
La Gestion des Risques Opérationnels

Cas : Natixis Algérie

TARI Mohamed Larbi¹
High School of Trade, Algeria
Tari.med.larbi@gmail.com

REDDA Khadidja
High School of Trade, Algeria
Reddakhadidja014@gmail.com

Operational Risk Management

Case study : Natixis Algeria

TARI Mohamed Larbi & REDDA Khadidja
Ecole Supérieure de Commerce / ALGERIA

Received: 02/05/2017

Accepted: 19/07/2017

Published: 31/12/2017

Abstract:

The banking environment is characterized by the diversification of the products and the suggested services, which have made the banking activity more complex and therefore, more vulnerable to various risks threatening it, especially the operational risks. That's why, the management of this latter becomes a necessity for banking and financial establishments. The Basel committee integrated the operational risk in the "Mc DONOUGH" solvency ratio in 2004, and its implementation was established in 2006. But, in Algeria, this was only introduced in 2011 via the Regulation N° 11-08 which imposes the risk mapping, which was completed by the new regulation 14-01 in 2014. lags far behind in this area and has introduced operational risk's management in 2011 via regulation 11-08, which requires risk mapping which was supplemented by the new regulation 14-01 in 2014.

Keywords: Management, Operational risk, risk mapping, regulation.

(JEL) Classification : E43, E44, E52, E58, G21.

Résumé:

L'environnement bancaire est caractérisé par la diversification des produits et des services proposés, ce qui a rendu l'activité bancaire plus complexe et donc plus vulnérable aux différentes risques le menaçant, notamment le risque opérationnel. De ce fait, la gestion de ce dernier devient une nécessité pour les établissements bancaires et financiers. Le comité de Bâle a intégré ce risque dans le ratio de solvabilité « Mc DONOUGH » en 2004, et son application fut établie en 2006. Mais en Algérie cela n'a été introduit qu'en 2011 via le règlement 11-08 qui impose la cartographie des risques, et qui a été complété par le nouveau règlement 14-01 en 2014.

Mots clés : Gestion, risque opérationnel, cartographie des risques, règlement.

Classification (JEL) : E43, E44, E52, E58, G21.

Introduction:

L'environnement économique mondial a connu au cours de ces dernières années, de nombreuses crises. Des faillites de plus en plus conséquentes, telle que l'affaire de Madoff qui est considérée comme l'une des plus grandes escroqueries qui ont engendré des pertes de 50 millions de dollars, et celle de la Barings Bank, sans oublier la crise de subprimes qui s'est traduite par un effondrement du système financier mondial avec une perte estimée à près de 500 milliards de dollars en un an. Ces scandales ont perturbés la stabilité du système bancaire international, et ont permis de prouver aux régulateurs ainsi qu'aux banques et institutions financières que les dysfonctionnements opérationnels peuvent générer des dégâts considérables. C'est la raison pour laquelle la gestion de risque opérationnel est devenue une nécessité.

En effet, le risque opérationnel n'est pas nouveau, il a toujours existé, mais était souvent passé sous silence. Afin de bien mener notre travail, nous allons essayer de répondre à la problématique suivante : « **Afin de bien gérer ses risques, dans quelle optique inscrit-elle Natixis la démarche d'une gestion des risques opérationnels ?** ».

Cette problématique ouvre le champ à des questions secondaires telles que :

- Quels sont les types des risques existants au niveau des banques ? Et est-ce qu'ils ont un lien avec les risques opérationnels ?
- Comment peut-on identifier, mesurer et évaluer les risques opérationnels ?
- Quelle est la démarche de gestion des risques opérationnels utilisée au sein de Natixis Algérie ?

Afin de traiter ces questions, nous allons nous baser sur une approche mixte qui regroupe l'approche descriptive et analytique :

- L'approche descriptive : elle sera utilisée lors de la présentation du cadre théorique de l'étude
- L'approche analytique : c'est celle que nous allons utiliser dans l'analyse et la présentation de la méthode de gestion des risques opérationnels au sein de Natixis Algérie.

Pour bien structurer notre travail, nous allons le subdiviser en deux grandes parties :

- La première sera dédiée à la notion des risques opérationnels ainsi qu'aux différents outils qui permettent une gestion pertinente de ces risques.
- La deuxième sera consacrée pour la présentation d'une étude de cas au sein de la Banque Natixis Algérie.

I- Première Partie :

1. Généralités sur la notion des risques opérationnels :

1.1. Définition :

Selon la nouvelle loi réglementaire, l'article n°20 de la loi n°14-01 du 16 février 2014 portant, coefficients de solvabilité applicable aux banques et établissements financiers, stipule que : « on entend par risque opérationnel, le risque de perte résultant de carences ou de défaillances inhérentes aux procédures, personnels et systèmes internes des banques et établissements financiers, ou à des événements extérieurs. Cette définition exclut les risques stratégiques et de réputation, mais inclut le risque juridique ».

1.2. Les principaux enjeux du risque opérationnel¹:

- La sécurisation des résultants en évitant ou en couvrant des risques qui entraînent des pertes nettes,
- Une plus grande compétitivité du fait des améliorations de tarif possibles si les pertes constatées sur les événements ont tendance à diminuer,
- Éviter la chute brutale du cours de bourse lorsque l'établissement bancaire ou une de ces filiales sont cotés,
- Amélioration la productivité en identifiant les processus « à risque » et en menant les plans d'action nécessaires à leur amélioration.

1.3. Les caractéristiques des risques opérationnels²:

- Une imbrication des causes, des événements et des effets,
- Une imbrication avec le risque de crédit et de marché (risque frontières),
- Une coexistence de pertes directes et indirectes,
- Une insuffisance des historiques des données,
- Une difficulté de mesure, car il n'est pas toujours apparent ou directement observable.

2. Les outils d'identification et de gestion des risques opérationnels :

2.1. L'auto-évaluation des risques opérationnels (RCSA : Risk Control Self Assessment):

L'auto-évaluation des risques (RCSA) est la plus ancienne des méthodes d'identification et de gestion des risques opérationnels, mais elle reste tout de même la plus dynamique et celle assurant une gestion prospective des risques auxquels peuvent être confrontés les différents départements de la banque. Cet exercice d'auto-évaluation peut se faire en suivant les types d'approche notant : l'approche de type Bottom-up, l'approche de type Top-Down, l'approche combinée et l'approche de Benchmarking.

2.2. La cartographie des Risques Opérationnels :

2.2.1. Définition :

Elle se définit comme étant le positionnement des risques majeurs selon différents axes, tels que l'impact financier potentiel, la probabilité d'occurrence ou le niveau actuel de maîtrise des risques³. La carte des risques est un document permettant de recenser les principaux risques d'une organisation et de le présenter synthétiquement sous une forme hiérarchisée pour assurer une démarche global d'évaluation et de gestion des risques.

2.2.2. Objectifs de la mise en place d'une cartographie : Les objectifs de l'élaboration d'une cartographie des risques sont⁴:

- Identifier et hiérarchiser les facteurs clés de risque et dresser un état de lieux complet des vulnérabilités,
- Orienter le plan d'audit interne,
- Aider le management dans l'établissement de son plan stratégique et dans la prise de décision,
- Veiller à la bonne image de l'établissement.

2.2.3 Les étapes de la démarche globale d'une cartographie des risques :

La démarche méthodologique pour l'élaboration d'une cartographie des risques passe par les étapes suivantes :

A- Représentation du processus d'activité et risque associé :

Elle consiste à établir une nomenclature des risques adoptée à la banque, en le découpant en ses lignes métiers et ses différents processus.

B- Identification et évaluation des risques bruts :

Le risque brut appelé aussi risque intrinsèque, est définie par Gilbert et Michelle comme étant le risque brut considéré sans éventuels moyens de protection ou de contrôle mis en place par l'organisation. La notion de risque brut permet d'évaluer le montant à couvrir des risques, de classer ces derniers, ainsi que de valider les facteurs de réduction⁵.

C- Appréciation du dispositif de maîtrise des risques(DMR) et évaluation du risque net :

Suite à l'identification et l'évaluation du risque brut, nous identifierons le dispositif de maîtrise de risque (DMR) existant, en l'occurrence le contrôle mise en place pour parer à l'éventualité de survenance du risque. Dans cette étape ce sont les opérationnels eux-mêmes qui vont porter le jugement sur le degré de maîtrise des risques ainsi que l'influence de ce dispositif sur l'impact et/ou la fréquence associés au risque par un ensemble d'analyse descriptive de ce dernier⁶.

D- Classification des risques :

Dès que le risque net est déterminé selon son impact et sa fréquence, une nouvelle classification et hiérarchie sera établie afin de permettre d'étudier le degré d'acceptation du risque résiduel après une prise en compte des mesures de prévention des risques. Cette classification va permettre de déterminer les priorités de traitement des risques afin d'améliorer les dispositifs⁷.

2.3. La constitution et l'exploitation d'une base de données opérationnelles :

Pour la constitution de la base des données opérationnelles, Il s'agit de la collecte des données des pertes internes (PI) survenus au titre du risque opérationnel, au niveau des différentes entités, départements et réseaux de la banque (Ariane CHAPELLE, George HUBNER et Jean-Philippe Peter, 2 février 2005, P.163). Chaque perte fait l'objet d'un reporting de la structure en cause à destination de la direction en charge du risque opérationnel, des dirigeants et des fonctions de contrôle permanent et périodique. Ainsi, la collecte des données des pertes interne constitue une étape absolument cruciale pour une bonne gestion des risques.

2.4. Les indicateurs clés des risques (KRI : Key Risk Indicator) :

Les indicateurs clés des risques constituent des indices possibles de perte ou des dangers futurs qui peuvent menacer l'activité de l'établissement⁸. Les indicateurs clés des risques sont des statistiques et/ou diverses mesures souvent d'ordre financier qui peuvent donner une idée de l'exposition d'une banque aux risques, ils sont généralement revus de façon périodique (chaque mois ou chaque trimestre) pour alerter les banques pour des opérations porteuse des risques⁹.

2.5. Les Tableaux de Bord des risques opérationnels:

Les tableaux de bord des risques opérationnels permettent de surveiller les pertes à travers le suivi des indicateurs clés. Ils reflètent la qualité de la politique des risques mise en œuvre et donnent une vision consolidée du risque aux différents niveaux de l'établissement et en particulier, aux instances dirigeants.

2.6. Quantification du risque :

Suite à l'accord de Bâle, les banques sont invitées à développer leur propre méthode de mesure de capital pour le risque opérationnel. Dont, les établissements ont commencé à quantifier leur exposition au risque opérationnel, en intégrant des données internes et externes des pertes¹⁰.

3. Détermination des exigences en fonds propres et la couverture des risques opérationnels:

3.1. Les méthodes d'évaluation du risque opérationnel :

3.1.1. Approche Indicateur de base (BIA) :

Elle se borne à constituer des fonds propres contre les risques opérationnels sur un mode forfaitaire. Cette méthode de base consiste en l'application d'un pourcentage fixe α à un indicateur qui représente l'exposition potentielle aux risques opérationnels, cet indicateur représente le produit annuel brut moyen (PB) sur les trois dernières années¹¹.

3.1.2. L'approche standard (SA) :

Dans cette approche, le capital réglementaire est calculée en fonction d'un pourcentage du revenu annuel brut appelé facteur Bêta (β). La formule est la suivante : $K_{sa} = \sum \beta_j \times PB_j$ avec : $j = 1, \dots, 8$. Où : K_{sa} : est le capital réglementaire ou l'exigence en fond propre selon l'approche standard ; B_j : pourcentage fixe pour chacune des huit lignes de métiers ; PB_j : produit annuel brut, positif pour les trois dernières années pour chacune des huit lignes de métiers.

3.1.3. L'approche des mesures avancées AMA :

Le comité de Bâle propose plusieurs alternatives au sein des mesures AMA à savoir : une méthode basée sur les paramètres internes, la méthode SCORECARD, l'analyse des scénarios, et enfin la méthode LDA (Loss Distribution Approach), la plus sophistiquée sur le plan technique. De ce fait, le calcul d'exigence en fonds propres dans cette méthode nécessite un calcul de la mesure de la perte attendue (EL : Expected Loss) pour chaque couple et aussi un facteur multiplicateur tels que : $EL = PE \times LGE \times E$ Où : PE : probabilité de l'événement, LGE : perte en cas d'événement, E : Exposition au risque opérationnel.

PE et LGE sont déterminés par la banque d'après ses modèles interne, alors que le facteur d'exposition E est donné par le régulateur.

3.2. Les couvertures des Risques Opérationnels :

3.2.1 La couverture interne des risques opérationnels :

La couverture interne des risques opérationnels comprend l'ensemble des actions d'amélioration des processus, des outils et des mesures internes de contrôle et de prévention visant à réduire l'impact des risques opérationnels. Ces outils internes servent à absorber les pertes attendues. Les outils de couvertures internes sont les suivantes : la continuité des activités, la délégation de pouvoir, les chartes d'éthique, la couverture budgétaire.

3.2.2. La couverture externe :

La banque ne peut pas toujours couvrir ses risques opérationnels par ses seuls moyens internes, elle préfère dans plusieurs cas les endosser à un tiers plus spécialisés qui dispose des moyens mieux adaptés à sa gestion et qui accepte de les assumer (externalisation), ou de modifier l'impact qui sera partiellement ou totalement assumée par un tiers contre

rémunération (assurance). Cette couverture peut se faire par différents outils, tels que : le contrat d'assurance et l'externalisation de l'activité.

II- Partie Pratique : La Gestion des Risques Opérationnels au sein de la Banque Natixis

1. Présentation de la filiale Natixis Algérie:

Natixis Algérie est la filiale du groupe BPCE adossée à Natixis (pôle service financier spécialisé issue de la fusion des groupes Caisses d'Epargne et Banque Populaire) installée en Algérie depuis 1999 et est la première banque française à être implantée en Algérie.

2. La mise en place d'une cartographie des risques opérationnels pour le processus «crédit documentaire » au sein de Natixis Algérie :

N.B : au niveau de Natixis Algérie nous n'avons pas été autorisés à accéder au module de calcul des cartographies des risques opérationnels. Pour cette raison, notre travail a été réalisé via une simulation simplifiée d'une cartographie thématique sur le « processus crédit documentaire ».

2.1. Identification des risques liés à chaque étape du processus « crédit documentaire » :

Nous avons suivi l'approche TOP-DOWN qui est adoptée par Natixis Algérie, et qui nous permettra d'identifier, de manière exhaustive tous les risques inhérents au processus crédit documentaire. Pour ce faire, Nous avons préparé dans un premier lieu une grille des questions concernant le degré de conformité de la pratique avec les règles de la chambre de commerce international (RUU600), ainsi qu'avec les procédures internes de la banque. Les questions étaient également fondées sur les scénarios pouvant affecter chaque opération du processus. Les résultats sont résumés dans le tableau ci-dessous :

Tableau 1 : résultats de l'identification des risques liés au processus de crédit documentaire :

Code Risque	Etape de processus	Description du risque	Sous catégorie selon la nomenclature de Bâle II
1	Domiciliation des opérations	Fausse domiciliation : c'est de la complicité entre l'opérationnel	Fraude interne (vol et Fraude)
2		Fausse domiciliation	Fraude externe
3		Falsification des documents	Fraude externe (vol et fraude)
4		Erreur de saisi des informations	Saisie, exécution et suivi des transactions
5		Dysfonctionnement du système	Interruption de l'activité et dysfonctionnement de système
6		Non consultation du fichier des interdits de domiciliation diffusé par la BA.	Exécution, livraison et gestion de processus
7		Numéro de domiciliation repris avec erreur sur la facture (erreur dans la monnaie, l'année, le trimestre,...etc.)	Client, produit et pratique commercial
8		Domiciliation d'un contrat de contact de produit prohibé, interdits ou faisant l'objet d'une quelconque restriction.	Activité non autorisée
9	Ouverture Credoc	Divulgaration d'informations confidentielles. d'informations	Conformité diffusion d'informations et devoir fiduciaire.
10		Non blocage de la provision sur un compte PREG	Fraude interne
11		Panne du système informatique	Interruption de l'activité et dysfonctionnement des systèmes
12		Panne d'électricité	Interruption de l'activité et dysfonctionnement des systèmes

13		Ouverture frauduleuse d'une LC (complicité entre l'opérationnel et le client)	Fraude interne (vol et fraude)
14		Erreur de saisi	Saisie, exécution et suivi des transactions
15		Indisponibilité Swift	Interruption de l'activité et dysfonctionnement des systèmes
16		Fraude au pli cartable	Fraude externe.
17		Violation de la confidentialité de la clientèle.	Conformité, diffusion d'information et devoir fiduciaire.
18	Réalisation et règlement Credoc	Erreur lors des contrôles des documents	Exécution, livraison et suivi des transactions.
19		Non déclaration d'une irrégularité portant atteinte à la réglementation de change	Fraude interne
20		Présentation des faux documents	Fraude externe
21		Insuffisance dans le contrôle des documents	Clients, produits et pratique commerciale
22		Violation de la confidentialité des informations d'un client.	Conformité, diffusion d'information et devoir fiduciaire.
23		Non respect des délais de vérification des documents.	Saisie, exécution et suivi des transactions.
24		Application des incoterms interdits en Algérie (le CIF par exemple)	Pratique commerciale de place incorrecte
25		Perte ou détérioration des documents	Dommages occasionnés aux actifs physiques
26		Non respect de délai de l'envoi des réserves à la banque notificatrice	Saisie, exécutions et suivi des transactions
27		Erreur dans le report de domiciliation	Erreur dans la saisie, le suivi et le changement
28		Défaut de programmation d'un règlement	Exécution, livraison et gestion des processus
29	Annulation d'un Credoc	Défaut de restitution PREG.	Fraude interne.
30		Erreur de saisie lors de l'annulation d'un Credoc	Fraude interne.
31	Apurement de l'opération	Erreur sur la déclaration	Saisie ,exécution et suivi des transactions
32		Défaut des documents	Exécution, livraison et gestion des processus
33		Déclaration tardive	Exécution, livraison et gestion des processus
34		Défaut de déclaration	Exécution, livraison et gestion des processus

Source : élaboration faite par les chercheurs

2.2. Evaluation qualitatifs des risques opérationnels liés au processus « crédit documentaire » :

Pour effectuer l'évaluation, nous avons établi un sondage avec les responsables des deux structures concernés par le processus crédit documentaire, il comporte trois cases pour chaque risque identifié, l'une pour la fréquence de survenance, l'autre pour l'impact de risque, et la dernière case pour le dispositif de maîtrise des risques (DMR). Nous avons travaillé avec

un échantillon de 20 personnes, où nous avons tenté d'expliquer chaque risque énuméré et dans quelle phase de processus ce risque a été détecté afin qu'ils puissent nous donner une évaluation réelles des paramètres le composant. L'évaluation finale du risque brut se fait par la combinaison de ces deux paramètres (fréquence et impact) en suivant la formule suivante : Risque brut= Fréquence X impact. D'après les réunions effectuées avec les responsables des deux structures, nous avons pu ressortir les résultats suivants :

- en matière de nombre, nous avons compté 74 risques opérationnels pour 34 risques de processus.
- nous avons utilisé les mêmes échelles des cotations de fréquence et d'impacts (financiers et image), les résultats de ces cotations se présentent comme suit :

Tableau 2 : les taux de répartition des risques selon les cotations :

Risque	Risque Brut	%	Risque Net	%
Faible	8	10,81%	25	33,78%
Moyen	23	31,08%	35	47,30%
Fort	40	54,05%	13	17,57%
Critique	3	4,06%	1	1,35%
Total	74	100%	74	100%

Source : élaboré par les chercheurs.

Avec une efficacité de DMR de 95%, une telle croissance dans l'efficacité des DMR a permis de mieux gérer certains risques au sein de Natixis Algérie. Pour ce qui concerne les degrés d'efficience des DMR existants, nous avons tenté d'effectuer une analyse basée sur un sondage auprès des structures concernées. On a effectué des calculs des nombre des DMR existants selon des intervalles de degrés d'efficience. Les résultats se présentent comme suit :

Tableau 3 : calcul de l'efficacité des Dispositifs de Maîtrise des Risques (DMR)

Intervalle d'efficacité DRM	Nombre de DMR existants	Moyenne	Total
[0%,50% [	20	25%	500%
[50%,65% [	35	57.5%	2012.5%
[65%,80% [	10	72.5%	725%
[80%,95% [	9	87.5%	787.5%
	74	95%	7030%

Source : élaboré par les chercheurs.

2.3. Présentation de la cartographie finale liée au processus « crédit documentaire » :

La cartographie présentée tout d'abord est celle des risques bruts afin de pouvoir déduire leur cotation pour le calcul des risques nets supportés par Natixis Algérie :

Tableau 4 : la cartographie des risques bruts

processus	Code risque	Catégorie des risques niveau 1 (typologie baloise)	Catégorie des risques niveau 2 (typologie baloise)	Description de l'évènement de risque	Risques Bruts			
					Impact financier		Cotation de risque brut	Impact d'image
					Fréquence	impact		
Domiciliation des opérations	1	Fraude interne	Vol et fraude	Fausse domiciliation le cas où il y a une complicité entre le personnel et le client	Rare	Fort	Fort	Moyen
	2	Fraude externe	Vol et fraude	Fausse domiciliation	Rare	Fort	Fort	Moyen
	3	Fraude externe	Vol et fraude	Falsification des documents	fréquent	Critique	Critique	Fort

				(facture pro forma, demande de client	t	que	que	
	4	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Erreur de saisi d'information	Fréquent	Faible	Moyen	Fort
	5	Interruption d'activité et dysfonctionnement des systèmes	Système	Dysfonctionnement du système	Rare	Critique	Critique	Moyen
	6	Exécution, livraison et gestion des processus	Surveillance et informations financières	Non consultation du fichier interdit de domiciliation diffusé par la BA	Très rare	Critique	Fort	Fort
	7	Clients, produits et pratiques commerciales	Conformité, devoir d'information et devoir fiduciaire	Numéro de domiciliation repris avec erreur sur la facture	Fréquent	Moyen	Moyen	Moyen
	8	Fraude interne	Activité non autorisée	Domiciliation d'un contrat interdit et prohibé ou faisant l'objet d'une quelconque restriction	Fréquent	Critique	Critique	Moyen
	9	Clients, produit et pratiques commerciales	Conformité, devoir d'information et devoir fiduciaire	Divulgaration d'informations confidentielles	Rare	Fort	Fort	Fort
	10	Fraude interne	Vol et fraude	Non blocage de la provision sur un compte PREG	Rare	Critique	Fort	Moyen
	11	Interruption d'activité et dysfonctionnement des systèmes	Système	Panne du système d'informatique	Rare	Critique	Critique	Moyen
	12	Interruption d'activité et dysfonctionnement des systèmes	systèmes	Panne d'électricité	Rare	Faible	Faible	Moyen
	13	Fraude interne	Vol et fraude	Ouverture frauduleuse d'une LC (complicité entre le personnel et le client)	Très rare	Critique	Fort	Fort
	14	Interruption d'activité et dysfonctionnement des systèmes	systèmes	Indisponibilité Swift	Rare	Critique	Fort	Fort
	15	Fraude externe	Vol et fraude	Fraude au pli cartable	Fréquent	Critique	Critique	Moyen
Réalisation et règlement	16	Clients, produit et pratiques	Conformité, devoir	Violation de la confidentialité de la	Rare	Fort	Fort	Critique

La Gestion des Risques Opérationnels. Cas : Natixis Algérie

CREDOC		commerciales	d'information et devoir fiduciaire	clientèle				e
	17	Exécution, livraison et gestion des processus	Exécution, saisie et suivi des transactions	Erreur lors du contrôle des documents	Fréquent	Critique	Critique	Moyen
	18	Fraude interne	Activité non autorisée	Non déclaration d'une irrégularité portant atteinte à la réglementation de change	Rare	Fort	Moyen	Moyen
	19	Fraude externe	Vol et fraude	Présentation de faux documents	Très rare	Critique	Fort	Fort
	20	Clients, produits et pratiques commerciales	Conformité, devoir d'information Et devoir fiduciaire	Insuffisance dans le contrôle des documents	Très rare	Critique	Fort	Moyen
	21	Clients, produits et pratiques commerciales	Conformité, devoir d'information Et devoir fiduciaire	Violation de la confidentialité d'une clientèle	Rare	Fort	Moyen	Fort
	22	Exécution, livraison et gestion des processus	Exécution, saisie et suivi des transactions	Non respect des délais de vérification des documents	Très rare	Critique	Fort	Fort
	23	Exécution, livraison et gestion des processus	Exécution, saisie et suivi des transactions	Erreur de saisie	fréquent	Moyen	Moyen	Faible
	24	Clients, produits et pratiques commerciales	Pratiques commerciales de marché incorrectes	Application des incoterms interdits en Algérie (par exemple le CIF)	Très rare	Critique	Fort	Moyen
	25	Dommages aux actifs corporels	Dommages occasionnés aux actifs physiques	Perte de détérioration des documents originaux	Très rare	Critique	fort	Moyen
	26	Exécution, livraison et gestion des processus	Exécution, saisie et suivi des transactions	Non respect des délais d'envoi des réserves à la banque notificatrice	Rare	Fort	Fort	Moyen
	27	Exécution, livraison et gestion des processus	Erreur dans la saisie, le suivi et le changement	Erreur dans le report de domiciliation	Critique	Fort	Critique	Fort
	28	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Défaut de programmation d'un règlement	Rare	Critique	Fort	Moyen

Annulation d'un CREDOC	29	Fraude interne	Vol et fraude	Défaut de restitution PREG	Fréquent	Critique	Critique	Moyen
	30	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Erreur de saisie lors de l'annulation de CREDOC	Critique	Fort	Critique	Fort
Apurement de l'opération	31	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Erreur sur déclaration	Fréquent	Critique	Critique	Moyen
	32	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Défaut des documents	Rare	Fort	Fort	Moyen
	33	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Déclaration tardive	Rare	Critique	Fort	Fort
	34	Exécution, livraison et gestion des processus	Saisie, exécution et suivi des transactions	Défaut de déclaration	Très rare	Critique	Fort	Moyen

Source : élaboré par les chercheurs.

Cette cartographie des risques bruts expose les risques potentiels liés au processus « crédit documentaire » auxquels fait face Natixis Algérie, ces risques ont un enjeu global qui concerne toute la place bancaire ces dernières années. Dans ce cadre Natixis Algérie a pris les devants en intégrant dans sa cartographie des risques opérationnels les risques cités ci-dessous ont prévu des actions de réduction des risques afin d'améliorer les niveaux de dispositif de maîtrise des risques relatifs.

- Les résultats de l'évaluation qualitative du risque net :

La confrontation des risques bruts avec le dispositif de maîtrise des risques, suivant la matrice présentée dans la section précédente, nous a permis de déduire les niveaux des risques opérationnels nets liés au processus « crédit documentaire ». Les résultats sont illustrés dans le tableau ci-après :

Tableau 5 : la cartographie des risques nets.

Etape de processus	Code risque	Description de l'évènement de risque	Dispositif de maitrise des risques					Cotation des risques nets
			DMR existant			Descriptif	Efficacité de DMR existant	
			contrôle	Procédure	humain			
Ouverture CREDOC	1	Fausse domiciliation (complicité entre opérationnel et clientèle)	50%	4%	8%	Assurer un deuxième contrôle par le supérieur et confirmer la relation	62%	Fort
	2	Fausse domiciliation	50%	8%	8%	Contracter le client	61%	Moyen
	3	Falsification des documents	75%	4%	8%	Le système fait la comparaison entre les signatures dans les	87%	Moyen

						documents		
	4	Erreur de saisie des informations	75%	4%	8%	Assurer un deuxième contrôle par le supérieur et possibilité de rectification	87%	Faible
	5	Dysfonctionnement du système	25%	8%	4%	Assurer un contrôle permanent	37%	Moyen
	6	Non consultation du fichier des interdits de domiciliation diffusé par la BA	50%	4%	8%	Liste des fichiers des interdits doit être mise à jour et transmise à tous les staffes du service CREDOC (agence et direction)	62%	Moyen
	7	Numéro de domiciliation repris avec erreur sur la facture	50%	8%	8%	Mention du nom du numéro du client sur la demande	66%	Moyen
	8	Domiciliation d'un contrat des produits prohibés, interdits ou faisant l'objet d'une quelconque restriction	50%	8%	4%	Mise à jour de la liste des produits interdits sur le système	62%	Fort
	9	Divulgaration d'informations confidentielles	50%	4%	8%	Signaler la banque quels renseignements confidentiels seront dévoilés. Un accord de confidentialité parfois appelé accord de non divulgation	62%	Fort
	10	Non blocage de la provision sur un compte PREG	50%	8%	4%	Il faut contacter le client et paramétrer le système pour ne pas donner la main à la saisie de l'ouverture	62%	Fort
	11	Panneau du système informatique	75%	8%	4%	Assurer un contrôle permanent et aussi la disponibilité de d'autres moyens fiables	87%	Moyen
	12	Panne d'électricité	50%	4%	0%	Groupe électrogène, onduleur	54%	Faible
	13	Ouverture frauduleuse d'une LC	50%	12%	4%	Séparation des tâches et confirmer la relation	66%	Moyen
	14	Indisponibilité SWIFT	75%	8%	0%	Relance de la banque en cas de retard	84%	Moyen
	15	Fraude au pli cartable	50%	12%	4%	Assurer un deuxième contrôle par le supérieur (contrôle hiérarchique) et existence d'une liste des clients autorisés à utiliser le pli cartable	66%	Fort
	16	Violation de la confidentialité des clients	50%	12%	8%	Veille déontologique permanente	70%	Moyen
Réalisation et règlement CREDOC	17	Erreur lors de contrôle des documents	50%	12%	4%	Assurer un 2 ^{ème} contrôle par le supérieur (contrôle hiérarchique)	66%	Fort
	18	Non déclaration d'une irrégularité portant atteinte à	50%	4%	4%	multiples contrôles par le supérieur (contrôle	66%	Moyen

		la réglementation de change				hiérarchique) sur les documents		
	19	Présentation des faux documents	75%	4%	4%	multiples contrôles par le supérieur (contrôle hiérarchique) sur les documents	83%	faible
	20	Insuffisance dans le contrôle des documents	50%	12%	4%	Multiplés contrôles par le supérieur (contrôle hiérarchique) sur les documents	66%	Moyen
	21	Violation de la confidentialité des informations d'un client	75%	4%	8%	Charte déontologique et sensibiliser l'effectif	87%	Faible
	22	Non respect des délais de vérification des documents	50%	8%	0%	Vérification organisée et obligatoire sur le système ou vérification de la saisie par une 2 ^{ème} personne	58%	Moyen
	23	Erreur de saisie	50%	4%	8%	Vérification et Validation hiérarchique	62%	Moyen
	24	Application des incoterms interdits en Algérie	75%	8%	8%	Mise à jour de la liste des incoterms interdits sur le système et transmettre à tous les staffs de Comex et assurer un 2 ^{ème} contrôle par le supérieur	91%	Faible
	25	Pertes ou détérioration des documents originaux	50%	4%	8%	Rangement alphabétique des dossiers. S'assurer que les dossiers soient existants en fichiers numériques et physiques	62%	Moyen
	26	Non respect des délais d'envoi des réserves à la banque notifiatrice	50%	8%	4%	Assurer un contrôle permanent	62%	Fort
	27	Erreur dans le report de domiciliation	50%	4%	4%	Sensibilisation du personnel Comex et assurer un contrôle hiérarchique	58%	Fort
	28	Défaut de programmation d'un règlement	50%	8%	0%	Assurer un contrôle permanent	58%	Fort
Annulation d'un CREDO C et apurement de l'opération	29	Défaut de restitution PREG	75%	4%	4%	Paramétrer le système pour ne pas donner la main à la saisie de l'ouverture	83%	Moyen
	30	Erreur de saisie lors de l'annulation d'un CREDOC	75%	4%	8%	Vérification de la saisie par un supérieur avant envoi	87%	Moyen
	31	Erreur sur la déclaration	50%	4%	8%	Assurer un contrôle permanent	62%	Fort
	32	Défaut des documents	50%	8%	8%	Enregistrement des documents lors de la réception et assurer un contrôle hiérarchique	62%	Moyen
	33	Déclaration tardive	50%	12%	4%	Assurer un contrôle hiérarchique manuel et centralisation des directions opérationnelles	66%	Moyen

	34	Défaut de déclaration	25%	4%	0%	Assurer un 2 ^{ème} contrôle par le supérieur hiérarchique	29%	Fort
--	----	-----------------------	-----	----	----	--	-----	------

Source : élaboré par les chercheurs.

Afin d'améliorer le dispositif de maîtrise des risques des événements de risque (par exemple le risque de falsification des documents), les activités de processus « crédit documentaire » sont centralisées au niveau centrale. Pour pouvoir interprétés les résultats obtenus, il serait préférable pour la banque de transformer les évaluations qualitatives obtenus à des évaluations quantitatives afin d'en déduire les risques qui menacent le plus cette dernière. Et cela permet la manipulation des chiffres et de ce fait de représenter les résultats sous formes de graphiques qui facilitent leur compréhension.

3. Quantification des évaluations qualitatives :

Afin de transformer les évaluations qualitatives obtenues à des évaluations quantitatives, on a suivi les étapes suivantes :

3.1 Quantification des combinaisons (fréquence/impact) :

On a tenté tout d'abord de changer les échelles de cotations des risques bruts et des risques nets afin de pouvoir les quantifier. Le tableau ci-dessous présente les nouvelles échelles de cotations « les notes » des deux facteurs (fréquences/ impacts) :

Tableau 6 : les nouvelles échelles de cotations des fréquences/impacts.

Note	1	2	3	4
Fréquence	Très rare	Rare	Fréquent	Très fréquent
impact	Faible	Moyen	Fort	Critique

Source : élaboré par les chercheurs.

3.2 Quantification des risques Bruts :

Cette étape nécessite tout d'abord l'adaptation de l'échelle de la note globale du risque brut présenté précédemment avec les règles statistiques de quantification des risques. Ainsi, nous proposons l'utilisation de cette méthode qui se base sur une démarche statistique plus valable et plus cohérente que nous avons tiré de livre de Jimenez et Merlier « Prévention et gestion des risques opérationnels ». L'application de cette méthode a donné les résultats suivants :

Tableau 7 : Echelle de notation des risques bruts.

Faible	Moyen	Fort	Critique
1×1=1	1×4=4	2×4=8	3×4=12
1×2=2	2×2=4	3×3=9	4×3=12
1×3=3	2×3=6	4×2=8	4×4=16
2×1=2	3×2=6		
3×1=3	4×1=4		

Source : élaboré par les chercheurs.

Afin de rendre ces combinaisons faciles à exploiter, nous avons opté pour un changement de notation en appliquant le principe du sinistre maximum possible, qui nous a permis de choisir pour chaque risque la notation la plus importante dans une classe d'évaluation. Faible : 1, 2, 3 seront changés par 3 ; Moyen : 4, 5 seront changés par 6 ; Fort : 6, 8, 9 seront changés par 9 ; Critique : 12, 16 seront changés par 16.

La matrice désignant ces combinaisons illustrera mieux les notations :

Tableau 8 : Matrice de quantification des risques bruts.

Impact	Fréquence	1	2	3	4
		Très rare	Rare	Fréquent	Très fréquent
1	Faible	1	2	3	4
2	Moyen	2	4	6	8
3	Fort	3	6	9	12
4	Critique	4	8	12	16

Source : élaboré par les chercheurs.

3.3 Quantification des risques nets :

La combinaison des risques bruts avec l'efficacité des DMR nous permettra par la suite d'attribuer une note aux risques nets. Nous avons adopté les mêmes notations données aux risques bruts afin de pouvoir comparer les résultats. Ces notations sont présentées dans le tableau ci-dessous :

Tableau 9 : changement des notations des risques nets.

Notation des risques nets	3	6	9	16
cotation des risques nets	Faible	Moyen	Fort	Critique

Source : élaboré par les chercheurs.

La matrice suivante montrera les notes attribuées à chaque combinaison (risques bruts/efficacité DMR :

Tableau 10 : Matrice de changement des notations des risques nets.

Efficacité DMR		Risques bruts			
		3	6	9	16
		Faible	Moyen	Fort	Critique
1	[80%,95% [	3	3	3	6
2	[65%,80% [	3	6	6	9
3	[50%,65% [	3	6	9	16
4	[0%,50% [	6	9	16	16

Source : élaboré par les chercheurs.

3.4 Quantification finale des risques :

La quantification finale des risques est présentée dans le tableau ci-dessous :

Tableau 11 : Quantification finales des risques liés au processus CREDOC :

Etape de processus	Code risque	Risques opérationnels	Note de la fréquence	Note de l'impact	Note de risque brut	Changement des notations des risques bruts	Note du risque net
Domiciliation des opérations	1	Fausse domiciliation (complicité entre le client et l'opérationnel)	2	3	6	9	9
	2	Fausse domiciliation	2	3	6	9	6
	3	Falsification des documents	3	4	12	16	9
	4	Erreur de saisie des informations	3	1	3	3	3
	5	Dysfonctionnement du système	2	4	8	9	6
	6	Non consultation des fichiers des interdits de domiciliation diffusés par la BA	1	4	4	6	6
	7	Numéro de domiciliation repris avec erreur sur la	3	2	6	9	6

La Gestion des Risques Opérationnels. Cas : Natixis Algérie

		facture					
	8	Domiciliation d'un contrat d'un produit prohibé	3	4	12	16	9
Ouverture CREDOC	9	Divulgarion d'informations confidentielles	2	3	6	9	9
	10	Non blocage de la provision sur un compte PREG	2	4	8	9	9
	11	Panne du système d'information	3	4	12	16	6
	12	Panne d'électricité	2	1	2	3	3
	13	Ouverture frauduleuse d'une LC	1	4	4	6	6
	14	Indisponibilité SWIFT	2	4	8	9	6
	15	Fraude au pli cartable	3	4	12	16	9
	16	Violation de la confidentialité de la clientèle	2	3	6	9	6
Réalisation et règlement CREDOC	17	Erreur lors du contrôle des documents	3	4	12	16	9
	18	Non déclaration d'une irrégularité portant atteinte à la réglementation de change	2	3	6	9	6
	19	Présentation des faux documents	1	4	4	6	3
	20	Insuffisance dans le contrôle des documents	2	3	6	9	6
	21	Violation de la confidentialité des informations d'un client	2	3	6	9	3
	22	Non respect des délais de vérification des documents	1	4	4	6	6
	23	Erreur de saisie	3	2	6	9	6
	24	Application des incoterms interdits en Algérie	1	4	4	6	3
	25	Perte ou détérioration des documents originaux	2	3	6	9	6
	26	Non respect des délais d'envoi des réserves à la banque notificatrice	4	3	12	16	9
	27	Erreur dans le report de domiciliation	2	4	8	9	9
	28	Défaut de programmation d'un règlement	3	4	12	16	9
	29	Défaut de restitution PREG	4	3	12	16	6
Annulation CREDOC Apurement de l'opération	30	Erreur de saisie lors de l'annulation de CREDOC	3	4	12	16	6
	31	Erreur sur la déclaration	2	3	6	9	9
	32	Défaut des documents	2	4	8	9	6
	33	Déclaration tardive	1	4	4	6	6
	34	Défaut de déclaration	3	3	9	9	9

Source : élaboré par les chercheurs.

Commentaire :

Le tableau ci-dessus nous a permis d'obtenir une notation des risques nets. A ce niveau, il est nécessaire de focaliser notre attention sur les risques nets notés « Majeurs », pour pouvoir par la suite proposer des plans de réduction des risques. Les risques « Majeurs » qu'encourt la banque Natixis Algérie selon cette simulation sont :

- Falsification des documents ;
- Domiciliation d'un produit prohibé ;
- Panne du système informatique ;
- Fraude au pli cartable ;
- Non respect des délais d'envoi des réserves à la banque notificatrice ;
- Défaut de programmation d'un règlement ;
- Défaut d'une restitution PREG ;
- Erreur de saisie lors de l'annulation CREDOC ;
- Erreur dans le contrôle des documents.

4. Représentation graphique et interprétation des résultats :

Les résultats présentés ci-dessous vont nous permettre de calculer les taux de couverture des risques et de concentration, ainsi que de les interpréter afin de mieux comprendre la situation de la banque, et de faciliter la mise en place des plans d'action visant à améliorer cette situation. De ce fait, la représentation graphique des résultats obtenus s'avère le meilleur moyen pour l'interprétation des résultats.

4.1 Représentation des résultats consolidés :

Nous avons effectué dans un premier lieu une consolidation des risques identifiés par phase dans le but de montrer les étapes les plus risquées du processus. On a calculé le taux de couverture des risques qui nous permet de déterminer l'efficacité et la qualité des DMR existants, les formules de calcul de ces taux sont données comme suit :

Ainsi que le taux de concentration des risques nets, qui nous permettra de montrer les phases les plus exposées aux risques. La formule utilisée est la suivante :

Les résultats sont exposés dans le tableau ci-après :

Tableau 12 : Grille de consolidation des notes des risques par étape.

Etape du processus	Risque brut	Risque net	Taux de couverture des risques	Taux de concentration du risque net
Domiciliation des opérations	77	54	29%	23.08%
Ouverture CREDOC	77	54	29%	23.08%
Réalisation CREDOC	120	75	37.5%	33.34%
Annulation CREDOC	32	12	62.5%	5.13%
Apurement des opérations	33	30	10%	13%
Total	339	225	33.63%	100

Source : élaboré par les chercheurs.

Pour faciliter la lecture de ce tableau nous avons opté pour une représentation sous forme de secteur afin de montrer les phases les plus exposées au risque.

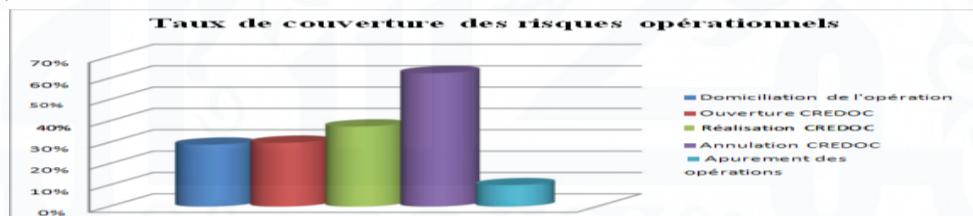
Graphique 1 : Représentation schématique de la contribution des risques nets dans chaque étape de processus.
Taux de concentration des Risques nets



Source : élaboré par les chercheurs.

Le schéma ci-dessus montre que la phase la plus risquée du processus CREDOC est la réalisation du CREDOC avec un taux de concentration des risques nets de 33.34%, alors que le DMR arrive à couvrir seulement 37.5% de ces derniers. Cependant les autres processus sont jugés moins risqués comparés au processus de réalisation avec des taux de concentration qui varient de 5% à 23. Pour mieux visualiser le degré de maîtrise du risque par les contrôles dans chaque étape du processus nous avons représenté les taux de couverture des risques comme suit :

Graphique 2 : Représentation schématique du taux de couverture des risques dans chaque étape du processus CREDOC :



Source : élaboré par les chercheurs.

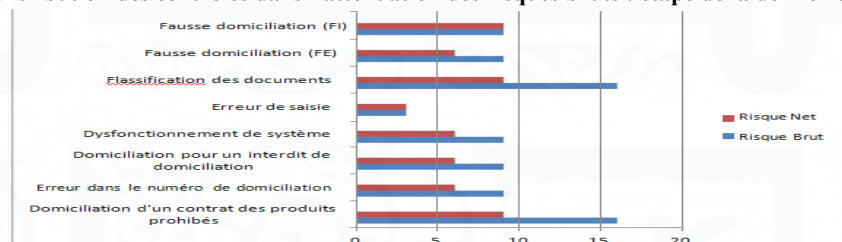
D'après ce graphique on peut constater que les contrôles sont les plus performants dans la phase d'annulation CREDOC avec un taux de couverture de 62.5%. La couverture des risques liés aux phases de domiciliation des opérations et d'ouverture et réalisation CREDOC s'élève à 29%, 29%, 30% respectivement. Le contrôle s'avère très pauvre concernant la phase d'apurement.

4.2 Représentation des résultats par étape du processus CREDOC :

Cette méthode qu'on a élaboré ne permet pas seulement de déduire les risques bruts et nets réellement supportés par la banque en matière de domaine mais on peut aussi les détailler plus pour chaque étape du processus de ce dernier. Pour cela nous avons représenté les risques bruts et nets de chacune dans un graphique comme suit :

4.2.1 Etape de la domiciliation des opérations :

Graphique 3 : Contribution des contrôles dans l'atténuation des risques bruts : étape de la domiciliation des opérations.



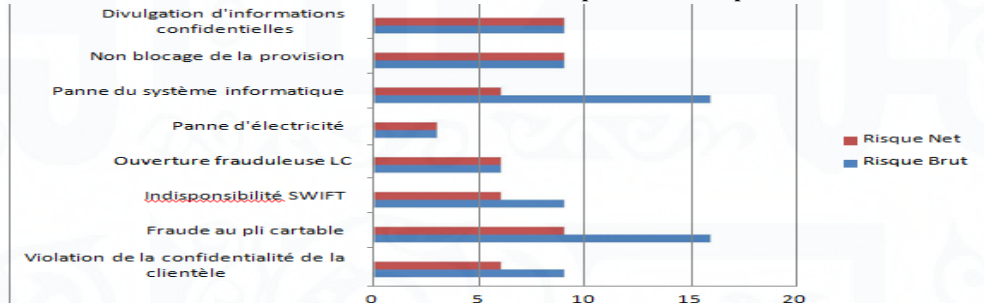
Source : élaboré par les chercheurs.

Dans la phase de la domiciliation des opérations tous les risques relevés ont un impact brut important, à l'exception des erreurs de saisie. On peut constater que les DMR ici

couvrent partiellement les risques qui sont jugés significatifs en les rendant moins dangereux pour la banque, et diminuant leurs impacts.

4.2.2 Etape de l'ouverture CREDOC :

Graphique 4 : contribution des contrôles dans l'atténuation des risques bruts : étape de l'ouverture CREDOC :

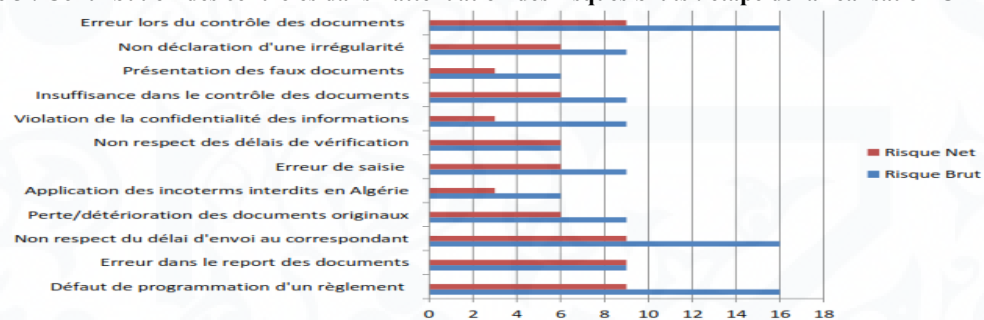


Source : élaboré par les chercheurs.

Cette figure montre que les risques bruts les plus importants liés à l'étape de l'ouverture CREDOC se manifestent à travers : les divulgations d'informations confidentielles, non blocage de la provision sur le compte PREG, panne du système informatique, indisponibilité SWIFT, fraude au pli cartable, et la violation de la confidentialité de la clientèle. Le dispositif de contrôle arrive à maîtriser les risques liés à : la panne du système informatique, indisponibilité SWIFT, et la violation de la confidentialité de la clientèle.

4.2.3 Etape de la Réalisation CREDOC :

Graphique 5 : Contribution des contrôles dans l'atténuation des risques bruts : étape de la réalisation CREDOC.

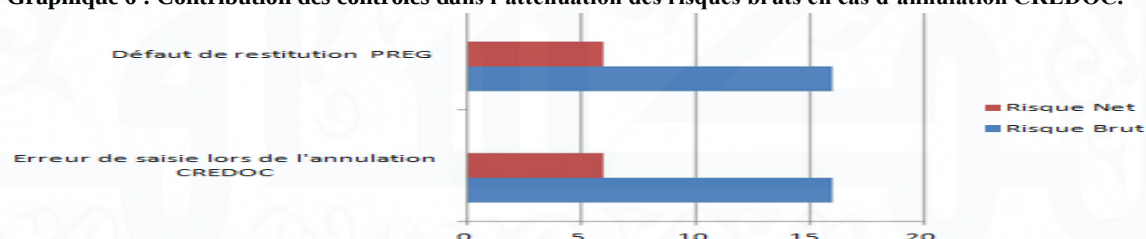


Source : élaboré par les chercheurs.

La figure ci-dessus montre que les risques bruts les plus importants auxquels Natixis Algérie peut être exposée lors de la réalisation des CREDOC sont liés : aux erreurs lors de contrôle des documents, au non déclaration d'une irrégularité, à l'insuffisance dans le contrôle des documents, à la violation de la confidentialité des informations d'un client, aux erreurs de saisie et aux erreurs dans le report des documents, aux pertes/détériorations des documents originaux, et enfin au défaut de programmation d'un règlement. Au niveau de cette étape la qualité de DMR associés est bonne et permet de réduire les risques bruts afin de limiter les risques qui menacent réellement la banque. Si on prend à titre d'exemple les risques liés aux erreurs lors de contrôle des documents qu'ils étaient considérés élevés et ils peuvent entraîner des pertes financières directes pour la banque et se sont devenues moyennes après la confrontation de contrôle.

4.2.4 Etape de l'annulation CREDOC :

Graphique 6 : Contribution des contrôles dans l'atténuation des risques bruts en cas d'annulation CREDOC.

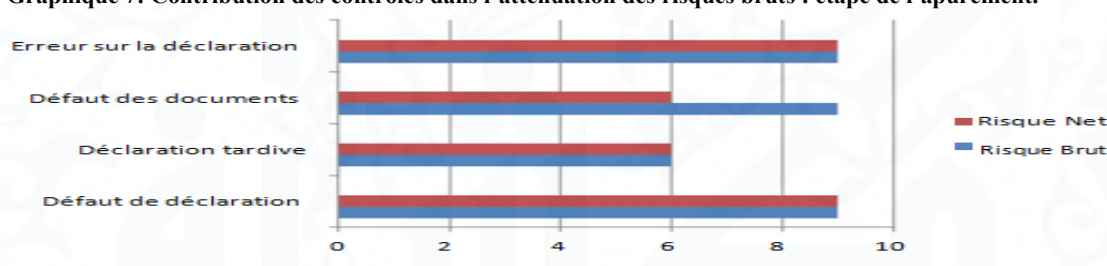


Source : élaboré par les chercheurs.

Dans le cas où le crédit documentaire fait l'objet d'une annulation, il n'y a aucun risque majeur qui puisse être détecté.

4.2.5 Etape de l'apurement des opérations :

Graphique 7: Contribution des contrôles dans l'atténuation des risques bruts : étape de l'apurement.



Source : élaboré par les chercheurs.

Tous les risques liés à l'apurement des opérations sont importants, et les dispositifs de contrôle qui y sont associés sont tous insatisfaisants, et ne font diminuer aucun de ces risques, à l'exception des défauts des documents. Ce qui rend les risques relatifs aux retards, défauts des déclarations, et erreurs sur les déclarations graves sont les sanctions imposées par la banque d'Algérie dans le cas de survenance de ces risques. Ces sanctions peuvent atteindre parfois plusieurs millions de dinars de pénalité.

5. L'utilisation des indicateurs clés des risques (KRI) :

Les indicateurs clés des risques présentent des outils de détection et de préventions qui doivent être mis en place, le choix de ces indicateurs se fait de telle sorte à ce qu'ils offrent une vision globale sur l'évaluation des risques opérationnels liés aux processus « crédit documentaire ». Nous pouvons présenter dans le tableau suivant, le choix de ces indicateurs :

Tableau 13 : le choix des indicateurs

Risque	Seuil	Action
Faible	De 10% à 40%	Pas de dispositions nécessaires
Moyen	De 40% à 60%	Risques à suivre (vérifier la nécessité de disposition de réduction du risque)
Fort	De 60% à 80%	Dispositions nécessaires pour réduire le risque
Critique	Plus de 80%	Des dispositions d'urgence sont nécessaires pour le réduire

Source : élaboré par les chercheurs.

Nous pouvons proposer dans ce cadre les indicateurs suivants :

Tableau 16 : Exemple d'indicateurs clés des risques processus « crédit documentaire ».

Risque	KRI	Périodicité	Seuil			Seuil
			Acceptable	D'alerte	De critique	
Falsification des documents	Nombre d'alerte aux opérations soupçonnées de fraude	trimestrielle	30%	10%	20%	60%
Domiciliation d'un produit prohibé						
Fraude au pli cartable						
Erreur de saisie lors des contrôles des documents	Nombre d'erreur dans la réalisation de CREDOC	Trimestrielle	15%	20%	35%	70%
Non respect du délai d'envoi des réserves à la banque						
Panneau de système informatique	Nombre d'interruptions du système informatique	Semestrielle	5%	10%	20%	35%

Source : élaboré par les chercheurs.

6. Recommandations :

Dans le but de mener à bien le dispositif de gestion des risques opérationnels au sein de Natixis Algérie, et pour éviter la confrontation à certains obstacles et difficultés, il est primordial de recommander certaines solutions, à savoir :

- Définir une nomenclature des risques qui soit plus adaptée à son environnement et à ses activités ;
- Formation des opérationnels sur le thème : la banque doit veiller à ce que son personnel maîtrise la notion du risque opérationnel, afin qu'il puisse s'auto contrôler et éviter de ce fait la survenance des différentes erreurs opérationnelles liées à leurs opérations et pouvant causer des pertes pour la banque. La formation concerne également les managers opérationnels, afin qu'ils puissent maîtriser les différents risques opérationnels qui peuvent survenir dans tous les départements de la banque.
- Favoriser le principe de la séparation des tâches et du contrôle à quatre yeux (deux niveaux de contrôle) et à six yeux (trois niveaux de contrôle).

Conclusion :

L'environnement économique d'aujourd'hui est devenu plus complexe et plus sophistiqué, ce qui rend les banques plus exposées aux divers risques, parmi eux les risques opérationnels.

Après une étude détaillée qui nous a permis de répondre aux questions secondaires émises au début. En effet, la première hypothèse a été confirmée, L'activité bancaire est l'une des activités les plus risquées, les risques qui menacent le bon fonctionnement de cette dernière sont classés sous trois catégories à savoir : le risque de crédit, le risque de marché, les risques opérationnels qui ont été intégré en 2006 au dispositif de Bâle II, et incluent le risque juridique, mais excluent le risque stratégique et de réputation. Concernant la deuxième hypothèse elle a été aussi confirmée. la couverture de ces risques se fait par le contrôle interne en mettant en place des plans de continuité d'activités, mais aussi par le contrôle externe qui peut se faire par l'assurance en prévenant la survenance de certains risques. Tandis que la troisième hypothèse est partiellement confirmée. Car Natixis Algérie a mis en place un dispositif de gestion des risques opérationnels qui permet l'efficacité de cette dernière, ainsi leurs évaluations inhérentes aux activités qu'elle exerce.

Références :

- 1- Christian JIMNEZ et Patrick MERLIER et Dan CHELLY, « **Risques opérationnels de la mise en place du dispositif à son audit** », Edition Banque Edition, Paris2008, p 21.
- 2- Serge DRABCZUK, Séminaire « **risque opérationnel et contrôle interne** », avril 2008.
- 3- KPMG, **Cartographie des Risques**, Institut Algérien des hauts Etudes Financiers,Alger, 22 mai 2014, p24.
- 4- idem, p64.
- 5- Christian JIMNEZ et Patrick MERLIER et Dan CHELLY, **opcit**, p68.
- 6- C.JIMENEZ, P.MERLIER, « Prévention et Gestion des risques opérationnels », Edition Revue Banque, 2004, p37.
- 7- Idem, p 40.
- 8- Ariane CHAPELLE, George HUBNER et Jean-Philippe Peter, « le risque opérationnel : implication de l'accord de Bâle pour le secteur financier », 2 février 2005, p169.
- 9- Comité de Bâle sur le contrôle bancaire : « **saine pratique pour la gestion et la surveillance du risque opérationnel** », Février 2003, p7.
- 10- Ariane CHAPELLE, George HUBNER et Jean-Philippe Peter, **OPCit**, p 169.
- 11- Idem, p 170.