'identification et d'évaluation des mesures de contrôle appliquées à chaque événement de risque opérationnel dans les différents sous processus se présentent dans l'Annexe N°6.

Sur la base des mesures de contrôle recensées, nous pouvons déduire les composantes du dispositif de maitrise des risques au sein de l'ATB :

- **L'organisation**

L'organisation des différentes unités intervenantes dans la gestion du processus crédits Corporate est conçue sur la base du principe de séparation des tâches. En effet, la procédure, l'organigramme et les fiches de postes définissent de manière claire les tâches de chaque collaborateur, ses habilitations, ses responsabilités et ses attributions. Ceci favorise la maitrise des processus en réduisant la fréquence des événements de risque et en assurant la traçabilité des opérations.

- **Le contrôle permanent**

Le contrôle permanent n'est autre que le contrôle hiérarchique. En effet, le supérieur hiérarchique assure le contrôle de la conformité et la validation des opérations.

- **Le contrôle périodique[19] (contrôle inopiné et/ou planifié)**

Le périmètre d'intervention couvre toutes les activités de la Banque : les canaux de distribution, les processus critiques et les fonctions de supports. Dans un souci d'optimisation des ressources et d'efficacité, l'Audit diversifie ses missions en adoptant des méthodes d'intervention diversifiées : Audit Opérationnel, Audit Procédural, Audit de Conformité, Audit, Organisationnel, Audit Financier…....etc.

Ainsi, durant l'exercice 2016, la ventilation des travaux s'est répartie comme suit :

- 70% : Missions d'Inspection Générale et d'Inspection Thématique des Agences ;
- 20% : Missions d'Audit de Processus ou de Fonction ;
- 10% : Missions d'Audit Informatique (sécurité informatique, continuité de l'activité, gestion des accès, les mesures de secours et la protection des données personnelles).

Les travaux d'audit se réalisent sur la base d'un Plan d'Audit Annuel, élaboré sur la base du « Risk Based Approach ».

- **Le dispositif du contrôle de la conformité**

Dans l'objectif du respect des dispositions législatives et réglementaires propres aux activités bancaires et financières et contribuant à préserver la confiance des parties prenantes à l'égard de la Banque, la Direction de la Conformité continue à piloter un nombre de projets on cite notamment : la mise en application de la loi américaine Foreign Account Tax Compliance Act (FATCA) et le projet « Data Quality ».

En ce qui concerne l'octroi de crédits Corporate, la direction de la conformité a mis en place, en plus de la procédure « Know Your Customer », la procédure «Identification des clients Corporate ». Ainsi, le chargé d'affaire, avant de commencer l'étude du dossier de crédit, il doit procéder à l'étude du risque client en consultant la base des clients black listés. Pour les clients à risque élevé, les clients à risque modéré avec un montant sollicité supérieur à 200 000 DT et les clients à risque faible avec un montant sollicité supérieur à 2 000 000 DT, le chargé d'affaires a l'obligation d'envoyer une copie de la demande de crédit à la direction de la conformité qui va entreprise les mesures de contrôle nécessaires et envoie par la suite son avis (rejet/accord) à la DCCOR pour suivre le traitement du dossier.

[19] Rapport annuel ATB 2016.

- **La fonction Risk Management[20]**

La fonction Risk management est au cœur de la stratégie de la Banque, une stratégie basée sur la maîtrise et l'anticipation de l'ensemble des risques dans une optique d'efficience et de croissance saine et durable. Dans le cadre du risque opérationnel et spécifiquement dans le cadre de la sécurité, la fonction Risk Management a procédé aux actions suivantes :

- Une mission d'Audit en conformité avec les termes du décret 2004-1250 du 25 mai 2004 de la sécurité du système d'information et de communication qui a été effectuée dans le but d'analyser et d'évaluer le niveau de sécurité.
- La certification de l'Internet & Mobile Banking par rapport à la norme internationale.
- Projet Anti-phishing : service dans le cadre de la protection des clients des opérations frauduleuses.
- Projet SIEM (Security Information Event Management) : identifier les problèmes techniques et contribuer à améliorer les mesures de sécurité.
- MSS : Managed Security Services : des services de sécurité managés pour protéger les actifs informationnels de la Banque exposés à l'internet.
- Formation de l'équipe RSSI : ISO 27001(sécurité), ISO 22301(PCA), CISA, CISSP.
- PCA V1 (2016) : Mettre en place un PCA avec réalisation d'un test global sur le site de secours.
- La certification selon la norme de sécurité 27001.

- **La qualification du personnel**

Le personnel a la compétence et l'expérience nécessaires pour faire face aux risques opérationnels. En effet, le recrutement est fait sur la base de la compétence du recruté et sa valeur ajoutée pour la banque, rien d'autre n'est pris en compte. En plus, des sessions de formation en interne et en externe sont planifiées régulièrement dans le but de mettre à jour et d'améliorer les acquis du personnel.

- **La centralisation du traitement des opérations**

La centralisation des opérations au niveau de l'Unité Centrale des Opérations (COU) est de nature à garantir la traçabilité des opérations, à réduire les délais de réponse et à renforcer le contrôle.

[20] Rapport annuel ATB 2016.

- **Le système d'information**

L'ATB utilise un système d'information composé de plusieurs applications informatiques de l'Arab Bank (maison mère). Elles sont jugées, par les collaborateurs, suffisantes à délimiter les risques opérationnels menaçant la banque.

6. Evaluation des risques résiduels

Selon les différents collaborateurs, le dispositif de maitrise des risques que possède l'ATB actuellement est destiné à réduire parallèlement la vraisemblance de l'événement et son impact.

Ainsi, en s'appuyant sur leurs appréciations par rapport à l'efficacité des mesures de contrôle existantes, nous avons pu déduire les niveaux de risques opérationnels résiduels. Sur la base de ces risques résiduels que nous allons proposer, par la suite, un plan d'actions permettant de traiter ces risques tout en prenant en compte les objectifs de la banque, son niveau d'appétence aux risques ainsi que les ressources allouées à ce propos.

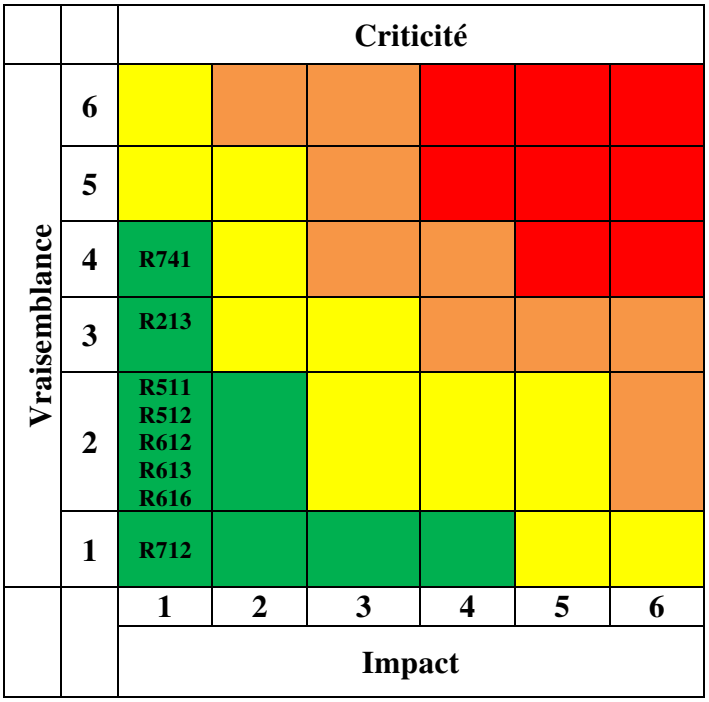
Les résultats d'évaluation des risques opérationnels résiduels pour chaque sous processus se présentent dans l'Annexe N°6.

7. Hiérarchisation des risques résiduels

Sur la base des résultats des travaux d'identification et d'évaluation des mesures de contrôle existantes, nous avons procédé à la hiérarchisation des risques résiduels par sous processus.

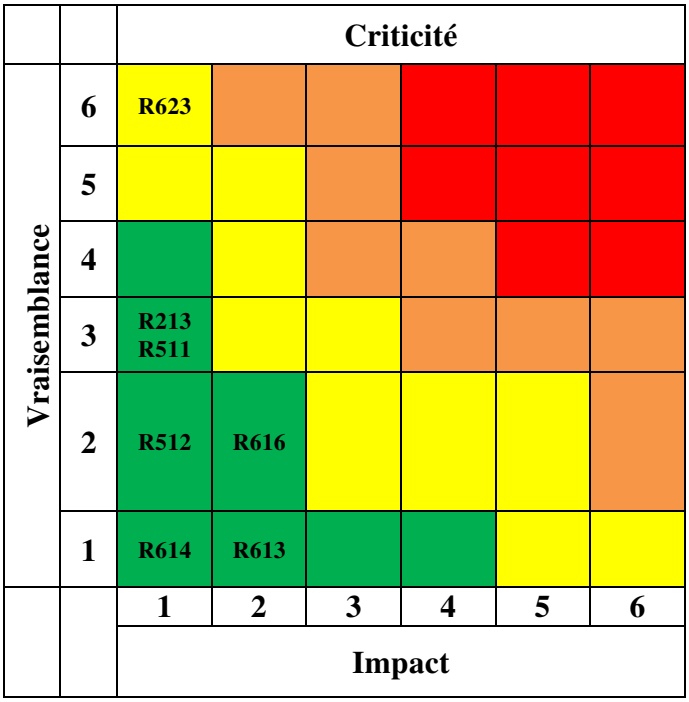
Les matrices des risques résiduels constituent une parfaite synthèse pour leurs utilisateurs. En effet, elles donnent une meilleure visibilité sur l'ensemble des risques liés à chaque sous processus et favorisent, ainsi, l'interprétation et la comparaison. Elles montrent aussi la concentration des risques par zone ce qui donne une idée sur le niveau global d'exposition au risque et facilite l'élaboration du plan d'actions (par zone de risque).

Figure 19 : Matrice des risques résiduels au sous processus « Réception du dossier de crédit par l'agence »



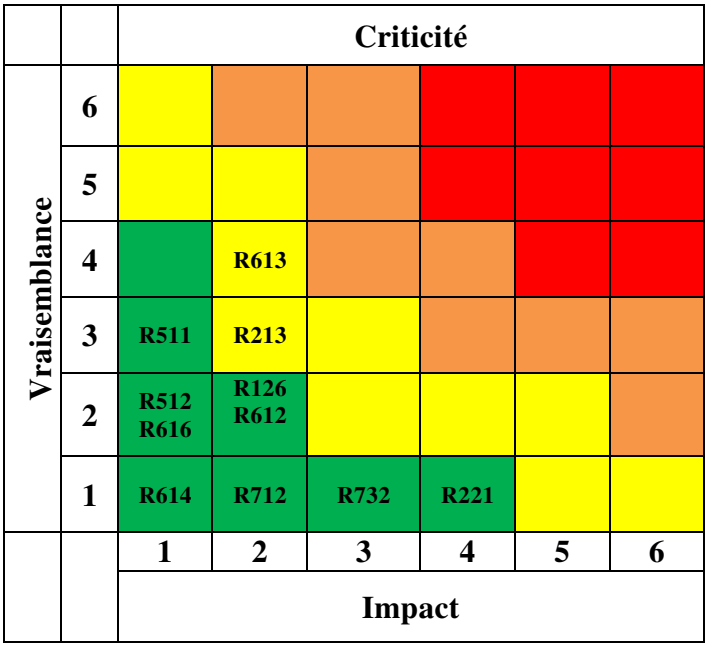
Source : Elaborée par nos soins

Figure 20 : Matrice des risques résiduels au sous processus « Vérification de la complétude des documents »



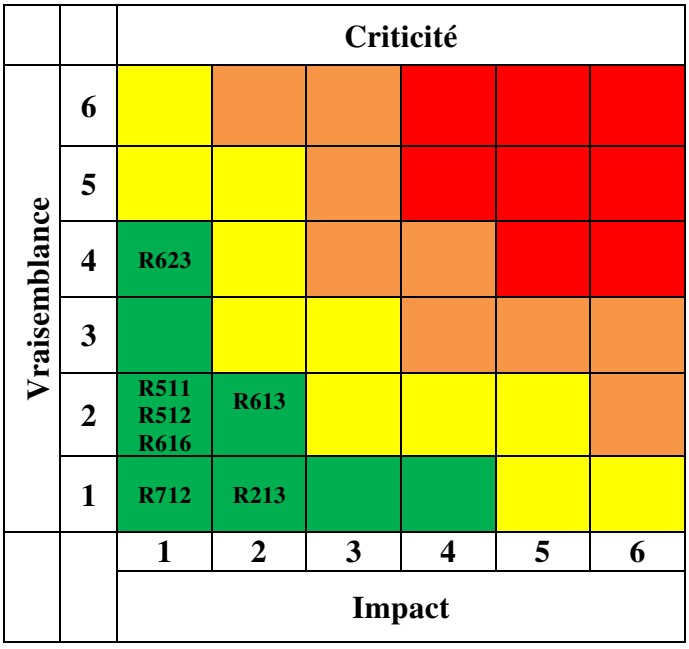
Source : Elaborée par nos soins

Figure 21 : Matrice des risques résiduels au sous processus « Etude de dossier de crédit »



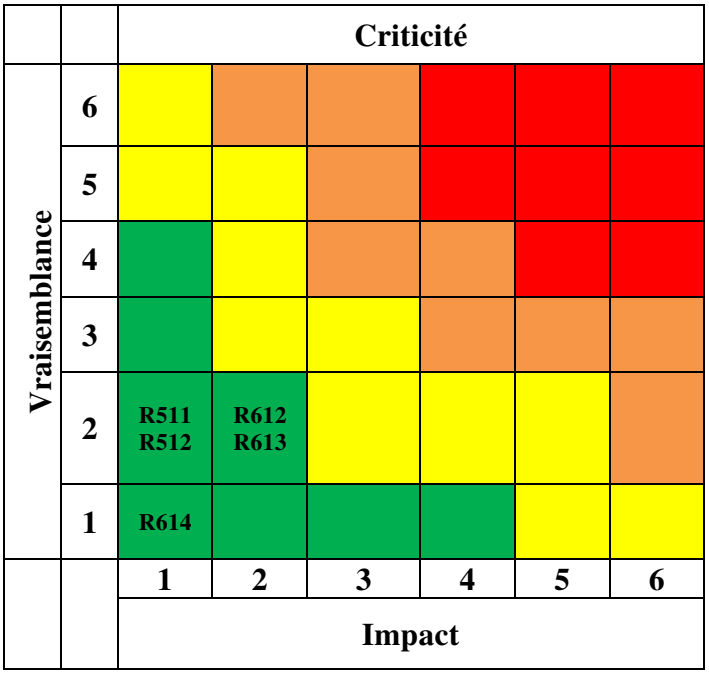
Source : Elaborée par nos soins

Figure 22 : Matrice des risques résiduels au sous processus « Etude de faisabilité des garanties »



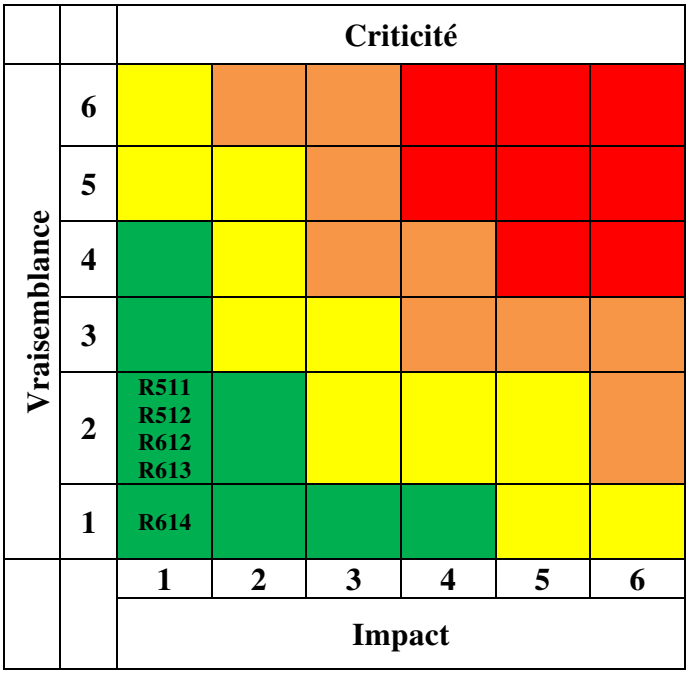
Source : Elaborée par nos soins

Figure 23 : Matrice des risques résiduels au sous processus «Evaluation et révision du dossier de crédit par la DCC »



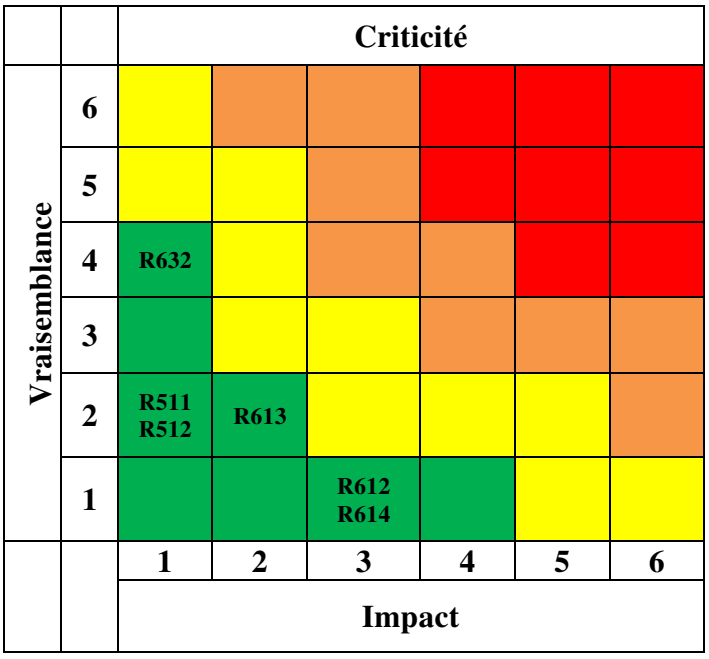
Source : Elaborée par nos soins

Figure 24 : Matrice des risques résiduels au sous processus «Prise de décision par le comité de crédit habilité»



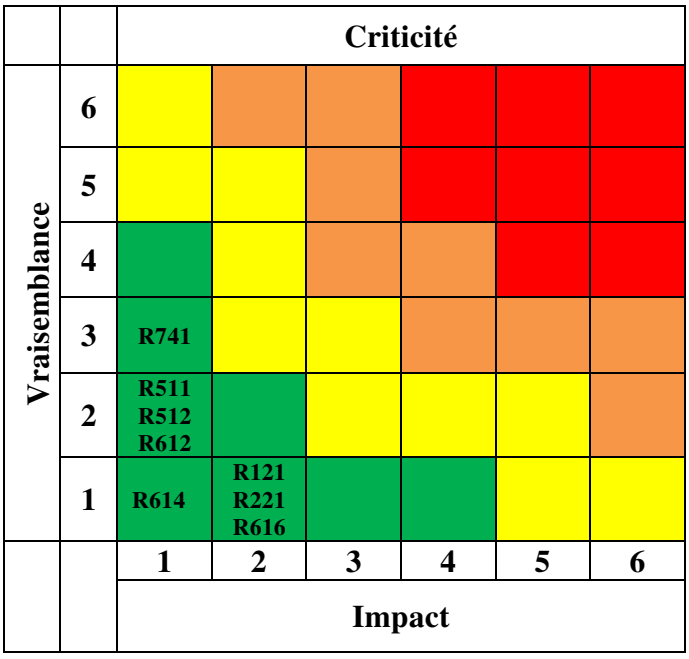
Source : Elaborée par nos soins

Figure 25 : Matrice des risques résiduels au sous processus «Constitution des garanties»



Source : Elaborée par nos soins

Figure 26 : Matrice des risques résiduels au sous processus «Déblocage du crédit»



Source : Elaborée par nos soins

SECTION 5 : L'ANALYSE DES RESULTATS ET PLAN D'ACTIONS

1. Analyse des résultats d'identification et d'évaluation des risques inhérents

A travers les travaux d'identification et d'évaluation des risques opérationnels que nous avons effectués, nous avons pu recenser 57 événements de risque, au niveau de l'ensemble des sous processus, lesquels ont été répartis entre les différentes catégories de risque et les différents sous processus comme l'indique le tableau ci- dessous :

Tableau 13 : Statistiques sur les risques identifiés

Code catégorie de risque	Code sous processus																	
	1		2		3		4		5		6		7		8		Somme	
	nb	%	Nb	%	Nb	%	nb	%	nb	%	nb	%	nb	%	nb	%	nb	%
R1	0	0%	0	0%	1	9%	0	0%	0	0%	0	0%	0	0%	1	13%	2	4%
R2	1	12%	1	14%	2	18%	1	14%	0	0%	0	0%	0	0%	1	13%	6	11%
R5	2	25%	2	29%	2	18%	2	29%	2	40%	2	40%	2	33%	2	25%	16	28%
R6	3	38%	4	57%	4	36%	3	43%	3	60%	3	60%	4	67%	3	37%	27	47%
R7	2	25%	0	0%	2	18%	1	14%	0	0%	0	0%	0	0%	1	13%	6	11%
Somme	8	14%	7	12%	11	19%	7	12%	5	9%	5	9%	6	11%	8	14%	57	100%

Source : Elaboré par nos soins

Commençons par l'analyse des résultats au niveau du processus global de gestion des crédits Corporate. Nous remarquons que la majorité des risques identifiés, avec un pourcentage de contribution de 47%, appartiennent à la catégorie « Exécution, livraison et gestion des processus » (R6). La catégorie « Interruptions d'activité et dysfonctionnements des systèmes » (R5) se présente à la deuxième place avec un pourcentage de contribution de 28%. Ensuite, les deux catégories « Fraude externe » (R2) et « Pratiques concernant les clients, les produits et l'activité commerciale » (R7) contribuent de façon égale, soit 11% chacune, dans le total des événements de risque identifiés. En dernier lieu, se présente la catégorie « Fraude interne » (R1) avec le pourcentage le plus faible, soit 4%.

Ainsi, le sous processus 3 « Etude de dossier de crédit » est qualifié le plus vulnérable aux risques opérationnels, il contribue avec 11 événements de risque, soit un pourcentage de 19%. Le résultat est attendu puisque c'est l'étape phare dans le processus global de gestion

des crédits Corporate. Dans le sens inverse, les deux sous processus 5 et 6 qui sont respectivement « Evaluation et révision du dossier de crédit » et « Prise de décision par le comité de crédit habilité », se présentent comme les moins exposés aux risques opérationnels. Ce résultat est aussi attendu étant donné que ces deux sous processus sont dirigés par deux directions dont leur fonction principale est le contrôle (des unités de contrôle) qui sont la Direction Centrale des Crédits, son rôle est de réviser l'étude faite par la DCCOR, et la Direction Administrative et Contrôle des engagements, son rôle est de contrôler la mise en place des crédits.

Tableau 14 : Affectation des catégories de risques

Code catégorie de risque	Code sous processus							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
R1			X					X
R2	X	X	X	X				X
R5	X	X	X	X	X	X	X	X
R6	X	X	X	X	X	X	X	X
R7	X		X	X				X

Source : Elaboré par nos soins

La catégorie « fraude interne » (R1) est présente dans deux sous processus seulement qui sont : « Etude de dossier de crédit **»** et « Déblocage de crédit ». Dans le premier sous processus, la fraude interne se manifeste par un seul événement qui est la « Corruption ». Il s'agit donc d'un événement spécifique à cette étape du processus global. Ce résultat était prévisible parce que, c'est à ce niveau du processus d'octroi de crédit que la corruption peut naitre sous la forme de collusion entre le chargé d'affaires et son client en manipulant les données pour vernir la situation financière du client ou gonfler les revenus futurs du projet. Pour la phase du « déblocage de crédit», la « fraude interne » se manifeste par un seul événement qui est le « Détournement de fonds », qualifié comme spécifique. En effet, c'est le seul point du processus global où il y a accès aux fonds de la banque.

La catégorie « fraude externe » (R2) est présente dans cinq sous processus. En effet, elle se manifeste par l'événement « documents falsifiés » dans quatre sous processus parmi les cinq : « Réception du dossier de crédit par l'agence », « vérification de la complétude des

documents », « Etude de dossier », « Etude de faisabilité des garanties » et « Déblocage de crédit ». L'explication logique de ce résultat est que le traitement des documents présentés par les clients se fait à ces niveaux du processus global. La « Fraude externe » est présente aussi avec l'événement « Piratage informatique » dans les deux sous processus « Etude de dossier » et « Déblocage de crédit » qui sont jugés comme les deux points critiques de tout le processus. Au niveau du premier point, le danger du piratage est la manipulation des données de la clientèle, le vol des données confidentielles de la clientèle ou encore la manipulation de l'application informatique responsable de l'analyse des dossiers de crédit. Pour le déblocage de crédit, le danger du piratage est encore plus important.

Pour la catégorie «Interruptions d'activité et dysfonctionnements des systèmes » (R5), elle touche à tous les sous processus, à travers les mêmes événements : « Panne matériel » et « Défaillance du système d'information », et avec la même intensité, sauf pour les deux sous processus : « Etude de dossier » et « Déblocage de crédit », l'impact est plus élevé à cause de la forte sensibilité de leurs tâches par rapport à la disponibilité des outils informatiques.

De même, la catégorie « Exécution, livraison et gestion des processus » (R6) touche à tous les sous processus.

Tableau 15 : Affectation des événements de la catégorie « Exécution, livraison et gestion des processus »

Evénement de risque	Code sous processus							
	1	2	3	4	5	6	7	8
R612 : Erreur de saisie	X		X		X	X	X	X
R613 : Non respect des délais d'exécution	X	X	X	X	X	X	X	
R614 : Non respect de la procédure		X	X		X	X	X	X
R616 : Perte de documents	X	X	X	X				X
R623 : Documents absents ou incomplets		X		X			X	

Source : Elaboré par nos soins

Ainsi, pour cette catégorie de risque, nous trouvons dans la sous-catégorie « Saisie, exécution et suivi des transactions » les événements suivants : « Erreur de saisie », « Non-respect des délais d'exécution », « Non-respect des délais d'exécution » et « Perte de documents » qui sont attribuables à des défaillances internes, et dans la sous-catégorie

« Admission et documentation clientèle, nous trouvons seulement l'événement « Documents absents ou incomplets ». Nous pouvons conclure donc que la majorité des événements relatifs à la mauvaise « Exécution, livraison et gestion des processus » sont à l'origine de défaillances internes à la banque. Sauf que l'exposition à ces événements diffère d'un sous processus à un autre pour des raisons particulières à chacun d'eux (le nombre et la qualification des collaborateurs, l'organisation des unités, la nature des tâches, …). A ce niveau, pour chaque événement de risque, nous allons déterminer le sous processus le plus exposé et celui le moins exposé.

- R612 : Le sous processus le plus exposé est « Déblocage de crédit » (criticité 18) et le sous processus le moins exposé est « Réception du dossier de crédit par l'agence » (criticité 5) ;
- R613 : Le sous processus le plus exposé est « Etude de dossier » (criticité 10) et les sous processus les moins exposés sont « Vérification de la complétude des documents » (criticité 4) et « Prise de décision par le comité de crédit habilité » (criticité 4) ;
- R614 : Le sous processus le plus exposé est « Déblocage de crédit » (criticité 12) et le sous processus le moins exposé est « Evaluation et révision du dossier de crédit » (criticité 2) ;
- R616 : Le sous processus le plus exposé est « Déblocage de crédit » (criticité 10) et les sous processus les moins exposés sont « Réception du dossier de crédit par l'agence » (criticité) et « Etude de faisabilité des garanties » (criticité 4) ;
- R623 : Pour cet événement, il n'y a pas un sous processus plus ou moins exposé que les autres, les trois sous processus « Vérification de la complétude des documents » (criticité 12), « Etude de faisabilité des garanties » (criticité 12) et « Constitution des garanties » (criticité 12) sont exposés au même niveau.

Enfin, pour la catégorie « Pratiques concernant les clients, les produits et l'activité commerciale », elle touche à quatre sous processus sous trois formes d'événements : « Utilisation frauduleuse d'informations confidentielles sur la clientèle », « Non-respect des procédures de lutte contre le blanchiment d'argent et le financement de terrorisme » et « Conflits sur l'efficience des prestations ».

Pour l'événement « Utilisation frauduleuse d'informations confidentielles sur la clientèle », nous le rencontrons dans trois sous processus à savoir « Réception du dossier de

crédit par l'agence » (criticité 3), « Etude de dossier » (criticité 8) et « Etude de faisabilité des garanties » (criticité 8).

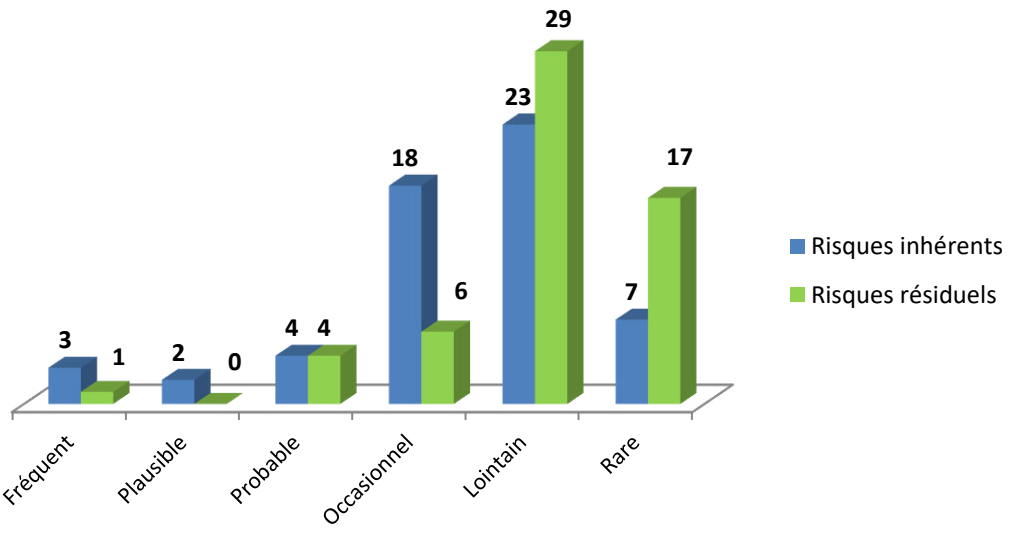
Concernant l'événement « Non-respect des procédures de lutte contre le blanchiment d'argent et le financement de terrorisme », il est spécifique au processus « Etude de dossier » (criticité 18) parce que l'étude du risque client, en termes de blanchiment d'argent et financement de terrorisme, est effectuée à ce niveau du processus global d'octroi de crédit Corporate avant d'entamer l'étude du dossier. Et sur la base de cette évaluation du risque client que les autres étapes seront établies.

En ce qui concerne l'événement « Conflits sur l'efficience des prestations », nous le trouvons au niveau des sous processus « Réception du dossier de crédit par l'agence » et « Déblocage de crédit ». En effet ces deux sous processus font intervenir le contact client ce qui favorise ce genre de conflits.

2. L'efficacité du dispositif de maîtrise des risques

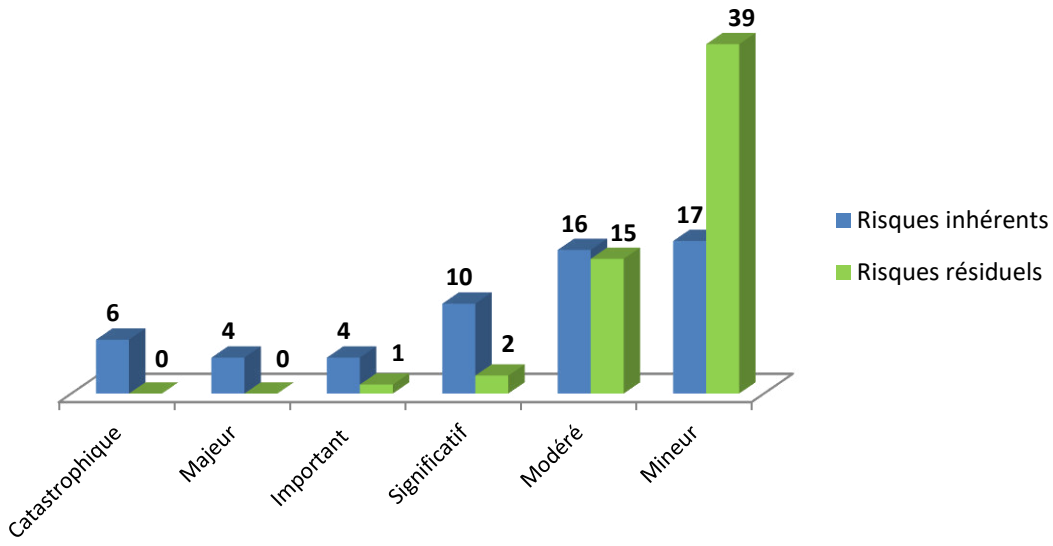
En comparant les matrices des risques inhérents et celles des risques résiduels pour l'ensemble des sous processus, nous avons pu apprécier le rôle du dispositif de maîtrise des risques dans la réduction de la criticité des risques inhérents. Pour affirmer ce constat, nous avons procédé à des statistiques sur la répartition des risques inhérents et résiduels selon les trois critères : vraisemblance, impact et criticité (voir Annexe N°7). Les graphiques ci-dessous présentent les résultats des statistiques effectuées.

Figure 27 : L'effet des contrôles sur vraisemblance des risques (en nombre)



Source : Elaborée par nos soins

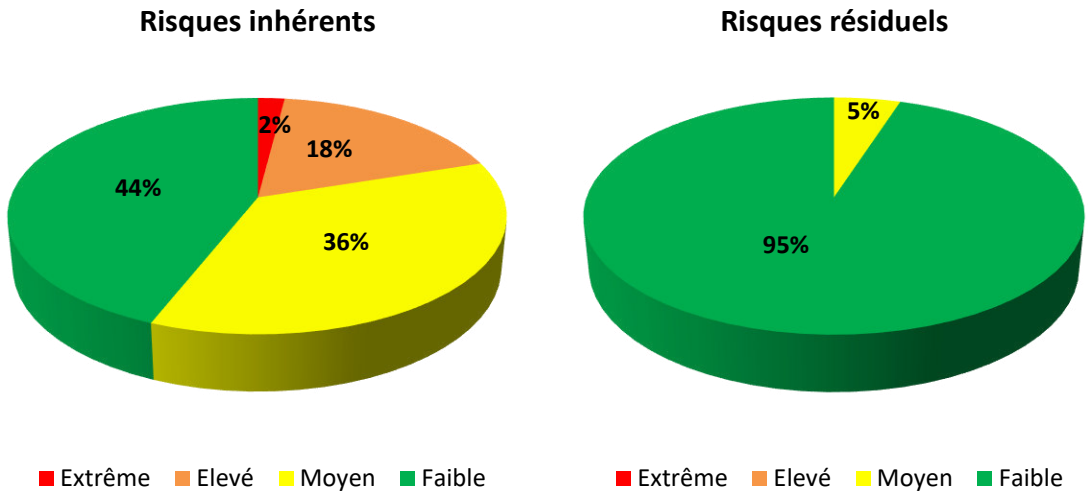
Figure 28 : L'effet des contrôles sur l'impact des risques (en nombre)



Source : **Elaborée par nos soins**

Grâce aux mesures de contrôle existantes, l'occurrence de survenance des risques opérationnels ainsi que leur impact ont diminué de façon significative. Cet effet combiné a permis de réduire la criticité des risques et donc le niveau global d'exposition aux risques opérationnels.

Figure 29 : L'effet des contrôles sur la criticité des risques (en nombre)

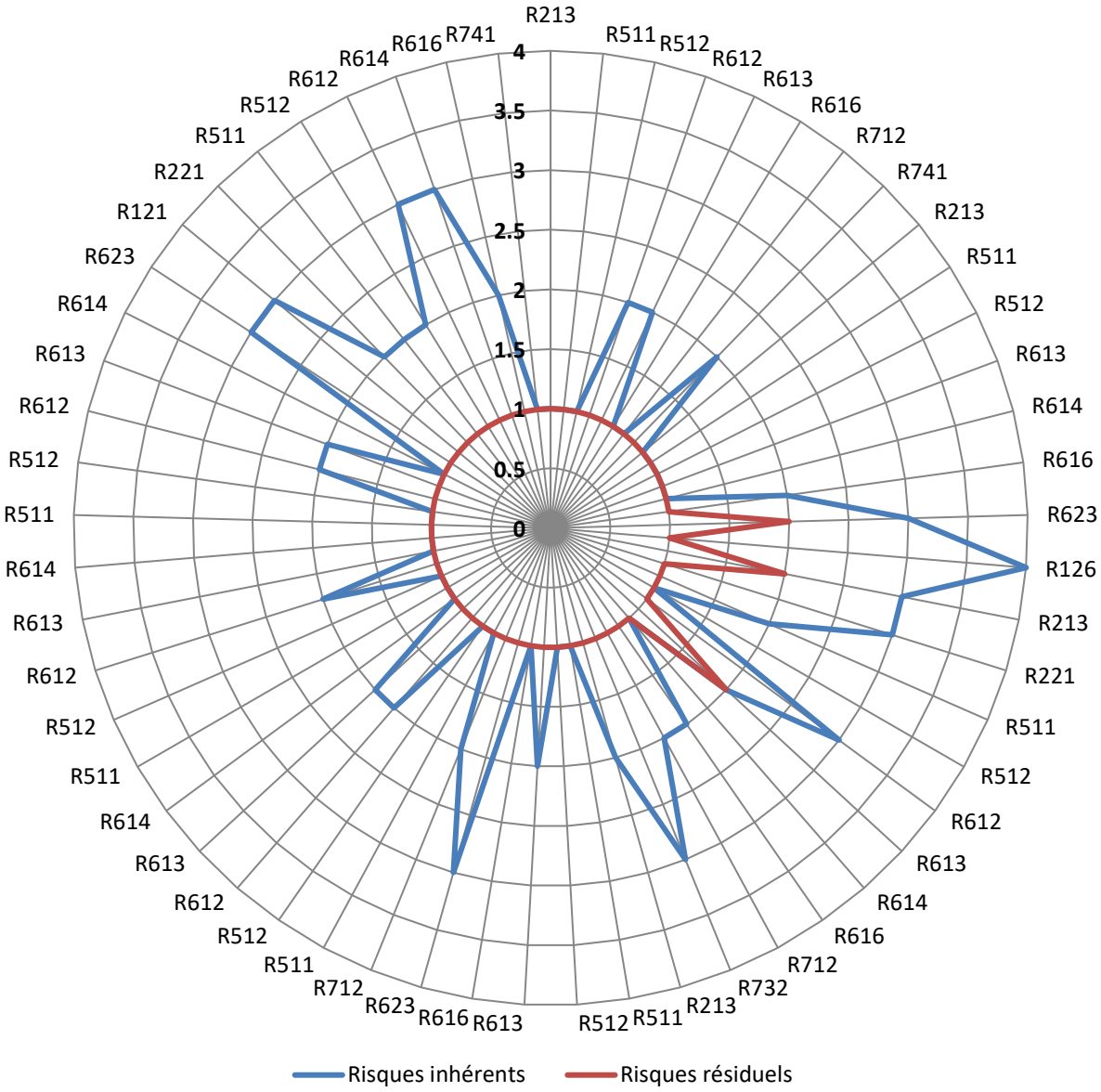


Source : **Elaborée par nos soins**

Grâce aux mesures de risques existantes, le processus de gestion des crédits Corporate au sein de l'ATB se trouve avec zéro risque extrême, zéro risque élevé, 3 risques moyens et 54 risques faibles.

Pour montrer davantage le mécanisme de réduction des risques par les contrôles existants, nous proposons un graphique en toile d'araignée incluant l'ensemble des risques identifiés. Ceci permet de montrer le déplacement des risques d'inhérents à résiduels.

Figure 30 : Risques inhérents et risques résiduels en toile d'araignée



Source : **Elaborée par nos soins**

3. Le traitement des risques résiduels

Les risques résiduels liés au processus global de gestion des crédits Corporate sont au nombre de 57 dont 3 risques moyens et 54 risques faibles. A ce niveau, nous allons procéder au traitement de ces risques en se basant sur le niveau d'appétence aux risques de l'ATB.

Tableau 16 : La classification des risques résiduels selon l'appétence aux risques de l'ATB

Niveau de risque	Classe de risque	Critères de niveau de risque
Risque extrême	4	Ce niveau de risque n'est pas justifiable. Quand l'impact est catastrophique, il faut que la probabilité de survenance du risque soit très rare. Tous les risques d'un niveau catastrophique doivent être présentés à la division exécutive de la Banque pour examen et approbation.
Risque élevé	3	On ne peut pas limiter les risques mais des opportunités et des profits d'activité suggérée peuvent les dépasser. Un niveau élevé des risques résiduels nécessite plus de mesure de contrôle sauf cas où la division exécutif de la banque prend la décision de l'accepter.
Risque moyen	2	La gestion de ce type de risque est effectuée par des méthodes novatrices qui dépassent les méthodes en vigueur. Les risques résiduels moyens demandent plus de contrôle sauf cas où la division exécutif de la banque décide de l'accepter.
Risque faible	1	Ce type de risque est considéré comme acceptable puisque leur traitement est actuel et continu. Il n'existe pas de procédures de contrôle pour réduire les risques à des niveaux acceptables. Le risque résiduel à niveau faible est considéré comme acceptable pour la banque, il ne nécessite pas de procédures ou de traitements supplémentaires, sauf exception de s'assurer de l'efficacité des procédures réglementaires adoptées. L'administration doit faire un suivi des procédures de contrôle des risques à ce niveau afin de s'assurer de la bonne mise en place des normes.

Source : Déclaration d'appétence aux risques de l'ATB

Concernant les risques moyens, ils sont les suivants :

- Au niveau du sous processus «Etude de dossier de crédit », nous trouvons R213 (Documents falsifiés présentés par le client) et R613 (Non respect des délais d'exécution) ;
- Et au niveau du sous processus «Vérification de la complétude des documents » nous trouvons le R623 (Documents absents ou incomplets).

Le traitement adéquat à ce type de risque est la réduction qui consiste à prendre des mesures pour réduire la fréquence du risque (la prévention) ou son impact (la protection) ou les deux à la fois. Dans notre cas, nous proposons les actions suivantes :

- Pour le R213, sa fréquence est indépendante de la banque donc nous pouvons jouer sur son impact en renforçant les procédures de détection des fraudes ;
- Pour le R613, son impact est ingérable donc nous pouvons réduire sa fréquence en renforçant le suivi régulier par les supérieurs hiérarchiques ;
- Pour le R623, nous pouvons réduire à la fois sa fréquence et son impact en faisant recours à l'affichage, au niveau des agences, des check list financiers et juridiques des documents requis pour les différents types de crédits Corporate.

En ce qui concerne les risques faibles qui représentent 95% de l'ensemble des risques opérationnels liés au processus crédits Corporate, nous allons citer les risques récurrents (ce sont les risques qui se répètent dans au moins cinq sous processus parmi les huit sous processus composant le processus global de gestion des crédits Corporate) :

- R511 : Défaillance matériel informatique ;
- R512 : Défaillance système d'information ;
- R613 : Non respect des délais ;
- R614 : Non respect de la procédure (interne).

La meilleure solution recommandée pour traiter ce niveau de risque est l'acceptation. Néanmoins, il faut assurer un suivi régulier des actions et des mesures de contrôle mises en place, dans le but de s'assurer de leur bonne application.

4. Insuffisances constatées et recommandations

Les insuffisances constatées au niveau de la gestion des risques opérationnels sont les suivantes :

- Le systéme d'information de l'ATB est jugé suffisant, par les collaborateurs, à délimiter les risques opérationnels menaçant la banque. Néanmoins, ce système d'information présente l'inconvénient de «dispersé [21] ». Prenons l'exemple du processus crédits Corporate, il fait intervenir 7 applications à savoir : Ultimus, Courrier, Oracle, XCREDIT, Equation, Crédit et Oracle 10G, ce qui favorise les erreurs en se déplaçant d'une application à une autre pour la réalisation d'une opération.

[21] L'ATB ne possède pas un Global Banking mais une multitude d'applications informatiques.

- L'ATB dispose actuellement d'une base de données d'incidents. Néanmoins, elle reste non exhaustive et ceci revient essentiellement à la réticence des collaborateurs à déclarer les incidents survenus.
- L'ATB ne dispose pas jusqu'à présent d'une cartographie globale des risques opérationnels.
- D'après les entretiens effectués avec les collaborateurs, nous avons remarqué que la notion du risque opérationnel est non encore maitrisée.

Pour remédier à ces insuffisances, nous recommandons :

- La diffusion de la culture du risque opérationnel par la programmation de formations et de conférences. Ainsi, il est nécessaire de sensibiliser le personnel du danger du risque opérationnel et l'impliquer dans sa gestion tout en insistant qu'il s'agit d'une responsabilité commune. Ceci permettra d'atténuer la survenance des risques, d'une part, et d'encourager les collaborateurs à déclarer leurs incidents survenus, d'autre part.
- L'accélération dans la mise en place de la cartographie des risques en commençant par les activités jugées critiques, telles que les opérations d'agence et les opérations de commerce extérieur.
- Le développement des outils de mesure, de monitoring et de reporting des risques opérationnels.

CONCLUSION

Le présent chapitre a été consacré à l'élaboration d'une cartographie des risques opérationnels liés au processus crédits Corporate au sein de l'ATB. Dans une première section, nous avons donné une idée générale sur le contexte du travail en présentant l'ATB et sa politique de gestion des risques. Ensuite, dans la deuxième section, nous avons explicité la méthodologie de travail. La troisième section a été consacrée à la phase de préparation, dans laquelle nous avons décrit le processus objet de notre travail. Dans la quatrième section, nous avons procédé à la conception de notre cartographie, commençant par l'identification des risques inhérents jusqu'au hiérarchisation des risques résiduels. La dernière section a été réservée à l'analyse des résultats et les recommandations jugées nécessaires pour une meilleure maitrise des risques opérationnels. Ainsi, les résultats ont montré que le processus de gestion des crédits Corporate est exposé à 57 risques opérationnels dont 3 risques moyens à réduire et 54 risques faibles à accepter.

CONCLUSION GÉNÉRALE

Les risques opérationnels présentent plusieurs spécificités par rapport aux autres risques bancaires classiques, ils sont diffus, multiformes, graves et non rémunérés, ce qui rend nécessaire leur gestion pour chaque institution bancaire. A ce niveau, la cartographie des risques se présente comme un outil d'aide à la décision en procurant une meilleure visibilité sur l'ensemble des risques opérationnels auxquels la banque fait face.

L'objectif du présent mémoire était ainsi l'élaboration d'une cartographie des risques opérationnels liés au processus crédits Corporate au sein de l'ATB.

Pour y parvenir, nous avons structuré notre mémoire autour de trois chapitres :

Dans le premier chapitre intitulé « Le risque opérationnel dans l'activité bancaire », nous avons présenté le cadre conceptuel du risque opérationnel. Nous avons commencé par un aperçu sur la spécificité de l'activité bancaire et les risques y afférents, ensuite nous avons exposé les concepts de base du risque opérationnel à savoir sa définition, ses spécificités et sa typologie, enfin nous avons passé au cadre réglementaire international et national du risque opérationnel.

« La démarche d'élaboration d'une cartographie des risques opérationnels » a fait l'objet du deuxième chapitre. En premier lieu, nous avons présenté le cadre conceptuel relatif à la cartographie des risques opérationnels, ensuite nous avons entamé la démarche de son élaboration et en dernier lieu nous avons exposé les étapes qui suivent l'élaboration d'une cartographie des risques opérationnels.

Le troisième et dernier chapitre a été consacré à l'élaboration d'une «Cartographie des risques opérationnels liés au processus crédits Corporate au sein de l'ATB ».

Avant d'entamer la conception de la cartographie des risques, nous avons procédé à la segmentation du processus de gestion des crédits Corporate en huit sous processus commençant par la Réception du dossier de crédit par l'agence jusqu'au Déblocage de crédit. Ensuite, dans le cadre d'identification et d'évaluation des risques, nous avons opté pour des questionnaires avec les collaborateurs des différentes unités intervenantes dans ce processus (Agence, DCCOR, Direction des garanties, DCC, DACE et Division portefeuille de la COU) ainsi qu'avec les collaborateurs à la Direction Centrale de Conformité et à la Division des risques opérationnels, en se basant sur les échelles d'évaluation de vraisemblance et d'impact mentionnées dans la déclaration de l'appétence aux risques de l'ATB. L'étape suivante consiste à l'identification et l'évaluation des mesures de contrôle existantes, pour les identifier

nous avons opté pour des questionnaires de contrôle interne et pour les évaluer nous avons utilisé une échelle de cotation à quatre niveaux allant d'inexistant à efficace. La superposition des risques inhérents et les mesures de contrôle existantes fait ressortir les risques résiduels. Ensuite nous avons procéder à la hiérarchisation des risques résiduels pour donner une meilleure visibilité facilitant la prise de décision concernant leur traitement. Ainsi, les risques résiduels ont été classés en quatre zones de risques : Risque Extrême, Risque Elevé, Risque Moyen et Risque Faible.

Selon notre étude, le processus de gestion des crédits Corporate est exposé à 57 risques opérationnels dont 27 risques appartiennent à la catégorie « Exécution, livraison et gestion des processus » et seulement deux risques de nature « Fraude interne ».

Pour le dispositif actuel de maitrise des risques, nous pouvons le qualifier « efficace ». En effet, c'est grâce à lui que le processus de gestion des crédits Corporate se trouve avec zéro risque extrême, zéro risque élevé, seulement trois risques moyens à réduire par des mesures de prévention et de protection et 54 risques faibles à accepter tout en assurant un suivi régulier des actions et des mesures de contrôle mises en place. Parmi ces risques faibles, il y a quatre risques récurrents (qui se répètent dans au moins cinq sous processus parmi les huit), qui sont : « Défaillance matériel informatique », « Défaillance système d'information », « Non respect des délais » et « Non respect de la procédure (interne)».

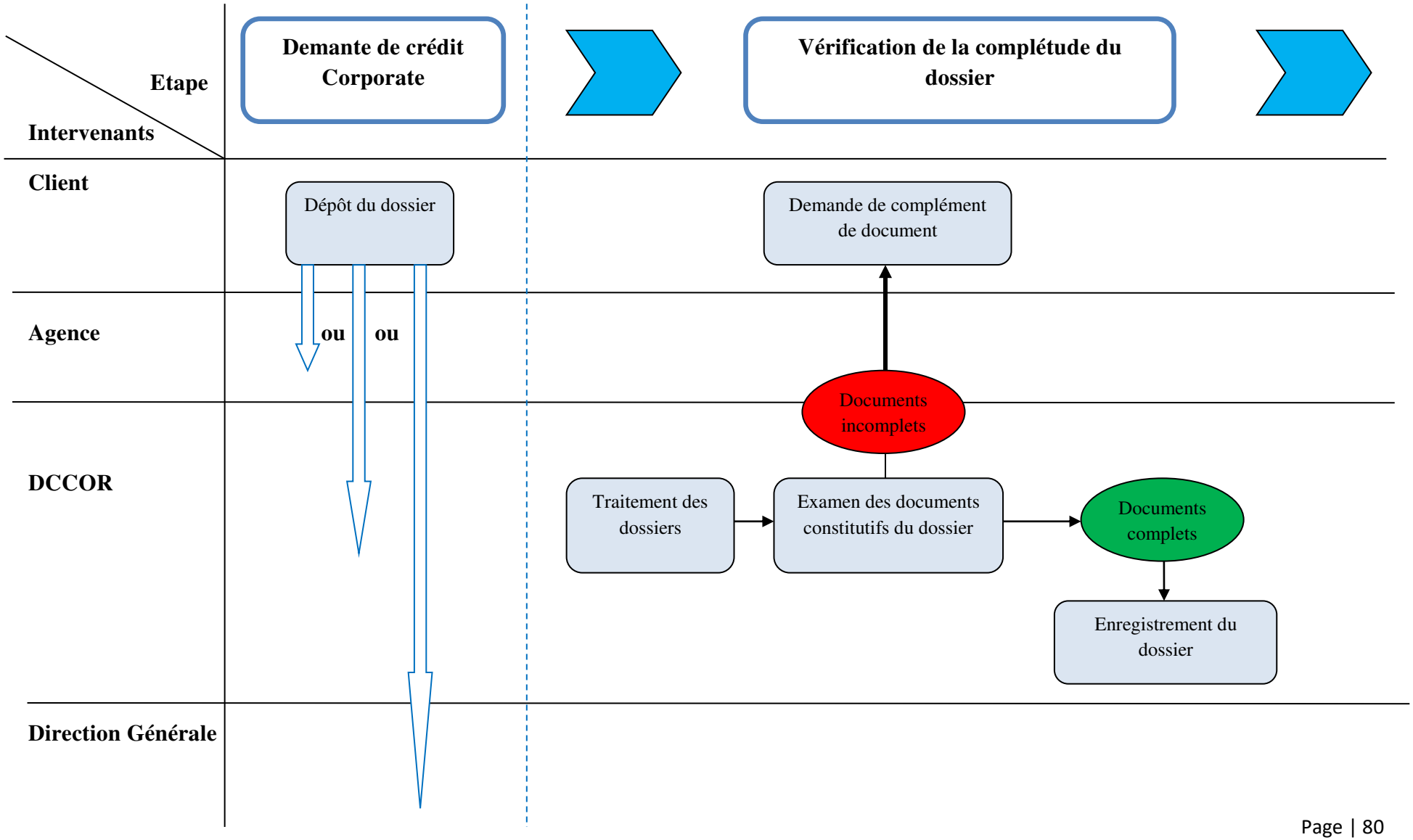
Pour une meilleure gestion des risques opérationnels au sein de l'ATB, nous avons recommandé la diffusion de la culture du risque opérationnel par la programmation de formations et de conférences sur le risque opérationnel, l'accélération dans la mise en placede la cartographie des risquesen commençant par les activités jugées critiques, telles que les opérations d'agence et les opérations de commerce extérieur et le développement des outils de mesure, de monitoring et de reporting des risques opérationnels.

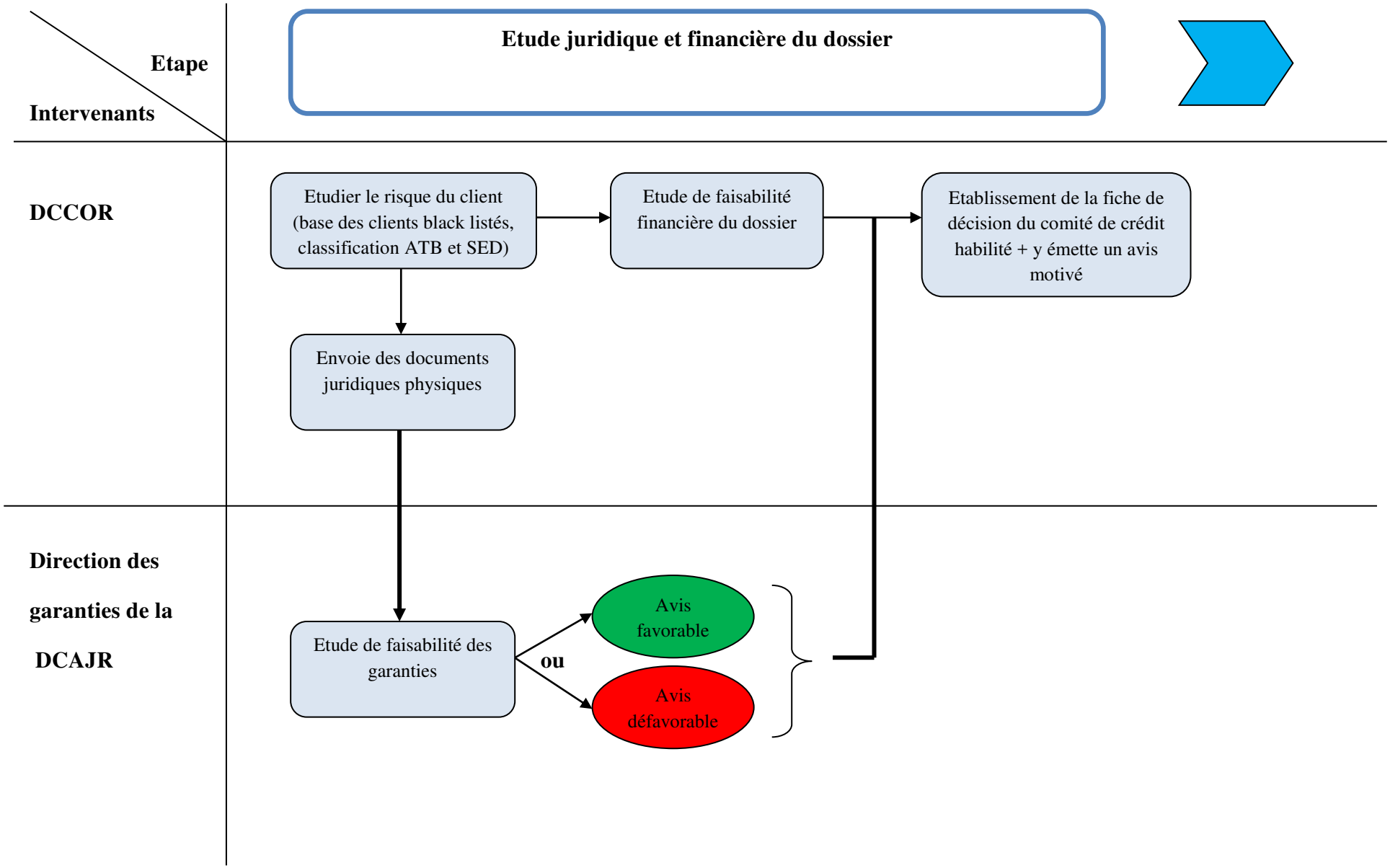
Enfin, nous tenons à conclure notre travail par cette citation de Trinh Xuan Thuan, afin de mettre l'accent sur la nécessité de gestion des risques.

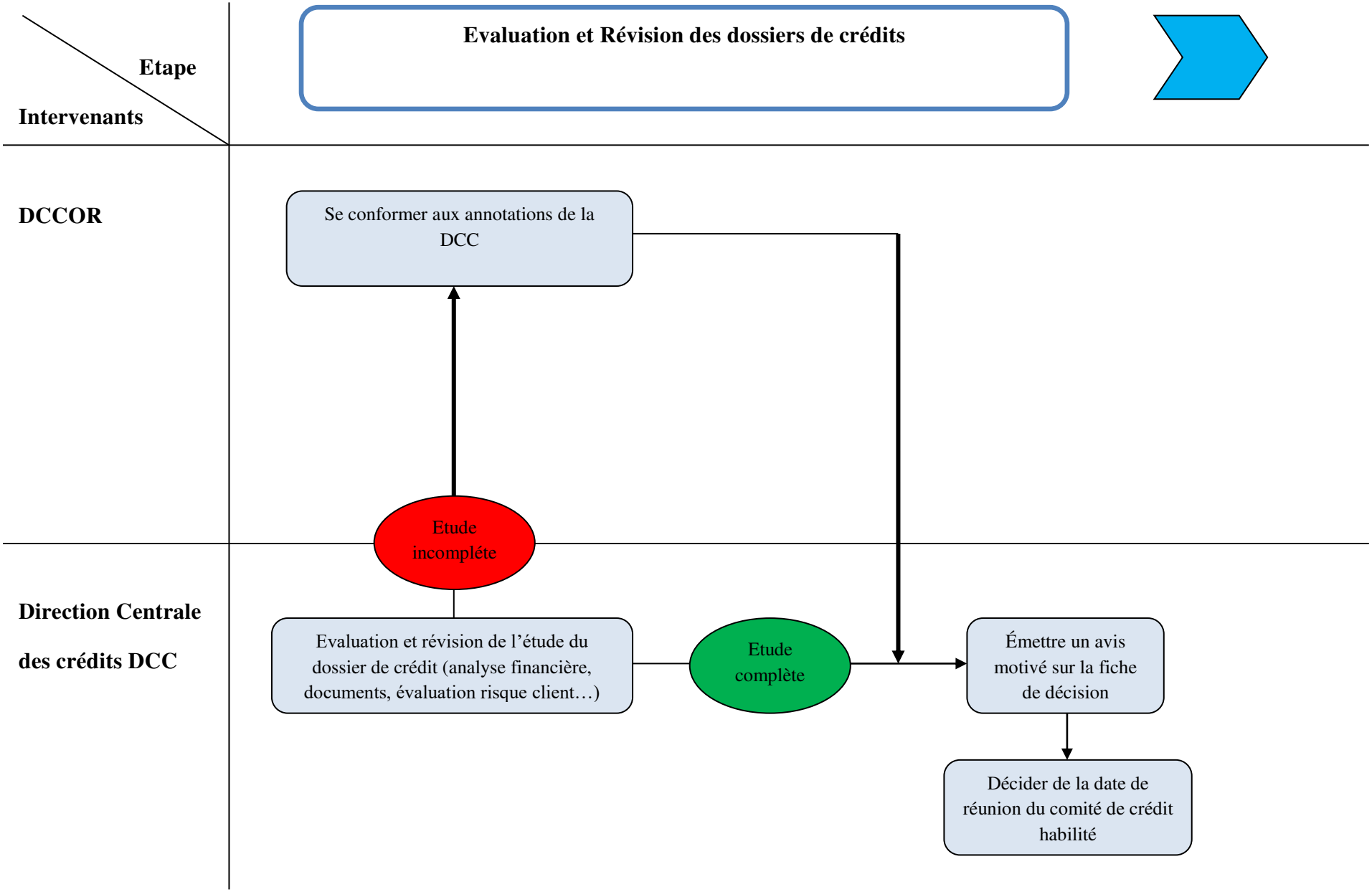
« La vraie perfection est stérile, alors que l'imperfection mesurée est génératrice de nouveauté ».

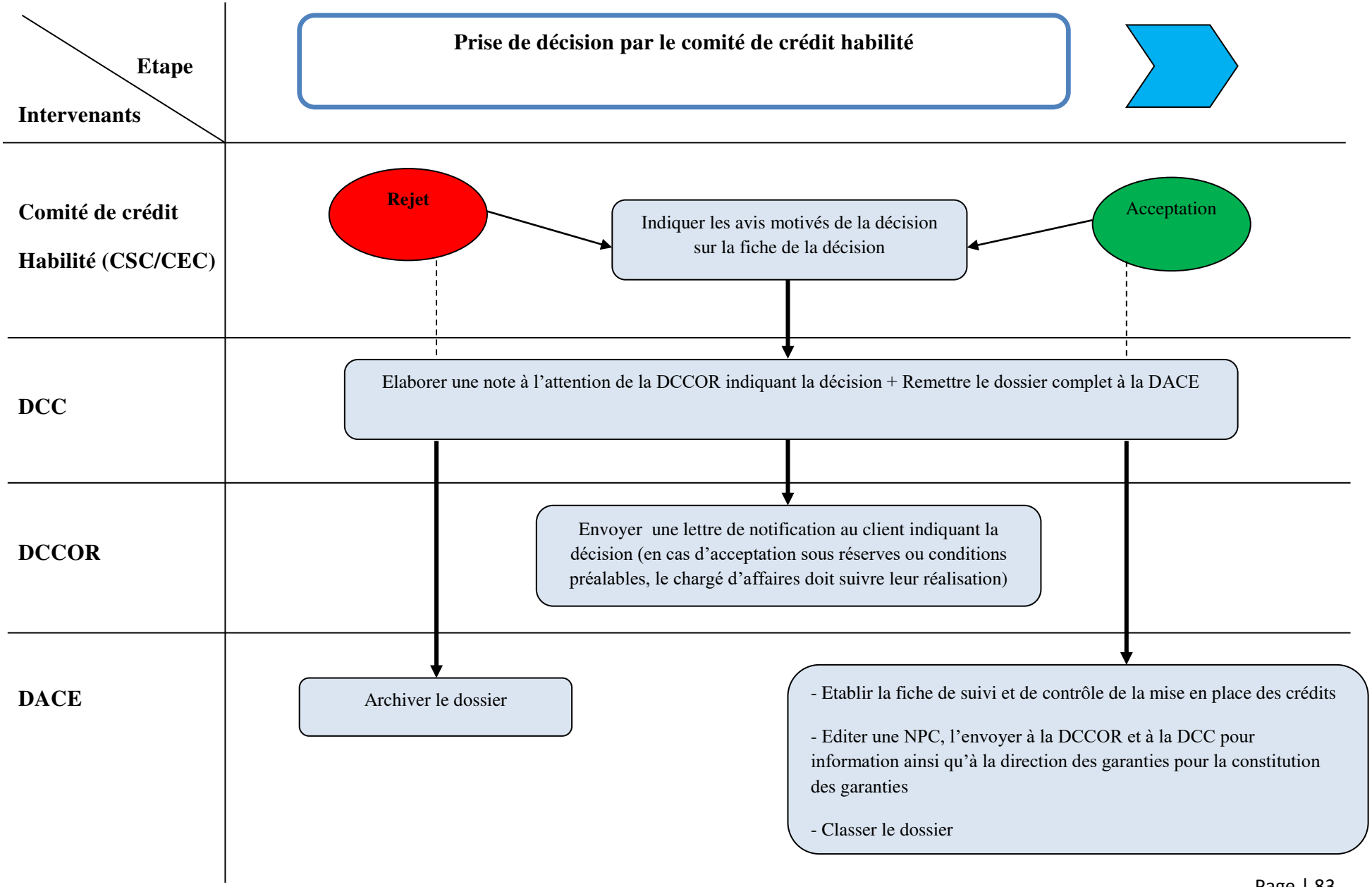
ANNEXES

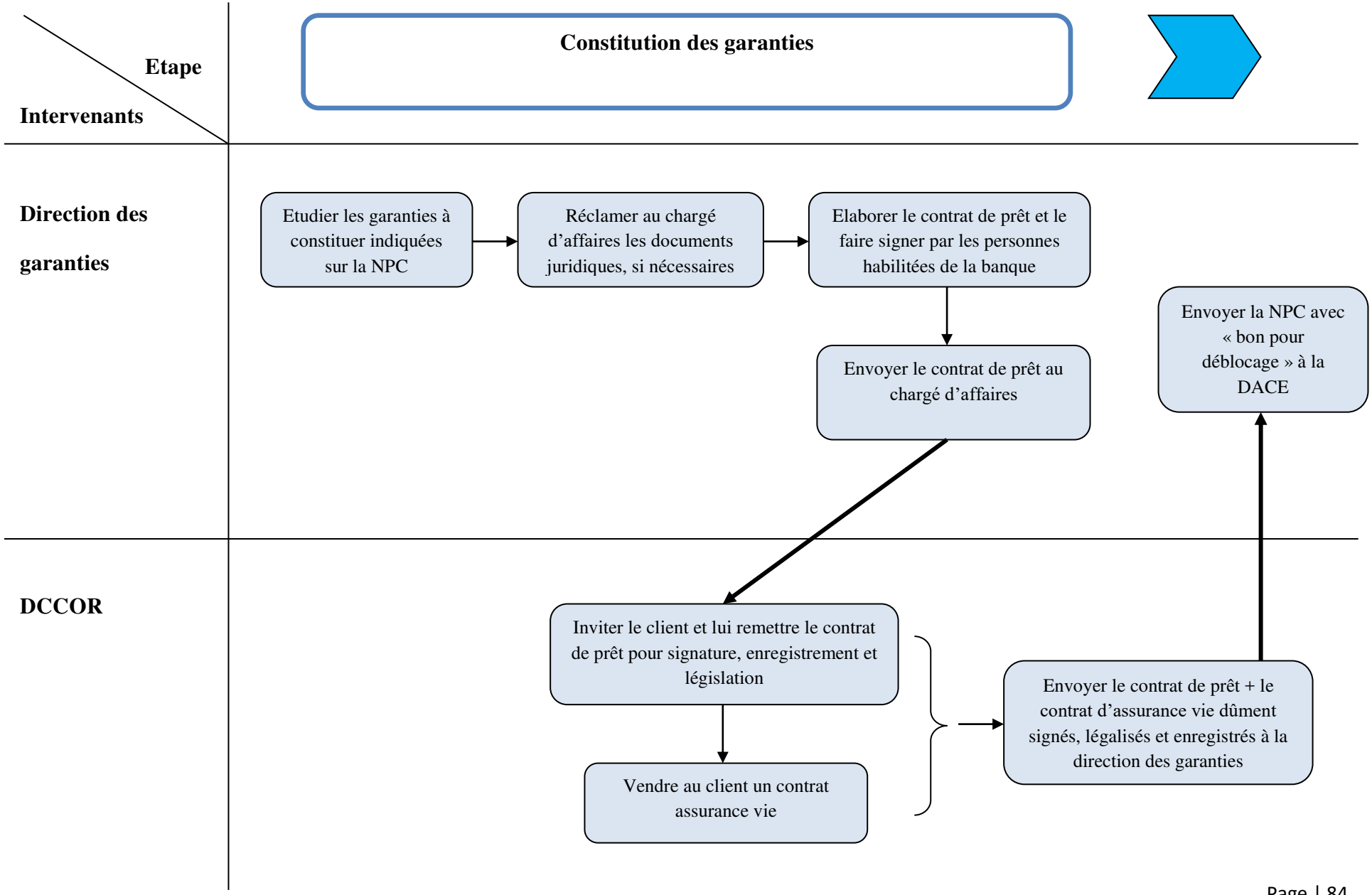
ANNEXE N°1 : PROCESSUS DE GESTION DE CREDITS CORPORATE

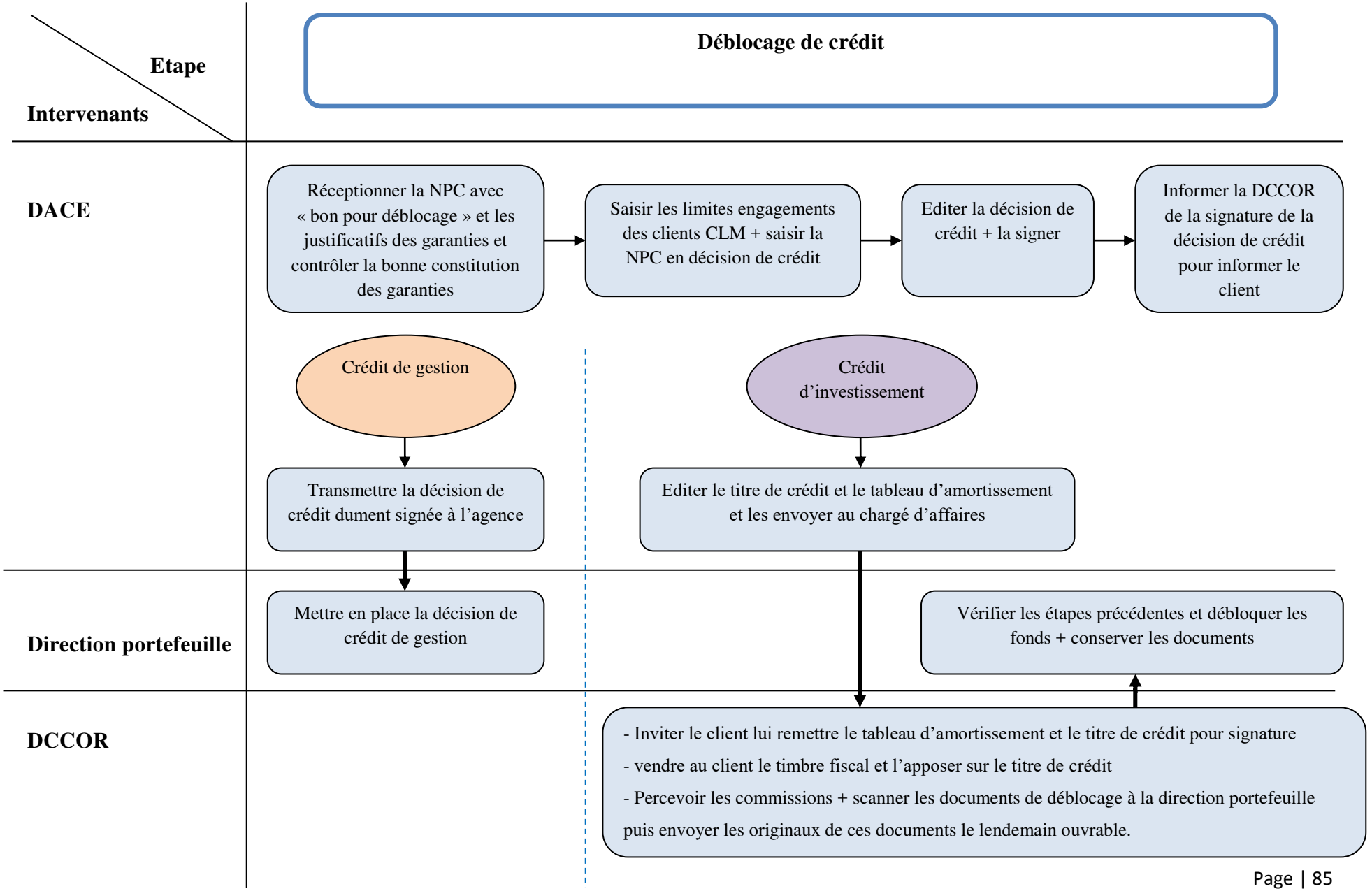



Etape
Intervenants
Etude juridique et financière du dossier
DCCOR
Etudier le risque du client (base des clients black listés, classification ATB et SED)
Etude de faisabilité financière du dossier
Etablissement de la fiche de décision du comité de crédit habilité + y émette un avis motivé
Envoie des documents juridiques physiques
Direction des garanties de la DCAJR
Etude de faisabilité des garanties
ou
Avis favorable
Avis défavorable


Etape
Intervenants
Evaluation et Révision des dossiers de crédits
DCCOR
Se conformer aux annotations de la DCC
Etude incompléte
Direction Centrale des crédits DCC
Evaluation et révision de l'étude du dossier de crédit (analyse financière, documents, évaluation risque client…)
Etude complète
Émettre un avis motivé sur la fiche de décision
Décider de la date de réunion du comité de crédit habilité


Etape
Intervenants
Prise de décision par le comité de crédit habilité
Comité de crédit
Habilité (CSC/CEC)
Rejet
Indiquer les avis motivés de la décision sur la fiche de la décision
Acceptation
DCC
Elaborer une note à l'attention de la DCCOR indiquant la décision + Remettre le dossier complet à la DACE
DCCOR
Envoyer une lettre de notification au client indiquant la décision (en cas d'acceptation sous réserves ou conditions préalables, le chargé d'affaires doit suivre leur réalisation)
DACE
Archiver le dossier
- Etablir la fiche de suivi et de contrôle de la mise en place des crédits
- Editer une NPC, l'envoyer à la DCCOR et à la DCC pour information ainsi qu'à la direction des garanties pour la constitution des garanties
- Classer le dossier


Etape
Intervenants
Constitution des garanties
Direction des garanties
Etudier les garanties à constituer indiquées sur la NPC
Réclamer au chargé d'affaires les documents juridiques, si nécessaires
Elaborer le contrat de prêt et le faire signer par les personnes habilitées de la banque
Envoyer le contrat de prêt au chargé d'affaires
Envoyer la NPC avec « bon pour déblocage » à la DACE
DCCOR
Inviter le client et lui remettre le contrat de prêt pour signature, enregistrement et législation
Vendre au client un contrat assurance vie
Envoyer le contrat de prêt + le contrat d'assurance vie dûment signés, légalisés et enregistrés à la direction des garanties


Etape
Intervenants
Déblocage de crédit
DACE
Réceptionner la NPC avec « bon pour déblocage » et les justificatifs des garanties et contrôler la bonne constitution des garanties
Saisir les limites engagements des clients CLM + saisir la NPC en décision de crédit
Editer la décision de crédit + la signer
Informer la DCCOR de la signature de la décision de crédit pour informer le client
Crédit de gestion
Crédit d'investissement
Transmettre la décision de crédit dument signée à l'agence
Editer le titre de crédit et le tableau d'amortissement et les envoyer au chargé d'affaires
Direction portefeuille
Mettre en place la décision de crédit de gestion
Vérifier les étapes précédentes et débloquer les fonds + conserver les documents
DCCOR
- Inviter le client lui remettre le tableau d'amortissement et le titre de crédit pour signature
- vendre au client le timbre fiscal et l'apposer sur le titre de crédit
- Percevoir les commissions + scanner les documents de déblocage à la direction portefeuille puis envoyer les originaux de ces documents le lendemain ouvrable.

ANNEXE N°2 : QUESTIONNAIRE D'IDENTIFICATION ET D'EVALUATION DES RISQUES

Q1 : Pour chaque sous processus, quels sont les risques inhérents ?

Sous processus : ……..1- …… 2- …… 3- …….

Sous processus : ……..…4- …… 5- …… 6- …….

Sous processus : …… 7- …… 8- …… 9- ……

Sous processus : …… 10- ……. 11- ……. 12- ……

Q2 : Comment jugeriez-vous la fréquence de survenance pour chaque risque identifié abstraction faite du dispositif de maitrise des risques existant ? (sur une échelle de 1 à 6)

Risque	Vraisemblance	Risque	Vraisemblance	Risque	Vraisemblance
1-		5-		9-	
2-		6-		10-	
3-		7-		11-	
4-		8-		12-	

Q3 : Comment jugeriez-vous l'impact financier en cas de survenance pour chaque risque identifié abstraction faite du dispositif de maitrise des risques existant ? (sur une échelle de 1 à 6)

Risque	Impact	Risque	Impact	Risque	Impact
1-		5-		9-	
2-		6-		10-	
3-		7-		11-	
4-		8-		12-	

ANNEXEN° 3 : NOMENCLATURE DES RISQUES SELON LES NORMES DE BALE 2

Catégorie (niveau 1)	Définition	Sous-catégorie (niveau 2)	Risques Génériques (niveau 3)
R1 : Fraude interne	Pertes dues à des actes visant à frauder, détourner des biens ou à contourner les règlements, la législation ou la politique de l'entreprise, impliquant au moins une partie interne à l'entreprise	R11 : Activité non autorisée	R111 : Transactions non notifiées (intentionnellement) R112 : Transactions de type non autorisé (avec perte financière) R113 : Evaluation (intentionnellement) erronée d'une position
		R12 : Vol et fraude	R121 : Détournement de fonds R122 : Détournement de biens R123 : Destruction malveillante de biens R124 : Contrebande R125 : Usurpation de compte/ d'identité R126 : Corruption/ commissions occultes R127 : Délit d'initié (pas au non de la banque)
R2 : Fraude externe	Pertes dues à des actes visant à frauder, détourner des biens ou contourner la législation, de la part d'un tiers	R21 : Vol et fraude	R211 : Vol/vol qualifié R212 : Contrefaçon R213 : Falsification de chèques/ documents
		R22 : Sécurité des systèmes	R221 : Dommages dus au piratage informatique R222 : Vol d'informations (avec perte financière)
R3 : Pratiques en matière d'emploi et de sécurité sur le lieu de travail	Pertes résultant d'actes non conformes à la législation ou aux conventions relatives à l'emploi, la santé ou la sécurité, de demandes d'indemnisation au titre d'un dommage personnel	R31 : Relations de travail	R311 : Questions liées aux rémunérations, aux avantages ou à la résiliation du contrat de travail R312 : Activité syndicale
		R32 : Sécurité du lieu de travail	R321 : Responsabilité civile R322 : Evénements liés à la réglementation sur la santé et la sécurité du personnel
		R33 : Egalité et discrimination	R331 : Tous types de discrimination

R4 : Dommages aux actifs corporels	Destruction ou dommages résultant d'une catastrophe naturelle ou d'autres sinistres	R41 : Catastrophes et autres sinistres	R411 : Incendie, inondation, infiltration d'eau R412 : Pertes humaines dues à des causes externes (terrorisme, vandalisme)
R5 : Interruptions d'activité et dysfonctionnements des systèmes	Pertes résultant d'interruptions de l'activité ou de dysfonctionnements des systèmes	R51 : Systèmes	R511 : Défaillance Matériel R512 : Défaillance Logiciel/ système d'information R513 : Problème de télécommunications R514 : Interruptions/perturbations d'un service
R6 : Exécution, livraison et gestion des processus	Pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou subies dans le cadre des relations avec les contreparties commerciales et les fournisseurs	R61 : Saisie, exécution et suivi des transactions	R611 : Problèmes de communication R612 : Erreurs dans la saisie, le suivi ou le changement R613 : Non-respect des délais R614 : Non-respect des procédures R615 : Dépassement des habilitations R616 : Perte de documents par négligence
		R62 : Admission et documentation clientèle	R621 : Absence d'autorisation clientèle ou de déni de responsabilité R623 : Documents (juridiques…) absents/incomplets
R7 : Pratiques concernant les clients, les produits et l'activité commerciale	Pertes résultant d'un manquement, non intentionnel ou dû 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 ou conception d'un produit	R71 : Conformité, diffusion d'informations et devoir fiduciaire	R711 : Violation de la confidentialité de la clientèle R712 : Utilisation frauduleuse d'informations confidentielles R713 : Atteinte à la vie privée R714 : Vente agressive
		R72 : Sélection, promotion et exposition	R721 : Insuffisance de l'analyse clientèle R722 : Dépassement des limites d'exposition d'un client
		R73 : Pratiques commerciales/ de place incorrectes	R731 : Délit d'initié (au non de la banque) R732 : Blanchiment d'argent et financement du terrorisme
		R74 : Service/ conseil	R741 : Conflits sur l'efficience des prestations

ANNEXE N°4 : ECHELLE D'EVALUATION DE L'IMPACT DES RISQUES

Niveau de risque	Cotation chiffré	Description	Critères d'impact
Catastrophique	6	- Perte potentielle ou réelle dépassant les 4 millions de dinars - Exige une action immédiate (généralement complété dans les 3 mois) - Un rapport mensuel de la situation aux parties concernées	- Des répercussions catastrophiques sur les affaires et le pays - Des risques opérationnels catastrophiques ou violation de la gouvernance de l'entreprise -Une forte faiblesse au niveau du contrôle -Impact législatif et réglementaires graves (révocation de la licence de la banque ou la prison) - Forte possibilité de risque de réputation - Informer immédiatement les autorités concernées des problèmes -Impact potentiel ou réel sur le prix de l'action de la banque
Majeur	5	- Perte potentielle ou réelle dépassant les 2 millions de dinars et inférieur à 4 millions de dinars - Exige une action immédiate (généralement complété dans les 3 mois) - Un rapport mensuel de la situation aux parties concernées	- Des fortes répercussions sur les affaires et le pays - Des risques opérationnels majeurs ou violation de la gouvernance de l'entreprise -Une forte faiblesse au niveau du contrôle - Impact législatif et réglementaires graves (révocation de la licence de la banque ou la prison) - Forte possibilité de risque de réputation - Informer immédiatement les autorités concernées des problèmes -Impact potentiel ou réel sur le prix de l'action de la banque
Important	4	- Perte potentielle ou réelle dépassant les 1 million de dinars et inférieur à 2 millions de dinars - Exige une action immédiate (généralement complété dans les 6 mois)	- Des répercussions importantes sur les affaires et le pays - Des risques opérationnels importants ou violation de la gouvernance de l'entreprise -Exposition inacceptable aux faiblesses de contrôle du risque de réputation à niveau moyen - Des problèmes périodiques qui ont été noté précédemment 1 ou 2 - Probabilité de sanctions réglementaires graves

Significatif	3	- Perte potentielle ou réelle dépassant les 0.2 million de dinars et inférieur à 1 million de dinars - Exige une action immédiate (généralement complété dans les 6 mois)	- Des répercussions significatives sur les affaires et le pays - Des risques opérationnels importants ou violation de la gouvernance de l'entreprise - Exposition inacceptable aux faiblesses de contrôle du risque de réputation à niveau moyen - Des problèmes périodiques qui ont été noté précédemment 1 ou 2 - Possibilité d'amendes/peines réglementaires - Pertes financières moyennes avec la possibilité de récupérer une partie - Problèmes au service de la clientèle qui nécessitent une intervention de l'administration
Modéré	2	- Perte potentielle ou réelle dépassant les 0.05 million de dinars et inférieur à 0.2 million de dinars - N'exige pas d'action immédiate	- Des répercussions moyennes sur les affaires et le pays - se référer aux problèmes posés -Des faiblesses de contrôle identifiées et qui pourraient dégénérer s'ils ne sont pas mis sous contrôle - Risque moyen de réputation - La résolution de ces problèmes se fait généralement dans le cadre d'affaire. - Exposition à des faibles sanctions règlementaires - Expositions faibles et donc acceptable dans le cadre de faire des affaires - Problèmes au service de la clientèle avec des niveaux acceptables - Exposition à des pertes financières ou des risques de réputation à faible vulnérabilité
Mineur	1	- Perte potentielle ou réelle est inférieur à 0.05 million de dinars - N'exige pas d'action immédiate	- Des répercussions minimes sur les affaires et le pays - se référer aux problèmes posés - Des faiblesses de contrôle identifiées et qui pourraient dégénérer s'ils ne sont pas mis sous contrôle - Faible risque de réputation - La résolution de ces problèmes se fait généralement dans le cadre d'affaire

ANNEXE N°5 : QUESTIONNAIRE D'EVALUATION DU DISPOSITIF DE MAITRISE DES RISQUES

Q1 : Quelles sont les mesures de contrôle existantes pour chaque risque identifié ?

Risque 1 : …… 1- …… 2- …… 3- ……

Risque 2 : …… 4- …… 5- …… 6- ……

Risque 3 : …… 7- …… 8- …… 9- ……

Risque 4 : ……10- ……. 11- ……. 12- ……

Q2 : Pour chacune des mesures de contrôle identifiée, comment jugeriez-vous sa performance sur une échelle allant d'efficace à insuffisant ?

Contrôle	Efficacité	Contrôle	Efficacité	Contrôle	Efficacité
1-		5-		9-	
2-		6-		10-	
3-		7-		11-	
4-		8-		12-	

Q3 : Quelles défaillances auriez-vous constaté ?

……...

……...

…….

Q4 : Quelles actions proposeriez-vous pour corriger ces défaillances ?

……...

……...

……...

……

ANNEXE N°6 : TABLEAU RECAPITULATIF DES TRAVAUX

Sous processus 1 : Réception du dossier de crédit Corporate par l'agence

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Fraude externe											
R213	Documents falsifiés	La compétence du personnel à détecter et reporter les opérations frauduleuses	3	1	3	1	2	3	1	3	1
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie des données par le chargé de clientèle agence	Auto contrôle + contrôle hiérarchique (vérification par le directeur d'agence)	5	1	5	2	4	2	1	2	1
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds	4	2	8	2	3	2	1	2	1
R616	Perte de documents lors de la transmission du dossier de crédit à la DCCOR	Le chargé de clientèle scanne les documents financiers et juridiques et la demande de crédit et les insère dans l'espace qui leur est réservé dans le portail ATB afin de les télécharger en cas de perte	2	2	4	1	3	2	1	2	1
Catégorie de risque : Pratiques concernant les clients, les produits et l'activité commerciale											
R712	Utilisation frauduleuse d'informations confidentielles sur la clientèle	Code de conduite de la profession (règles déontologiques) + Certification selon la norme de sécurité ISO 27001	1	3	3	1	4	1	1	1	1
R741	Conflits sur l'efficience des prestations	La capacité du chargé de la clientèle à gérer ce genre de conflits (des formations commerciales sont programmées régulièrement)	5	1	5	2	2	4	1	4	1

Sous processus 2 : Vérification de la complétude des documents de crédit par le chargé d'affaires Corporate DCCOR

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Fraude externe											
R213	Documents falsifiés	La compétence du personnel à détecter et reporter les opérations frauduleuses	3	1	3	1	2	3	1	3	1
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	3	1	3	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds	2	2	4	1	3	1	2	2	1
R614	Non respect de la procédure	Contrôle hiérarchique + contrôle périodique	1	3	3	1	3	1	1	1	1
R616	Perte de documents	Les documents sont déjà scannés et insérés dans le portail ATB	2	3	6	2	3	2	2	4	1
R623	Documents absents ou incomplets	Le chargé d'affaires rapproche le dossier de crédit par rapport au check list financiers et juridiques des documents selon le type de crédit + Remplir la note de complément de documents, la faire signée par la personne habilitée et la remettre au client	6	2	12	3	4	6	1	6	2

Sous processus 3 : Etude de dossier de crédit par le chargé d'affaires Corporate DCCOR

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Fraude interne											
R126	Corruption	L'étude sera vérifiée en premier lieu par le supérieur hiérarchique et en deuxième lieu par le directeur central DDCOR puis elle sera révisée par la DCC	4	5	20	4	4	2	2	4	1
Catégorie de risque : Fraude externe											
R213	Documents falsifiés	La compétence du personnel à détecter et reporter les opérations frauduleuses.	3	4	12	3	3	3	2	6	2
R221	Piratage informatique	Certification selon la norme de sécurité ISO 27001	2	6	12	3	4	1	4	4	1
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	2	6	2	2	3	1	3	1
R512	Défaillance du système d'info.	Contacter la direction des services informatiques	2	2	4	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie des données	Auto contrôle + Contrôle hiérarchique + contrôle DCC	4	3	12	3	3	2	2	4	1
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds.	5	2	10	2	2	4	2	8	2
R614	Non respect de la procédure	Contrôle hiérarchique + contrôle périodique	1	3	3	1	4	1	1	1	1
R616	Perte de documents	Les documents présentés par le client sont déjà scannés et insérés dans le portail ATB + Pour les documents de l'étude, l'analyse est faite de manière informatisée donc on peut les récupérer à tout moment	3	3	9	2	3	2	1	2	1
Catégorie de risque : Pratiques concernant les clients, les produits et l'activité commerciale											
R712	Utilisation frauduleuse d'informations confidentielles	Code de conduite de la profession + Certification selon la norme de sécurité ISO 27001	2	4	8	2	4	1	2	2	1
R732	Non respect des procédures de lutte contre le blanchiment d'argent et le financement de terrorisme	Avant de commencer l'étude du dossier, le chargé d'affaires doit étudier le risque client (consulter la base des clients black listés) + une enquête sur l'identité du client sera effectuée au niveau de la direction centrale de conformité	3	6	18	3	4	1	3	3	1

Sous processus 4 : Etude de faisabilité des garanties par la direction des garanties DCAJIR

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Fraude externe											
R213	Documents falsifiés	La compétence du personnel à détecter et reporter les opérations frauduleuses	2	3	6	2	4	1	2	2	1
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds	3	2	6	2	3	2	2	4	1
R616	Perte de documents	Les documents sont déjà scannés et insérés dans le portail ATB par le chargé de la clientèle agence	2	2	4	1	3	2	1	2	1
R623	Documents juridiques absents ou incomplets	Remplir la note complément de documents, la faire signée par la personne habilitée, la remettre au chargé d'affaires DCCOR pour informer le client	6	2	12	3	3	4	1	4	1
Catégorie de risque : Pratiques concernant les clients, les produits et l'activité commerciale											
R712	Utilisation frauduleuse d'informations confidentielles sur la clientèle	Code de conduite de la profession (règles déontologiques) + Certification selon la norme de sécurité ISO 27001	2	4	8	2	4	1	1	1	1

Sous processus 5 : Evaluation et révision du dossier de crédit par la DCC

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie des données	Auto contrôle + Contrôle hiérarchique	2	3	6	2	3	2	2	4	1
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds.	3	2	6	2	3	2	2	4	1
R614	Non respect de la procédure	Contrôle hiérarchique + contrôle périodique	1	2	2	1	4	1	1	1	1

Sous processus 6 : Prise de décision par le comité de crédit habilité

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie des données	Auto contrôle + Contrôle hiérarchique	3	2	6	2	3	2	1	2	1
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds.	2	2	4	1	3	2	1	2	1
R614	Non respect de la procédure	Contrôle hiérarchique + contrôle périodique	1	4	4	1	4	1	1	1	1

Sous processus 7 :Constitution des garanties

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	1	3	1	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	1	2	1	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie lors de l'élaboration du contrat de prêt	Auto contrôle + contrôle hiérarchique	2	5	10	2	3	1	3	3	1
R613	Non respect des délais d'exécution	Procédure interne sur les délais de traitement d'un dossier de crédit Corporate de la date de la demande du crédit jusqu'au déblocage des fonds.	3	2	6	2	3	2	2	4	1
R614	Non respect de la procédure	Contrôle hiérarchique + contrôle périodique	1	3	3	1	4	1	1	1	1
R632	Documents juridiques absents ou incomplets	Remplir la note complément de documents, la faire signée par la personne habilitée, la remettre au chargé d'affaires DCCOR pour informer le client	6	2	12	3	3	4	1	4	1

Sous processus 8 :Déblocage du crédit

Code risque	Risque opérationnel	Mesure de contrôle	Risque inhérent				Efficacité du contrôle	Risque résiduel			
			V	I	C	C'		V	I	C	C'
Catégorie de risque : Fraude interne											
R121	Détournement de fonds	Contrôle automatisé (Détection automatique de la fraude par l'application informatique) + séparation des tâches	2	6	12	3	4	1	2	2	1
Catégorie de risque : Fraude externe											
R221	Piratage informatique	Certification selon la norme de sécurité ISO 27001	1	6	6	2	4	1	2	2	1
Catégorie de risque : Interruption de l'activité et dysfonctionnement des systèmes											
R511	Panne matériel informatique	Contacter la direction des services généraux	3	2	6	2	2	2	1	2	1
R512	Défaillance du système d'information	Contacter la direction des services informatiques	2	3	6	2	3	2	1	2	1
Catégorie de risque : Exécution, livraison et gestion des processus											
R612	Erreur de saisie lors du déblocage des fonds	Auto contrôle + contrôle hiérarchique + contrôle automatisé (système d'alerte intégré dans l'application informatique utilisée pour le déblocage des fonds)	3	6	18	3	4	2	1	2	1
R614	Non respect de la procédure dans la mise en place du crédit	Contrôle hiérarchique + contrôle périodique	2	6	12	3	4	1	1	1	1
R616	Perte des documents de déblocage	Conservation des documents par scannage	2	5	10	2	3	1	2	2	1
Catégorie de risque : Pratiques concernant les clients, les produits et l'activité commerciale											
R741	Conflits avec les clients	La capacité du chargé de la clientèle à gérer ce genre de conflits (des formations commerciales sont programmées régulièrement)	4	1	4	1	2	3	1	3	1

ANNEXE N°7 : STATISTIQUES SUR L'EFFICACITE DU DMR

Répartition des risques inhérents et résiduels selon leur vraisemblance

	Risques inhérents	%	Risques résiduels	%
6. Fréquent	3	5%	1	2%
5. Plausible	2	4%	0	0%
4. Probable	4	7%	4	7%
3. Occasionnel	18	32%	6	11%
2. Lointain	23	40%	29	51%
1. Improbable/rare	7	12%	17	30%
Somme	57	100%	57	100%

Répartition des risques inhérents et résiduels selon leur impact

	Risques inhérents	%	Risques résiduels	%
6. Catastrophique	6	11%	0	0%
5. Majeur	4	7%	0	0%
4. Important	4	7%	1	2%
3.Significatif	10	18%	2	4%
2.Modéré	16	28%	15	26%
1.Mineur	17	30%	39	68%
Somme	57	100%	57	100%

Répartition des risques inhérents et résiduels selon leur criticité

	Risques inhérents	%	Risques résiduels	%
4. Extrême	1	2%	0	0%
3. Elevé	10	18%	0	0%
2. Moyen	20	36%	3	5%
1.Faible	26	44%	54	95%
Somme	57	100%	57	100%

BIBLIGRAPHIE

ARTICLES

-BON-MICHEL Béatrice, « La cartographie des risques : de la rationalisation du futur à l'apprentissage du risque. Cas de l'identification du risque opérationnel au sein d'un établissement de crédit », Management et avenir, 300p, 2011/8(n°48), pp.326-341.

- Comité de Bâle sur le contrôle bancaire. 2004. Convergence internationale de la mesure et des normes de fonds propres (dispositif révisé). Bâle : Banque des règlements internationaux. 216 pages. Annexe 8.

- Comité de Bâle sur le contrôle bancaire. 2003. Saines pratiques pour la gestion et la surveillance du risque opérationnel. Bâle : Banque des règlements internationaux, 12pages.

- DE MARESCHAL, Gilbert (2003), la cartographie des risques, Edition Anfor, Paris, 45P.

- David OSPITAL, « Le risque opérationnel ou l'apportuniété unique pour les banques de s'approprier une véritable culture du risque », Revue d'économie financière, No. 84, LE RISQUE OPÉRATIONNEL (JUIN 2006), pp. 105-119.

- Éric Lamarque, Frantz Maurer«Le risque opérationnel bancaire. Dispositifd'évaluation et système de pilotage », *Revue française de gestion* 2009/1 (n° 191),pp. 93-108.

- Meriem Haouat Asli, « Risque opérationnel bancaire : le point sur la réglementation prudentielle », *Management & Avenir*2011/8 (n° 48), p. 225-238.

- Norme internationale ISO 31000 :2009(F), « Management du risque-Principes et lignes directrices ».

OUVRAGES

- Frédéric Cordel, Gestion des risques et contrôle interne. De la conformité à l'analyse décisionnelle, Vuibert, « Gestion », 2016, 2éme édition, 304p.

- Henri-Pierre Maders, Jean-Luc Masselin, Contrôle interne des risques.Cibler - Evaluer - Organiser - Piloter – Maîtriser, Editions d'organisation, « Finance », 2009, 262p.

- IFACI – PWC, COSO. Référentiel intégré de contrôle interne. Principes de mise en œuvre et de pilotage, Eyrolles, 2014, 264p.

- IFACI, Guide d'audit : étude du processus de management et de cartographie des risques : Conception, mise en place et évaluation, Paris, IFACI, « les cahiers de la recherche », 2003, 88p.

- IFACI. Groupe Professionnel Assurance, La cartographie des risques. 2éme édition, Paris, « cahier de recherche », 2013, 136p.

- IFACI. Groupe Professionnel Banque, De la cartographie des risques au plan d'audit, Paris, « cahier de recherche », 2013, 72p.

- Jack L. King, Operational Risk, New York, Wiley Finance, 2011, 276p.

- Laurent Pierandrei, Risk Management. Gestion des risques en entreprises, banque et assurance, DUNOD, « Management sup », 2015, 320p.

- Yvon Mougin, La cartographie des processus. Maitriser les interfaces, Editions d'Organisation, 2004, 348p.

- Zied Boudriga, L'audit interne : Organisation et pratiques, Tunis, Azyrite, 2012, 356p.

TEXTES JURIDIQUES

-Circulaire aux établissements de crédit n° 2006-06, «Mise en place d'un système de contrôle de la conformité au sein des établissements de crédit ».

- Circulaire aux établissements de crédit n° 2006 – 19, « Contrôle Interne ».

- Circulaire aux établissements de crédit n° 2011 -06, « Renforcement des règles de bonne gouvernance dans les établissements de crédit ».

TABLE DES MATIERES