International Journal of Business Marketing and Management (IJBMM)
Volume 8 Issue 5 Sept-Oct. 2023, P.P. 166-178
ISSN: 2456-4559
www.ijbmm.com

La performance opérationnelle des banques marocaines : indicateurs à améliorer et remèdes en cas de l'infogérance

Directeur de la thèse : Docteur Rachid MCHICH
Professeur d'Enseignement Supérieur à l'ENCG Tanger - Université Abdelmalek Essaadi

Doctorant : Abdelmoujib BENDRISS AMRAOUI
Tél : 06 60 00 59 95 / E-mail : moujib.amraoui@yahoo.com
CED : Droit, Economie et Gestion –
Formation Doctorale : Economie, Gestion et Développement Durable
ENCG Tanger - Université Abdelmalek Essaadi

Résumé

La performance est une notion polysémique, complexe et difficile à définir. Elle s'appuie largement sur les notions d'efficacité et d'efficience et elle est la plupart du temps centrée sur la seule dimension financière. En effet, à une ère où la concurrence s'exerce sur plusieurs facteurs et où les risques se multiplient, la réussite de la banque ne se traduit plus en termes d'augmentation des bénéfices. Ainsi la performance devient un concept multidimensionnel qui intègre différentes dimensions pour la définir et différents indicateurs de mesure.[1]

La performance est à la fois multidimensionnelle et subjective, c'est-à-dire qu'elle ne peut être définie d'un seul point de vue opérationnel, social, environnemental ou financier, mais comme un mélange de toutes ces dimensions. Or, une amélioration de la performance environnementale, par exemple, se fait parfois au détriment de la performance financière (Berland et de Rongé, 2013)[2]

La performance opérationnelle est l'une des nouvelles mesures qui sont introduites dernièrement, elle est fondée sur la bonne utilisation des ressources mobilisées dans la production d'activité, elle se concentre sur la position de l'action, l'introduction de nouveaux produits, la qualité des produits, l'efficacité opérationnelle et la satisfaction du client.

Tchankam (2000)[3] *définit l'entreprise performante comme celle qui fait mieux que ses concurrents sur le court, moyen et long terme.*

[1] « LA PERFORMANCE DE L'ENTREPRISE : UN CONCEPT COMPLEXE AUX MULTIPLES DIMENSIONS » Projectique 2017/2 (n°17), pages 93 à 103 -Zineb Issor
[2] « Contrôle de Gestion : perspectives stratégiques et managériales » - 2ème édition (N Berland et Y de Rongé) 2013
[3] « Intelligence économique et performance des entreprises : le cas des PME de haute technologie », Saida Habhab–Rave, 2007/1 (N° 174 – 175), p. 100-118

Les banques s'inspirent du domaine militaire. Elles ne sont pas en guerre mais se battent toujours pour améliorer leur performance. Alors si elles arrivent à améliorer leur performance opérationnelle ca va impacter positivement leur performance globale.

Nous soulignons également l'intérêt opérationnel de cette nouvelle mesure de la performance ainsi son impact sur la prise d'une décision stratégique voire l'externalisation du système d'information.

Cet article vise à étudier les différents indicateurs de la performance opérationnelle des banques marocaines et comment les améliorer en cas de l'infogérance ?

Notre travail s'insère dans le cadre de la recherche de la performance opérationnelle des banques marocaines. Pour assurer sa pérennité, une banque doit être performante opérationnellement. Elle doit, entre autre, faire face à plusieurs risques et en particulier le risque de l'infogérance.

L'intérêt de cette recherche est double :

- *Le 1er est d'ordre pratique : pour démontrer l'importance des mesures opérationnelles de la performance au sein de la banque marocaine.*
- *Le 2ème est d'ordre méthodologique : pour améliorer la capacité d'une banque à atteindre ses objectifs stratégiques en faisant bon usage des ressources à disposition.*

***Mots clés** : Risque, Infogérance, Banque, Performance Opérationnelle, Client*

Abstract

Performance is a polysemous notion, complex and difficult to define. It is largely based on the notions of effectiveness and efficiency and it is most of the time centered on the financial dimension alone. Indeed, in an era where competition is exercised on several factors and where risks multiply, the success of the bank is no longer reflected in terms of increased profits. Thus performance becomes a multidimensional concept which integrates different dimensions to define it and different indicators of measure.

Performance is both multidimensional and subjective, that is to say, it cannot be defined from a single operational, social, environmental or financial point of view, but as a mixture of all these dimensions. However, an improvement in environmental performance, for example, sometimes comes at the expense of financial performance (Berland and de Rongé, 2013)

Operational performance is one of the new measures that are introduced recently, it is based on the good use of resources mobilized in the production of activity, it focuses on the position of the action, the introduction of new products, product quality, operational efficiency and customer satisfaction.

Tchankam (2000) defines a successful company as one that does better than its competitors in the short, medium and long term.

Banks take inspiration from the military field. They are not at war but are always fighting to improve their performance. So if they manage to improve their operational performance it will have a positive impact on their overall performance.

We also highlight the operational interest of this new performance measurement and its impact on strategic decision-making or even the outsourcing of the information system.

This article aims to study the different indicators of the operational performance of Moroccan banks and how to improve them in the case of outsourcing?

Our work is part of the research into the operational performance of Moroccan banks. To ensure its sustainability, a bank must be operationally efficient. It must, among other things, face several risks and in particular the risk of outsourcing.

The interest of this research is twofold:

The 1st is practical: to demonstrate the importance of operational performance measures within the Moroccan bank.

The 2nd is methodological: to improve the ability of a bank to achieve its strategic objectives by making good use of the resources available.

***Keywords**: Risk, Outsourcing, Bank, Operational Performance, Customer*

I. Introduction

Ayant des répercussions sur les entreprises, et aussi sur les clients, seuls ou associés à d'autres risques, les risques de l'infogérance peuvent impacter l'atteinte des objectifs d'une banque, voire mettre en question sa survie. Les enjeux liés à la maîtrise de ces risques sont donc bien réels.

Cependant, la sophistication accentuée des produits et l'apparition de nouvelles technologies, ou encore la complexité et l'interconnexion des activités et services sont autant de facteurs qui rendent le spectre des risques de l'infogérance plus large, tant en termes de fréquence que de sévérité des évènements ; d'où la nécessité de mieux les cerner dans toutes les composantes.

Vue l'importance et l'impact des risques de l'infogérance sur la performance opérationnelle des banques quand ils surviennent, la problématique de notre recherche consiste à exposer les facteurs de succès de la gestion des risques de l'infogérance ainsi les conditions d'amélioration de la performance opérationnelle. Alors cet objectif nous amène à répondre aux interrogations principales : Comment se manifestent les différents risques d'infogérance auxquels s'exposent les banques ? Quelles sont les répercussions de ces risques sur leur performance opérationnelle ?

En conséquence, la gestion qui met l'accent sur l'identification des risques et la mise en œuvre de meilleures pratiques pour y faire face, améliore la prise de décision et, ce faisant, augmente la probabilité d'atteindre avec succès ses objectifs. C'est pourquoi la gestion des risques doit être considérée parmi les priorités dans la stratégie de toute banque.

A cet effet, il s'avère indispensable d'étudier d'abord les facteurs de succès de la gestion des risques de l'infogérance, avant de découvrir les conditions d'amélioration de la performance opérationnelle.

II. Les facteurs de succès de la gestion des risques de l'infogérance

La gestion des risques de l'infogérance par les banques a évolué depuis ces dernières années dont la (prévention / gestion) porte sur des aspects essentiels tels que :

- La surveillance des risques de l'infogérance par les organes d'administration et de direction,
- Le système d'identification, de mesure, de suivi, de maîtrise et d'atténuation de ces risques,
- Le contrôle du système de gestion de ces risques,
- L'établissement d'un plan de continuité d'activité.

1. Mise en place d'un environnement adéquat pour la gestion des risques de l'infogérance

Le Conseil d'Administration doit être au courant des principaux risques de l'infogérance de la banque en tant que catégorie de risques nécessitant une gestion spécifique, et doit approuver et revoir régulièrement la structure et l'organisation de la fonction de gestion de ces risques. Il doit fournir une définition consolidée des risques de l'infogérance et en déterminer les principes d'identification, de mesure, de suivi, de contrôle et d'atténuation.

Aussi, le Conseil d'Administration doit s'assurer que la gestion des risques de la banque est soumise à des audits internes pertinents et exhaustifs par des personnes indépendantes, formées et compétentes.

Les banques doivent donc mettre en place un audit interne permettant de vérifier que les politiques et procédures en matière d'exploitation ont bien été appliquées. Il incombe au conseil d'administration d'assurer que la portée et la périodicité du programme d'audit soient appropriées aux risques courus. L'audit doit valider périodiquement que le cadre de gestion des risques de la banque est effectivement impliqué dans l'ensemble de celui-ci.

Par ailleurs, la direction générale doit mettre en place une structure pour l'organisation de la fonction de gestion des risques telle qu'approuvée par le Conseil d'Administration. Ce cadre doit être mis en place dans la banque, et l'ensemble du personnel doit être informé de ses responsabilités en matière de gestion des risques. Le management doit également être en charge du développement de politiques, processus et procédures de gestion des risques pour tous les processus et activités des systèmes d'information de la banque.

2. Les conditions de réussite du processus de la Gestion des risques de l'infogérance

Les banques doivent identifier et mesurer les risques inhérents à tous leurs produits, activités, processus et systèmes informatiques. Les banques doivent également s'assurer qu'avant toute externalisation de nouvelles activités, ou processus, que les risques qui leur sont inhérents, ont fait l'objet de procédures d'évaluation adéquates.

En effet, l'identification du risque présente une importance primordiale pour le développement ultérieur d'un système de surveillance et de contrôle des risques qui soit viable. Une identification effective du risque porte à la fois sur des facteurs internes (tels que la structure de l'entreprise, la nature de ses activités, la qualité de ses ressources humaines, les changements dans son organisation) et sur des facteurs externes (évolution du métier, avancées technologiques, par exemple) qui sont susceptibles d'affecter défavorablement la réalisation des objectifs de l'entreprise.

Cependant, les banques ne doivent pas se contenter d'identifier les risques; mais il faut évaluer aussi leur vulnérabilité à ces risques. Une appréciation effective des risques permet à la banque de mieux connaître son profil de risque et d'affecter les moyens adéquats pour une gestion efficace.

Les banques doivent mettre en place un processus de surveillance des profils des risques de l'infogérance et des expositions significatives. Un reporting régulier d'informations pertinentes à la Direction Générale et au Conseil d'Administration doit être réalisé de manière à permettre une gestion proactive de ces risques.

Cette procédure de surveillance efficace présente une importance primordiale pour une gestion des risques qui soit adéquate. Une détection et un traitement rapides de ces insuffisances peuvent fortement réduire la fréquence et/ou la gravité d'une perte. La périodicité de la surveillance doit être en fonction de la nature et de la gravité des risques en cause, de la fréquence et de la nature des changements dans l'environnement de la banque et de son prestataire.

D'une manière générale, il faudrait que le conseil d'administration soit destinataire de suffisamment d'informations de haut niveau pour lui permettre de connaître le profil général de la banque au regard des risques de l'infogérance et de se focaliser sur les conséquences matérielles et stratégiques pour l'établissement.

Dans cet objectif, les banques doivent se doter de politiques, de processus et de procédures visant à contrôler ou atténuer les risques de l'infogérance ; elles doivent donc évaluer l'opportunité de stratégies alternatives de limitation et de contrôle des risques et doivent ajuster leur profil de risque à l'aide de stratégies adaptées, en fonction de leur exposition globale aux risques.

En principe, les activités de contrôle sont destinées à traiter les risques qui auront été identifiés par une banque. Pour tous risques tant soit peu importants identifiés par elle, la banque devra décider si elle mettra en œuvre des procédures de contrôle et/ou d'atténuation des risques ou bien si elle supportera ceux-ci.

S'agissant de risques échappant à un contrôle, la banque devra décider si elle les accepte et réduire le niveau de l'activité correspondante ou bien s'en retirer complètement. Aussi, les banques doivent mettre en place des plans de gestion de crise et de continuité d'activité afin de limiter l'impact des dysfonctionnements sur les opérations et de minimiser les coûts en cas de dysfonctionnements majeurs.

En fait, pour des raisons qui peuvent échapper au contrôle d'une entreprise, il se peut qu'une circonstance grave entraîne l'incapacité de cette dernière à s'acquitter de tout ou partie de ses obligations, en

particulier lorsque ses infrastructures physiques ou informatiques ont été endommagées ou rendues inaccessibles. Ce genre de situation peut entraîner des pertes financières significatives, ce qui justifie la nécessité pour les banques de mettre en place des plans de maintien de la continuité de l'activité permettant une reprise du service en cas d'interruption.

En outre, Il convient de prêter une attention particulière à la capacité à rétablir les archives électroniques ou physiques nécessaires à une reprise d'activité. Lorsque ces archives sont doublées de copies de sauvegarde entreposées dans des installations hors site ou lorsque les activités de la banque doivent être délocalisées sur un nouveau site, il conviendra de veiller à ce que ces sites soient situés à une distance suffisante des services affectés, de façon que soit réduit à un minimum le risque d'indisponibilité simultanée des archives et de leurs sauvegardes.

On estime qu'il est de la responsabilité de la direction générale d'établir et de promouvoir une culture de gestion vigoureuse des risques, qui favorise les comportements professionnels et responsables, dans l'ensemble de l'organisation.

D'un autre côté, les banques sont tenues de prévoir dans leurs dispositifs de gestion des risques d'autres composantes fondamentales dont nous allons faire l'analyse dans le point suivant à savoir : la gouvernance[4] et les processus de la Gestion des Risques de l'infogérance.

3. Le cadre organisationnel du dispositif de la gestion des risques de l'infogérance

L'organisation d'un dispositif de maîtrise des risques fait intervenir de nombreux acteurs parce que ces risques se retrouvent à tous les niveaux et dans toutes les fonctions de la banque.

La sensibilité à la prévention des risques est plus forte que l'on réfléchit à la gestion des risques comme à l'un des éléments clés de la performance opérationnelle, le dispositif sera donc plus long à mettre en œuvre car il impliquera d'en faire l'un des éléments de la culture de la banque et de l'inclure très en amont dans la mise en place d'indicateurs permanents.

Le dispositif de base d'une bonne maîtrise des risques doit donc comporter plusieurs éléments qui peuvent se traduire par :

- Une politique bien définie et documentée ;
- Un réseau de responsables en charge de l'animation du dispositif et de leur propre réseau de correspondants au sein de leur structure ;
- Un dispositif d'identification et de gestion des risques au quotidien ;
- La mise en place d'indicateurs avancés pertinents assurant des alertes sur toute perturbation d'un

[4] **La gouvernance** est une notion parfois controversée, car définie et entendue de manière diverse et parfois contradictoire. Cependant, malgré la multiplicité des usages du mot, il semble recouvrir des thèmes proches du « bien gouverner ». Il renvoie à la mise en place de nouveaux modes de pilotage ou de régulation plus souples et éthiques, fondés sur un partenariat ouvert et éclairé entre différents acteurs et parties prenantes.

processus donné ;

- Des reportings adaptés au profil des risques de l'entité ;
- Des évaluations régulières du dispositif par les personnes en charge de son animation et par des intervenants externes.

Cette maîtrise des risques doit se traduire par des plans d'action pour les réduire, les transférer ou les traiter. Alors, Ces plans d'actions peuvent comprendre des actions à entreprendre, des contrôles supplémentaires à mettre en place, et/ou la recherche de transfert financier ou de responsabilité. Les actions « permanentes ou récurrentes » relèvent, en général du dispositif de contrôle interne, s'inscrivant ainsi dans les modes de fonctionnement de la banque.

Dans les faits, il y a des contrôles manuels dont les coûts d'exécution et de surveillance sont généralement élevés et le risque de défaillance est plus important qu'avec les contrôles automatisés. Toutefois, pour que les contrôles manuels soient efficaces, il faut qu'ils soient exécutés correctement et de manière constante.

En revanche, l'automatisation des contrôles préventifs qui sont habituellement moins coûteux et plus efficaces que les contrôles de détection manuels, peut aider à améliorer la gestion des risques et à fournir des données commerciales plus prévisibles et à repérer les opérations non autorisées[5].

En fait, les risques de l'infogérance peuvent être plus prononcés lorsque les entreprises s'engagent dans des activités nouvelles ou développent de nouveaux produits (surtout lorsque ces activités ou ces produits sont étrangers aux métiers de base de l'entreprise), ou s'introduisent sur des marchés qu'elles ne connaissent pas bien et/ou dans des activités éloignées du siège social. De plus, il arrive fréquemment que les dirigeants ne s'assurent pas que l'infrastructure de contrôle de la gestion des risques progresse au rythme du développement des activités de l'établissement.

III. Conditions d'amélioration de la performance opérationnelle

Afin d'améliorer sa performance, une banque doit mettre la gestion des risques au cœur de sa stratégie. Aussi, l'impact économique et juridique des risques seront plus forts si la banque n'a pas, en amont, souscrit les polices d'assurances adéquates, et mis en place un Plan de Continuité d'Activité (PCA) pour gérer de manière efficace les crises imprévues.

1. La communication sur les risques via les reportings[6]

[5] **KPMG,** « Gouvernance, gestion des risques et conformité : Accroître la valeur grâce à la surveillance des contrôles ». Etude organisée par le SERVICES-CONSEILS, page 10.

[6] **Le mot reporting** (en anglais) peut désigner le document analysant et évaluant le fonctionnement et l'activité d'une entreprise dans un ou plusieurs domaines, pour une période donnée. C'est La communication de données qui consiste, pour une entreprise, à faire rapport de son activité.

Lorsqu'on parle de reporting, il est essentiel de connaitre le destinataire ou « client » de ce dernier. En effet, la remontée d'informations, sa synthèse et son traitement ne seront pas les mêmes si le destinataire du reporting est : Bank Al-Maghrib, la direction générale, le responsable hiérarchique, le risk manager ou tout autre acteur du dispositif de gestion des risques.

De même, il faut identifier les attentes vis-à-vis du reporting ; s'agit-il d'une alerte pour action, d'un extrait pour prise de décision ou d'une simple information ?

En d'autres termes, l'utilité et le rôle d'un reporting se matérialise par la définition des objectifs auxquels il doit répondre :

- Pour le responsable d'un processus, le reporting est un outil d'alerte et de prévention pour éviter les situations à risque ;
- Pour le risk manager, le reporting est un indicateur de l'évolution des risques et du degré de leur maîtrise à un instant « t ».
- Quand aux dirigeants, le reporting leur donne une vision synthétique des principales zones de risques, et leur permet la prise de décision sur une base réelle.

Il convient alors, que lorsque la direction générale est destinataire de rapports périodiques sur la gestion des risques, ces rapports doivent contenir des données d'origine interne, ainsi que des données d'origine externe provenant du marché, et concernant les circonstances et les conditions utiles au processus décisionnel.

Aussi, ces rapports doivent être diffusés aux niveaux appropriés de la direction et auprès des secteurs de la banque sur lesquels des zones d'inquiétude sont susceptibles d'avoir un impact.

D'un autre côté, la direction doit vérifier périodiquement et d'une manière générale la ponctualité, l'exactitude et la pertinence des systèmes de déclaration et des contrôles internes, afin d'assurer l'utilité et la fiabilité de ces rapports.

Enfin, pour ce qui est des reportings réglementaires, et dans le prolongement de ses actions visant à aligner la réglementation prudentielle sur les meilleurs standards internationaux, Bank Al-Maghrib a mis en place un nouveau reporting[7]: « Le COREP[8] » (Common Reporting) qui recouvre les informations prudentielles que les banques doivent adresser à Bank Al-Maghrib dans le cadre du dispositif Bâle II. Il s'agit d'un canevas

[7] **Bank Al-Maghreb**, « Rapport de la Supervision Bancaire » - Exercice 2011. Page 16.

[8] **Le terme COREP** est créé par la contraction des termes anglais COmmon solvency ratio REPorting. Il est est l'appellation d'un projet de reporting prudentiel promu par le Comité européen des superviseurs bancaires (CEBS). L'harmonisation du cadre de reporting prudentiel (COREP) a été arrêtée par le Comité des superviseurs bancaires européens (CEBS). Il s'inscrit dans la nécessaire convergence des états réglementaires, qui fait suite à l'application des nouvelles normes IFRS et à la réforme Bâle II. En outre, cette volonté d'harmonisation à l'échelle européenne prend forme au travers d'une préconisation forte en faveur du format de reporting eXtensible Business Reporting Language (XBRL).

formaté dans lequel les établissements bancaires doivent inscrire les renseignements demandés, ce canevas va permettre à Bank Al-Maghrib de comparer et d'analyser aisément les informations mises à sa disposition.

Cependant, l'établissement bancaire conserve le droit de préserver toute information confidentielle dont la divulgation au grand public est de nature à nuire à la conduite de son activité[9].

Par conséquent, la communication financière est un élément clé de la transparence du marché et constitue une condition essentielle de la confiance des clients, de la crédibilité et de la qualité d'une place financière dans son ensemble.

Passer donc de l'information financière à la communication financière, c'est passer d'un reporting chiffré à une véritable stratégie de communication qui repose sur une palette d'outils. Le premier d'entre eux consiste à identifier des cibles de destinataires : actionnaires existants et actionnaires potentiels, susceptibles un jour ou l'autre de remplacer les premiers[10].

En définitive, l'impact économique, juridique et médiatique sera d'autant plus fort si l'entreprise n'a pas, en amont, mis en place un Plan de Continuité d'Activité (PCA) pour gérer de manière efficace les crises imprévues.

2. La gestion de crise par le Plan de Continuité d'Activité (PCA)11

Le Comité de la Réglementation Bancaire et Financière (CRBF) a défini le Plan de continuité d'activité comme un « ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités ».[12]

Aussi, Bank Al-Maghreb[13] exige que les établissements bancaires doivent disposer d'un plan de continuité de l'activité leur permettant d'assurer le fonctionnement continu de leurs activités et de limiter les pertes en cas de perturbations dues aux événements majeurs liés aux risques opérationnels de nature informatique.

Historiquement, les premiers PCA ont été mis en place suite au développement de l'informatique qui

[9] **Bank Al-Maghreb**, « Transparence et diffusion de l'information ». Directive n° 50/G/2007. Op-cit, page 17.
[10] **L'Observatoire de la Communication Financière** « Cadre et Pratiques de Communication Financière » étude réalisée avec la participation de NYSE Euronext en Juin 2011 - Page 5. Pour plus de détails, consultez le site : www.observatoirecomfi.com/
[11] **Le plan de continuité** ou plan de continuité d'activité (PCA) est à la fois le nom d'un concept, d'une procédure et du document qui la décrit. Ce plan doit permettre à un groupe (gouvernement, banque, institution, entreprise, etc...) de fonctionner même en cas de désastre, ou en situation de crise majeure. C'est un document stratégique, formalisé et régulièrement mis à jour, de planification de la réaction à une catastrophe ou à un sinistre grave. Son objectif est de minimiser les impacts d'une crise ou d'une catastrophe naturelle, technologique ou sociale sur l'activité (et donc la pérennité) d'une banque, d'un gouvernement, d'une institution, etc… Ces plans se sont répandus depuis les attentats du 11 septembre 2001, les attentats de Londres (juillet 2005). Les leçons tirées de la catastrophe de Tchernobyl ont également contribué à une profonde révision de certains plans.
[12] **DELAVIS Olivier**, « la préparation d'une place financière à une crise opérationnelle : l'approche française» Bulletin de la Banque de France - N° 174 - Juillet-août 2008, page 2.
[13] **Circulaire BAM n° 40/G/2007.** Op-cit, article 79.

rationalise les activités en les rendant dépendantes des systèmes et les exposent par conséquent à des interruptions de service grandissantes; Puis, cela s'est répandu suite au passage à l'an 2000, puis au passage à l'Euro, et enfin aux attentats du 11 septembre 2001.

Quand au Maroc, il a été le premier pays d'Afrique du Nord[14] à avoir publié une réglementation contraignante au niveau du Plan de continuité d'activité, intégrant la gestion de crise.

D'une manière générale, La continuité d'activité englobe la gestion de crise, la continuité des opérations, la continuité des systèmes d'information et la reprise d'activité.[15]

Par conséquent, un plan de continuité d'activité a pour but d'assurer à la banque la reprise de ses activités suite à un risque potentiel qu'elle pourrait subir et ce, de la manière la plus efficace possible tout en garantissant la continuité des services de la banque, et lui permettre de répondre aux engagements pris à l'égard de ses partenaires et en particulier vis-à-vis de ses clients. Aussi, le PCA permet d'anticiper et maîtriser les risques opérationnels de grande envergure, et d'analyser et réduire les impacts potentiels d'une interruption d'activité.

De ce fait, pour qu'un plan de continuité soit réellement adapté aux exigences de la banque, il doit reposer sur une analyse de risque et une analyse d'impact. L'analyse d'impact consiste à évaluer quel est l'impact d'un risque qui se réalise et à déterminer à partir de quand cet impact est intolérable ?

Les incidents majeurs (catastrophes naturelles, actes terroristes, risques sanitaires…) engendrent de multiples impacts sur la banque :

- Impacts Financiers (pertes de revenus, coûts directs et indirects de la reprise d'activité…),
- Impacts Juridiques (sanctions disciplinaires, financières ou pénales pour non-respect des obligations réglementaires),
- Impacts Commerciaux (pertes de clients, des parts de marché, de partenaires…),
- Impacts d'image (conséquences négatives sur l'image et la réputation de la banque).

On peut diviser la démarche de mise en œuvre d'un PCA en trois grandes phases[16] :

- Identifier les enjeux : phase préliminaire et indispensable qui permet de déterminer les enjeux auxquels doit répondre le PCA (par exemple : garantir le Chiffre d'Affaires, garder la confiance des clients, conserver son image de marque, tenir ses engagements avec ses partenaires en cas de crise…),

- Répertorier les risques : phase qui identifie les menaces et les scénarios qui seront pris en compte dans

[14] **MOUNADI Mohamed**, « Management des risques: Le Maroc à la traîne » journal 'L'ECONOMISTE' du 20 octobre 2008.
[15] **PROST Frédéric**, « Calculer les impacts financiers en cas d'arrêt de l'activité » Revue Banque n° 736 – mai 2011.
[16] **MASANOVIC Serge**, « Le PCA… pour quoi faire ? » journal Finyear publié le 15 décembre 2011.

le PCA. Les scénarios les plus communs envisagent une destruction des bâtiments, une perte du système d'information, des sabotages, des épidémies…,

- ❖ Analyser les impacts sur les activités : phase conduite en collaboration avec le management de chaque métier de l'établissement. Son but est d'identifier les processus sensibles et de déterminer les enjeux et les conséquences de l'arrêt de ces processus en termes d'impacts : financiers, clients, réglementaires….

Ces trois phases doivent mettre en lumière les besoins de continuité de l'établissement bancaire en identifiant les processus critiques qui, en cas de crise, sont les plus sensibles.

Cependant, certains points méthodologiques ne doivent pas être négligés :

- La base documentaire constitue un pilier indispensable à tout PCA : toutes les procédures de continuité seront formalisées (du plan d'alerte, au plan de gestion de crise en passant par le plan de secours informatique). Cette base doit être mise à jour régulièrement, adaptée au contexte, testée et disponible en cas de sinistre auprès de l'ensemble des interlocuteurs concernés par le PCA.
- Le PCA, pour être opérationnel, doit être testé régulièrement. Sa validation va permettre, à travers un exercice, de déceler les incohérences et insuffisances du système défini, d'améliorer les procédures et surtout, d'entraîner et de s'assurer que les acteurs de la continuité d'activité sont formés et familiarisés avec leurs rôles et responsabilités respectives. L'exercice sera réalisé à partir de l'élaboration d'un scénario de sinistre et donnera lieu à un plan d'action d'amélioration du PCA.
- Le PCA doit durer et être maintenu en conditions opérationnelles, au risque de finir au "fond d'un tiroir". La tendance est d'associer le management de la continuité d'activité aux systèmes de management de la qualité, de la sécurité et de l'environnement. Le PCA doit rester à jour par rapport aux processus de la banque et à leurs évolutions (technologiques, économiques, réglementaires…). Ce maintien en conditions opérationnelles doit être planifié et formalisé selon les règles de l'amélioration continue.

Une fois en place, le maintien du dispositif en condition opérationnelle est contrôlé grâce à des tests et assuré par des réactualisations. Plus généralement, au-delà de la seule mise en œuvre d'un dispositif ad hoc[17], c'est une culture de gestion de continuité d'activité qui doit se répandre au sein des institutions financières.

L'irrigation de cette culture au sein du corps social peut s'organiser par la publication de chartes énonciatrices des principes réglementaires et organisationnels de la gestion de continuité d'activité, mais aussi une formation ad hoc devrait être mise au point, adaptée au contexte de l'institution et par études de cas adaptées aux métiers, ou fonctions.

Un PCA Global doit traiter les 4 scénarios suivants[18] :

[17] **Ad hoc** : est une locution latine qui signifie « Qui a été institué spécialement pour répondre à un besoin ». D'une manière qui convient, se dit d'une règle, d'un raisonnement élaborés uniquement pour rendre compte du phénomène qu'ils décrivent, ne permettant donc aucune généralisation. Autre sens : Qui convient parfaitement à une situation, un usage… !

- Indisponibilité des locaux. Exemple: destruction partielle ou totale suite à un incendie.
- Indisponibilité du personnel. Exemple: absentéisme suite à une épidémie.
- Indisponibilité du Système d'Information. Exemple: attaque virale.
- Indisponibilité des sous-traitants stratégiques. Exemple: disparition de sous-traitants clés.

3. La couverture des risques par l'assurance

L'assurance ne réduira pas les risques auxquels est exposée la banque, mais peut être utilisée comme un outil financier de protection contre les pertes associées à certains risques. Cela signifie qu'en cas de perte, la banque obtient une certaine indemnisation financière surtout lorsqu'il peut s'avérer crucial pour la survie de l'activité, par exemple, en cas d'incendie qui détruit le siège social d'une banque[19].

L'enquête du Comité de Bâle[20] sur les risques opérationnels où les données concernant les recouvrements et les remboursements par les assurances ont été présentées en parallèle aux données de pertes proprement dites, montre que de nombreux établissements financiers ont rencontré des difficultés à mettre les données de remboursement des assurances en face des événements de pertes les ayant générés, mais aussi que certaines catégories de risque sont relativement bien couvertes :

La fraude externe et les dommages aux actifs corporels, avec des taux de recouvrement respectivement de 62 % et 72 %. Sur l'ensemble des catégories de risque, le taux moyen de récupération est de 58,4 %. On observe également dans les historiques de pertes internes que la catégorie « dommages aux actifs corporels » est très bien couverte par les assurances, à hauteur de 80 %.[21]

Aussi, nous remarquons que certains risques ne peuvent faire l'objet d'une assurance, tels que les dommages à la réputation et l'image d'une banque. Par contre, l'assurance est obligatoire dans certains domaines (l'assurance responsabilité, l'assurance incendie, l'assurance-vie pour les employés).

IV. Conclusion

Cet article a apporté un éclairage sur l'organisation du diapositif de gestion des risques et son management par les différentes procédures et les divers intervenants. Il a aussi mis en lumière le niveau de développement des technologies de l'information qui demeure un levier de compétition redoutable pour l'avenir des banques. Parmi ses avantages compétitifs, citons la rapidité et la qualité du traitement de l'information relative à la banque et à ses clients, ce qui permet de mieux analyser les attentes et les profils des clients et d'anticiper leurs besoins et partant s'accaparer des parts de marché plus rapidement que ses concurrents.

[18] **MINASSIAN Vazrik**, « Comment réussir le maintien opérationnel de son PCA? » Journées d'Etudes DECISIO Consulting - 1ère édition le 09 avril 2010 à Casablanca.
[19] **Tel a été le cas de l'incendie** du siège du Crédit Lyonnais survenu le 5 mai 1996.
[20] **The 2002 Loss Data Collection** Exercise for Operational Risk:Summary of the Data Collected, Basel Committee on the Banking Supervision, March 2003.
[21] **PENNEQUIN MAXIME**, « Problèmes méthodologiques : le risque opérationnel ». Revue d'économie financière N° 73 – 2003 page 275.

Donc, le revirement stratégique des banques marocaines de dépendre de leurs avantages compétitifs : La taille du réseau, le niveau de développement de la technologie de l'information et la qualité des ressources humaines seront les véritables clés de succès aspirant à une meilleure compétitivité.

Aucune banque n'est à l'abri d'un sinistre, ou d'une interruption de ses services, se préoccuper de la préservation de ses actifs matériels et immatériels devient un enjeu stratégique, il s'avère donc obligatoire de garantir la continuité des activités et les revenus qui en résultent. Pour cela, des mesures sont à prévoir en cas de graves crises ou catastrophes pour maintenir la continuité des activités essentielles dans un premier temps puis pour un retour à une situation normale par la suite.

Quand il est difficile voire impossible de prévoir si un évènement va avoir lieu et quand celui-ci va se matérialiser, la question ne se pose plus sur la probabilité d'occurrence mais sur la continuité d'activité en cas de risque avéré. La question posée est de savoir si la banque est capable de résister lorsque le risque avéré est survenu.

Références bibliographiques

[1]. **ISSOR Zineb**, (2017), « LA PERFORMANCE DE L'ENTREPRISE : UN CONCEPT COMPLEXE AUX MULTIPLES DIMENSIONS », Projectique 2017/2 (n°17), pages 93-103

[2]. **N. Berland & Y. Rongé**, (2013) « Contrôle de Gestion : perspectives stratégiques et managériales » - 2ème édition

[3]. **HABHAB Saida**, (2007), « Intelligence économique et performance des entreprises : le cas des PME de haute technologie », Rave, 2007/1 (N° 174 – 175), p. 100-118

[4]. **DELAVIS Olivier**, (2008), « la préparation d'une place financière à une crise opérationnelle : l'approche française» Bulletin de la Banque de France - N° 174 - Juillet-août 2008, page 2

[5]. **MOUNADI Mohamed**, (2008), « Management des risques: Le Maroc à la traîne » journal 'L'ECONOMISTE' du 20 octobre 2008.

[6]. **PROST Frédéric**, (2011), « Calculer les impacts financiers en cas d'arrêt de l'activité » Revue Banque n° 736 – mai 2011.

[7]. **MASANOVIC Serge**, (2011), « Le PCA… pour quoi faire ? » journal Finyear publié le 15 décembre 2011

[8]. **MINASSIAN Vazrik**, (2010), « Comment réussir le maintien opérationnel de son PCA? » Journées d'Etudes DECISIO Consulting - 1ère édition le 09 avril 2010 à Casablanca.

[9]. **PENNEQUIN MAXIME**, (2003), « Problèmes méthodologiques : le risque opérationnel ». Revue d'économie financière N° 73 – page 275.