UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

ÉCOLE DOCTORALE MATHEMATIQUES ET INFORMATIQUE

Année : 2019

THESE DE DOCTORAT UNIQUE

Présentée pour obtenir le grade de Docteur de l'Université Cheikh Anta DIOP de Dakar

Mention : Mathématiques et Informatique

Spécialité : Informatique

Présentée par :

Marie Elisa Adam NDAW

Titre : Management des risques bancaires de L'UEMOA: Modélisation des risques résiduels

Soutenue le devant le jury composé de :

Président	Diaraf	SECK	Professeur Titulaire	UCAD
Rapporteurs	Bitra	GOORE	Maitre de Conférences	INPHP, Yamoussoukro
	Mamadou	BOUSSO	Maitre de Conférences	Université de Thiès
Examinateurs	Cheikh Thiécoumba	GUEYE	Professeur Titulaire	UCAD
	Seydi Ababacar	DIENG	Maître de Conférences	UCAD
Directeur de Thèse	Samuel	OUYA	Maitre de Conférences	UCAD
Co-directeur de Thèse	Gervais	MENDY	Maître de Conférences	UCAD

Thèse effectuée au sein du :
Laboratoire d'Informatique, Réseaux-Télécoms
(LIRT)

Et

Laboratoire de Mathématiques de la Décision et de l'Analyse Numérique (LMDAN)
Dakar, Fann, UCAD
Sénégal

Management des risques bancaires de L'UEMOA: Modélisation des risques résiduels

Dédicaces

A mes parents, pour leur sacrifice sans limite, leur encouragement et leur accompagnement tout au long de ces années pour mon éducation et ma réussite professionnelle.

A mon mari, pour sa compréhension et son soutien infaillible à tous les niveaux car une thèse est une aventure difficile et délicate, en réalité c'est le couple qui se lance dans le projet.

A mes sœurs, pour leur assistance, leur encouragement et leur disponibilité pour la garde de mes enfants pendant mes week-ends et congés studieux.

Remerciements

Faire une recherche tout en menant une activité professionnelle est un exercice difficile sur le plan organisationnel, personnel et familial. Sans le support constant de mon entourage, ce projet n'aurait pas pu aboutir. Avant d'entamer l'exposé de la synthèse de mes travaux de recherche, je tiens à adresser mes vives et sincères remerciements à tous ceux qui m'ont soutenu et encouragé de près ou de loin.

Mes très sincères remerciements au **Maitre de conférences Samuel OUYA**, Enseignant chercheur à l'ESP et Chef du laboratoire LIRT (Laboratoire Informatique Réseaux Télécoms). Il m'a accueilli au LIRT au tout début de ce projet de recherche malgré toutes mes contraintes professionnelles, me permettant ainsi d'effectuer mes travaux dans un cadre propice à la réussite. Je lui en suis infiniment reconnaissante pour sa disponibilité, sa flexibilité, son soutien infaillible et ses précieux conseils sans lesquels ce projet n'aurait pas pu se concrétiser.

Mes très sincères remerciements au **Maitre de conférences Gervais MENDY**, Enseignant chercheur à l'ESP pour son accompagnement constant depuis toutes ces années. Je lui exprime ma profonde gratitude pour son soutien, ses encouragements, ses observations pertinentes et pour la façon dont il a su me coacher tout en tenant compte de mes contraintes professionnelles.

Je tiens à remercier vivement tous les membres du jury qui ont accepté de prendre part à cette soutenance. Un grand merci **au Professeur Diaraf SECK, au Professeur Cheikh Thiécoumba GUEYE et au Maitre de conférences Seydi Ababacar DIENG** pour avoir consacré du temps dans l'examen, la validation et la signature de mon dossier de demande de soutenance. Ils ont donc valablement contribué à l'aboutissement de ces travaux.

Mes très sincères remerciements aux rapporteurs de cette thèse, **les Maitres de conférences Bitra GOORE** et **Mamadou BOUSSO** pour avoir accepté de rapporter sur mon manuscrit. Je leur en suis très reconnaissante pour leur lecture rigoureuse et leurs observations pertinentes qui m'ont permis d'améliorer le contenu et la qualité de ce rapport.

Le rapport du **Dr GOORE** m'a permis de revoir la structure du chapitre 1 et le titre du chapitre 2, de décliner les avantages et limites de chaque modèle proposé, de motiver le changement de coefficient de maturité d'un modèle à l'autre, de spécifier la façon d'obtenir le nombre de contrôles par risque selon les modèles et le gain de temps moyen octroyé, d'expliquer le choix de la taille des échelles de probabilité de survenance et de gravité potentielle des risques, de justifier la structure des équations de régressions linéaires, etc.

Le rapport du **Dr BOUSSO** m'a permis de spécifier les références ayant permis de définir les modèles proposés et les caractéristiques d'un contrôle, d'indiquer et d'expliquer le rôle de la constante de l'équation 2 ainsi que la nature, la taille et la représentativité des données collectées, de spécifier que les modèles sont créés à partir des données d'apprentissage avant d'être testés sur les données de test et de mesurer l'erreur mais aussi de démontrer l'applicabilité des résultats obtenus, etc.

Mes chaleureux remerciements au **Professeur Seydou KONATE, Aboudramane REHMI, Alex CORENTIN et Ahmadou Bamba MBACKE** pour leur disponibilité, leur sens de l'écoute, leurs conseils avisés et leur soutien permanent.

Je remercie **tous les membres du LIRT** particulièrement au **Dr Ndiaga BA**, pour sa disponibilité, son aide et son assistance. Une mention toute spéciale au **Dr Ibrahima GAYE** pour la pertinence de ses suggestions qui ont considérablement contribué à la qualité de mes résultats. Je lui exprime ma gratitude pour sa disponibilité et son soutien lors de la production de mes documents latex mais aussi pour les démarches administratives.

Mes sincères remerciements au **Directeur Général et au Directeur des Ressources Humaines du GIM-UEMOA** pour m'avoir permis de planifier mes congés en fonction des dates de conférences ou de rédaction du rapport de thèse. Mes chaleureux remerciements aux **Directeurs Mme Fama NDIAYE DIOP et Mr Luc Edmond ADJAHO** pour leurs compréhensions, leurs encouragements et leurs conseils durant les moments difficiles.

Je voudrais également remercier **l'ensemble des membres du CREA** (Docteurs, Enseignants, permanents, chercheurs, doctorants, stagiaires,…) pour leur accueil lors de mon premier exposé et leurs suggestions qui ont permis d'améliorer les modèles.

Je voudrais remercier très sincèrement le **Dr Joseph BASSAMA, Dr Evrad NGOM, Dr Assane GUEYE** pour leurs conseils avisés et leurs apports constructifs mais aussi **Aboudramane KEITA, Annie Teixeira, Maimouna DIA et Mohamed DIA** pour leurs assistances, leurs précieuses relectures et leurs observations pertinentes qui m'ont permis de finaliser certaines publications et de parfaire ce document.

J'adresse mes remerciements à **tous celles et ceux qui, à des titres divers**, ont témoigné de l'intérêt pour ces travaux de recherche. Ils m'ont accueilli et accordé du temps dans le cadre de la collecte de mes données de test et de la réalisation effective des différents tests relatifs aux modèles proposés.

Résumé

De nos jours, les banques sont confrontées à des problématiques nombreuses et complexes dans un monde en perpétuelle évolution. Ainsi, plusieurs types de risques cohabitent dans cet environnement et peuvent avoir des conséquences financières, juridiques, etc. Face aux innombrables risques encourus avec les nouvelles vulnérabilités liées au paiement électronique et à la cybercriminalité, de nombreux contrôles sécuritaires informatiques sont implémentés par les banques en complément aux contrôles existants. Les risques résiduels représentent le niveau de risque qui subsiste après la mise en œuvre des contrôles définis. Leur estimation s'effectue avec la méthode RSCA qui demeure la plus utilisée et qui est basée sur l'AMDEC. Ce dernier procède à l'analyse des modes de défaillance, de leurs effets et leurs criticités. Cependant, cette méthodologie est fastidieuse, requiert plusieurs sessions d'évaluation, nécessite souvent un consensus entre les évaluateurs en cas de désaccord.

Pour traiter cette problématique, nous avons utilisé une approche globale et intégré et avons tenu compte des principes de base de la gestion des risques et du contrôle interne pour définir des modèles mathématiques permettant de calculer les risques résiduels bancaires. Ainsi, quatre modèles mathématiques ont été proposés, il s'agit notamment de deux modèles initiaux basés sur les caractéristiques et la maturité des contrôles mais aussi de deux modèles améliorés axés sur la maturité et les types de contrôles. Par la suite, les modèles initiaux et améliorés sont traduits en équations de régressions linéaires avant de définir les algorithmes y afférents. Pour tester les équations de régressions linaires au niveau de l'outil Eviews, les quatorze tests économétriques préconisés ont été réalisés en utilisant les données d'apprentissage collectées au niveau de quatre banques de l'UEMOA ayant des typologies et des dispositifs de maitrise des risques différents. A l'issu de ces tests, la seconde équation obtient le meilleur résultat avec la réussite de l'ensemble des tests effectués, cela a permis de la valider .Au niveau de l'outil R, les algorithmes correspondants aux modèles mathématiques ont été appliqués sur les risques du système d'information avant d'étendre les tests aux autres risques bancaires. Les valeurs ainsi obtenues ont été comparées aux données de test qui ont été collectées au niveau des banques. Les résultats sont très satisfaisants avec un taux de corrélation moyen égal à 98% pour le modèle 4. L'analyse des valeurs résiduelles a également été effectuée et nous a permis de conclure que les valeurs des modèles couvrent tout le spectre des données de référence. Le modèle 4 est stable et possède le meilleur taux de corrélation moyen, il est donc être le meilleur. De façon générale, les modèles proposés permettent d'automatiser le calcul de la criticité résiduelle des risques bancaires, d'harmoniser les méthodes d'évaluation et de gagner du temps dans l'évaluation des risques résiduels. Ce gain de temps pourra être exploité par les banques pour déployer des contrôles supplémentaires permettant d'améliorer la maitrise de l'ensemble des risques ainsi que la qualité des produits et services bancaires. Cela va entrainer une diminution du taux de fraude, une augmentation des bénéfices de la banque et une meilleure satisfaction des clients.

Mots clés: Risques, contrôles, criticité, modèles, RSCA, AMDEC, sécurité informatique, système d'information

Abstract

Nowadays, banks are confronted with numerous and complex issues in a world in perpetual evolution. Thus, several types of risks coexist in this environment and may have financial, legal consequences, etc. Considering risks associated with new vulnerabilities related to electronic payment and cybercrime, many IT security controls are implemented by banks in addition to existing controls. Residual risks represent the level of risk that remains after the implementation of the defined controls. Their estimation is done using the RSCA method, which remains the most used and is based on FMEA; this method analyzes the failure modes, their effects and their criticalities. However, this methodology requires several evaluation sessions, often requires consensus among the evaluators in case of disagreement.

To address this issue, we have considered the basic principles of risk management and internal control to define mathematical models for calculating banking residual risks. Thus, four mathematical models have been proposed, including two initial models based on the characteristics and maturity of the controls as well as two improved models focusing on maturity and types of controls. Subsequently, the initial and improved models are translated into linear regression equations before defining the related algorithms. To test the linear regression equations at the Eviews tool, the fourthly recommended econometric tests were performed using data of four WAEMU banks. At the end of these tests, the second equation obtains the best result with the success of all the tests carried out, it allows to conclude on its validity. Using R tool, the algorithms corresponding to mathematical models were applied to the information system risks before extending the tests to other banking risks. The obtained values were compared to reference data that were collected at the banks. The results are very satisfactory for model 4 which obtain a correlation rate equal to 98%. Also, residual values analysis was conducted and concluded that model values cover the full spectrum of reference data. Therefore, the model 4 is the best because it is stable and has the best correlation rates with references values. Globally, the proposed models allow automatic calculation of banking residual risks, harmonize evaluation methods and help to save considerable time in evaluation of residual risks. This time saving can be exploited by banks to deploy additional controls to improve mitigation of all risks and quality of services. This will lead decrease of fraud rate, increase of bank's profit and improvement of customers' satisfaction.

Keywords: Risk, Control, Criticality, models, RSCA, FMECA, Information system, Information security

Glossaire

Le risque : Tout évènement susceptible d'empêcher la réalisation d'un objectif, c'est l'effet de l'incertitude sur l'atteinte des objectifs.

La gestion du risque : Ensemble d'activités qui consistent à recenser les risques auxquels l'organisation est exposée, à définir et à mettre en place les mesures appropriées en vue de supprimer ou d'atténuer leurs conséquences.

La gestion intégrée du risque : Gestion des risques qui repose sur une approche globale et continue du risque de toute nature et à tous les échelons de l'organisation.

L'identification des risques : Processus permettant de définir les risques et d'en déterminer les principales caractéristiques à savoir les libellés, les causes et les conséquences

L'évaluation du risque : Processus d'appréciation qualitative et quantitative du risque.

La probabilité de survenance: c'est la possibilité qu'un risque se produise.

La gravité potentielle : c'est l'ampleur, les conséquences négatives associées au risque.

La criticité: c'est la mesure agrégée du risque, elle est le produit de la gravité potentielle et de la probabilité de survenance du risque

La criticité brute : c'est la criticité sans la prise en compte des contrôles à mettre en œuvre.

La criticité résiduelle: c'est la criticité après la prise en compte des contrôles mis en œuvre.

Un contrôle : Ensemble de mesures permettant de maitriser les risques.

Un contrôle préventif : repose sur l'empêchement que le risque se produise.

Un contrôle détectif : repose sur la communication du risque avéré.

Un contrôle correctif : repose sur la prise en charge du risque détecté.

L'appétence au risque : correspond au niveau de risque acceptable par l'entreprise.

La tolérance au risque : correspond au niveau de variation que l'organisation accepte en vue de l'atteinte d'un objectif spécifique.

Cadre organisationnel de management des risques: Ensemble d'éléments établissant les dispositions organisationnelles nécessaires à la conception, à la mise en œuvre, à la surveillance et à l'amélioration continue du management du risque dans tout l'organisme.

Appréciation des risques : processus d'identification, d'analyse et d'évaluation des risques.

Source de risque : tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque à engendrer un risque.

Analyse du risque : processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque.

Niveau de risque : importance d'un risque, exprimée en termes de combinaison des conséquences et de leur vraisemblance.

Traitement du risque : permet de mitiger un risque à travers quatre options de traitement.

Propriétaire du risque : personne ou entité ayant la responsabilité et l'autorité pour le gérer.

Etablissement du contexte : définition des paramètres externes et internes à prendre en compte lors du management des risques et définition du domaine d'application ainsi que des critères de risque pour la politique de management des risques.

Politique de management des risques : programme inclus dans le cadre organisationnel de management des risques, spécifiant l'approche, les composantes et les ressources auxquelles doit avoir recours le management des risques.

Communication sur les risques: processus itératifs et continus mis en œuvre par un organisme afin de fournir, de partager ou d'obtenir des informations et d'engager un dialogue avec les parties prenantes et autres parties, concernant le management des risques.

Partie prenante : personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

Surveillance : vérification, supervision, observation critique ou détermination de l'état afin d'identifier des changements par rapport au niveau de performance exigé ou attendu.

Revue risque : actions entreprises afin de déterminer l'adaptation, l'adéquation et l'efficacité du dispositif pour atteindre les objectifs établis. Ces actions répondent à des règles de gestion, mais également et nécessairement à des règles d'arbitrage.

Règle des 5M : Diagramme Ishikawa basé sur les cinq composants suivants : Milieu, Matériel, Matière, Méthodes et Main-d'œuvre.

Opportunité : Un risque devient une opportunité lorsqu'un évènement incertain, améliore la capacité d'une ou plusieurs ressources, ouvrant de nouvelles perspectives.

Processus : est un ensemble d'activités corrélées ou interactives qui transforment des éléments d'entrée en éléments de sortie, des biens ou des services, cette transformation s'accompagnant d'une création de valeur.

Liste des sigles

UCAD: Université Cheikh Anta DIOP

ESP: Ecole Supérieure Polytechnique

LIRT: Laboratoire Informatique Réseaux Télécoms

LMDAN: Laboratoire de Mathématiques de la Décision et de l'Analyse Numérique

GIM-UEMOA: Groupement Interbancaire Monétique- Union Economique Monétaire Ouest Africaine

RSCA: Risk Self Control Assessment

AMDEC: Analyse des Modes de Défaillance des Effets et de leur Criticité

FMECA: Failure Mode and Effect Criticality Analysis

5M: Milieu, Matière, Matériel, Main d'Œuvre, Méthodes

UEMOA: Union Economique Monétaire Ouest africaine

UMOA: Union Monétaire Ouest africaine

CEMAC: Communauté Economique et Monétaire de l'Afrique Central

GAB: Guichet Automatique Bancaire

DAB: Distributeur Automatique Bancaire

TPE: Terminal de Paiement Electronique

COSO: Committee Of Sponsoring Organizations of the Treadway Commission

COSO ERM: Committee Of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management

DSI: Direction des Systèmes d'Information

RSSI: Responsable de la Sécurité du Système d'Information

COBIT: Control Objectives for Information and Related Technology

ITIL: Information Technology Infrastructure Library

ISO 27001: Norme internationale relative à la gestion de la sécurité de l'information

ISO 22301: Norme internationale relative au système de management de la continuité d'activité

SMSI: Système de Management de la Sécurité de l'Information

SMCA: Système de Management de la Continuité d'Activité

EMV: Europay Mastercard Visa

SDA : sont l'authentification statique des données

DDA: l'authentification dynamique des données

CDA: et l'authentification combinée des données

PCI DSS: Payment Card Industry Data Security Standards

PA-DSS: Payment Application Data Security Standards

PCI-P2PE: Payment Card Industry Point to Point Encryption

PCI PTS: Payment Card Industry PIN Transaction Security

PCI-HSM: Payment Card Industry Host Security Module

SFD: Systèmes Financiers Décentralisés

BCEAO: Banque Centrale des Etats de L'Afrique de l'Ouest

ALM: Asset Liability Management

BIA: Basic Indicator Approach

TSA: Approche Standard

AMA: Approche Mesure Avancée

AMDEC: Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité

HAZOP: Hazard and Operability Study

HACCP: Hazard Analysis Critical Control Points

SDLC: Software Development Life Cycle

FCC: Fédéral Communications Commission

NMLRA: National Money Laundering Risk Assessment

MCO: Moindres carrées Ordinaires

Liste des figures

Liste des tableaux

TABLE DES MATIERES

Introduction générale

Les banques et autres établissements financiers ont toujours été confrontés au risque dans tous les aspects de leurs activités. De ce fait, ils utilisent le concept de risque pour déterminer les taux applicables aux prêts en fonction de leurs propres coûts de financement. Le système bancaire de l'Union Economique et Monétaire Ouest Africaine(UEMOA) a connu de nombreuses mutations depuis les indépendances. Malgré ces mutations salvatrices, les banques sont exposées à des risques élevés pouvant mettre en péril leur solvabilité. Elles sont aussi confrontées à de nombreux défis comme des besoins en financement des PME, de ceux en consommation de sa clientèle, etc.). De plus, les banques doivent accentuer leur rôle dans le développement des entreprises en mettant à leur disposition, une panoplie d'instruments financiers. Elles doivent aussi être capables de développer la banque de détail en pénétrant les segments non bancarisés, notamment celles des zones rurales et en facilitant aussi les financements de masse. Ainsi, ces banques cherchent à pénétrer de nouveaux segments de marché et à toucher des cibles jusque-là exclues du système bancaire. Pour ce faire, elles déploient également des services innovants comme les produits et services monétiques. Elles développent également leur réseau commercial en multipliant les agences et conçoivent des produits adaptés à leurs segments de clientèle. Après l'indépendance, le secteur bancaire africain comprenait uniquement les filiales de banques européennes. Il a fallu attendre les années 1980 pour voir apparaître les banques locales. Suite aux crises généralisées de liquidité et de solvabilité des années 1970 et 1980, le secteur bancaire africain a connu de profondes mutations. Au moment où certaines banques européennes comme le Crédit Agricole quittaient l'Afrique, des groupes locaux, régionaux et multirégionaux se sont progressivement transformés respectivement en groupes régionaux et en groupes bancaires panafricains, grâce à l'émergence de marchés régionaux et de leur intégration financière. De nos jours, le secteur bancaire africain est dominé par quatre types d'acteurs, à savoir les banques européennes, les banques panafricaines à capitaux essentiellement africains, les banques multirégionales et régionales affichant une stratégie d'expansion opportuniste et enfin les banques nationales.

Le dynamisme du secteur bancaire des pays africains est soutenu principalement par la stabilité politique, la croissance de l'économie, la qualité de l'environnement des affaires. Ces dernières années, nous assistons à une évolution des comportements et des modifications structurelles aboutissant à la création des commissions bancaires et la mise en place d'un meilleur suivi des risques dans la plupart de ces banques**[1]** selon le rapport annuel de la Commission Bancaire de 2010. Dans ce contexte, le risque doit être dorénavant au cœur du management de ces banques comme c'est le cas dans les pays européens ou maghrébins. Le pilotage technique est une solution incontournable dans la réalisation de ces challenges. De plus, il répond aux normes de la réglementation locale et aux règles internationales du dispositif de Bâle par extension, permettant de mettre en place des outils

capables de capter efficacement la dynamique des risques de crédit, de liquidité et opérationnel comme indiqué dans l'article de Gbongué **[2]**.

Le risque systémique bancaire est le risque qu'un événement particulier entraine par réactions en chaîne, des effets négatifs considérables sur l'ensemble du système bancaire pouvant occasionner une crise générale de son fonctionnement. Il peut donc mettre en danger la survie du système financier et pour le maitriser, des mesures limitatives et quantitatives comme la séparation des activités bancaires et financières, la limitation du champ d'action des banques ayant des dépôts, l'interdiction de certaines activités sont mises en œuvre. Par ailleurs, suite aux scandales financiers, les pouvoirs publics ont aussi pris conscience que les vulnérabilités des grands groupes pouvaient avoir de graves conséquences dans le cas d'un risque avéré, sur les économies nationales. C'est la raison pour laquelle, des législations ont été adoptées dans le but de garantir la stabilité de l'économie en imposant aux banques de prendre certaines mesures relatives à la gestion de leurs risques financiers. D'où la nécessité de recruter des experts du risque dans les banques. La conception des outils de maitrise de ces risques doit être faite par des spécialistes du domaine. Ainsi, les actuaires et les gestionnaires de risques ont un rôle très important à jouer.

Selon la définition du COSO**[3]**, le management des risques est un processus mis en œuvre par le Conseil d'Administration, la Direction générale, le management et l'ensemble des collaborateurs de l'organisation pour identifier les événements potentiels susceptibles d'affecter la capacité de l'organisation à réaliser ses objectifs et à gérer les risques dans les limites de l'appétence définie. En 2013, Ki-ZERBO analyse le nouveau COSO et ses 17 principes fondateurs, elle spécifie que les objectifs de l'organisation peuvent être stratégiques, opérationnels, de type reporting ou conformité **[4]**. Le dispositif de management des risques peut être évalué sur la base de plusieurs éléments. Il s'agit notamment de l'environnement interne, de la fixation des objectifs, de l'identification des risques, de l'évaluation des risques inhérents et résiduels, du traitement des risques, des activités de contrôle, de l'information, de la communication et enfin du pilotage.

Curtis et Carey procèdent à une analyse en profondeur des pratiques de gestion des risques **[5]**, il en résulte que c'est en analysant les risques dans le cadre d'une perspective globale que le management pourra les gérer de manière optimale en respectant l'appétence définie. Ainsi, les banques recrutent des experts du risque qui intègrent une direction des risques dont le but est de maitriser les risques dans leurs aspects. Il est important de considérer les effets du traitement des risques de façon globale ou agrégée ; dans certains cas, un traitement donné du risque peut ne pas apparaître comme le meilleur ou le plus rentable pour un risque en particulier. Cependant, si ce traitement contribue à gérer d'autres risques, l'avantage qui en découle pour l'organisation peut justifier le choix de cette option. En outre, le système d'information bancaire devient de plus en plus complexe, compte tenu de

l'avènement des produits et services monétiques. Ces nouveaux usages sont à l'origine de plusieurs vulnérabilités exploitables par les fraudeurs.

Par ailleurs, la préoccupation des dirigeants de banques en matière de gestion et de maîtrise des risques est de plus en plus importante, eu égard au contexte économique actuel caractérisé par les précédentes crises mais aussi par l'émergence d'une grande variété de risques. Afin d'assurer la pérennité et l'accroissement de leur part de marché et chiffre d'affaires, il devient impératif pour les banques de mettre en place un dispositif de management des risques plus efficace. En 2011, une circulaire relative à l'organisation du contrôle interne du système de contrôle interne dans les établissements de l'UEMOA est publiée dans le but de maitriser ces nombreux risques de différentes natures et aux conséquences néfastes **[6]**. Le suivi de l'efficacité des dispositifs de contrôle interne et de maitrise des risques représente un challenge certain pour les comités d'audit. A cet effet, les banques ont fait évoluer leur contrôle interne pour assurer une pérennité de leur activité. Le contrôle de la conformité aux normes de la déontologie bancaire a également été introduit, avec pour conséquence le développement des métiers du contrôle dans une problématique d'anticipation et de conseil plutôt que de répression.

L'importance des engagements que les banques et établissements financiers portent et du risque systémique que leur défaillance fait courir à l'ensemble de l'économie justifient la mise en œuvre de telles mesures. Ainsi, l'exercice de la profession bancaire dans l'espace économique et monétaire ouest africain est régi par des dispositions décrites dans l'article relatif aux évolutions de la régulation et de la supervision bancaires publié en 2011 **[7].** Ces dispositions relèvent aussi bien des législations nationales (droit des affaires), que du droit d'essence communautaire (loi bancaire, règlement portant plan comptable bancaire, réglementation prudentielle). Cette réglementation spécifique vise essentiellement à garantir leur solvabilité, leur liquidité, la protection des déposants et, de manière générale, la sécurité du système bancaire dans son ensemble. A cela s'ajoutent, les accords de « Bâle II», qui sont des dispositifs règlementaires élaborés par le Comité de Bâle, comme indiqué dans l'article y afférent publié en 2016 **[8].** Ces accords concernent les établissements financiers et visent à améliorer leur capacité de mesure, de gestion et de couverture de leurs risques afin de préserver leur solvabilité et de renforcer leur stabilité financière. Ils apportent une méthodologie décomposant les risques suivant leur nature et précisant les axes d'amélioration. La principale innovation des accords de Bâle II par rapport à ceux de Bâle I est la prise en compte des risques opérationnels dans le calcul des fonds que les banques doivent immobiliser pour couvrir leurs propres risques. Depuis Bâle II, les banques appliquent le nouveau ratio de solvabilité fondé sur une gestion fine des risques. Bâle III, a davantage renforcé le dispositif de sécurisation de solvabilité et de liquidité des banques, ces aspects sont décrits dans les travaux de Gomes et Wilkins publiés en 2013 **[9]**.

En définitive, il ressort que plusieurs risques cohabitent dans le secteur bancaire et différents types de contrôles sont mis en œuvre par les banques en vue de les maitriser. Malgré la mise en place de plusieurs dispositifs de controles, il subsiste des risques résiduels représentant le niveau de risque qui persiste après la mise en œuvre des contrôles. Il est

donc impératif pour les banques de déterminer leur niveau exact dans l'optique d'implémenter les contrôles appropriés ou supplémentaires permettant de ne pas dépasser l'appétence au risque que la banque s'est fixée.

L'estimation de ces risques résiduels est généralement effectuée avec la méthode RSCA basée sur l'AMDEC qui est essentiellement prédictive et permet l'analyse des modes de défaillance de leurs effets et de leurs «*criticités* ». Lipol et Haq analysent l'utilisation de la méthode AMDEC dans le processus de gestion des risques d'une organisation **[10].** Cependant, il en découle que cette méthode est manuelle, fastidieuse, requiert plusieurs sessions d'évaluation, comporte parfois des erreurs d'estimation et nécessite souvent des compromis de la part des évaluateurs en cas de divergences. Pour venir à bout de cette problématique, nous nous proposons de tenir compte des principes de base de la gestion des risques et du contrôle interne pour proposer des modèles qui mesurent le niveau de risque résiduel en calculant l'impact des contrôles mis en œuvre sur les risques inhérents. L'objectif visé étant d'être plus efficace et efficient dans l'estimation des risques résiduels.

Ce rapport est composé de cinq chapitres. Le premier permettra de se familiariser avec les terminologies et concepts utilisés dans la gestion des risques bancaires. Le deuxième chapitre abordera la problématique liée à l'estimation des risques résiduels dans le secteur bancaire tout en spécifiant les enjeux, la complexité et les difficultés. Au niveau du troisième chapitre, une analyse approfondie de l'état de l'art sera effectuée pour identifier les limites de l'actuelle méthode utilisée pour l'estimation des risques résiduels à savoir le RSCA basé sur l'AMDEC. Le quatrième chapitre va s'appesantir sur notre contribution, à travers l'exposé détaillé des principes utilisés et des spécificités des modèles mathématiques, équations de régressions linéaires et algorithmes ainsi que les équations de régressions linéaires qui ont été proposés. Au niveau du dernier chapitre, nous détaillerons les différents tests réalisés pour éprouver les différents modèles proposés avant validation.

Chapitre I : Métiers et produits bancaires, typologies des risques et contrôle interne

Introduction

Dans ce chapitre, nous commençons par rappeler les différents métiers de la banque ainsi que quelques produits et services. Par la suite, nous expliquerons l'historique, la définition du risque, les typologies de risques bancaires et quelques concepts clés du management des risques. Nous allons également définir les différentes étapes de la gestion des risques ainsi que les méthodes d'évaluation des risques. Au niveau de la dernière partie de ce chapitre, nous parlerons de l'organisation de contrôle interne et de son évaluation afin de définir avec précision la notion de risque résiduel qui fait l'objet de notre recherche.

I.1 Les métiers et produits bancaires

Le secteur bancaire connaît depuis plusieurs années de profondes mutations. Parmi les principales évolutions qui ont eu des conséquences fortes sur les métiers de la banque, on peut citer : le renforcement des obligations réglementaires à savoir la mise en place de Bâle II et Bâle III, le développement des risques, la pression de la concurrence, l'introduction des nouvelles technologies incluant le développement de la banque en ligne et l'évolution de la relation client. Dans ce contexte, le rôle des banques est de plus en plus tourné vers la satisfaction client, le contrôle interne, l'évaluation des risques, la bonne application des règles de déontologie, le pilotage d'activités, la maîtrise des coûts, le conseil et l'expertise, mais aussi l'innovation et l'adaptation à de nouvelles formes d'organisation.

I.1.1 Les métiers de la banque

Les principaux métiers bancaires sont décrits ci-après **[12]** :

a. Banque commerciale

Les services financiers spécialisés sont essentiellement axés sur le crédit à la consommation (Automobile, équipement de la maison, vente par correspondance…), les financements immobiliers, le crédit-bail, l'affacturage et les prêts sur gage.

b. Banque de détails

La banque de détails est destinée aux particuliers, professionnels et entreprises ; elle déploie des agences et banque à distance (internet, mobile) tout en mettant à la disposition de ses clients des services comme les moyens de paiement, les crédits immobiliers et de consommation, l'épargne, le placement, l'assurance dommage et prévoyance, la gestion de patrimoine, etc.

c. Banque d'investissement

La banque d'investissement se caractérise par le profil de ses clients. Ces derniers sont principalement formés d'entreprises et d'investisseurs. Dans ce sens, elle ne reçoit aucun dépôt de particuliers, et œuvre dans l'émission d'emprunt obligataire, la souscription d'action ou encore l'introduction en bourse.

d. Banque de financement

La banque de financement est une banque dont l'activité d'octroi de crédit repose sur l'accompagnement des grandes entreprises, investisseurs institutionnels, collectivités territoriales et États dans leurs opérations financières importantes et complexes, souvent dans un contexte international. Il s'agit notamment des opérations de fusions-acquisitions, de financements structurés, financements de projet et financements export.

e. Banque de marché

Les activités de la banque de Marché portent sur la trésorerie, le change, les matières premières, les dérivés de taux, le trading, la vente et l'arbitrage, les dérivés actions, les indices et fonds, le courtage mais également les activités de la banque d'investissement.

I.1.2 Les produits et services monétiques

De nos jours, les banques mettent à la disposition de leurs clients, divers produits et services monétiques, d'après KORTEX PSI **(2016) [13].** Il s'agit essentiellement des cartes bancaires et des transactions monétiques.

a. Les cartes bancaires

La carte bancaire est un moyen de paiement présenté sous forme de carte plastique, équipée d'une bande magnétique ou d'une puce électronique. Il existe plusieurs sortes de cartes parmi lesquelles on peut citer:

- **La carte de débit**

C'est une carte de paiement qui permet au porteur d'effectuer différentes types de transactions comme le retrait GAB (Guichet Automatique Bancaire), le paiement TPE (Terminal de Paiement Electronique, ou le paiement en ligne et sur mobile avec la possibilité d'utilisation dans un réseau régional ou international.

- **La carte prépayée**

C'est un moyen de paiement qui dérive de la carte de débit. La différence fondamentale est l'absence de connexion avec le compte bancaire du porteur. Elle est communément appelée carte bancaire prépayée ou carte bancaire rechargeable.

- **La carte de crédit**

Elle présente généralement les mêmes caractéristiques que la carte de débit, mais elle est associée à une réserve d'argent, dont l'utilisation induit le calcul d'intérêts. Il s'agit en fait d'une carte de débit dont le débit est différé sur le compte du client, c'est-à-dire que tout achat réalisé à « J » passe sur le compte bancaire *a posteriori* accordant ainsi au client titulaire du compte un crédit de courte durée.

b. Les transactions monétiques

En 2008, VANTET expose en détail les différentes transactions monétiques **[14]. A**insi, le porteur détendeur d'une carte bancaire peut effectuer plusieurs types de transactions, à savoir**:**

- **Transactions GAB**

Un guichet automatique bancaire est un dispositif informatisé qui offre aux clients d'une institution financière la possibilité d'effectuer des retraits d'espèces et de vérifier le solde de leurs comptes sans passer par un employé de banque ou un préposé guichet. Au niveau du GAB, l'utilisateur s'identifie par le biais de la carte bancaire avant de composer un code confidentiel pour s'authentifier.

- **Transactions TPE**

Un terminal de paiement électronique est un appareil électronique capable de lire les données d'une carte bancaire, d'enregistrer une transaction et de communiquer avec un serveur d'authentification à distance via le réseau GPRS ou par internet. Il est souvent accompagné d'un pin-pad permettant au porteur de saisir le code confidentiel.

- **Transactions en ligne**

Parallèlement aux autres canaux de distribution, les banques mettent en œuvre des services de paiement en ligne. Cela permet au client inscrit d'avoir accès à ses comptes et d'effectuer des transactions financières par internet. Dans la zone UEMOA, les paiements en ligne sont pour la plupart de type international, où des porteurs ressortissants de la zone achètent des biens et services sur des sites étrangers en utilisant des ordinateurs ou des mobiles. Pour

l'utilisateur, c'est un gain de temps considérable qu'il mettra à profit pour comparer les prix et les produits des différents sites de vente en ligne.

I.2 Notion et définition du risque

I.2.1 Historique du risque

Le mot français *risque* dérive du latin « *resecare* », qui a donné l'italien « *rischiare* », verbe qui signifie « *oser*» ; il s'agit de faire un choix dans des conditions incertaines, plutôt que de s'en remettre au destin. La clé de cette définition est la notion d'incertitude. Partant de cela, le Committee of Sponsoring Organizations of the Treadway Commission (COSO) définit le risque comme «*la possibilité qu'un événement se produise et ait une incidence défavorable sur la réalisation des objectifs d'une organisation*» **[3]**.

I.2.2 Définition du risque bancaire

Le risque bancaire n'est pas un phénomène récent, les banques et autres établissements financiers ont toujours été confrontés au risque dans tous les aspects de leurs activités selon les travaux de CHELLY et SEBELOUE publiés en 2014 **[11]**. Les banques utilisent le concept de risque pour déterminer les taux applicables aux prêts en fonction de leurs propres coûts de financement.

I.3 Typologies des risques bancaires

Il existe plusieurs types de risques bancaires, les deux principaux sont le risque de crédit et le risque de marché. Avec des économies presque similaires, les banques de l'espace UEMOA présentent le même profil de risques avec quelques petites différences. Les établissements financiers de cette zone présentent un profil de risque légèrement différent. En revanche, elles sont soumises à trois principaux risques à savoir les risques de crédit, de liquidité et opérationnel. La circulaire N°07 relative à l'organisation du système de contrôle interne des établissements de crédit de l'UEMOA et de la CEMAC (Communauté Economique et Monétaire de l'Afrique Central) spécifie les dispositifs de contrôle interne nécessaires à la maitrise des risques bancaires **[15]**. En Afrique subsaharienne francophone, nous pouvons distinguer les principaux types de risques bancaires décrits ci-dessous.

a. Le risque de crédit

En Afrique subsaharienne francophone, les banques sont en majorité des banques commerciales, l'octroi de crédit constitue leur activité principale. Il s'agit du risque le plus important auquel ces banques sont confrontées. Toutefois, l'article 19 de la réglementation du système financier de l'UEMOA résume la vision ultime du régulateur. Il stipule que : «*Les établissements de crédit doivent disposer d'une procédure de gestion du risque de crédit qui tient compte du profil de risque de l'établissement et de politiques et procédures prudentes permettant l'identification, la mesure, le suivi et le contrôle du risque. L'appréciation de ce risque repose non seulement sur la situation financière du bénéficiaire, sa capacité de remboursement et le cas échéant, sur les garanties reçues, mais également, en ce qui concerne les entreprises, sur une analyse de l'environnement, de l'actionnariat et des dirigeants*».

Dans la pratique, la décision d'octroi de crédit est principalement prise en analysant l'historique de la situation du client. Cette analyse porte généralement sur des éléments

quantitatifs et qualitatifs en rapport avec la relation. La banque s'appuie sur son expérience et éventuellement sur des outils statistiques pour son évaluation du risque de crédit.

b. Le risque de liquidité

C'est le risque, pour une banque ou un établissement financier, de ne pas pouvoir faire face à ses engagements financiers ou de ne pas pouvoir dénouer ou compenser une position dans un délai déterminé. La crise de 2007 a montré que les banques sont constamment confrontées au risque de liquidité, et le passage de Bâle II à Bâle III, intégrant principalement des ratios prudentiels de liquidité en est une illustration. La réglementation prudentielle de l'UEMOA aborde la question à l'article 25 : « *Les établissements de crédit doivent disposer de politiques et de procédures pour mesurer et gérer le risque de liquidité, sur une base permanente. Ils doivent à cet effet suivre leurs positions de liquidité au jour le jour et établir des plans d'urgence pour faire face à toute crise de liquidité, sur la base de différents scénarios …* ». En pratique, les établissements de crédit disposent d'une direction financière intégrant généralement une entité trésorerie chargée de gérer au jour le jour la liquidité de la banque, soit en trouvant de la liquidité pour la banque en cas d'indisponibilité, soit en trouvant des opportunités d'investissement en cas de surplus de liquidité.

c. Le risque opérationnel

La réglementation de l'UEMOA définit le risque opérationnel dans son article 26 comme suit : «*En matière de gestion de risques opérationnels, les établissements de crédit doivent définir des politiques et procédures conformes à leur profil de risque et à l'évolution du marché. Ces mesures incluent de manière non limitative, une surveillance particulière des risques de fraudes et de détournements, une couverture adéquate des valeurs par des polices d'assurance, des plans de continuité et de reprise de l'activité en cas de sinistre majeur, un dispositif de sécurité physique et logique du système d'information et des infrastructures de télécommunication, ainsi qu'un encadrement précis des activités externalisées prévenant de manière efficace les pertes opérationnelles. La source de perte la plus récurrente provient principalement des fraudes. Par conséquent, les banques ont d'énormes progrès à réaliser dans ce sens car la banque d'aujourd'hui doit être capable de prévenir les fraudes. Le Comité de Bâle définit le risque opérationnel comme le risque de pertes provenant de processus internes inadéquats ou défaillants, de personnes et systèmes ou d'événements externes*».
Dans ce contexte, les risques opérationnels ont un champ d'application très large et couvrent plusieurs aspects, il s'agit notamment de la fraude interne et externe, de la sécurité de système, des pratiques en matière d'emploi et sécurité sur le lieu de travail, des clients, des produits et pratiques commerciales mais également des dysfonctionnements de l'activité et des systèmes.

d. Risque de marché

Le risque de marché est le risque de perte qui peut résulter des fluctuations des prix des instruments financiers qui composent un portefeuille. Le risque peut notamment porter sur le cours des actions, les taux d'intérêts, les taux de change, les cours de matières premières. Par extension, c'est le risque des activités économiques directement ou indirectement liées à un tel marché. Il est dû à l'évolution de l'ensemble de l'économie, de la fiscalité, des taux d'intérêt, de l'inflation, et aussi du sentiment des investisseurs vis-à-vis des évolutions futures. Il affecte plus ou moins tous les titres financiers.

e. Risque de non-conformité

C'est le risque de réputations, de pertes financiers ou de sanctions résultant de l'inobservation des dispositions légales et règlementaires ainsi que des normes et pratiques applicables aux activités bancaires. Les risques de non- conformité ont pour conséquence des sanctions administratives, judiciaires, disciplinaires ou relatives au non-respect de la déontologie.

f. Risque de concentration

Le risque de concentration est le risque en rapport avec une concentration importante des investissements dans certaines catégories d'actifs ou sur certains marchés. C'est le risque découlant de l'exposition envers les contreparties opérant dans le même secteur d'activités, la même région ou ayant le même produit de base.

g. Risque de taux d'intérêt global

C'est un risque encouru en cas de variations des taux d'intérêts en raison de l'ensemble des opérations bilan et hors bilan. Ce risque est dû à une évolution défavorable de la marge de la banque à la suite d'une évolution des taux d'intérêts du marché.

h. Risque de règlement

C'est le risque encouru au cours de la période entre le moment ou l'instruction de paiement ou de livraison d'un instrument financier vendu ne peut plus être annulée et la réception définitive de l'instrument financier acheté ou des sommes correspondantes.

i. Risque juridique

C'est le risque de litige avec une contrepartie résultant d'une erreur, d'une omission, d'une imprécision susceptible d'être imputable à l'établissement au titre de ses opérations.

I.4 Management des risques

I.4.1 Définition

Le management des risques est un processus permanent mis en œuvre par l'ensemble des collaborateurs à tous les niveaux. Il prend en compte la stratégie de l'organisation et se caractérise par la mise en œuvre à chaque niveau et dans chaque entité, l'assurance raisonnable quant à la réalisation des objectifs, l'identification des événements susceptibles d'affecter l'organisation, l'orientation vers l'atteinte d'objectifs indépendants, l'obtention d'une vision globale de l'exposition aux risques et une prise en compte de l'appétence **[3]**.

I.4.2 Les catégories d'objectifs

Lorsque l'organisation se dote d'une mission et d'une vision, le top management fixe divers objectifs favorables à la réalisation de la mission. Des buts cohérents pour comprendre et traiter les incertitudes susceptibles d'affecter la capacité de l'organisation à atteindre ses objectifs répartis en quatre catégories **[4]**: il s'agit des objectifs stratégiques liés à la stratégie de l'organisation et en phase avec sa mission, des objectifs opérationnels visant l'utilisation efficace et efficiente des ressources, des objectifs de reporting qui peuvent être internes et externes et sont axés sur la fiabilité du reporting et enfin les objectifs de conformité qui visent la conformité aux lois et aux réglementations.

Tout en étant distinctes, ces catégories se recoupent ; un objectif donné peut relever de plusieurs d'entre elles et répondre aux divers besoins de l'organisation. Pour ce qui est de l'atteinte des objectifs liés au reporting et à la conformité aux lois et aux règlements, le management des risques peut donner une assurance raisonnable pour les résultats escomptés. Concernant l'atteinte des objectifs stratégiques et opérationnels, elle dépend parfois d'événements extérieurs à l'organisation. Dans ce cas, le management des risques ne peut donner qu'une assurance raisonnable.

I.4.3 Etapes de la gestion des risques

La gestion du risque relève de la direction générale, il est important qu'elle puisse être intégrée le plus facilement possible et à moindre coût dans le système de management. La politique de gestion des risques découle de la politique de l'organisation; elle est planifiée, mise en œuvre, contrôlée et constamment améliorée. Cette politique a pour but l'amélioration de la marge de manœuvre de l'entreprise, la gestion des risques et des opportunités à l'échelle de l'entreprise, le contrôle du risque pour mieux profiter des opportunités et l'amélioration de la communication.

La première étape de la gestion des risques correspond à la définition de système. A ce niveau des objectifs clairs doivent être fixés par le management. Ces objectifs ne doivent pas uniquement être ancrés dans l'esprit des dirigeants, mais également fixés par écrit. La deuxième étape correspond à l'identification des risques qui permet de lister tous les risques potentiels sous forme de scénario. L'identification des risques consiste à identifier les événements potentiels survenant en interne ou en externe et qui sont susceptibles de nuire à l'exécution de la stratégie et à la réalisation des objectifs de l'organisation. A ce niveau, deux approches sont possibles: l'approche par les objectifs stratégiques permettant de faire une déclinaison des objectifs stratégiques en objectifs opérationnels et d'identifier les risques relatifs à chaque objectif mais aussi l'approche par les processus permettant de réaliser une analyse dysfonctionnelle du processus en identifiant tous les risques susceptibles d'intervenir du début à la fin du processus. La troisième étape consiste à L'analyse du risque à travers l'évaluation des scénarii selon leur probabilité et leur potentiel de dommages ainsi que l'analyse des causes y afférentes. L'évaluation des risques permet de déterminer quand un risque est supportable et peut donc être accepté ou pas. En ce qui concerne la quatrième étape, elle correspond au traitement du risque qui permet d'introduire des mesures pour éviter ou réduire le risque grâce aux informations acquises. A cet effet, un seuil de tolérance de risque est souvent indiqué dans la politique de gestion des risques. Les risques qui sont situés au-delà de ce seuil ne doivent pas être tolérés; par contre, ceux qui sont situés sous ce seuil sont acceptables. Le scénario est évalué selon la probabilité de survenance et la gravité potentielle des risques.

La dernière étape de gestion des risques est relative au contrôle du risque qui consiste à appliquer correctement les mesures de maîtrise du risque par des activités continues ou par des contrôles périodiques. En effet, le risque n'est pas seulement un sinistre soudain, il peut également se manifester sous formes de dysfonctionnements inattendus. De ce fait, le contrôle continu des risques doit se faire en temps réel et s'adapter très rapidement à des conditions qui évoluent.

I.5 Organisation du contrôle interne

Les principaux composants d'un contrôle interne efficace sont décrits ci-dessous **[23]**.

I.5.1 Environnement de contrôle

Il se caractérise par l'intégrité et l'éthique. En effet, il faut s'assurer qu'une parfaite intégrité et de solides valeurs éthiques sont établies et comprises, en particulier chez les cadres dirigeants. Le conseil d'administration est un des composants de cet environnement, il doit comprendre et exercer ses responsabilités de surveillance de l'information financière et du contrôle interne. Il y a également la philosophie et le style de management des dirigeants qui doit favoriser l'exercice efficace d'un contrôle interne à l'égard de l'information financière. De plus, la structure organisationnelle de l'entreprise doit faciliter l'exercice d'un contrôle interne efficace. Quant à l'entreprise, elle doit employer des personnes compétentes pour le traitement optimal de l'information financière. Il y a aussi la délégation de pouvoirs et des domaines de responsabilité, en effet, la direction et les salariés doivent avoir des niveaux d'autorité et de responsabilité appropriés pour faciliter l'exercice d'un contrôle interne efficace. Pour finir, il faut concevoir et mettre en œuvre une politique et des pratiques de gestion des ressources humaines qui permettent d'avoir un contrôle interne efficace.

I.5.2 Évaluation et traitement des risques

L'évaluation des risques consiste à déterminer dans quelle mesure des événements potentiels sont susceptibles d'avoir un impact négatif sur la réalisation des objectifs. Le management évalue la probabilité d'occurrence et l'impact de ces événements. Pour ce faire, il recourt habituellement à une combinaison de méthodes qualitatives et quantitatives. Il convient d'évaluer à la fois les risques inhérents qui représentent le risque brut mais aussi les risques résiduels qui représentent le risque net. De manière spécifique, le risque inhérent **[5]** est celui auquel l'organisation est exposée en l'absence de mesures correctives prises par le management pour en modifier la probabilité d'occurrence ou la gravité potentielle. Il peut être inhérent au modèle économique ou découler des décisions prises par le management sur la manière d'appliquer ce modèle. Suite à l'évaluation des risques, le management détermine les traitements à appliquer à chacun de ces risques. Il convient de considérer l'effet des différentes solutions en termes de probabilité, d'impact, de coûts et de bénéfices. Selon le COSO, il y a quatre options possibles **[24]** : la première option est l'évitement, c'est le fait de cesser les activités qui sont à l'origine du risque. L'évitement peut aussi bien avoir pour conséquence l'interruption d'une ligne de produits, le ralentissement de l'expansion prévue sur un nouveau marché géographique ou la vente d'une activité. La deuxième option est l'acceptation, il s'agit de ne prendre aucune mesure pour modifier la probabilité de survenance et la gravité potentielle du risque. Cela signifie que l'organisation préfère accepter le risque à son niveau actuel plutôt que de dépenser de précieuses ressources pour appliquer l'une des autres options de traitement du risque. Quant à la troisième option, elle fait référence à la stratégie de réduction qui a pour objectif de prendre les mesures nécessaires afin de réduire la probabilité d'occurrence du risque, la gravité potentielle du risque, ou encore les deux à la fois. Il s'agit habituellement d'une multitude de décisions prises quotidiennement comme la mise en place de contrôles. La dernière option de traitement du risque est relative à la stratégie de partage qui permet de diminuer la probabilité de survenance ou la gravité potentielle en transférant ou en partageant le risque. Parmi les techniques courantes de partage du risque, on peut citer l'achat de produits d'assurance, les opérations de couverture ou l'externalisation d'une activité. Pour ce qui est du risque résiduel **[25]**, il représente le risque auquel l'organisation reste exposée après la mise en œuvre des différentes options de traitement définies par le management. En effet,

les risques inhérents sont évalués dans un premier temps, par la suite les risques résiduels seront évalués à partir des réponses du management. Le choix doit porter sur une solution ramenant le risque résiduel en deçà du seuil de tolérance souhaité par le management. Les risques et opportunités sont appréhendés de manière transversale ou agrégée de façon à déterminer si le risque résiduel global correspond à l'appétence de l'organisation.

I.5.3 Les activités de contrôle

Les activités de contrôle sont constituées de politiques et de procédures qui permettent de s'assurer que les options de traitements retenues par la direction ont été effectivement mises en place. Elles sont présentes dans toute l'organisation, à tout niveau et dans toutes les fonctions. Elles englobent diverses activités qui peuvent être préventives ou détectives, manuelles ou automatiques et intervenir au niveau de tous les processus **[26]**. Cette évaluation porte sur plusieurs aspects. D'abord, l'entreprise définit les objectifs relatifs à l'information financière de façon suffisamment claire et établit des critères qui permettent d'identifier les risques menaçant la fiabilité de la communication de l'information financière. Ensuite, l'entreprise identifie et analyse les risques que les objectifs relatifs à l'information financière ne soient pas atteints, en vue de déterminer comment ces risques devraient être gérés ; l'entreprise va aussi mettre l'accent sur les risques de fraude. Les activités de contrôle concernent également l'intégration avec l'évaluation des risques, ce sont des mesures prises pour contrer les risques associés à l'atteinte des objectifs relatifs à l'information financière. Enfin, il y a l'élaboration des activités de contrôle qui sont choisies en fonction de leur coût et de leur efficacité éventuelle dans l'atténuation des risques associés à l'atteinte des objectifs relatifs à l'information financière. Les normes et procédures font parties des activités de contrôles, ils concernent les politiques visant la communication d'une information financière fiable, elles sont mises en place et diffusées à l'ensemble de l'entreprise. Des contrôles liés aux technologies de l'information sont aussi conçus et mis en œuvre pour favoriser l'atteinte des objectifs relatifs à l'information financière.

I.5.4 Information, communication et pilotage

L'information se compose de deux volets essentiels. Le premier volet est relatif à l'information financière, c'est 'information pertinente identifiée, saisie, utilisée à tous les niveaux de l'entreprise et distribuée sous une forme et dans un délai qui permettent l'atteinte des objectifs relatifs à l'information financière. Il y a aussi l'information sur le contrôle interne qui est utilisée pour mettre en application d'autres composantes du contrôle identifiées, saisies et distribuées sous une forme et dans un délai qui permettent aux membres du personnel de s'acquitter de leurs responsabilités relatives aux contrôles internes. Pour ce qui est de la communication, le premier aspect est relatif aux communications internes qui favorisent la compréhension et la réalisation des objectifs alors que le second aspect est lié aux communications externes permettant de communiquer avec les parties externes. Concernant le pilotage, il est axé sur des évaluations continues ou des évaluations distinctes qui permettent à la direction de déterminer si le contrôle interne de l'information financière est effectif et fonctionne de manière adéquate.

I.6 Evaluation du contrôle interne

Les exigences croissantes en termes de qualité comptable et financière ont conduit les banques à renforcer leur démarche de contrôle interne. Une préoccupation légitime de tout dirigeant de banque est de connaître les attentes en matière de contrôle interne pour les confronter à ses propres pratiques. L'objectif des échelles d'évaluation des risques est de répondre à cette attente en permettant, à partir d'un système de cotation, d'évaluer la maîtrise des risques. La maturité d'un contrôle interne peut être appréhendée au travers de trois dimensions : la première concerne les paliers du contrôle interne avec une échelle de maturité qui identifie les étapes successives et logiques dans le renforcement d'un contrôle interne. A partir de cette échelle, il est possible de se positionner sur l'un des cinq paliers allant d'une absence totale de maîtrise à un dispositif optimal permettant un pilotage performant des risques. La seconde dimension est relative à la profondeur du dispositif, en effet, pour chacun des paliers identifiés dans l'échelle de maturité, les trois leviers liés à l'organisation, à la documentation et à la traçabilité peuvent avoir un contenu différent qu'il importe de bien distinguer dans l'appréciation de la maturité du dispositif. La troisième dimension est liée au périmètre et permet de s'interroger sur les processus couverts par le dispositif; les processus peuvent être inégalement couverts par le dispositif de maîtrise des risques.

I.6.1 Les leviers opérationnels

Un dispositif optimisé de gestion des risques doit permettre d'apprécier toutes ces dimensions. Il n'y a pas de dispositif de maitrise des risques type et homogène en matière de contrôle interne; chaque dispositif doit être adapté à son environnement et résulter d'arbitrages du management quant à la décision de couvrir un risque et sur ses modalités pratiques de traitement. Ainsi chaque entité définit la profondeur des mesures de contrôles internes retenus et les processus priorisés pour gérer ses risques. Etant donné que le but de cette échelle de maturité est de permettre à tout responsable de comparer sa démarche de contrôle interne par rapport à un schéma théorique et d'évaluer sa maturité essentiellement dans sa dimension, cette échelle a pour vocation de constituer un outil d'évaluation du contrôle interne pour l'ensemble des banques.
De ce fait, un contrôle interne optimisé se construit dans la durée en franchissant différents paliers. La progressivité de la démarche peut être représentée sous la forme d'une échelle de maturité comportant plusieurs niveaux. Chaque niveau correspond à un degré de maturité supplémentaire intégrant les acquis du palier précédent tout en l'améliorant. Cette échelle de maturité est structurée autour des étapes de la démarche de maîtrise des risques. Elle prend en compte les leviers du contrôle interne rassemblant les différentes composantes du dispositif. Ces leviers opérationnels du dispositif de contrôle interne reposent sur l'organisation de la fonction comptable et financière, la documentation des procédures, la traçabilité des acteurs et des opérations et le pilotage du contrôle interne que sont la cartographie des risques et le plan d'actions à mettre en œuvre.

I.6.2 Les niveaux de maturité

Les leviers opérationnels du dispositif de contrôle interne sont évalués selon l'échelle de maturité à cinq niveaux décrite ci-dessous **[27]**:

- **Niveau 1 (Non fiable):** Il s'agit d'un environnement imprévisible où il n'y a pas d'organisation maîtrisée, ni de procédures définies. Ce niveau est exceptionnel.

- **Niveau 2 (Informel):** L'organisation et les procédures sont définies et mises en place mais restent non documentées de façon adéquate et leur réalisation n'est tracée que de manière aléatoire.
- **Niveau 3 (Systématique) :** Il existe des procédures standards, mais en l'absence d'évaluation, les faiblesses du contrôle interne ne sont pas détectées. Cette situation est la plus fréquente.
- **Niveau 4 (Intégré) :** La surveillance de la conformité aux règles de contrôle interne par des évaluations périodiques est assurée. Les évaluations s'étendent au sens large en intégrant les contrôles de supervision, les audits, les contrôles des comptables sur les opérations ou encore les contrôles de supervision. De plus, l'évaluation de son effectivité et de son efficacité par des tests périodiques permettant d'identifier les points forts et les points faibles est effective. Cependant il n'y a pas reporting à la direction permettant l'adoption de mesures de correction.
- **Niveau 5 (Optimisé):** Il s'agit de l'existence d'un cadre de gestion des risques évolué reposant sur une organisation structurée, des procédures documentées, une traçabilité assurée, la réalisation de tests, la prise en compte des constats des évaluations pour orienter la gestion des risques et prendre, les mesures nécessaires pour corriger les points de faiblesse. Le niveau « d'optimisation » confère à la direction une connaissance précise des risques qui lui permet de piloter le dispositif de contrôle interne en engageant des actions ciblées pour améliorer de manière continue la maîtrise des processus.

1.6.3 Evaluation du contrôle interne

L'évaluation du contrôle interne à l'aide de l'échelle de maturité peut avoir lieu à tout moment. L'échelle de maturité des controles a pour objectif d'apprécier la maturité de la démarche. La profondeur et le périmètre de ces différentes composantes sont également pris en compte. Le dispositif est considéré comme pleinement mature quand il a la capacité de s'autoréguler, c'est-à-dire d'adapter son contenu à l'évolution des risques dans une logique d'amélioration continue. De par sa nature, un contrôle interne n'est pas figé et doit en permanence être ajusté pour permettre une gestion efficace des risques. C'est l'évaluation de cette capacité de pilotage qui est centrale dans cette échelle de maturité. S'il est essentiel d'organiser, de documenter et de tracer les opérations, c'est le pilotage qui permet de déterminer de manière pertinente la profondeur et le périmètre de la démarche de maîtrise des risques. Seule la connaissance et l'évaluation des risques, vont permettre de définir le niveau d'exigence requis pour telle ou telle mesure de contrôle interne pour un processus donné.

L'actualisation des supports formalisant la stratégie de maîtrise des risques de l'entité (cartographie des risques, plan d'actions) peut constituer une opportunité pour évaluer les dispositifs existants. Les résultats de l'évaluation contribuent ainsi à affiner et à objectiver l'analyse des risques menée dans ce cadre. Pour inscrire cette démarche dans une logique d'amélioration continue, il convient d'évaluer au moyen de l'échelle de maturité au début de l'année en cours, les dispositifs de maîtrise des risques mis en œuvre au cours de l'exercice précèdent. Les conclusions de l'évaluation ainsi menée permettront d'enrichir les travaux d'actualisation de la cartographie des risques et du plan d'actions. Compte tenu de la dimension transversale du chantier «Contrôle interne», l'ensemble des acteurs sont amenés à participer à l'évaluation de la maturité de la gestion des risques en jouant un rôle spécifique. Ainsi le risque manager aura la charge de piloter les travaux d'évaluation dans le

cadre des dispositifs de gouvernance mis en place pour la cartographie des risques et le plan d'actions.

Le contrôleur interne sera chargé de la mise en œuvre pratique de l'évaluation, sur la base d'une trame contenue dans un tableur. La participation de ces services se révèle primordiale, dans la mesure où, en tant qu'acteurs chargés des dispositifs de contrôle interne, ils disposent des informations et des éléments probants nécessaires à l'évaluation de ces derniers. Quant au comptable, c'est un acteur majeur intervenant dans la partie aval des processus comptables. Une fois l'évaluation réalisée, le service d'audit interne pourra être consulté, sur la base des éléments de notations et des éléments probants fondant l'évaluation. Les échanges de l'ensemble de ces acteurs doivent permettre de dégager, par corroboration, une notation qui soit la plus objective possible.

Conclusion

Ce chapitre nous a permis de nous familiariser avec les différents métiers de la banque, la notion de risque, les typologies de risques bancaires ainsi que les différentes étapes de gestion des risques. Nous avons également décrit les cinq niveaux de l'échelle de maturité du contrôle interne permettant d'obtenir les risques résiduels à partir des risques inhérents. Etant donné que le risque résiduel correspond au risque qui persiste après la mise en œuvre des différentes contrôles définis par le management, il est impératif pour les banques de déterminer leur niveau exact et de définir des contrôles supplémentaires permettant de les ramener à l'appétence au risque souhaité par le management. Nous allons donc poser la problématique liée à la gestion des risques bancaires au niveau du prochain chapitre.

Chapitre II : Problématique de la gestion des risques bancaires

Introduction

Dans ce chapitre, nous aborderons d'abord la gestion des risques du système d'information tout en spécifiant sa complexité et les conséquences néfastes des risques encourus. Par la suite, nous parlerons de la gestion des risques spécifiques à l'activité bancaire notamment ses enjeux et les évolutions majeures avant de poser la problématique liée à l'estimation des risques résiduels bancaires.

II.1 Gestion des risques du système d'information

II.1.1 Contexte

La conjugaison de nouvelles tâches de traitement de l'information automatisée avec la nécessité de mise à jour technique de leur propre activité développe chez les banques de nouvelles compétences, en termes de contrôle, de gestion des *processus* et modes opératoires, de respect des délais et réglementation, entre autres. Cette évolution technologique pousse souvent au nomadisme numérique et couramment à l'éclatement géographique de l'exercice de certains métiers, nécessitant des déplacements en continu. Par ailleurs, l'impact du multimédia, de l'Internet, des réseaux sociaux sur la relation avec la clientèle, a fait évoluer l'importance du contact humain vers une plus grande valeur ajoutée, dont celle du conseil. Ceci est à mettre en parallèle avec le besoin de transparence revendiqué par le client et son degré d'information personnelle sur les produits bancaires. Ainsi, le client cherche avant tout à faire jouer la concurrence et à rentabiliser au mieux ses opérations bancaires. Il cherche aussi à ne pas perdre de temps dans la réalisation de ses opérations. Dans ce contexte de profondes transformations technologiques et de forte concurrence, les banques ont dû remettre le client au centre de leurs activités. Grâce à des engagements professionnels majeurs, l'information bancaire a été renforcée, rendant plus accessible la relation du client avec sa banque.

II.1.2 Contribution de la DSI dans la gestion des risques

De nos jours, la direction du système d'information (DSI) contribue fortement à la démarche de gestion des risques. Cette contribution s'exerce généralement sous la forme d'une influence directe lors de la mise en œuvre d'une politique globale et intégrée de gestion des risques dans l'entreprise, ou indirectement par la mise en place d'outils, de méthodes ou de formations en support aux activités du gestionnaire de risque. Cela n'empêche pas à la direction du système d'information de participer de *facto* à la démarche d'entreprise par la gestion de ces propres risques liés aux systèmes d'information.
Le niveau de contribution de la DSI dans la démarche de gestion des risques dépend de l'importance pour l'entreprise de «l'information » et du système qui lui est associé, du niveau de maturité de la démarche de gestion des risques mise en œuvre dans l'entreprise et de l'existence d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) dans l'entreprise**[28]**. Au fil des années, il est apparu que plus la production ou l'activité d'une entreprise sont liées à son système d'information, plus la DSI contribue forcément à la démarche de gestion des risques. Cependant, cette participation devient plus faible dans les entreprises où la production est moins dépendante du système d'information.

Il faut noter que pour les entreprises où « l'information » est un produit en tant que tel comme dans les banques, une grande partie des risques est liée au système d'information. La DSI joue alors un rôle important dans la démarche de gestion des risques. Le rôle de la DSI dans la démarche de gestion des risques est inversement proportionnel au niveau de maturité de l'entreprise en matière de gestion des risques. En effet, elle agit souvent comme un moteur dans la mise en place d'une démarche globale de gestion des risques. La prise en compte par les directions métiers de risques qu'elles n'ont pas envisagé peut être aussi favorisée par un questionnement des différents services de l'entreprise lors de la définition d'un plan de secours informatique. Les moyens par lesquels la DSI peut participer indirectement à la démarche de gestion des risques sont nombreux et l'on peut encore citer : la création d'applications informatiques destinées à diminuer certains risques, la vérification du bon fonctionnement de la gestion intégrée, la mise en place d'outils anti-fraude, l'élaboration des indicateurs de conformité requis selon le secteur d'activité, ou encore le développement d'outils consacrés à la gestion des risques **[29]**.

II.1.3 Dispositifs de maitrise des risques spécifiques au système d'information

Un système d'information est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures permettant d'acquérir, traiter, stocker, communiquer des informations sous forme de données, textes, images, sons, etc. A ce titre, le système d'information est stratégique car il doit procurer aux dirigeants les informations nécessaires et fiables et surtout aider à la prise de décision en simulant les conséquences des choix possibles. Au début des années 2000, les risques industriels sont traités dans un contexte de changements technologiques, d'une concurrence féroce et d'une préoccupation croissante du public tout en posant la problématique de la circulation de l'information parmi les décideurs à tous les niveaux de l'entreprise **[30]**. On assiste alors à l'avènement des PGI

(Progiciels de Gestion Intégré) qui présentent néanmoins une incertitude sur le bon déroulement des projets **[31]**.

En 2008, une approche systémique **[32]** ainsi qu'une approche par l'implémentation des métriques de modèles **[33]** sont proposées pour la gestion des risques. En effet, la sécurité des systèmes d'information est de plus en plus abordée à l'aide d'approches basées sur les risques. Le but final visé étant de réduire de manière considérable les pertes liées aux faiblesses de la sécurité des systèmes d'information. Ces faiblesses, lorsqu'elles sont exploitées peuvent être à l'origine de plusieurs risques aux conséquences néfastes comme la diffusion non autorisée d'informations, l'interruption d'activité suite à une défaillance du matériel ou du logiciel ou le comportement désinvolte des utilisateurs. Toujours dans la même optique, DIASIM est développé en 2009 pour tester les risques sur les applications sans les modifier en effectuant davantage de vérifications statiques **[34].** Des méthodes comme MEHARI sont définies et fournissent une base de vulnérabilités, de menaces, de *scenarii* et de services de sécurité **[35]**. Parallèlement, une vue d'ensemble des principaux outils qui pourraient être utilisés dans la gestion des risques qualité par l'industrie et les organismes de réglementation est réalisée **[36]**. En effet, la gestion des risques se définit comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque avec trois principaux objectifs, il s'agit notamment d'améliorer la sécurisation des systèmes d'information, de justifier le budget alloué à la sécurisation du système d'information et de prouver la crédibilité du système d'information à l'aide des analyses effectuées.

La gestion des risques projet est aussi abordée et suggère la mise en avant des objectifs du projet pour assurer sa réussite **[37].** Parmi les risques projets, on peut citer l'échec ou le retard dans la mise en œuvre en raison d'une mauvaise planification et d'un pilotage hasardeux pouvant entrainer des surcouts ou des pénalités**.** C'est dans ce contexte que des logiciels permettant d'automatiser les tests de fonctionnalité sur les applications critiques sont implémentés et déployés **[38]**. A cet effet, une méthode est proposée pour traiter les exigences de sureté de fonctionnement en amont pour un traitement optimal **[39].** Toujours dans ce cadre, un logiciel de gestion électronique de documents est mis en place pour une meilleure visibilité des vérifications et validations effectuées au sein de l'entreprise **[40] ; l**es risques relatifs à l'externalisation du développement d'application sont également traités **[41].** En complément, une analyse des processus d'ingénierie système est proposée pour aider les concepteurs et les ingénieurs de sécurité dans la gestion de la sécurité des systèmes complexes **[42]**. Par ailleurs, une méthode d'évaluation des risques PGI d'une entreprise **[43]** ainsi qu'un système de pilotage du processus d'innovation dans le secteur de la finance sont également proposés **[44].**

Un modèle général de gestion du risque par le pilotage et la conduite des activités de biens et de services est également proposé. Cependant, on note le caractère statique du processus de gestion des risques [**45].** En 2012, la problématique de la sécurité dans une infrastructure

est abordée par une approche de gestion des risques permettant d'identifier les différents types de risques et de proposer des mesures de sécurité plus adaptées au contexte. Cependant, pour une gestion efficace, il faut tenir compte des risques liés aux différents partenariats**.** Il est donc impératif donc d'avoir une approche globale et intégrée dans la gestion des risques bancaires en tenant compte des risques par processus mais aussi des typologies de risques afin de définir une démarche pertinente permettant la maitrise de l'ensemble des risques. Ainsi, dans l'optique de sécuriser tous les composants système d'information, les banques implémentent divers mesures et dispositifs permettant d'assurer la disponibilité, l'intégrité, la confidentialité et la traçabilité de leur système d'information. Il s'agit notamment de la sécurisation des connexions et des échanges, du suivi régulier de l'activité du réseau informatique, du contrôle d'accès aux données sensibles et aux applications, des contrôles d'accès physique et patches des systèmes critiques, de la mise à disposition d'outils de détection d'intrusions mais aussi de la mise à jour régulière des antivirus, antispyware, logiciels, navigateurs, systèmes d'exploitation, etc.

A cela s'ajoute, la mise en conformité des banques à un certain nombre de normes informatiques dans le but de maitriser tous les risques liés à leur système s'information. Parmi ces normes, il y a ceux qui sont relatives à la gouvernance et au management du système d'information comme COBIT **(**Control Objectives for Information and Related Technology**)** et ITIL (Information Technology Infrastructure Library). En effet, COBIT propose un modèle de référence et un langage commun pour tous ceux qui, dans une entreprise, doivent utiliser ou gérer les activités informatiques, c'est un cadre de référence pour mesurer et surveiller la performance, communiquer avec les fournisseurs de services et intégrer les meilleures pratiques de gestion **[46]**. Il permet aussi d'apprécier les activités et les risques informatiques pour une gouvernance efficace du système d'information. Il y a également ITIL dont les activités liées à la stratégie de services informatiques s'articulent autour de la définition de la stratégie IT et de la création d'un schéma directeur définissant les objectifs IT à moyen et long terme **[47].** Pour ce qui est des normes relatives à la sécurité du système d'information, il y a essentiellement les normes ISO 27001 et ISO 22301**.** La norme ISO 27001 spécifie les exigences permettant de mettre en place, d'exploiter et d'améliorer un SMSI (Système de Management de la Sécurité de l'Information) **[48].** Un SMSI désigne l'approche globale par laquelle une organisation veille à la sécurité des informations sensibles. Basé sur le principe de management du risque, un SMSI englobe les personnes, les processus et les systèmes de technologies de l'information. Ces exigences permettent l'implémentation de mesures de sécurité adaptées aux besoins de l'organisation en vue de fournir une protection des actifs d'information mais aussi le patrimoine informationnel, les biens sensibles et la confiance aux parties prenantes. Elle est applicable à tout type d'organisation indépendamment de la nature de l'activité. Cela passe nécessairement par la définition, l'utilisation, la tenue à jour et la gestion d'une politique de sécurité du système d'information. Quant à la norme ISO 22301, elle est relative au Système de Management de la Continuité d'Activité(SMCA). Elle intègre des notions d'objectifs, de suivi des performances

et d'indicateurs pour la gestion de la continuité d'activité permettant de garantir le maintien en condition opérationnelle de la démarche de continuité d'activité en cas de sinistre **[49]** .

II.1.4 Dispositifs de maitrise des risques spécifiques à la monétique

Par ailleurs, compte tenu de l'avènement des produits et services monétiques, les banques sont obligés de se conformer aux normes sécuritaires monétiques dans le but de sécuriser les transactions électroniques et de lutter contre la fraude monétique. En effet, les standards EMV définissent l'ensemble des fonctionnalités et des procédures nécessaires au dialogue entre une carte et un terminal pour effectuer des transactions de paiement et de retrait. Ils précisent notamment les caractéristiques physiques, électriques et d'étanchéité que doivent respecter la carte et le terminal, les traitements à effectuer de part et d'autre ainsi que les échanges de données entre la carte et le terminal pendant tout le déroulement de la transaction. Les trois méthodes d'authentification utilisées par EMV sont l'authentification statique des données (SDA), l'authentification dynamique des données(DDA) et l'authentification combinée des données(CDA). Parmi les normes sécuritaires monétiques, on peut citer, la norme PCI DSS qui couvre de multiples facettes telles que la politique de sécurité du système d'information, les procédures, l'architecture du réseau, le développement sécurisé et bien d'autres mesures de protection. Elle gère aussi la protection de la confidentialité des données des porteurs de carte, ces données peuvent être sensibles ou non. Les avantages de cette norme sont nombreux ; en effet, au lieu de se concentrer sur une catégorie de fraude spécifique, elle prend en charge tout ce qui permet de limiter la disponibilité des données des porteurs. Elle atteint ses objectifs de sécurité en garantissant l'intégrité des composantes qui conduisent aux données d'identification sensibles et à celles du titulaire de carte, contre des attaques physiques et logiques. Elle permet aussi de protéger la confidentialité des données du titulaire lorsqu'elles sont stockées au sein d'un environnement donné, ou celle des données du titulaire et d'identification sensibles lorsqu'elles sont transmises sur un réseau ouvert ou public. Toujours dans la famille des normes PCI (Payment Card Industry), Il y a la norme PA-DSS (Payment Application Data Security Standards) qui s'applique aux fournisseurs qui développent des applications de paiement, stockent, traitent ou transmettent des données porteurs **[50].** Concernant le standard PCI-P2PE (Payment Card Industry Point to Point Encryption), c'est une liste d'exigences de sécurité associée à des procédures de tests des applications et des solutions P2PE **[51]**. Il a pour but de s'assurer que les applications et les solutions P2PE peuvent répondre aux exigences nécessaires à la protection des données de cartes de paiement. Pour ce qui est de la norme PCI PTS (Payment Card Industry PIN Transaction Security), c'est la norme de sécurité actuellement en vigueur pour les terminaux de paiement avec saisie du code PIN. Il existe aussi d'autres normes PCI, parmi lesquelles on peut citer : PCI-HSM (Payment Card Industry Host Security Module) pour la sécurisation des HSM utilisés dans le paiement électronique et PCI Card Production pour la sécurité des données lors de la fabrication et la personnalisation des cartes de paiement.

Par ailleurs, Le 3DSecure a été mis en place pour sécuriser le paiement en ligne des clients et réduire la fraude commerçant **[52]**. Le concept de base consiste à lier le processus d'autorisation financière avec une authentification en ligne. Cette authentification est basée sur un modèle comportant 3 domaines qui sont : le commerçant et la banque qui recevra les fonds, la banque qui a délivré la carte de paiement et l'accepteur ou le point de service **[53]**. Le protocole 3DSecure permet de vérifier que la banque émettrice et le consommateur prennent part au procédé 3D avant d'autoriser un paiement en ligne. L'utilisation de 3DSecure comporte de nombreux avantages parmi lesquels on peut citer : l'authentification du porteur avant la validation de la transaction financière, la protection contre les risques de l'utilisation frauduleuse de cartes bancaires et la décharge du vendeur de la responsabilité concernant presque toutes les transactions frauduleuses ayant eu lieu sur son site.

II.2 Gestion des risques spécifiques à l'activité bancaire de l'UEMOA

II.2.1 Contexte

Au fil du temps, avec le développement et la complexité croissante des opérations bancaires et financières, la réglementation et le système de surveillance des établissements de crédit n'ont cessé de s'enrichir et de s'adapter à un domaine lui-même en constante évolution. Aussi, il n'est pas toujours aisé pour les dirigeants des établissements de crédit, dont les fonctions sont particulièrement exigeantes, de se tenir parfaitement et constamment informés de l'évolution et de l'état de la législation bancaire et des règles prudentielles, alors qu'il leur appartient de veiller à ce que l'ensemble de ces textes législatifs et réglementaires soit rigoureusement respecté par la banque ou l'établissement financier qu'ils dirigent. L'activité bancaire s'exerce dans un contexte d'uniformisation des pratiques et des règles, justifiée par l'unicité de l'espace monétaire **[1]**. La réglementation et la surveillance de son application relèvent de la compétence d'institutions ou d'organes communautaires, responsables de la politique monétaire et du crédit, de la réglementation de l'activité d'intermédiation bancaire, du contrôle du système bancaire, de la réglementation des Systèmes Financiers Décentralisés (SFD), de l'harmonisation du droit des affaires (OHADA) mais aussi de la réglementation de l'appel public à l'épargne et du marché financier.

II.2.2 Evolutions de la règlementation prudentielle

La réglementation prudentielle a considérablement évolué ces vingt dernières années sous l'impulsion des travaux du Comité de Bale. Les principales dates de l'´évolution de la réglementation sont les suivantes: Bâle I en 1988, Bâle II en 2008, et Bâle III en 2013. Les principes fondamentaux ont été conçus en étroite concertation avec plusieurs autorités de contrôle du monde entier. Leur publication constitue une nouvelle étape dans le renforcement de la coopération internationale entre autorités de surveillance et confirme l'audience mondiale du comité de Bâle sur le contrôle bancaire. L'élaboration de ces principes a par ailleurs associé le Fonds monétaire international et la Banque mondiale, qui ont intégré les préoccupations prudentielles dans leurs propres travaux sur la stabilité financière. Ces principes constituent ainsi une réponse aux attentes qui ont pour but de contribuer au renforcement de la stabilité du système financier mondial et d'aider les

économies émergentes dans l'adaptation de leurs systèmes financiers et de leurs normes prudentielles. Ils couvrent ainsi l'agrément des banques, la réglementation prudentielle, les techniques de contrôle et les prérogatives des autorités de surveillance. Ils ont vocation à s'appliquer aux banques de tous les pays **[54]**.

Ainsi, en 1988 le Comité de Bâle, réunissant les principales autorités de contrôle bancaire du monde, a publié l'accord de Bâle I qui est un ensemble d'exigences de fonds propres minimales pour les banques. Bâle I était principalement axé sur le risque de crédit et la quantité de fonds propres que devait comporter le passif des banques afin de faire face à d'éventuelles pertes. Les actifs des banques étaient classés en fonction de leur risque de crédit, du risque de défaut et d'un coefficient de pondération du risque leur était attribué.
Il est apparu que Bâle I n'était qu'une étape sur le chemin de la régulation bancaire. En effet, la pondération des engagements de crédit était insuffisamment différenciée pour rendre compte des différents niveaux effectifs du risque de crédit. Ensuite, les années 1990 ont vu l'émergence d'un phénomène nouveau, à savoir l'explosion du marché des produits dérivés et donc des risques "hors-bilan". Ces risques furent traités en 1996 dans l'amendement à l'accord de Bâle I, imposant la prise en compte des risques de marché et des risques liés aux flux des postes du hors-bilan et des produits dérivés. En outre, cet amendement permet aux banques d'utiliser soit une approche standard, soit leurs modèles internes. Mais il devint rapidement évident qu'une refonte de l'accord était nécessaire, ce que le Comité a réalisé à partir de 1999, débouchant sur Bâle II publié en 2004 **[55]**. Ainsi, Bâle II visait à élargir la gamme des risques couverts et à améliorer la méthode de calcul des coefficients de pondération des risques. Les normes Bâle II constituent un dispositif prudentiel destiné à mieux appréhender les risques bancaires et principalement le risque de crédit ou de contrepartie ainsi que les exigences en fonds propres. Elles visent notamment, la mise en place du ratio McDonough destiné à remplacer le ratio Cooke. Depuis Bâle II, les banques appliquent le nouveau ratio de solvabilité fondé sur une gestion fine des risques. La crise bancaire de 2007-2008 a eu des conséquences énormes pour la société en termes de destruction de richesses, de hausse du chômage et d'augmentation du niveau de la dette publique. Elle a également démontré que les fonds propres des banques étaient insuffisants et qu'ils doivent être beaucoup plus élevés. En 2010, le Comité de Bâle a publié l'accord Bâle III, qui est un ensemble actualisé de règles internationales concernant les exigences de fonds propres imposés aux banques **[56]**. Bâle III est le troisième des accords de Bâle, il a pour but de mettre à jour les règles définissant la quantité de capital minimum avec lequel les banques doivent se financer, et dont l'objectif principal est d'améliorer la stabilité du système financier, afin de réduire la probabilité de survenance et la gravité potentielle des futures crises. L'impact de Bâle III dépendra fortement de la manière dont l'accord sera mis en place au sein de la banque, ainsi que des autres règlementations implémentées pour l'accompagner. Ses principaux avantages sont l'augmentation des fonds propres des banques, la limitation des actifs des banques par rapport à leurs fonds propres et l'assurance que les banques disposent de liquidités suffisantes. Bâle III, a donc permis de renforcer le dispositif de sécurisation de solvabilité et de liquidité des banques.

II.2.3 Supervision du système bancaire de l'UEMOA

La supervision des établissements de crédit dans l'UEMOA est assurée par un organe supranational doté de pouvoirs étendus, à savoir la Commission bancaire. La Banque Centrale assure son secrétariat. Du point de vue organisationnel, la Commission bancaire,

présidée par le Gouverneur de la BCEAO, comprend un représentant de chaque Etat membre de l'UEMOA ainsi qu'un collège de membres désignés *personae* par le Conseil des ministres de l'Union. Ces représentants jouissent d'une indépendance dans l'exercice de leurs fonctions. Dans le cadre de l'accomplissement de ses missions, la Commission bancaire est habilitée à prendre des mesures administratives et dispose, par ailleurs, de larges pouvoirs de sanctions disciplinaires pour toute infraction à la réglementation bancaire. Elle peut étendre, dans le cas échéant, ses contrôles aux sociétés apparentées et proposer la nomination d'administrateurs provisoires ou de liquidateurs pour les banques et établissements financiers. Le dispositif prudentiel vise principalement deux objectifs: renforcer la solvabilité et la stabilité du système bancaire et assurer une protection accrue des déposants, dans un contexte de libéralisation des activités monétaires, bancaires et financières. Trois principales normes sont utilisées pour apprécier la solvabilité des banques: la représentation du capital minimum, la règle de couverture des risques mais aussi la règle de limitation des immobilisations en liaison avec le niveau des fonds propres réglementaires de chaque établissement. Ainsi, plusieurs outils peuvent être implémentés par les banques dans l'optique de maîtriser leurs différentes typologies de risques.

a. Systèmes de notation interne

Pour répondre aux exigences de leur réglementation locale, les banques de la zone UEMOA doivent être capables de mesurer leur risque de crédit en estimant les trois paramètres y afférents, en l'occurrence la probabilité de défaut, la perte étant donné le défaut et l'exposition au défaut au moyen des systèmes de notation interne. Par contre, les réflexions sur l'estimation des paramètres de risque n'ont pas encore démarré car les banques de la zone cherchent plutôt à mettre en place un dispositif de notation interne basé sur une approche du scoring. L'analyse de la situation actuelle montre que les systèmes de notation interne existent dans les filiales des banques européennes et panafricaines. Toutefois, ce projet est en cours de réflexion dans certains groupes régionaux et locaux sous la pression de leur commission bancaire.

b. Modèles de gestion actif-passif

Le modèle de gestion actif-passif permet de maîtriser le risque de liquidité et le taux de la banque. Plus connu sous le nom d'ALM (Asset Liability Management), il est plus utilisé dans les banques occidentales. Cette pratique est rarement appliquée dans les banques de l'Afrique subsaharienne francophone. De manière concrète, l'utilisation des modèles ALM ne pourra se faire qu'avec l'impulsion du régulateur, à savoir la Commission bancaire. Les banques de l'UEMOA ont beaucoup à gagner en développement ces outils qui sont une source indéniable de création de valeur en ce sens qu'ils pourront d'une part contribuer à réduire l'impact du risque et d'autre part, ils serviront à tarifier leurs produits.

c. Modèles de quantification du risque opérationnel

Les réglementations de l'UEMOA ne sont pas explicites sur les aspects quantitatifs du risque opérationnel. En revanche, leurs banques doivent être capables de le prévenir et d'estimer sa perte espérée, afin de calculer un capital risque agrégé adapté à leur profil de risque et *in fine* le ratio McDonough, leur permettant ainsi de se conformer à l'esprit de Bâle II. Le dispositif Bâle II propose trois méthodes de calcul des exigences de fonds propres au titre du

risque opérationnel, il s'agit notamment de l'approche simple BIA (Basic Indicator Approach), l'approche standard (TSA) et l'approche mesure avancée (AMA).

Par ailleurs, la supervision bancaire basée sur les risques se présente comme un processus permettant aux superviseurs, à travers des contrôles sur pièces et sur place, d'évaluer les risques encourus et la politique de gestion mise en place par les établissements de crédit mais aussi de mettre en adéquation leurs ressources disponibles en fonction du profil des risques et de l'importance systémique des dits établissements. Comparée à l'approche traditionnelle qui repose sur un contrôle de conformité de la situation financière à une date donnée, la supervision basée sur les risques met l'accent sur la connaissance de l'institution et l'évaluation de la qualité des systèmes de gestion mis en place par les établissements de crédit pour identifier, mesurer, surveiller et contrôler les risques, de manière appropriée. Au-delà des gains pour les superviseurs, cette technique permet également aux banques d'améliorer la gestion et la surveillance de leurs risques. Cette approche rejoint les recommandations de l'accord de Bâle II et les principes fondamentaux de Bâle qui, pour une supervision efficace, requièrent d'une part, la mise en place des systèmes efficients de gestion des différents risques par les banques et d'autre part, requièrent des superviseurs de s'assurer de l'efficacité de ces dispositifs. Les principaux risques recensés de manière non limitative sont les risques de crédit, de marché, de liquidité, opérationnel, juridique, stratégique, et de réputation. Cette approche repose sur les six (6) étapes suivantes :

- **L'identification et la connaissance du profil de risque de l'institution** : il s'agit de définir le profil de la banque (historique, capital, actionnariat, réseau, effectif, stratégie, principaux risques inhérents et situation financière) sur la base de différentes informations disponibles, notamment au niveau du contrôle sur pièce. Le profil doit être régulièrement actualisé et au moins avant et après chaque contrôle sur place.
- **L'évaluation des risques de l'institution**: le superviseur doit évaluer les forces et faiblesses de la banque dans la gestion des différents risques identifiés, en vue de concevoir une matrice des risques et de rédiger une note d'évaluation. La matrice identifie pour chaque type d'activité, le niveau du risque inhérent, la qualité des systèmes de réduction du risque, le niveau et la tendance du risque résiduel.
- **La planification des actions de supervision** : tenant compte du profil de risque de l'institution, le plan doit permettre de déterminer la fréquence des contrôles sur place à réaliser dans un horizon déterminé, en fonction des ressources du superviseur. Il doit indiquer le type de contrôle, les domaines cibles et les techniques à utiliser.
- **La définition du champ de contrôle** : elle est liée au profil de risque et à la planification des actions de supervision. Les domaines d'investigation sont identifiés et font l'objet d'une répartition entre les membres de l'équipe de vérification.
- **La conduite de la mission de contrôle** : en fonction de la sévérité des risques encourus, les diligences effectuées peuvent varier de procédures de contrôles simples à des vérifications approfondies. Les contrôles sont matérialisés par des feuilles de travail permettant de voir les contrôles opérés, les résultats obtenus et les recommandations à faire. La mission doit se conclure par une réunion de restitution avec la banque et donner lieu à la notation de l'institution.

- **La communication des conclusions** : les recommandations de la mission doivent faire l'objet d'un suivi approprié. Le cas échéant, des actions prudentielles peuvent être déclenchées sous forme d'injonctions ou de sanctions plus sévères.

II.3 Problématique liée à l'estimation des risques résiduels

L'environnement bancaire de l'UEMOA est aujourd'hui caractérisé par plusieurs facteurs importants comme l'instabilité conjoncturelle dans un contexte mondialisé, l'impact rapide des nombreuses règlementations, la diversité des risques liée aux différentes évolutions, la responsabilité juridique mise en cause par le client, la prise de risque sur l'activité de marché pour générer du résultat. Ainsi, la gestion des risques est devenue une activité fondamentale pour les banques, car il y va de leur survie. Cela concerne le risque de crédit, le risque de marché, le risque opérationnel et d'autres risques dont les contrôles à mettre en œuvre sont devenus de plus en plus complexes. L'évolution de la règlementation bancaire implique que les métiers affectés au contrôle et à l'audit s'adaptent régulièrement et acquièrent de nouvelles compétences. Cela impacte l'audit interne, le contrôle technique des opérations bancaires du réseau, du back et du middle office via les services des inspections. Le contrôle des risques s'est alors enrichi de la mise en place des services de conformité qui doivent anticiper tout manquement à l'observance des normes et réglementations en vigueur. Ces métiers requièrent une solide expérience et un très bon niveau de compétences techniques, à savoir la maîtrise de la réglementation bancaire, des normes informatiques et monétiques, des techniques de contrôle interne et d'évaluation des risques. Le dispositif de contrôle interne des banques de l'UEMOA est complexe, il se compose d'une part de l'implémentation des mesures sécuritaires au niveau système d'information bancaire et de la conformité aux normes informatiques et monétiques et d'autre part, du respect des accords de Bâle, des règlementations spécifiques à la zone UEMOA mais aussi de la supervision basée sur les risques et du dispositif prudentiel y afférent **[7]**. A ce propos, le management de la banque est responsable de la conception, de la mise en œuvre et de la supervision des systèmes de contrôle interne et de gestion des risques. Il appartient alors aux administrateurs de déterminer le niveau de risque résiduel qu'il est prêt à accepter. Dans ce contexte, les risques doivent être évalués de manière continue et les activités de contrôle doivent être conçues pour répondre aux risques spécifiques. Il faut également que la gouvernance définisse comment le management doit réagir en cas de défaillance et comment les systèmes doivent être adaptés à la suite d'une défaillance. En vue de faire face à ce défi aussi bien sur le plan organisationnel que sur le plan méthodologique, des documents complémentaires permettant de suivre l'efficacité des systèmes de contrôle interne et de gestion des risques sont élaborés et mis en disposition.

Dans ce contexte, les banques de l'espace UEMOA ont mis en place des dispositifs de contrôle interne, cependant beaucoup reste à faire pour améliorer leur efficacité. Les efforts doivent être dorénavant faits sur la quantification de ces risques. Au regard de la réglementation locale, il s'agit d'une obligation pour les banques. En effet, la Commission bancaire de l'UEMOA recommande aux banques de l'Afrique de l'ouest, de disposer d'outils d'évaluation des risques adaptés à leurs activités dont le but est de déterminer la perte potentielle ou avérée, ainsi que tout dommage d'une autre nature, que leur réalisation pourrait engendrer **[6].** Il s'agit notamment les risques de crédit, de taux d'intérêt, de règlement, de manque de liquidité et de marché ainsi que les risques opérationnels. Les outils de gestion des risques dont les banques ont besoin sont les systèmes de notation

interne, les modèles de gestion actif-passif et de quantification du risque opérationnel qui ont été décrits précédemment.
En outre, l'accroissement de la concurrence accompagné d'un rééquilibrage entre l'intermédiation traditionnelle et le rôle du marché a contribué à la modification de la nature des métiers exercés par les banques. Ainsi, les métiers de la banque de détails sont devenus plus complexes et diversifiés, ceux de la banque de financement et d'investissement exigent un haut niveau de qualification et sont fortement concurrentiels par rapport aux banques étrangères. Les banques sont aujourd'hui caractérisées par une exposition plus forte aux pressions de la concurrence et aux fluctuations des marchés d'où l'importance de déterminer leur niveau de risque résiduel.

L'estimation des risques résiduels consiste à mesurer l'impact des contrôles mis en œuvre sur la criticité des risques inhérents**.** Elle se fait généralement avec la méthode RSCA qui repose sur un dispositif de notation permettant d'estimer chaque risque résiduel, à partir d'un système de notes basées sur les niveaux de maturité du contrôle mais aussi sur les échelles de probabilité de survenance et de gravité potentielle des risques inhérents. L'exercice de notation se doit d'être le plus objectif possible, il est réalisé au moyen d'un fichier Excel qui constitue le registre des risques et contrôles évalués **[57].** Pour limiter la part d'arbitraire inhérente à cette démarche, l'évaluation de chacune des composantes s'appuie sur des critères permettant de décrire et de caractériser chacun des paliers indiqués au titre de chacune des composantes. L'évaluateur se reportera ainsi à ces critères pour apprécier la note qu'il portera à chaque composante. La participation la plus large possible des acteurs intéressés dans le cadre d'échanges contradictoires et de corroboration permettra de faire émerger un consensus proposé à la validation de la structure de gouvernance **[19].** Cette méthode « d'experts » peut certes être empreinte de subjectivité, mais en s'inscrivant dans la démarche globale de contrôle interne, elle est elle-même soumise à évaluation et doit s'appuyer sur le diagnostic de procédures, des rapports d'audit interne et externe ainsi que sur des éléments probants**.** Ces éléments probants correspondent aux supports, documents relatifs au renforcement du contrôle interne et existant dans les services, dont la communication et l'analyse permettent d'étayer l'évaluation réalisée. L'analyse de ces éléments probants contribue ainsi à la justification de la note attribuée à chacune des composantes évaluées. Par conséquent, il est important d'indiquer les références des documents probants qui fondent le niveau de cotation choisi et de s'assurer de leur disponibilité dans la perspective de l'évaluation des résultats de la gestion des risques.
A l'issu de cette cotation, les niveaux de risques résiduels obtenus par les évaluateurs doivent être exacts et en deçà de l'appétence au risque définie par le top management **[77].** Dans le cas échéant, cela signifie la banque encoure des risques dont le niveau de maitrise est inconnu ou que ses risques sont mal maitrisés. Cela a pour conséquence, l'imminence de la concrétisation de ces risques qui peuvent avoir des impacts de nature financier, juridique, image voir même l'apparition d'un risque systémique pouvant paralyser tout le système financier **[75].** A titre d'exemple, ci-dessous, cinq risques relatifs des processus phares de la banque, à savoir les processus système d'information, conformité aux normes et règlementations, ressources humaines, audit et contrôle, finances et comptabilité :

- **Risque 1 :** Indisponibilité du système d'information bancaire ou de la plateforme monétique en raison d'un bug applicatif ou d'un malware pouvant entrainer la non satisfaction des clients et une perte de flux pour la banque

- **Risque 2 :** Mise en conformité tardive aux réglementations bancaires ou normes édictées par les réseaux internationaux en raison d'un manque de budget ou de l'absence de ressources compétents pouvant entrainer le paiement de pénalités
- **Risque 3 :** Risque lié au biais de la commission de recrutement en raison de conflits d'intérêts ou de l'absence de procédure de recrutement rigoureuse pouvant entrainer un recrutement inadéquat à des postes sensibles
- **Risque 4:** Fraude interne en raison de l'insuffisance de contrôle interne, d'une distribution inadéquate des tâches ou de l'inexistence d'une séparation de taches pouvant entrainer des pertes financières
- **Risque 5 :** Non exhaustivité de la facturation en raison du défaut de transmission de certains éléments de facturation au service comptable pouvant entrainer une sous-estimation des revenus de la banque

Ainsi, une mauvaise maitrise de ces risques aura pour conséquence un niveau de risques résiduels au-delà de l'appétence définie par la banque. A coup sûr, cela expose la banque à des pertes financières, des réclamations clients et à la dégradation de son image pouvant aboutir à un risque systémique sur le moyen terme. Par ailleurs dans le cas où le niveau de risques résiduels est deçà de l'appétence définie par la banque suite à une évaluation erronée en interne, la banque va se croire dans une position confortable alors que la réalité est autre. Cela peut également être à l'origine d'un risque systémique à moyen terme.

Conclusion

Au niveau de ce chapitre, nous avons pu découvrir les dispositifs de maitrise des risques liés au système d'information bancaire mais aussi ceux relatifs risques spécifiques à l'activité bancaire. En effet, le système d'information bancaire est devenu très complexe compte tenu de l'avènement des nouveaux produits et services monétiques. Ces nouveaux usages sont à l'origine de plusieurs vulnérabilités exploitables par les fraudeurs pour perpétrer des attaques. A cela s'ajoutent, les risques qui sont spécifiques à l'activité bancaire. Pour maitriser ces nombreux risques de natures différentes et aux conséquences néfastes, plusieurs contrôles sont mis en œuvre au sein des banques. Dans l'optique d'assurer la pérennité de leur part de marché, l'évaluation des contrôles mis en place et le suivi de leur efficacité représentent désormais un challenge certain pour les banques de l'UEMOA. De ce point de vue, l'un est des défis majeurs des banques est d'obtenir le niveau exact du risque résiduel qui correspond l'exposition réelle de la banque. Dans le prochain chapitre, nous exposerons les méthodes actuelles utilisées pour déterminer les risques résiduels bancaires.

Chapitre III : Etat de l'art sur l'estimation des risques résiduels

Introduction

Au niveau de ce chapitre, nous allons commencer par évoquer la diversité des contrôles mis en œuvre par les banques pour maitriser leurs différentes typologies de risques avant de définir la notion de risque résiduel et de décliner ses différentes caractéristiques. Nous ferons également un focus sur les spécificités des méthodes AMDEC et RSCA. Par la suite, nous analyserons les différentes méthodes et variantes permettant d'obtenir les risques résiduels tout en spécifiant les avantages et limites de chacune d'elles. Tout au long de cette analyse, nous exposerons les méthodes utilisées pour évaluer les risques résiduels liés au système d'information et aux autres risques bancaires.

III.1 Diversité des contrôles bancaires

Les métiers de la banque se complexifient de plus en plus, c'est ce qui pousse les banques à durcir leur dispositif de contrôle interne en vue de maitriser au mieux les différentes

typologies de risques auxquels elles sont confrontées; le risque étant tout évènement susceptible d'empêcher la réalisation des objectifs.

Le dispositif de contrôle interne des banques est essentiellement basé sur le COSO qui stipule que pour cerner le modèle économique qui spécifie les objectifs d'une organisation et la manière dont ses processus sont structurés pour atteindre ces objectifs, la première source d'information est le propriétaire du processus et la documentation existante sur les politiques et les procédures dudit processus **[24].**Selon le COSO II, les objectifs d'une organisation sont classés en quatre catégories. En effet, il y a des objectifs stratégiques qui sont liés à la stratégie de l'organisation, les objectifs opérationnels qui visent l'utilisation efficace et efficiente des ressources, les objectifs de reporting qui sont axés sur la fiabilité du reporting externe et interne et enfin les objectifs de conformité qui visent la conformité aux lois et aux réglementations **[4].**

La gestion des risques bancaires inclut l'identification et l'évaluation des risques, la détermination de l'appétence au risque mais aussi le pilotage effectif de ce dispositif de maitrise des risques en vue de s'assurer que le niveau de risque résiduel est conforme à l'appétence définie par la banque. Dans ce contexte, l'identification des risques consiste à identifier les événements potentiels survenant en interne ou en externe et qui sont susceptibles de nuire à l'exécution de la stratégie et à la réalisation des objectifs de la banque. A ce niveau, deux approches sont possibles, il s'agit d'une part de l'approche top down qui fait une déclinaison des objectifs stratégiques en objectifs opérationnels et identifie les risques relatifs à chaque objectif et d'autre part l'approche bottom-up qui fait une analyse dysfonctionnelle du processus en identifiant tous les risques susceptibles d'intervenir du début jusqu'à la fin du processus. Face à la complexité de la tâche, un guide couvrant tous les aspects et étapes de la gestion des risques est proposé et régulièrement mis en application par les banques **[58]**. De plus, compte tenu de l'avènement des produits et services monétiques, le système d'information bancaire est de plus en plus vulnérable **[59]**;c'est ainsi que plusieurs mesures sécuritaires sont déployées par les banques dans le but de maitriser les risques liés à leur système d'information **[60]**. A cet effet, un guide explicite est également proposé pour la maitrise des risques y afférents **[61]**.

S'agissant des transactions electroniques, les types de fraude monétique sont différents et peuvent être classés en trois catégories, à savoir les fraudes GAB, les fraudes TPE et les fraudes en ligne; ils peuvent avoir de graves conséquences dans le cas où les risques y afférents ne sont pas gérés de manière efficace **[62]**. Sullivan dans **[63]** a montré que les mesures sécuritaires déployées pour mitiger les risques sécurité auxquels les banques sont exposées avec le paiement sur internet ne sont pas forcément efficaces. Ainsi, la sécurité doit être renforcée avec l'authentification du titulaire de la carte bancaire qui est impérative dans le cadre de la gestion de la fraude sur Internet, comme indiqué dans [**64].** Dans le même ordre d'idées, les risques spécifiques aux métiers de la banque sont analysés en profondeur et les fondements de bases des risques crédit et marché fortement liés aux cadres règlementaires des institutions financières sont d'abord définis **[65].** Ensuite, une analyse globale du risque bancaire est effectuée par Sonja et fournit la synthèse de

l'évaluation, de l'analyse et du traitement des risques dans le secteur bancaire tout en précisant les acteurs clés **[66]**. Dans la même foulée, des méthodes sont proposées pour analyser les risques commerciaux **[67]**, les risques d'efficacité [**68**] ainsi que les risques crédit **[69]**.

L'évaluation des risques bancaires est aussi abordée avec la proposition d'un modèle d'arbre de décision pour évaluer les risques crédit **[70].** Depuis 2013, des travaux d'évaluation des risques bancaires basés sur le réseau DEA ont été proposés pour apprécier le management effectué [**71].** Etant donné que l'exposition des banques de l'UEMOA par rapport aux différentes typologies de risques est en constante évolution entrainant la possibilité d'apparition d'un risque systémique **[72]**, plusieurs méthodes sont utilisées pour évaluer les risques **[16].** Ces méthodes vont de l'identification des risques au monitoring en passant par l'évaluation des risques inhérents et résiduels. Les risques résiduels sont les risques qui persistent après que le traitement des risques ait été mis en œuvre ou lorsque les contrôles ne sont pas réalisables. La direction des banques doit donc accepter la façon dont les risques ont été traités ; ainsi l'acceptation du risque devrait toujours être une décision de gestion**.**

III.2 Spécificités des risques résiduels bancaires

Les risques résiduels bancaires sont obtenus en évaluant l'impact des contrôles mis en œuvre sur les risques inhérents. Un contrôle mis en œuvre peut réduire le risque inhérent en réduisant la probabilité de survenance ou la gravité potentielle ou les deux. L'évaluation de l'effet du contrôle sur le risque inhérent conduit à déterminer le niveau de risque résiduel. De manière spécifique, les contrôles préventifs réduisent la probabilité de survenance des risques alors que les contrôles detectifs et correctifs réduisent leurs impacts **[73]**.

Compte tenu de la diversité des produits et services offerts par les banques, il s'avère nécessaire de déterminer les risques résiduels liés aux différents processus, d'où l'importance de connaitre le niveau exact de risque résiduel dans l'optique de définir les stratégies de traitement adaptées à chaque typologie de risques **[74].** Etant donné que certains risques résiduels peuvent être des risques systémiques **[75],** le dispositif de contrôle interne de la banque doit être périodiquement évalué dans le but de déterminer la pertinence ou non de définir et de mettre en œuvre des contrôles supplémentaires **[25].**

Ainsi les banques peuvent définir de nouveaux contrôles qui s'imposent selon les niveaux de criticité des risques résiduels qui peuvent être illustrés par des codes couleurs en vue de faciliter leur interprétation**.** Lorsque ces contrôles définis sont effectifs et efficaces, le niveau de risque résiduel sera alors inférieur au niveau de risque inhérent **[76].** Cela signifie que les facteurs du risque résiduel sont réduits; ce qui se concrétise par une réduction de la probabilité d'occurrence et/ou de la gravité potentielle**.** Puisque le risque résiduel correspond au niveau de risque qui subsiste après la mise en œuvre des contrôles, il est impératif de s'assurer qu'ils ne dépassent pas l'appétence que la banque s'est fixée **[77].** De manière plus concrète, les risques résiduels sont obtenus avec deux principales méthodes, il s'agit de la méthode outillée qui préconise l'utilisation de logiciels informatiques conçus à cet effet et de la méthode RSCA (Risk Self Control Assessment) largement utilisée et qui est basée sur l'AMDEC **[78].** En effet, l'AMDEC permet d'identifier les causes et les effets de l'échec potentiel d'un procédé ou d'un moyen de production ainsi que les actions pouvant éliminer ou réduire l'échec potentiel.

III.3 Méthodologie AMDEC

En 2006, Weese décrit l'ensemble des méthodes d'évaluation de risques ayant fait leurs preuves **[16]**. Parmi elles, on peut citer la méthode AMDEC (Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité), la méthode HAZOP (Hazard and Operability Study) qui est utilisée dans l'industrie chimique et la méthode HACCP (Hazard Analysis Critical Control Points) utilisée dans l'industrie alimentaire. Il y a également la méthode de la matrice des risques qui convient aussi bien à la gestion du risque des organisations et celle des systèmes. L'arbre des défaillances et la méthode Value at Risk sont aussi d'autres méthodes d'évaluation du risque.

III.3.1 Définition AMDEC

L'AMDEC est l'un des plus célèbres outils inductifs. L'analyse causale est effectuée par la règle des 5M (Milieu, Matériel, Matière, Méthodes, Main-d'œuvre) et permet d'identifier les causes ou les effets **[17]**. Les sources de risques d'un système peuvent être des défauts de conception, des dysfonctionnements techniques, organisationnels, environnementaux ou humains ou la fin de vie. Il existe plusieurs types d'AMDEC parmi lesquels on peut citer **[18]** : l'AMDEC procédé qui permet identifier les défaillances du procédé de fabrication dont les effets agissent directement sur la qualité du produit fabriqué, l'AMDEC machine qui permet d'identifier les défaillances du moyen de production dont les effets agissent directement sur la productivité. Il s'agit de l'analyse des pannes et de l'optimisation de la maintenance et enfin l'AMDEC sécurité qui permet de réduire les risques liés à l'utilisation d'un moyen de production.

III.3.2 Principes de l'AMDEC

La réalisation d'une AMDEC suppose d'abord la constitution d'un groupe de travail, ensuite l'analyse fonctionnelle du procédé et des défaillances potentielles est effectuée ainsi que l'évaluation de ces défaillances et la détermination de leur criticité avant la planification des actions définies. Dans le cadre de la mise en œuvre d'un AMDEC, il est nécessaire de constituer un groupe de travail composé de 4 à 8 individus issus de divers services de l'entreprise comme la production, la maintenance, la qualité. Les membres du groupe de travail ont tous un rapport avec l'objet de l'analyse et en ont une expérience significative qui leur permet d'argumenter au cours des réunions **[19]**. L'animateur a pour rôle de conduire et d'orienter les débats, de veiller au respect des limites du sujet, de désigner la personne qui doit trancher en cas de litige, de rédiger l'AMDEC et de planifier les réunions. Les réunions durent au maximum une demi-journée et sont planifiées au rythme d'environ une fois tous les 15 jours. Puisqu'il n'est pas aisé de réunir toutes les personnes, l'effort de présence consenti par chacun doit se concrétiser par de la discipline et de l'efficacité. Même si d'apparence, l'AMDEC ressemble à une discussion où s'opposent des points de vue différents, elle demeure une méthode caractérisée par une certaine rigueur devant déboucher sur des actions pertinentes et concrètes. Le système dont on étudie les défaillances doit d'abord être décortiqué sur la base des questions suivantes : A quoi sert-il ? Quelles fonctions doit-il remplir ? Comment fonctionne-t-il ? Par la suite, le système est analysé sous les aspects externes en relation avec le milieu extérieur et les aspects internes en diagnostiquant des flux et des activités spécifiques. Le mode de défaillance exprime de quelle manière cette fonction ne fait plus ce qu'elle est censée faire. Ainsi, l'analyse fonctionnelle recense les fonctions alors que l'AMDEC envisage pour chacune d'entre-elles

sa façon de ne plus se comporter correctement. Un mode de défaillance peut résulter de la combinaison de plusieurs causes. Une cause peut être à l'origine de plusieurs modes de défaillances. C'est l'anomalie qui conduit au mode de défaillance. La défaillance est un écart par rapport à la norme de fonctionnement. Les causes trouvent leurs sources dans cinq grandes familles (5M) cités en amont **[20]**. On en fait l'inventaire dans des diagrammes dits "diagrammes de causes à effets". Chaque famille peut, à son tour, être décomposée en sous-famille. Quant à l'effet, elle concrétise la conséquence du mode de défaillance et peut lui-même devenir la cause d'un autre mode de défaillance. Il dépend également du type de l'AMDEC, en effet l'AMDEC procédé a des effets sur la qualité du produit, l'AMDEC machine à des effets sur la productivité et enfin l'AMDEC sécurité agit sur la sécurité.

III.3.3 L'évaluation des défaillances et la définition des actions

L'évaluation se fait selon trois critères principaux, il s'agit notamment de la gravité, de la fréquence et de la non-détection **[21]**. La gravité est l'importance de l'effet sur la qualité du produit (AMDEC procédé) ou sur la productivité (AMDEC machine) ou sur la sécurité (AMDEC sécurité). Quant à la fréquence, elle est la période à laquelle la défaillance est susceptible de se reproduire alors que la non-détection est l'efficacité du système permettant de détecter le problème. Ces critères ne sont pas limitatifs, en effet le groupe de travail peut en définir d'autres plus judicieux par rapport au problème traité ou au secteur d'activité concerné. Chaque critère est évalué dans une plage de notes par exemple: de 1 à 4 et de 1 à 10. Plus la note est élevée, plus sa sévérité est grande. Une plage d'évaluation large oblige à plus de finesse dans l'analyse. Ce qui peut donner lieu à des controverses au sein du groupe de travail. Le nombre de niveaux d'évaluation doit être pair pour éviter le compromis moyen systématique sur une note globale. A l'issu des séances d'évaluation, le groupe de travail doit alors décider d'un seuil de criticité au-delà duquel, l'effet de la défaillance n'est pas supportable. Une action est alors nécessaire. La criticité est obtenue en faisant le produit des trois notes relatives à la gravité, à la fréquence et à la non-détection **[18]**.

Criticité =gravité* fréquence* non-détection
C = G * F * N

Dans le secteur industriel, le risque est une combinaison de la probabilité à laquelle survient un événement et de la gravité de ses conséquences. La gravité traduit dans ce cas l'importance des dommages et dépend de l'importance des enjeux, de leurs vulnérabilités et de l'intensité du phénomène considéré. Dans ce cas, la criticité du risque se calcule comme suit **[22]** :

Criticité = Probabilité de survenance * Gravité des conséquences
C = P*G

Suite à la mise en évidence des défaillances critiques, la finalité de l'AMDEC est de définir des actions qui vont traiter le problème identifié. Ces actions sont de trois types **:**

- **Actions préventives:** permettant de prévenir la défaillance avant qu'elle ne se produise, pour l'empêcher de se produire. Ces actions sont planifiées. La période d'application d'une action résulte de l'évaluation de la fréquence.

- **Actions correctives**: lorsque le problème n'est pas considéré comme critique, on agit au moment où il se présente. L'action doit alors être la plus courte possible pour une remise aux normes rapide.
- **Actions amélioratives**: Il s'agit de modifications de procédé ou de modifications technologiques du moyen de production destinées à faire disparaître totalement le problème. Le coût de ce type d'action n'est pas négligeable et est souvent considéré comme un investissement.

Ces actions, pour être efficaces, doivent faire l'objet d'un plan d'actions suivi, d'une désignation d'un responsable de chaque action, d'une détermination d'un délai et d'un budget mais aussi d'une révision de l'évaluation après mise en place de l'action afin de s'assurer que le problème identifié a été résolu.

III.4 Méthode outillée

Plusieurs travaux ont porté sur la détermination des risques résiduels, qui est une problématique d'actualité depuis plus d'une dizaine d'années. Certaines de ces études portent notamment sur le développement d'outils de gestion des risques. Ainsi en 2008, Ciorciari dans **[79]** propose un outil de management de risque basé sur les huit étapes du COSO et permettant d'évaluer le niveau de maturité du risque d'entreprise de manière automatisée et guidée. A titre indicatif, les huit composantes du COSO sont relatives à l'environnement interne, à l'établissement d'objectif, à l'identification d'événements, à l'évaluation des risques inhérents et résiduels, aux activités de contrôle, à l'information, à la communication et enfin au pilotage de ce dispositif de maitrise. Les fonctionnalités de l'outil ainsi développé comprennent, entre autres, l'évaluation du niveau de maturité, la gestion et la documentation du risque d'entreprise, l'aperçu des résultats compte tenu des différentes dimensions, l'évaluation multi-périodes sur différentes dates de référence, l'identification des faiblesses et forces ainsi que la définition d'une liste de mesures hiérarchisées.

Les risques identifiés au niveau de l'outil sont associés à des objectifs susceptibles d'être affectés avant d'être analysés dans le but de déterminer comment ils devraient être gérés. Les risques sont évalués à la fois de façon inhérente et résiduelle, l'évaluation tenant compte aussi bien de la probabilité de survenance que de la gravité potentielle du risque. Cependant, nous pouvons noter que l'outil comporte une limite certaine car il ne prend pas en compte les évolutions et les changements au sein de l'entreprise. En effet, la gestion des risques ne peut pas être considérée comme un processus ponctuel et statique, l'outil est juste un support à une démarche globale qui doit être intégrée dans l'organisation et dynamiquement adaptée à l'évolution de l'environnement interne et externe.

Dans la même lancée, en 2013 Marvell et Creasey dans **[80]** proposent un outil dédié à la gestion des risques liés à l'information. L'outil l'IRAM qu'ils ont développé permet l'analyse des risques liés à l'information, l'évaluation de l'impact sur les entreprises, l'évaluation des menaces et des vulnérabilités mais aussi la sélection des contrôles. Ainsi, l'IRAM intègre une large gamme de contrôles et offre la possibilité de sélectionner des contrôles supplémentaires permettant de réduire le niveau de risque résiduel en tenant compte des différents facteurs y afférents comme la fréquence des menaces, les vulnérabilités et les contrôles implémentés. Cependant, nous avons constaté que l'outil ne permet de quantifier

le risque résiduel et ne constitue pas une solution web intégrée car il ne fournit pas d'outils destinés à la surveillance continue et nécessaire à la maitrise des risques à temps réel.

Par ailleurs, le volet sécurité est également pris en charge dans la méthodologie outillée. Ainsi en 2005, Peter dans **[81]** propose un outil intégré d'analyse des risques incluant l'évaluation des actifs, des menaces et des vulnérabilités tout en adoptant les techniques de gestion des risques logiciels. La contribution majeure consiste à appliquer le concept et les techniques de gestion des risques logiciels à l'analyse des risques de sécurité. Ainsi, le risque de sécurité peut être évalué quantitativement sur la base de la perte des actifs et de sa probabilité de survenance. De plus, il utilise les techniques d'atténuation des risques pour réduire les risques pertinents et maitriser les risques résiduels. Les quatre phases de l'outil ainsi proposé constituent un processus d'analyse des risques sécurité des systèmes d'information. La première étape identifie les actifs, les menaces et vulnérabilités de l'organisation cible et les évalue. Les résultats de cette étape sont utilisés pour analyser le risque de sécurité dans la deuxième étape. Au niveau de la troisième étape, des méthodes appropriées d'atténuation des risques sont appliquées. La dernière étape résume les risques inhérents, les types et les coûts des mesures sécuritaires, les risques résiduels liés à la sécurité ainsi que leur retour sur investissement. Cela va aider les décideurs à optimiser les ressources pour minimiser les risques relatifs à la sécurité. Cependant, l'étude ne permet pas l'élaboration de lignes directrices détaillées avec des exemples et ne constitue pas un outil d'analyse des risques prenant en compte la visualisation et l'optimisation des politiques de sécurité informatique. Dans le même ordre d'idées, en 2010, Pagett dans **[82]** propose un outil intégrant le Cadre d'Efficacité de la Sécurité de l'Information (ISEF) qui facilite la définition, la visualisation et la comparaison des métriques de sécurité pour améliorer la gestion des risques résiduels. Le framework ISEF utilise le concept de regroupement des contrôles en fonction de leur type d'implémentation et des objectifs temporels pour présenter des caractéristiques communes pouvant être mesurées. Il utilise aussi la relation entre les contrôles et les risques pour aligner les mesures de sécurité et les visualiser pour soutenir les efforts consentis. L'ISEF est conçu pour compléter les modèles et normes de gouvernance informatique actuels tels que COBIT et ISO 27002.

Cependant pour rendre la mesure de l'efficacité plus précise, nous remarquons que des recherches de contrôles supplémentaires pourraient être réalisées. De plus, l'ISEF calcule l'efficacité des contrôles en faisant la moyenne des mesures de contrôles ; bien que cela fournisse une méthode d'agrégation simple, certaines caractéristiques peuvent être plus importantes que d'autres pour la réduction des risques et devraient donc être pondérées par rapport à l'agrégation de la mesure. L'ISEF pourrait donc être amélioré en menant des recherches sur l'importance des différentes caractéristiques dans la réduction des risques. Les étapes, avantages et limites des différents outils sont déclinées ci-après.

METHODES OUTILLEES	ETAPES	AVANTAGES	INCONVENIENTS
• **Outil basé sur les étapes du COSO**	• l'évaluation du niveau de maturité • la définition d'une liste de mesures hiérarchisées. • Evaluation des risques inhérents et résiduels • l'évaluation multi-périodes sur différents dates de référence	• la gestion et la documentation du risque • l'aperçu des résultats des différentes dimensions • l'identification des faiblesses et forces • complète les modèles et normes de gouvernance informatique actuels tels que COBIT et ISO27002	• ne prend en compte les évolutions et les changements au sein de l'entreprise
• **Outil IRAM**	• intègre une large gamme de contrôles et offre la possibilité de sélectionner des contrôles supplémentaires permettant de réduire le niveau de risque résiduel • l'évaluation des menaces et des vulnérabilités mais aussi la sélection des contrôles	• permet l'analyse des risques liés à l'information, l'évaluation de l'impact sur les entreprises • Prise en compte des différents facteurs y afférents comme la fréquence des menaces, les vulnérabilités et les contrôles implémentés	• ne permet de quantifier le risque résiduel et ne constitue pas une solution web intégrée • il ne fournit pas d'outils destinés à la surveillance continue et nécessaire à la maitrise des risques à temps réel.

Figure 1:Comparaison des méthodes outillées (début)

METHODES OUTILLEES	ETAPES	AVANTAGES	INCONVENIENTS
•**Outil intégré d'analyse des risques**	•identifie les actifs, les menaces et vulnérabilités de l'organisation cible et les évalue. •analyser le risque de sécurité dans la deuxième étape • application des méthodes appropriées d'atténuation résume les risques inhérents, les types et les coûts des mesures sécuritaires, et les risques sécurité résiduels.	•le risque de sécurité est évalué quantitativement sur la base de la perte des actifs et de sa probabilité de survenance •incluant l'évaluation des actifs, des menaces et des vulnérabilités •en adoptant les techniques de gestion des risques logiciels •réduire les risques pertinents et maitriser les risques résiduel	•ne permet pas l'élaboration de lignes directrices détaillées • ne constitue pas un outil d'analyse des risques prenant en compte la visualisation et l'optimisation des politiques de sécurité informatique
•**Framework ISEF**	•utilise aussi la relation entre les contrôles et les risques pour aligner les mesures de sécurité et les visualiser pour soutenir les efforts consentis	•compléter les modèles et normes de gouvernance informatique actuels tels que COBIT et ISO27002	• ne tient pas compte de l'importance des différentes caractéristiques dans la réduction des risques.

Figure 2:Comparaison des méthodes outillées (suite et fin)

III.5 Méthode RSCA (Risk Self Control Assessment)

La méthode RSCA est la plus utilisée pour déterminer la criticité résiduelle des risques. Le RCSA est basé sur le COSO et fait partie intégrante du cadre global de gestion des risques **[83]**. Il constitue une excellente opportunité pour une entreprise, lui permettant ainsi d'intégrer et de coordonner toutes les actions liées à son dispositif de maitrise des risques. Le RCSA fournit également un moyen systématique d'identifier les lacunes des contrôles qui menacent la réalisation des objectifs d'entreprise ou des processus définis, il permet aussi de surveiller les actions entreprises par la direction pour combler ses lacunes. Les résultats d'un RCSA sont utilisés pour formuler des plans d'action appropriés en matière de contrôle tout en tenant compte des considérations en termes de coûts et avantages. De plus le RCSA agit comme un outil d'audit et de gestion complémentaire, tout en étant un moyen efficace permettant de satisfaire la gouvernance d'entreprise et la conformité aux exigences réglementaires. Les caractéristiques de base d'un RCSA typique comprendront l'identification des objectifs stratégiques qui peuvent être traduits en objectifs processus, l'identification des risques qui pourraient menacer la réalisation de ces objectifs ainsi que les activités et processus affectés par les différents risques identifiés, l'identification des contrôles mis en place et destinés à empêcher la cristallisation des risques.

Les deux dernières étapes correspondent à la détermination des responsabilités dans l'exécution de ces contrôles, à l'évaluation de l'efficacité des contrôles mis en œuvre à travers l'estimation du niveau de risque résiduel. Nous pouvons donc conclure que le RCSA doit être soigneusement conçu, planifié et exécuté afin qu'il ait le succès attendu et la réalisation de toute sa gamme de bénéfices potentiels. Les principales étapes du RSCA sont synthétisées ci-dessous :

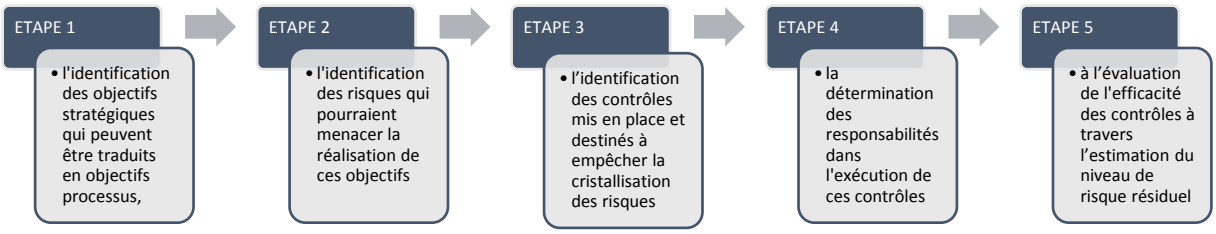


Figure 3: Les principales étapes du RSCA

III.5.1 Les approches du RSCA

En mars 2010, toutes les étapes du RSCA ont été décrites et des précisons ont été apportées sur ses trois approches dans **[57].** Chacune de ces approches peut être mise en œuvre avec succès selon la taille de l'entreprise, à condition qu'il y ait un engagement suffisant à l'égard du concept de RCSA aussi bien au niveau des cadres que dans les échelons inférieurs.

- **l'approche workshop**

L'approche workshop ou atelier est un mécanisme pour amener les gens à parler de leurs risques, de leurs contrôles et des potentielles améliorations à faire. Elle permet également de mettre en évidence les événements factuels et peut être exécutée en conjonction avec les listes de contrôle figurants dans les procédures. Les avantages d'une telle approche incluent la sensibilisation aux risques transversaux et hiérarchiques, l'évaluation et l'amélioration des mécanismes, la communication, la formation ainsi que le transfert des compétences liées à la gestion des risques à travers l'organisation. Les principales étapes de cette approche sont la planification, l'identification des participants et de leur nombre, la durée des ateliers, la terminologie à adopter, le nombre et la durée des sessions, les règles de bases et les compétences requises ainsi que la méthodologie collecte des données. Ces étapes sont représentées dans le schéma ci-dessous :

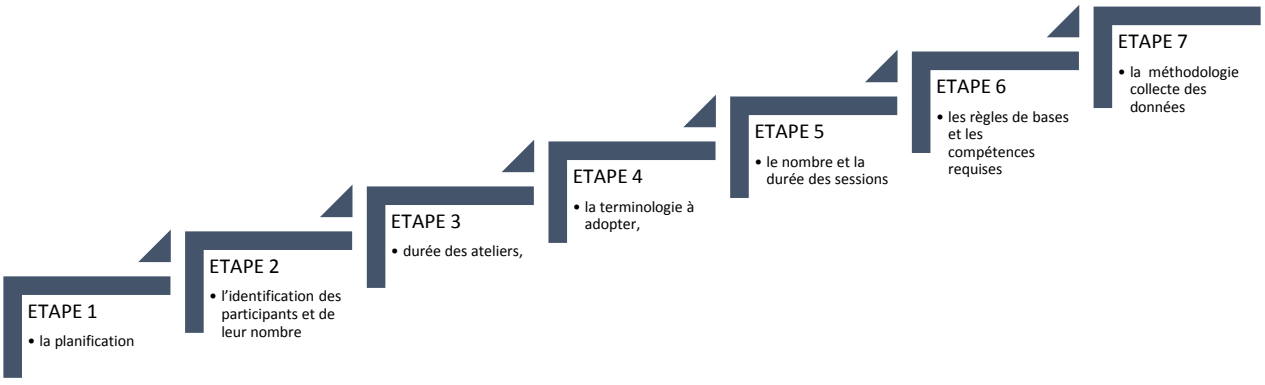


Figure 4: les différentes étapes du RSCA workshop

- **L'approche questionnaire**

L'approche questionnaire peut aussi être utilisée, certaines entreprises préfèrent l'avantage qu'offre la mise en place d'une liste étendue et complète de questionnaires avec des questions attribuées aux répondants en fonction de la pertinence des activités qui sont sous leurs responsabilités. Les RCSA basés sur un questionnaire peuvent avoir de la valeur ajoutée en permettant de démontrer une compréhension des rôles et responsabilités liés au risque opérationnel de chaque secteur de l'entreprise, une identification des risques opérationnels rencontrés, une évaluation du risque résiduel non contrôlé en tenant compte des contrôles effectifs mais aussi la performance de l'ensemble des contrôles mis en œuvre. Les principales étapes de cette l'approche sont la structuration du questionnaire, la détermination de la durée d'administration du questionnaire et la définition de la périodicité d'administration du questionnaire. Ces étapes sont résumées dans le schéma ci-après :

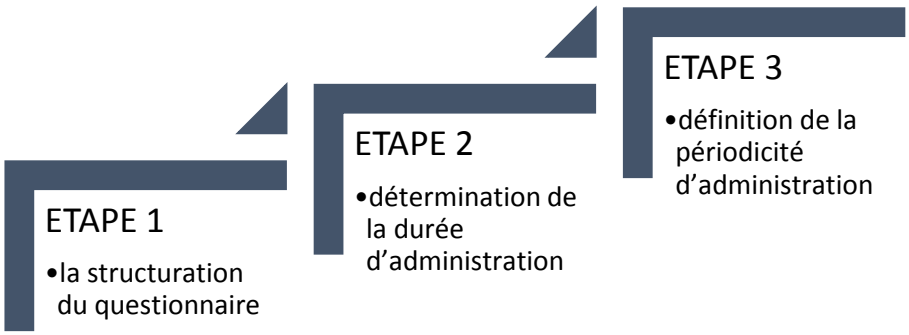


Figure 5:les différentes étapes du RSCA questionnaire

- **L'approche hybride**

L'approche hybride consiste à démarrer avec une approche workshop qui sera suivie par la suite d'un format de questionnaire pour les prochaines utilisations de la méthode RCSA avec la possibilité de tenir un autre workshop si un nouvel événement déclencheur majeur se produit. L'approche hybride a pour principal avantage de réussir à maintenir de façon dynamique tout le dispositif de maitrise des risques au fil du temps sans surcharger les participants.

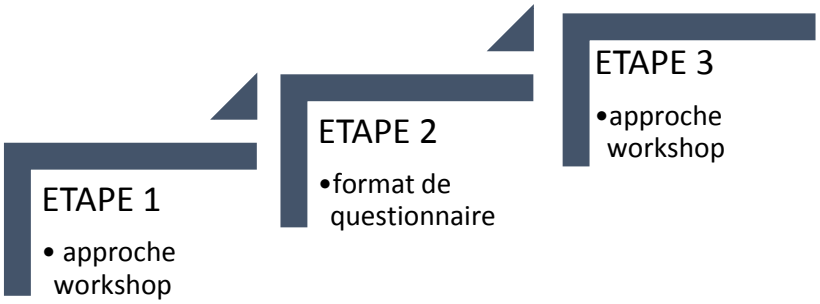


Figure 6:les différentes étapes du RSCA hybride

III.5.2 Estimation du risque résiduel selon RSCA

Selon la méthode RSCA, le risque résiduel est obtenu en tenant compte du niveau de risque inhérent et des contrôles mis en œuvre. Les contrôles sont définis pour réduire la probabilité de survenance et/ou la gravité des conséquences du risque. La gravité potentielle et la probabilité de survenance des risques résiduels doivent donc être estimées en prenant en compte les contrôles effectivement déployés. Le niveau de risque résiduel est calculé en évaluant l'effet des contrôles mis en œuvre sur le risque inhérent et en utilisant des échelles permettant d'établir les valeurs de probabilité de survenance et de gravité potentielle résiduelles; le niveau de risque résiduel étant le produit de ces deux valeurs **[84].**

Ces valeurs peuvent ensuite être repositionnées sur la matrice de criticité avec la gravité potentielle en ordonnée et la probabilité de survenance en abscisse afin d'être analysées et interprétées **[85].** A ce niveau, la stratégie de traitement à adopter dépendra du niveau de criticité de ces risques résiduels. En 2003, Kellogg dans **[86]** relate que ce niveau de risque résiduel doit être réduit constamment. Il s'agit essentiellement de déterminer si le risque résiduel s'améliore, est stable ou s'érode avec le temps. Il faut également communiquer sur le niveau de risque résiduel et définir des stratégies de traitement adaptées afin qu'ils ne dépassent pas l'appétence au risque que l'organisation s'est fixée **[87].** Par la suite, des mesures supplémentaires doivent être implémentées au besoin pour maintenir les risques résiduels à un niveau acceptable. En 2015, Mathur et Pandya dans **[88]** démontrent qu'il est difficile de surmonter ou d'atténuer l'impact des risques à 100%. Par conséquent, le management de l'organisation doit décider du niveau d'acceptation des risques, ce niveau d'acceptation doit correspondre au niveau de risque résiduel. De manière spécifique, la méthode RSCA est utilisée dans la gestion des risques liés au système d'information, ainsi en 2014 Unuakhalu, Sigdel et Garikapati dans **[89]** passent en revue chaque phase du cycle de développement d'un logiciel SDLC (Software Development Life Cycle) et fournissent un ensemble d'étapes de sécurité qui doivent être efficacement intégrées dans un système au cours de son développement. Selon l'étude, pour atteindre les objectifs de sécurité, il faut identifier les exigences de sécurité dès le début du processus de développement et les intégrer au cycle SDLC. Ainsi, le responsable ordonnateur du RSCA est chargé de déterminer si le risque résiduel est à un niveau acceptable ou si des contrôles de sécurité supplémentaires doivent être mis en œuvre pour le réduire ou l'éliminer avant d'autoriser l'exploitation du système d'information. Toujours dans ce même contexte, le risque résiduel relatif au cyber sécurité est analysé avec l'approche RSCA. Ainsi, en 2017, Simpson dans **[90]** relatent que la FCC (Fédéral Communications Commission) a un rôle et une responsabilité

dans la gestion du risque résiduel lié au cyber sécurité. Ces risques correspondent au risque subsistant après que les acteurs du marché ont agi pour remédier au cyber risque.

Le risque résiduel peut être important et malheureusement imposé aux acteurs qui ne sont pas sensibilisés sur son existence ou sur les moyens d'y remédier**.** Cela est particulièrement vrai car les consommateurs ne sont pas conscients du risque qu'on leur demande de supporter. A ce propos, les entreprises qui intériorisent leurs risques ont un avantage concurrentiel car ils renoncent aux investissements liés au cyber sécurité et réduisent le coût de leurs services. Cependant il s'expose à une perte de part de marché à moyen ou long terme. De manière générale, la méthode RSCA est également très utilisée pour déterminer les autres risques résiduels spécifiques aux métiers bancaires. En 2015, les accords de Bale s'appesantissent sur le risque résiduel bancaire qui se définit comme étant le niveau de risque qui subsiste après la mise en œuvre des traitements pouvant concerner la règlementation ou la surveillance comptable **[8].** A cet effet, les évaluations de probabilité de survenance et de gravité potentielle des risques constituent un moyen de quantifier les risques inhérents mais aussi les risques résiduels qui prennent en compte les contrôles effectivement mis en œuvre. Les mesures de probabilité de survenance et de gravité potentielle du risque peuvent être rapportées séparément ou en combinaison avant d'être classées selon les quatre niveaux de criticité très élevé, élevé, moyen ou faible. En guise d'exemples, le risque de taux d'intérêt peut être évalué comme élevé en termes de probabilité et très élevé en termes de gravité; le risque global de taux d'intérêt peut alors être considéré comme élevé. La stratégie d'atténuation des risques résiduels peut potentiellement réduire la probabilité de survenance et/ou la gravité potentielle du risque inhérent. Quoi qu'il en soit, dans le volet reporting des risques, il va falloir prendre compte les risques résiduels. Dans ce contexte, en 2015, la méthodologie de la NMLRA (National Money Laundering Risk Assessment) qui est une structure nationale qui évalue le risque de blanchiment d'argent aux Etats Unis est décrit dans **[91].** L'objectif de la NMLRA est d'expliquer les méthodes de blanchiment d'argent utilisées aux États-Unis pour traiter les menaces et les vulnérabilités qui créent des opportunités de blanchiment d'argent ainsi que le risque résiduel pour le système financier et la sécurité nationale. Le processus d'établissement des faits et de l'évaluation proprement dite consiste essentiellement à utiliser les recherches et analyses précédentes pour identifier les risques résiduels de blanchiment d'argent. Les concepts de base de l'évaluation des risques sont les crimes sous-jacents associés au blanchiment d'argent, les opportunités qui facilitent le blanchiment d'argent et l'impact des vulnérabilités. Ainsi, la méthodologie utilisée est basée sur la recherche des menaces, des vulnérabilités et des conséquences mais aussi sur l'identification des risques qui correspondent à une synthèse de ces trois paramètres. Par la suite, il faut identifier la nature et le volume des crimes financiers, comptabiliser les méthodes de blanchiment d'argent identifiées par des enquêtes civiles et pénales, évaluer l'effet dissuasif de la réglementation, de la supervision et leur l'application à l'échelle nationale sur les potentiels méthodes de blanchiment d'argent et enfin utiliser les recherches et analyses précédentes pour identifier les risques résiduels de blanchiment d'argent. Nous pouvons donc en déduire que cette méthodologie requiert du temps, de l'expertise et de la documentation. La synthèse des différents travaux basés sur le RSCA est schématisée ci-après :

DATE	UTILISATION RSCA	DESCRIPTION	APPORT
•2014	•gestion des risques liés au système d'information	•il s'agit d'identifier les exigences de sécurité dès le début du processus de développement et les intégrer au cycle SDLC	•déterminer si le risque résiduel est acceptable ou si des contrôles supplémentaires doivent être mis en œuvre
•2015	•détermination des risques résiduels spécifiques au métier de la banque	•les évaluations de probabilité de survenance et de gravité potentielle sont un moyen de mesurer les risques inhérents et les risques résiduels qui prennent en compte les contrôles effectivement	• Les mesures de probabilité de survenance et de gravité potentielle du risque peuvent être rapportées séparément ou en combinaison
•2015	•traitement des menaces et les vulnérabilités qui créent des opportunités de blanchiment d'argent ainsi que le risque résiduel pour le système financier	•recherche des menaces, des vulnérabilités et des conséquences mais aussi sur l'identification des risques de blanchiment d'argent	•utiliser les recherches et analyses précédentes pour identifier les risques résiduels de blanchiment d'argent
•2017	•analyse du risque résiduel relatif à la cyber sécurité	•Le risque résiduel peut être important et être malheureusement imposé aux acteurs qui ne sont pas sensibilisés sur son existence ou sur les moyens d'y remédier.	•les entreprises qui intériorisent leurs risques ont un avantage concurrentiel car ils renoncent aux investissements liés à la cyber sécurité et réduisent le coût de leurs services

Figure 7: La synthèse de ces travaux basés sur le RSCA

Eu égard ce qui précède, il s'avère que la méthode RSCA est fastidieuse quelle que soit l'approche utilisée. Face à cette complexité, différents travaux ont tenté d'alléger la démarche en automatisant le volet calcul des risques résiduels avec le RSCA.

III.5.3 Variante RSCA : Calcul du risque résiduel avec le Pourcentage de réduction

En 2017, Toburen dans **[92]** propose une méthodologie basée sur le RSCA pour identifier l'information qui doit être protégée dans le but de réduire le risque commercial, localiser des informations importantes au sein de l'organisation et évaluer le risque lié à l'information ainsi que les contrôles mis en place pour gérer ces risques. Par la suite, il définit la formule suivante pour déterminer le risque résiduel qui correspond au risque qui subsiste après avoir évalué les traitements déjà appliqués:

Risque résiduel = Risque inhérent x Pourcentage de réduction des risques par rapport aux traitements appliqués

Il précise également qu'étant donné qu'aucun traitement de risque ne peut être considéré comme efficace à 100%, le résultat de ce type de calcul ne devrait jamais être nul. Cela conforte l'idée selon laquelle la gestion des risques n'est pas l'élimination des risques; c'est plutôt l'effort continu pour équilibrer les traitements contre les risques afin que le risque de l'entreprise ne dépasse jamais l'appétence définie.

Cela nécessite un re-calcul constant des niveaux de risque et une attention particulière aux changements dans le profil de risque de l'entreprise. Pour ce faire, le cadre mis en place doit inclure les moyens permettant de mesurer la tolérance au risque et l'appétit pour le risque, de façon à pouvoir détecter quand est que le risque menace l'appétence définie et déterminer en connaissance de cause ce qu'il faut faire. Cependant, il apparait clair que la formule proposée n'est pas testée et que ses forces et faiblesses ne sont pas identifiées. Le tableau synthétisant les avantages et limites de cette méthode est décliné ci-après :

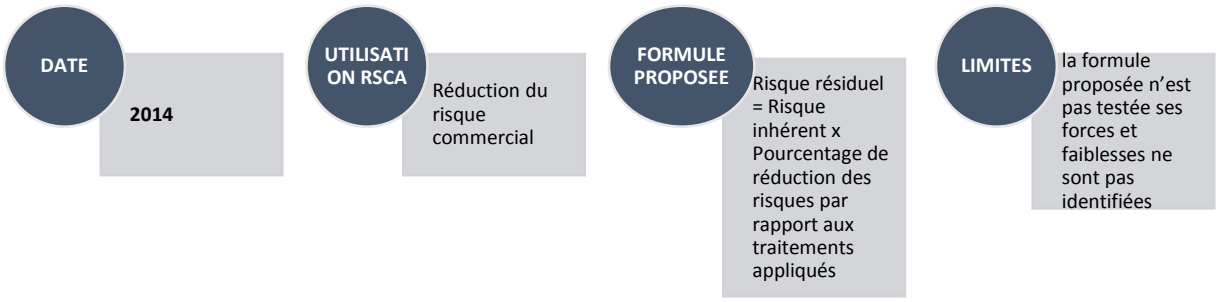


Figure 8: Spécificités de la variante RSCA utilisant le Pourcentage de réduction

III.5.4 Variante RSCA : Calcul du risque résiduel avec la soustraction

En 2011, AMANCEI dans **[93]** propose une méthode basée sur l'utilisation du RSCA questionnaire. Cette méthode démarre par l'évaluation des risques inhérents liés à la sécurité de l'information avant de procéder au calcul des risques résiduels. La méthode proposée contient tous les éléments clés qui concourent à la gestion des risques. Il s'agit notamment des éléments proposés pour le questionnaire d'évaluation à savoir: la liste des menaces, la classification et l'évaluation des ressources, la corrélation entre risques et contrôles et le calcul du risque résiduel. Elle se base sur une liste de menaces qui sous-tendent la définition des scénarii de risque. Par la suite les ressources affectées par les scénarii de risque sont évaluées en termes de perte de confidentialité, d'intégrité, de disponibilité et de fiabilité. Pour obtenir le risque résiduel, il calcule d'abord le risque inhérent en évaluant la probabilité de survenance et la gravité potentielle de chaque

scénario de risque appliqué aux ressources de l'entreprise. Les contrôles mis en œuvre sont évalués par le questionnaire dans le but d'identifier la valeur de chaque contrôle permettant ainsi de déterminer le niveau de risque résiduel. Pour ce faire, le risque résiduel subsistant après la mise en œuvre des contrôles est obtenu en utilisant la formule proposée ci-après :

Risque résiduel = Risque inhérent - Maturité de tous les contrôles évalués

Les risques résiduels ainsi calculés sont classés dans la matrice selon leurs criticités; les risques très critiques et critiques seront inclus dans le plan de traitement qui permettra de les réduire à un niveau acceptable par l'entreprise. Cependant nous constatons que les valeurs du modèle proposée ne sont comparées aux valeurs de référence dans l'optique d'éprouver le modèle. Dans le même ordre d'idées, en 2018 dans **[94]**, le risque résiduel de blanchiment d'argent est analysé en comparant pour chaque scénario, le risque inhérent et le niveau de maturité des contrôles. Concrètement, le risque résiduel est déterminé en soustrayant le niveau de contrôle au niveau de risque inhérent comme nous l'avons vu précédemment. Les niveaux de criticité des risques résiduels sont au nombre de quatre, le premier correspond au niveau faible pour lequel il est peu probable que le risque cause des dommages alors que le deuxième niveau correspond au niveau modéré pour lequel Il y a une légère possibilité que le risque cause des dommages. Les derniers niveaux de criticité des risques sont la criticité élevée qui signifie qu'il existe une probabilité considérable pour que le risque cause des dommages importants et la criticité extrême pour lequel Il y a une certitude que le risque ait un impact dramatique. Après avoir déterminé le niveau de risque résiduel, il faudra toujours vérifier qu'il se situe dans les limites de l'appétence défini par l'entreprise. Si la réduction est impossible en raison de la nature du risque, il va falloir s'assurer que des mesures de contrôle supplémentaires sont définies. L'étude précise qu'il sera impossible de réduire tous les risques à zéro car le risque résiduel peut subsister après la mise en place de mesures supplémentaires. Cette méthode est donc plus explicite que la précédente bien qu'elles soient toutes les deux basées sur la soustraction entre les risques inhérents et les contrôles déployés. Mais, nous remarquons qu'elle ne donne pas de précisions sur la manière de soustraire et ne procède pas à des tests de validation pour approbation.

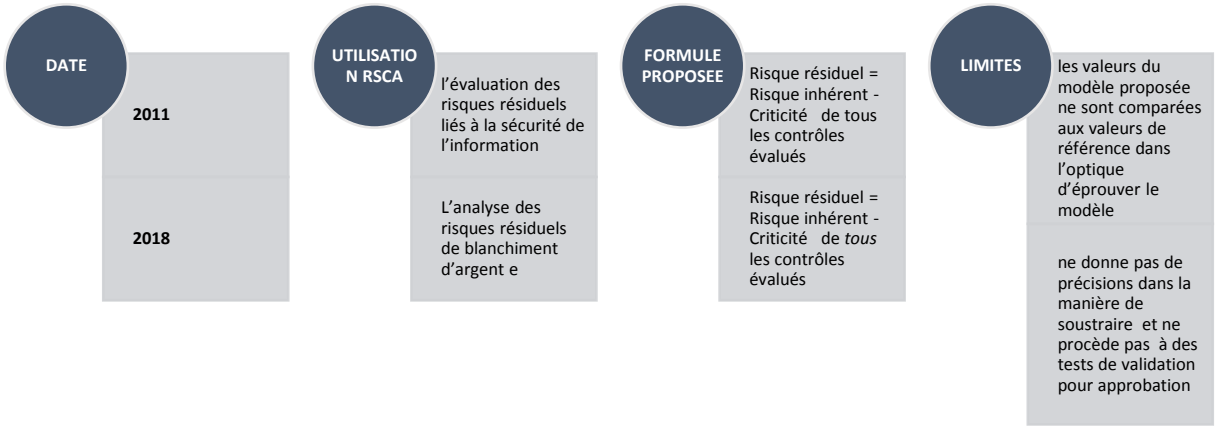


Figure 9:Spécificités de la variante RSCA utilisant la soustraction

Suite à ce qui précède, Il s'avère que quelle soit l'approche utilisée pour évaluer les risques résiduels selon la méthode RSCA, il faudra au préalable identifier chacun des contrôles mis en œuvre et évaluer honnêtement leur pertinence et leur capacité à atténuer les risques inhérents. Les résultats obtenus permettront de vérifier par la suite si le risque résiduel se situe dans l'appétence de l'entreprise en termes de probabilité de survenance et de gravité potentielle résiduelles.

III.5 Synthèse

La détermination des risques résiduels bancaires est une tâche à la fois complexe et difficile compte tenu de la diversité des typologies risques bancaires et des contrôles mis en œuvre. Ainsi, les principales méthodes utilisées sont la méthode outillée basée sur l'utilisation de logiciels dédiés à la gestion des risques et la méthode RSCA qui possède trois approches principales, à savoir l'approche workshop, l'approche questionnaire et l'approche hybride qui constitue une synthèse des deux premières approches**.** Le RSCA consiste à attribuer à chaque risque, une estimation du niveau de risque résiduel que ce soit pour les risques liés au système d'information **[95]** ou pour les autres risques bancaires **[96].** Aussi, il apparait que la méthode RSCA demeure la plus utilisée et se base sur l'AMDEC qui permet de faire une analyse des modes de défaillance, de leurs effets et leurs criticités **[10]**. C'est d'ailleurs la raison pour laquelle, l'estimation des risques résiduels se fait au cours de plusieurs sessions de travail avec des évaluateurs de profil différents et nécessite souvent un consensus en cas de désaccord **[97].** A cet effet, la probabilité de survenance et la gravité potentielle des différents risques résiduels sont estimées puis combinés en vue de déterminer le niveau de criticité des risques résiduels. La méthode RSCA actuellement utilisée passe nécessairement par plusieurs étapes préliminaires, il s'agit notamment de la définition des objectifs de processus, de l'identification des risques liés à chaque processus, de l'évaluation des risques

inhérents identifiés et de l'évaluation des contrôles mis en œuvre [**98].** L'estimation de l'impact des contrôles mis en œuvre sur les risques inhérents permet d'obtenir le niveau de risque résiduel. Par la suite, les résultats obtenus sont représentés sur une matrice permettant de distinguer les risques résiduels de criticité faible, moyenne, élevée ou extrême [**99].** Cette évaluation est minutieuse et requiert une prise en charge spécifique pour chaque type de produit et service avec des profils d'intervenants adaptés selon le type de risque **[100].** De plus, cette méthodologie est manuelle, fastidieuse et comporte un certain nombre de limites à savoir: une perte de temps, un investissement personnel de la part des intervenants, un certain niveau d'expertise de leurs part et de potentiels erreurs d'estimation. Dans l'optique d'alléger cette démarche, les récents travaux relatifs au RSCA proposent une soustraction entre les risques inhérents et les contrôles implémentés pour obtenir les risques résiduels**.** Cependant il n'y a pas de précision dans la manière de soustraire et les valeurs des modèles ne sont pas comparées aux données de référence **[93]** .Notre contribution va donc s'inscrire dans ce cadre et s'articuler autour de la définition détaillée de modèles permettant de calculer les risques résiduels tout en effectuant des tests explicites afin de les éprouver avant validation.

Conclusion

A l'issu de ce chapitre, nous avons pu constater que les dispositifs de maitrise des risques mis œuvre par les banques sont divers et sont liés aux typologies de risques. Le pilotage effectif de ce dispositif s'appuie essentiellement sur le COSO qui peut être implémenté selon la particularité de la banque. Ainsi, l'évaluation des risques résiduels se fait généralement avec la méthode RSCA basée sur l'AMDEC dont les spécificités ont été décrites au niveau de ce chapitre. L'analyse effectuée révèle que le RSCA est fastidieux, requiert plusieurs séances de travail, des évaluateurs expérimentés et nécessite des compromis en cas de divergence et comporte parfois des erreurs. Etant donné que ces limites ne sont pas corrigées par les tentatives d'allègements existants, on se propose d'utiliser une nouvelle approche pour définir des modèles qui vont permettre de calculer les risques résiduels en quantifiant l'impact des contrôles implémentés sur les risques inhérents. Cela permettra de déterminer le niveau exact de risque résiduel sachant qu'une détermination approximative du niveau de risque résiduel peut mettre la banque dans une situation de confort irréel pouvant entrainer l'augmentation des cas de fraude, des réclamations clients, des pertes financières, la dégradation de son image ou encore la diminution de son chiffre d'affaire.

Chapitre IV : Contribution sur la modélisation des risques résiduels bancaires

Introduction

Dans ce chapitre, nous allons apporter notre contribution à la problématique soulevée en explicitant les modèles que nous proposons pour calculer la criticité résiduelle des risques bancaires. Pour ce faire, nous avons tenu compte des normes et règlementations en vigueur dans le secteur bancaire, des principes de base de la gestion des risques et du contrôle interne mais également des normes sécuritaires informatiques et monétiques. A cet effet, nous avons d'abord défini des modèles mathématiques initiaux basés sur la maturité et les caractéristiques des contrôles. Par la suite, nous avons amélioré ces modèles en changeant d'approche et en nous focalisant sur la maturité et les types de contrôles dans le but d'améliorer le coefficient de corrélation entre les valeurs obtenues avec les modèles et les données de test collectées au niveau des banques. Nous avons également défini les équations de régressions linéaires et les algorithmes correspondants aux modèles mathématiques proposés dans le but de les éprouver avant validation.

IV.1 Modèles mathématiques

IV.1.1 Modèles mathématiques initiaux

a. Approche

La criticité résiduelle des risques représente le niveau d'exposition réelle de la banque par rapport aux risques encourus. Elle donne une appréciation de l'impact des contrôles mis en place sur la criticité brute des risques. Ces contrôles sont définis et mis en œuvre dans le but de réduire la probabilité de survenance et/ou la gravité potentielle des risques. Pour définir les modèles mathématiques initiaux, nous nous sommes appesantis sur la maturité des contrôles d'une part, et d'autre part sur les caractéristiques spécifiques d'un contrôle qui découlent de l'exploitation des documents de référence **[23], [24], [26]**, **[27] et [57]** et qui sont décrites ci-après :

1. **Existence** : le contrôle relatif au risque est défini et donc il existe
2. **Documentation** : le contrôle est documenté sur la façon d'être exécuté
3. **Effectivité** : le contrôle défini est effectivement mis en œuvre
4. **Traçabilité** : la mise en œuvre du contrôle est traçable
5. **Efficacité** : le contrôle défini et mis en œuvre est efficace
6. **Efficience** : le contrôle défini et mis en œuvre est efficient
7. **Auto-Evaluation** : le contrôle mis en œuvre a la possibilité de s'autoévaluer
8. **Management** : la mise en œuvre du contrôle est surveillée par les supérieurs
9. **Reporting** : un reporting périodique est effectué sur la mise en œuvre du control
10. **Archivage** : tous les documents et justificatifs liées au contrôle sont archivés

L'approche utilisée pour définir les modèles mathématiques initiaux est schématisée ci-dessous :

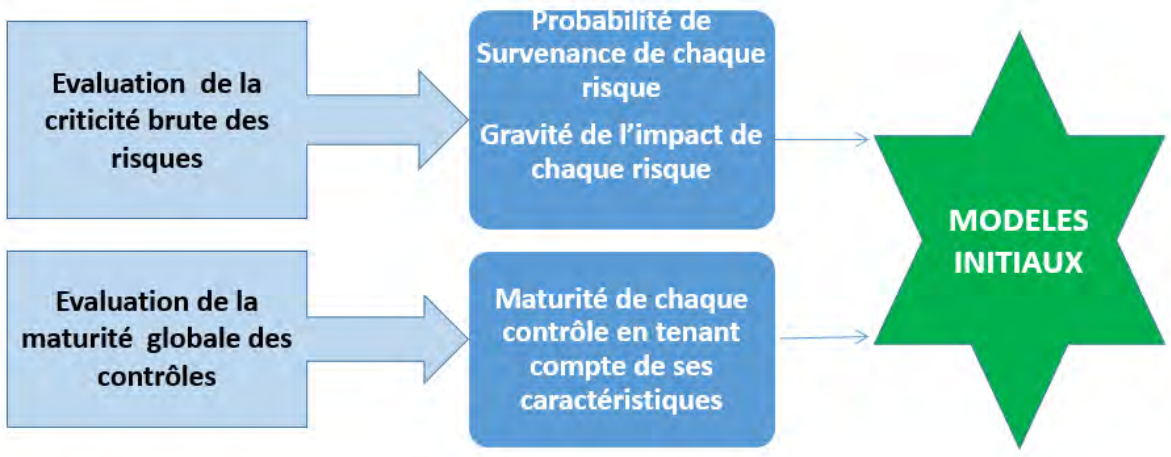


Figure 10: Approche utilisée pour définir les modèles mathématiques initiaux

A la lecture de ce schéma, il apparait que les modèles mathématiques initiaux auront des paramètres liés à la criticité brute des risques et à la maturité globale des contrôles.

b. Principes

Pour proposer les modèles initiaux, nous avons défini les principes ci-dessous qui découlent de l'exploitation documentaire des références **[3], [5], [24], [26], [29], [57], [58], [69], [69] [70], [95], [96] et [97]:**

Principe 1
Un risque peut avoir un ou plusieurs contrôles. En effet, les contrôles sont définis et mis en œuvre dans le but de mitiger les risques. Ainsi selon la nature du risque, un ou plusieurs contrôles y afférents peuvent être définis.

Principe 2
Les contrôles sont définis pour réduire les risques identifiés et évalués. En effet, suite à l'identification des risques, une première évaluation basée sur les échelles de la probabilité de survenance et de la gravité potentielle permet d'assigner à chaque risque, une valeur de criticité brute correspondant au niveau de criticité qui ne tient pas compte des contrôles effectivement mis en œuvre.

Principe 3
Un contrôle a une seule maturité. Cette maturité correspond au niveau de mise en œuvre du contrôle, elle peut être inexistante, informelle, opérationnelle, intégrée ou optimisée.

Principe 4
Seuls les contrôles matures ont la possibilité de réduire les risques associés. En effet, les contrôles matures peuvent réduire significativement la probabilité de survenance brute et/ou la gravité potentielle brute des risques. Pour qu'un contrôle puisse mitiger un risque de façon considérable, il faut qu'il soit mature, cela signifie que sa maturité a un niveau opérationnel au minimum.

c. Modèle 1

Pour définir le modèle 1, nous nous sommes focalisés sur la maturité des contrôles tout en tenant compte des quatre principes définis ci-dessus. Ainsi la criticité résiduelle des risques est obtenue en déduisant la criticité brute des risques de la maturité globale des contrôles. Ce modèle est défini sur la base de la probabilité de survenance brute du risque, de la gravité potentielle brute du risque, du nombre de contrôles par risque et de la maturité globale des contrôles associés à chaque risque. Le premier modèle mathématique proposé est le suivant **:**

Criticité résiduelle = Criticité brute - Maturité globale des contrôles

La criticité brute du risque est obtenue avec la formule existante qui fait le produit de la probabilité de survenance brute et de la gravité potentielle brute du risque **[22].**

Ainsi : Criticité brute= Probabilité brute * Gravité Brute

La probabilité de survenance brute du risque est une estimation des facteurs qui rendent favorable l'apparition du risque; il peut s'agir de facteurs internes ou externes. Elle correspond à la probabilité de survenance du risque en l'absence de contrôles mis en œuvre. Pour obtenir les échelles de probabilité de survenance et de gravité potentielle des risques à utiliser, nous avons procédé à une analyse approfondie des documents **[3], [23] [24]** et **[73]** dans le but de définir des échelles qui tiennent comptent de la diversité des typologies de risques bancaires. Il en résulte la nécessité d'utiliser des échelles de niveaux paires pour éviter d'avoir des risques critiques qui seront considérés comme des risques moyens. Par la suite, il fallait savoir combien de niveaux choisir sachant que les normes préconisent l'utilisation d'échelle à 4 ,6 , 8 ou 10 niveaux, l'échelle de niveau 2 n'ayant aucune finesse. Sur cette base nous avons dressé un tableau comparatif permettant des mettre en exergue les avantages et inconvénients de chaque niveau.

Tableau 1 : Avantages et Inconvénients de niveaux d'échelle

Niveaux	**Spécificités**	**Avantages ou Limites**
4	Evaluation facile grâce à un nombre très réduit de niveaux	Manque de finesse dans l'évaluation
6	**Evaluation relativement facile grâce à un nombre réduit de niveaux**	**Finesse dans l'évaluation**
8	Evaluation fastidieuse à cause du nombre niveaux	Beaucoup de finesse dans l'évaluation
10	Evaluation très fastidieuse à cause du grand nombre de niveaux	Beaucoup plus de finesse dans l'évaluation

D'après le tableau ci-dessous, nous avons choisi l'échelle à 6 niveaux pour ses spécificités et avantages, nous allons donc l'utiliser tout au long de notre modélisation.

Ainsi, l'échelle utilisée pour évaluer la probabilité brute des risques est décrit ci-dessous :

Tableau 2: Echelle de la Probabilité de Survenance brute du risque

Echelle de la Probabilité de Survenance brute du risque	
Coefficient	**Signification**
1	Très peu probable
2	Peu probable
3	Probable
4	Très probable
5	Certain
6	Très Certain

Selon cette échelle, les coefficients affectés à la probabilité de survenance brute du risque ont la valeur 1,2, 3, 4, 5 et 6. Ainsi, lors de l'évaluation de la probabilité de survenance brute de chaque risque, le coefficient approprié est assigné au risque concerné.

La gravité potentielle brute du risque est définie comme étant une estimation des impacts potentiels du risque sur la réalisation des objectifs de la banque. L'échelle utilisée pour évaluer la gravité brute potentielle des risques est également basée sur l'exploitation documentaire évoquée ci-dessus, elle est déclinée ci-après:

Tableau 3:Echelle de la Gravité potentielle brute du risque

Echelle de la Gravité potentielle brute du risque	
Coefficient	**Signification**
1	Très peu grave
2	Peu grave
3	Grave
4	Très grave
5	Situation de crise
6	Crise majeure

Selon cette échelle, les coefficients affectés à la gravité potentielle brute du risque ont les valeurs 1, 2, 3, 4, 5 ou 6. Ainsi, lors de l'évaluation de la gravité potentielle brute de chaque risque, le coefficient approprié est assigné au risque concerné.

La maturité globale des contrôles correspond à la somme des coefficients affectés à la maturité des contrôles. Les valeurs et coefficients relatifs à la maturité des contrôles sont décrits ci-dessous:

Tableau 4: Coefficients affectés à la maturité des contrôles du modèle 1

Echelle de maturité des contrôles			
Valeur	**Descriptif**	**Signification**	**Coefficient affecté à la maturité des contrôles**
1	Inexistant	Le contrôle n'est pas défini	0
2	Informel	Le contrôle est défini mais elle n'est pas formalisée	0
3	Systématique	Le contrôle est défini et opérationnel	1
4	Intégré	Le contrôle est efficace, traçable et autoévalué	1
5	Optimisé	Le contrôle est managé et reporté et archivé	2

Selon cette échelle, les coefficients affectés à la maturité des contrôles ont la valeur 0, 1, ou 2. A chaque contrôle sera assignée une valeur du coefficient de maturité lors de l'évaluation des contrôles. Au début de notre modélisation, nous sommes restés dans la logique des valeurs relatives à la maturité des contrôles telles que définies par le COSO en définissant des coefficients qui traduisent la réalité en termes de niveau de mise en œuvre opérationnel des contrôles et de leurs impacts sur la criticité brute des risques. Ainsi, lorsque le contrôle est inexistant ou informel, il est considéré comme n'ayant aucun impact sur la criticité brute du risque ; le coefficient affecté à sa maturité qui lui est assigné est alors égal à 0. Dans le cas où le contrôle est systématique ou intégré, il a un impact moyen sur la criticité brute du risque ; le coefficient affecté à sa maturité qui lui est assigné est alors égal à 1. Lorsque le contrôle est optimisé, il a un impact maximal sur la criticité brute du risque ; le coefficient affecté à sa maturité devient alors égal à 2.
En définitive :

Criticité résiduelle= (Probabilité de survenance brute * Gravité potentielle Brute) - (Somme des coefficients affectés à la maturité des contrôles)

NB : Il faut noter que le contrôle est mature à partir du niveau 3(contrôle systematique).
Le modèle 1 se décline alors comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i \qquad 4.1.1$$

Compte tenu des échelles et coefficients préalablement définis, les valeurs des paramètres de cette équation sont indiquées ci-dessous :

- **P_{brute} :** coefficient affecté à la probabilité de survenance brute du risque; **P_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute} :** coefficient affecté à la gravité potentielle brute du risque ; **G_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **m_i:** coefficient affecté à la maturité du contrôle i ; **m_i** pouvant prendre la valeur=0, 1 ou 2
- S'agissant du nombre de contrôles n, ses valeurs sont obtenues à partir de l'équation du modèle 1 et des valeurs maximales des paramètres connus qui sont listées ci-après : 6 pour **P_{brute} et G_{brute}**, 2 pour **m_i**. Ainsi, en tenant compte de l'équation du modèle 1, la valeur maximale de **n** est obtenu en divisant 36 (6*6) par 2 ce qui donne 18. Par conséquent, le nombre n de contrôles est égal à 18 au maximum.

Ainsi, le modèle 1 possède 4 paramètres :

- **m_i** : coefficient affecté à la maturité des contrôles
- **n** : nombre de contrôles par risque
- **P_{brute}**: coefficient affecté à la probabilité de survenance brute du risque
- **G_{brutes} :** coefficient affecté à la gravité potentielle brute du risque

Les 9 avantages du modèle 1 sont déclinés comme suit :

- Un modèle conviviale avec une équation ayant quatre paramètres
- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'efforts de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles sur le risque
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels
- Gain de temps moyen de 10 min par risque lors de l'estimation des risques résiduels

Les 4 limites du modèle 1 qui découlent des principes utilisés au niveau de ce chapitre et tests qui seront décrits dans le chapitre 5 sont listées ci-après :

- Non prise en compte des types de contrôles dans l'équation du modèle 1
- Réussite de quelques tests économétriques sur les quatorze recommandés
- Taux de corrélation avec les données de référence égal à 94.5%
- Modèle instable car les taux de corrélation diffèrent selon les types de risques

d. Modèle 2

Le modèle 2 est basé sur les mêmes principes que le modèle 1, il est défini dans le but de pallier aux limites du modèle 1. Pour ce faire, nous avons défini une constante calculée sur la base des pourcentages de l'impact des contrôles qui tiennent compte des différentes caractéristiques d'un contrôle.

Pour identifier les différentes caractéristiques propres à un contrôle, nous avons exploité les documents de référence **[23], [24], [26]**, **[27] et [57].** Il en découle l'existence une dizaine de caractéristiques, chacune d'elle correspondant à un niveau ayant autant d'importance que les autres. Cela donne une stratification à 10 niveaux, chaque niveau conservant les acquis du précèdent niveau comme indiqué dans le tableau ci-dessous :

Tableau 5: Les niveaux relatifs aux caractéristiques d'un contrôle

NIVEAU	SIGNIFICATION
1	Existe
2	existe et documenté
3	existe, documenté et effectif
4	existe, documenté, effectif, traçable
5	existe, documenté, effectif, traçable, efficace
6	existe, documenté, effectif, traçable, efficace et efficiente
7	existe, documenté, effectif, traçable, efficace efficiente, autoévalué
8	existe, documenté, effectif, traçable, efficace efficiente, autoévalué et managé
9	existe, documenté, effectif, traçable, efficace efficiente, autoévalué, managé et reporting
10	existe, documenté, effectif, traçable, efficace efficiente, autoévalué, managé,

	reporting et archivé

Cette stratification permet de calculer les pourcentages d'impact des contrôles par niveau. Les pourcentages d'impact ont été définis en tenant compte de l'échelle de maturité à 10 niveaux relatifs aux caractéristiques d'un contrôle. Ainsi le pourcentage de l'impact du premier niveau correspondant à l'existence du contrôle est de 10%, les autres pourcentages sont obtenus en augmentant 10% à chaque niveau.
En tenant compte des 5 niveaux de maturité définis par le COSO **[23]**, la constante du modèle 2 qui représente la valeur de l'impact des contrôles non prise en compte par la criticité brute des risques et la maturité des contrôles, elle est calculée de la façon suivante:

|Constante| = Somme des pourcentages de l'impact par niveau/ 5

Cette constante est liée à la maturité des contrôles qui est déduite de la criticité brute des risques au niveau du modèle 1, par conséquent la constante s'obtient comme suit :

Constante **= (-)** (Somme des pourcentages de l'impact par niveau/ 5)

A l'issu des calculs du pourcentage de l'impact des contrôles par niveau, les valeurs obtenues sont consignées au niveau du tableau ci-après :

Tableau 6: Pourcentage et valeur de l'impact par niveau

Valeur du niveau	**Pourcentage de l'impact des controles par niveau**
1	10%
2	20%
3	30%
4	40%
5	50%
6	60%
7	70%
8	80%

9	90%
10	100%
SOMME	5**50% soit 5,5**

En considérant le tableau ci-dessus, la constante représentant la valeur de l'impact des contrôles non prise en compte par la criticité brute des risques et la maturité des contrôles s'obtient de la façon suivante :

Constante =(-) (5,5/5) =-1,1

Par ailleurs, les coefficients affectés à la maturité des contrôles ont légèrement changé lors de la deuxième modélisation. Les nouveaux coefficients relatifs à la maturité des contrôles sont décrits ci-dessous:

Tableau 6 : Coefficients affectés à la maturité des contrôles du modèle 2

Echelle de maturité des contrôles			
Valeur	**Descriptif**	**Signification**	**Coefficient affecté à la maturité des contrôles**
1	Inexistant	Le contrôle n'est pas défini	0
2	Informel	Le contrôle est défini mais elle n'est pas formalisée	0
3	Systématique	Le contrôle est défini et opérationnel	1
4	Intégré	Le contrôle est efficace, traçable et autoévalué	2
5	Optimisé	Le contrôle est managé et reporté et archivé	2

Compte tenu des limites du modèle 1 évoqués en amont et des suggestions qu'on nous a faites lors de la présentation de l'une de nos publications dans une conférence, nous nous sommes proposé de considérer le niveau intégré comme ayant un impact maximum sur la criticité brute des risques au lieu d'un impact moyen. Ainsi, le changement du coefficient de maturité qui lui est assigné au niveau du modèle 2 est donc dû au fait que l'on considère ce niveau de maturité très confortable et beaucoup plus réaliste que le niveau optimisé qui est rarement atteint par les banques. Ainsi, les coefficients affectés à la maturité des contrôles ont toujours la valeur 0, 1 ou 2 ; lorsque le contrôle est inexistant ou informel, il est considéré comme n'ayant aucun impact sur la criticité brute du risque ; le coefficient affecté

à sa maturité qui lui est assigné est toujours alors égal à 0. De même, dans le cas où le contrôle est systématique ou optimisé, le coefficient affecté à sa maturité est maintenu et respectivement égal à 1 et 2. Cependant, lorsque le contrôle est intégré, le coefficient affecté à sa maturité qui lui est assigné a été modifié et devient égal à 2.

Le modèle 2 sera alors défini sur la base de la constante, du nombre de contrôles par risque et des quatre principes cités en amont**.**

Criticité résiduelle = Criticité brute – Maturité globale des contrôles + Constante

En tenant compte de la formule existante **[22]** et en remplaçant la criticité brute par sa valeur, on obtient :

Criticité résiduelle= [(Probabilité potentielle brute * Gravité potentielle Brute)- (Somme des coefficients affectés à la maturité des contrôles)] + Cste

En définitive, le modèle 2 se décline comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i + cste \qquad 4.1.2$$

Compte tenu des échelles et coefficients préalablement définis, les valeurs des paramètres de cette équation sont indiquées ci-dessous :

- **P** $_{brute}$: coefficient affecté à la probabilité de survenance brute du risque; **P** $_{brute}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G** $_{brute}$: coefficient affecté à la gravité potentielle brute du risque ; **G** $_{brute}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **m_i:** le coefficient affecté à la maturité du contrôle i ; **m_i** pouvant prendre la valeur=0, 1 ou 2
- S'agissant du nombre de contrôles n, ses valeurs sont obtenus à partir de l'équation du modèle 2 et des valeurs maximales des paramètres connus qui sont listées ci-après : 6 pour **P_{brute} et G_{brute}**, 2 pour **m_i**. Ainsi, en tenant compte de l'équation du modèle 2, la valeur maximale de **n** est obtenu en divisant 36(6*6) par 2 ce qui donne 18. Par conséquent, le nombre n de contrôles est égal à 18 au maximum.
- Pour ce qui est de la constante, sa valeur est égale à -1,1 comme calculée en amont

Ainsi, le modèle 2 possède 4 paramètres

- **m_i** : le coefficient affecté à la maturité des contrôles
- **n** : nombre de contrôles
- **P** : coefficient affecté à la probabilité de survenance brute du risque

- **G** : coefficient affecté à la gravité potentielle brute du risque

Et possède une constante

- **Cste** = -1,1

Les 10 avantages du modèle 2 sont déclinés comme suit :

- Un modèle conviviale avec une équation ayant quatre paramètres
- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'efforts de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles sur les risques
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels
- Gain de temps moyen de 10 min par risque lors de l'estimation des risques résiduels
- *Taux de corrélation avec les données de référence égal à 97%*

Les 3 limites du modèle 2 qui découlent des principes utilisés au niveau de ce chapitre et des tests qui seront décrits dans le chapitre 5 sont listées ci-après :

- Non prise en compte des types de contrôles dans l'équation du modèle 2
- Réussite de quelques tests économétriques sur les quatorze recommandés
- Modèle instable car les taux de corrélation diffèrent selon les types de risques

IV.1.2 Modèles mathématiques améliorés

a. Approche

Pour définir les modèles mathématiques améliorés, nous avons tenu compte des types de contrôles notamment du fait qu'un contrôle est soit préventif, détectif, correctif et qu'il possède une seule valeur de maturité. L'approche utilisée est résumée dans le schéma ci-dessous :

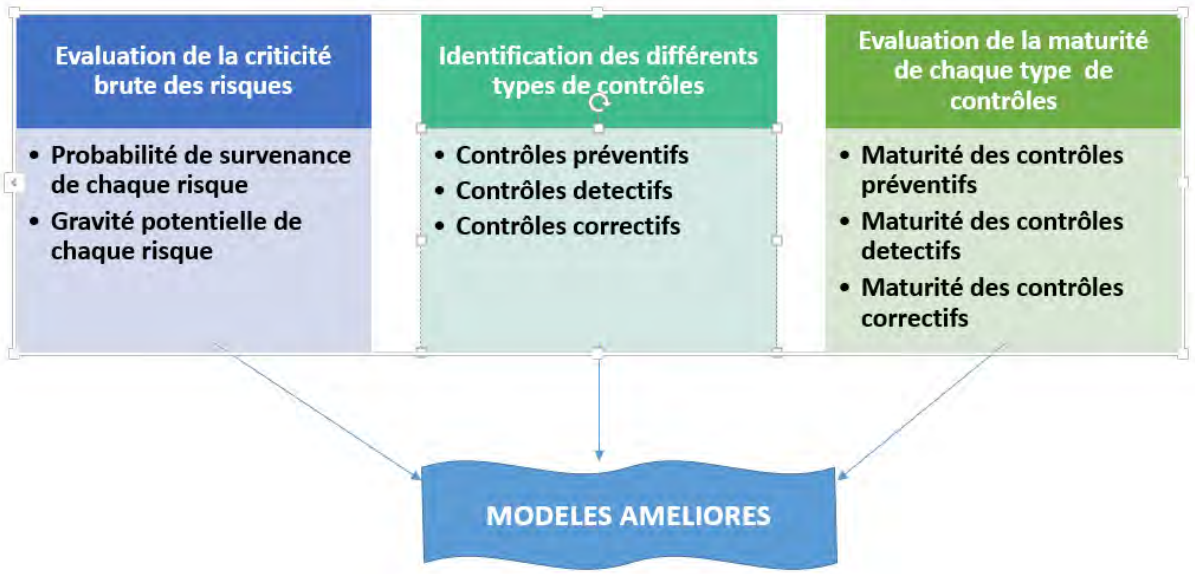


Figure 11: Approche utilisée pour concevoir les modèles mathématiques améliorés

A la lecture de ce schéma synthétique, il apparait que les modèles mathématiques améliorés auront des paramètres liés à la criticité brute des risques, aux nombres et types de contrôles mais aussi à la maturité des différents types de contrôles.

b. Principes

Pour proposer ces modèles mathématiques améliorés, nous avons définis les 7 principes suivants qui découlent de l'exploitation documentaire des références **[3], [5], [8], [24], [26], [29], [57], [58], [60] [64] [65] [69][70], [73], [95], [96],[97], [107] et [108] :**

Principe 1
Un risque peut avoir un ou plusieurs contrôles. En effet les contrôles sont définis et mis en œuvre dans le but de mitiger les risques. Ainsi, selon la nature du risque, un ou plusieurs contrôles y afférents peuvent être définis.

Principe 2
Les contrôles sont mis en œuvre pour maitriser les risques identifiés et évalués. En effet suite à l'identification des risques, une première évaluation basée sur les échelles de probabilité de survenance et de gravité potentielle permet d'assigner à chaque risque, une valeur de criticité brute correspondant au niveau de criticité qui ne tient pas compte des contrôles effectivement mis en œuvre.

Principe 3
Un contrôle possède une maturité et un type. En effet la maturité correspond au niveau de mise en œuvre du contrôle, elle peut être inexistante, informelle, systématique, intégrée ou optimisée. Quant au type du contrôle, il fait référence à la nature proprement dite du contrôle qui peut être soit préventive, détective ou corrective.

Principe 4
Seuls, les contrôles matures peuvent réduire la probabilité de survenance brute et/ou la gravité potentielle brute des risques. Pour qu'un contrôle puisse considérablement réduire ou mitiger un risque, il faut qu'il soit mature, cela signifie que sa maturité est au niveau opérationnel au minimum.

Principe 5
Les contrôles préventifs contribuent à faire baisser la probabilité de survenance brute du risque (P_{brute}). Ces contrôles sont définis pour agir en amont et empêcher que le risque se produise.

Principe 6
Les contrôles detectifs contribuent à faire baisser la gravité potentielle brute du risque (G_{brute}). L'utilité de ce type de contrôle repose sur la communication du risque avéré.

Principe 7
Les contrôles correctifs contribuent à faire baisser la gravité potentielle du risque (G_{brute}). Ce sont des contrôles qui sont définis dans le but de prendre en charge le risque détecté.

c. Modèle 3

Pour définir le modèle 3, nous allons écrire l'équation y afférente en calculant les deux facteurs principaux qui le composent, il s'agit notamment de la probabilité de survenance résiduelle et la gravité potentielle résiduelle des risques. La probabilité de survenance résiduelle des risques correspond à la probabilité de survenance du risque qui subsiste après la mise en œuvre des contrôles préventifs. Pour l'obtenir, on se base sur les principes 1, 2, 3, 4 et 5 définis en amont ainsi que sur les coefficients affectés à la maturité des contrôles qui sont décrits ci-dessous:

Tableau 7: Coefficients affectés à la maturité des contrôles du modèle 3

Echelle de maturité des contrôles			
Valeur	**Descriptif**	**Signification**	**Coefficients affectés à la maturité des contrôles**
1	Inexistant	Le contrôle n'est pas défini	0
2	Informel	Le contrôle est défini mais elle n'est pas formalisée	0
3	Systématique	Le contrôle est défini et opérationnel	1
4	Intégré	Le contrôle est effectif et traçable	1
5	Optimisé	Le contrôle est managé et reporté	2

Compte tenu des limites du modèle 2 et des nouveaux principes que nous avons définis pour proposer le modèle 3, nous sommes restés conformes à ce qui a été fait pour le modèle 1. En effet, nous avons maintenu la logique des valeurs relatives à la maturité des contrôles telles que définies par le COSO en définissant des coefficients qui traduisent la réalité en termes de niveau de mise en œuvre opérationnel des contrôles et de leurs impacts sur la criticité brute des risques. Ainsi, lorsque le contrôle est inexistant ou informel, il est considéré comme n'ayant aucun impact sur la criticité brute du risque ; le coefficient affecté à sa maturité qui lui est assigné est alors égal à 0. Dans le cas où le contrôle est systématique ou intégré, il a un impact moyen sur la criticité brute du risque ; le coefficient affecté à sa maturité qui lui est assigné est alors égal à 1. Lorsque le contrôle est optimisé, il a un impact maximal sur la criticité brute du risque ; le coefficient affecté à sa maturité devient alors égal à 2. Ainsi, à chaque contrôle sera assignée une valeur du coefficient affecté à sa maturité lors de l'évaluation des contrôles.

Concernant, le coefficient affecté aux controles préventifs, il dépend essentiellement du fait que le contrôle soit préventif ou non. Ainsi, si le contrôle est préventif, le coefficient qui lui est affecté est égal à 1, dans le cas échéant, le coefficient qui lui est affecté est égal à 0 comme indiqué dans le tableau ci-dessous.

Tableau 8: Coefficients affectés aux contrôles préventifs

Echelle des contrôles préventifs		
Descriptif	**Signification**	**Coefficients affectés aux contrôles préventifs**
préventif	Le contrôle agit sur la probabilité de survenance du risque brute	1
non préventif	Le contrôle n'a pas d'effet sur la probabilité de survenance du risque brut	0

En résumé, un coefficient affecté à la maturité du contrôle et un coefficient affecté au controle préventif seront donc assignés à chaque contrôle de type préventif. En tenant compte de ces coefficients et du fait qu'un risque peut avoir un ou plusieurs contrôles préventifs, la probabilité de survenance résiduelle d'un risque se calcule comme suit :

Probabilité résiduelle = Probabilité brute – Maturité des contrôles préventifs

La probabilité de survenance brute est une estimation des facteurs qui rendent favorable l'apparition du risque ; il peut s'agir de facteurs internes ou externes. Elle correspond à la

probabilité de survenance du risque en l'absence de contrôles mis en œuvre. L'échelle utilisée pour évaluer la probabilité de survenance brute des risques est décrite ci-dessous :

Tableau 9: Echelle de la Probabilité de survenance du risque

Echelle de la Probabilité de survenance brute du risque	
Valeur	**Signification**
1	Très peu probable
2	Peu probable
3	Probable
4	Très probable
5	Certain
6	Très Certain

D'après cette échelle, la probabilité de survenance brute possède des valeurs entières comprises entre 0 et 6. Plus la valeur de la probabilité est élevée, plus le risque a des chances de survenir et de se concrétiser. En tenant compte des échelles et coefficients précédemment définis, la probabilité de survenance résiduelle brute du risque se calcule comme suit :

$$P_{résiduelle} = \left[[P_{brute} - \sum_{i=1}^{r} a_i * m_i \right]$$

Les valeurs des paramètres de cette équation sont obtenues à partir de l'échelle relative à la probabilité de survenance brute du risque mais aussi des coefficients affectés à la maturité et au contrôle de type préventif. Elles sont indiquées ci-dessous :

- P_{brute} : coefficient affecté à la probabilité de survenance brute du risque; P_{brute} = 1, 2, 3, 4, 5 ou 6
- m_i: coefficient affecté à la maturité du contrôle préventif i; m_i=0, 1 ou 2
- a_i : coefficient affecté au contrôle de type préventif i; a_i=0 ou 1
- S'agissant du nombre **r** de contrôles préventifs par risque, ses valeurs sont obtenues à partir de l'équation du modèle 3 et des valeurs maximales des paramètres connus qui sont listées ci-après : 6 pour P_{brute}, 2 pour m_i, 1 pour a_i. Ainsi, en tenant compte de l'équation du modèle 3, la valeur maximale de **r** est obtenue en divisant 6 par 2 ce

qui donne une valeur entière 3. Par conséquent, le nombre **r** de contrôles préventifs est égal à 3 au maximum.

La gravité potentielle résiduelle des risques correspond à la gravité qui subsiste après la mise en œuvre des contrôles detectifs et correctifs. Pour l'obtenir, on se base sur les principes 1, 2, 3, 4 ,6 et 7, sur les coefficients affectés à la maturité des contrôles précédemment définis et des coefficients affectés aux controles de type detectif et correctif indiqués ci-après :

Tableau 10: Coefficients affectés aux contrôles detectifs

Echelle des contrôles detectifs		
Descriptif	**Signification**	**Coefficients affectés aux contrôles detectifs**
détectif	Le contrôle agit sur la gravité potentielle du risque	**1**
non détectif	Le contrôle n'a pas d'effet sur la gravité potentielle du risque	**0**

Le coefficient affecté aux controles detectifs dépend du fait que le contrôle est détectif ou non. Ainsi si le contrôle est détectif, le coefficient qui lui est affecté est égal à 1, dans le cas échéant, le coefficient qui lui est affecté est égale à 0 comme indiqué dans le tableau ci-dessus.

Tableau 11: Coefficients affectés aux contrôles correctifs

Echelle des contrôles correctifs		
Descriptif	**Signification**	***Coefficients affectés aux contrôles correctifs***
correctif	Le contrôle agit sur la gravité potentielle du risque	1
non correctif	Le contrôle n'a pas d'effet sur la gravité potentielle du risque	0

Le coefficient affecté aux controles correctifs dépend du fait que le contrôle est correctif ou non. Ainsi si le contrôle est correctif, le coefficient qui lui est affecté est égale à 1, dans le

cas échéant, le coefficient qui lui est affecté est égale à 0 comme indiqué dans le tableau ci-dessus.

En définitive, un coefficient affecté à la maturité du contrôle et un coefficient affecté au controle detectif seront donc assignés à chaque contrôle de type detectif. De la même façon, un coefficient affecté à la maturité du contrôle et un coefficient affecté au controle correctif seront donc assignés à chaque contrôle de type correctif.

En tenant compte de ces coefficients mais aussi du fait qu'un risque peut avoir un ou plusieurs contrôles detectifs ou correctifs, la gravité résiduelle d'un risque se calcule comme suit :

Gravité résiduelle = Gravité brute - Maturité des contrôles détectif et correctifs

La gravité potentielle brute des risques est définie comme étant une estimation des impacts potentiels de la survenance du risque sur la réalisation des objectifs. L'échelle utilisée pour évaluer la gravité brute des risques est déclinée ci-dessous :

Tableau 12: Echelle de la Gravite potentielle brute du risque

Echelle de Gravité potentielle brute du risque	
Echelle	**Signification**
1	Très peu grave
2	peu grave
3	Grave
4	Très grave
5	Situation de crise
6	Crise majeure

D'après cette échelle, la gravité potentielle brute des risques possède des valeurs entières comprises entre 0 et 6 ; plus la valeur de la gravité est élevée, plus les conséquences du risque avéré sont désastreuses. En tenant compte de cette échelle et des coefficients précédemment définis, la gravité résiduelle se calcule comme suit :

$$G_{résiduelle} = \left[G_{brute} - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \right]$$

Les valeurs des paramètres de cette équation sont obtenues à partir de l'échelle relative à la gravité potentielle du risque mais aussi des coefficients affectés à la maturité des contrôles et des coefficients affectés aux contrôles detectifs et correctifs. Elles sont indiquées ci-dessous :

- **G_{brute} :** coefficient affecté à la gravité potentielle brute du risque ; **G_{brute} =** 1, 2, 3, 4, 5 ou 6
- **n_j:** coefficient affecté à la maturité du contrôle detectif ; **n_j** =0, 1 ou 2
- **l_k:** coefficient affecté à la maturité du contrôle correctif ; **l_k** =0, 1 ou 2
- **b_j** : coefficient affecté au contrôle de type detectif ; **b_j** =0 ou 1
- **c_k** : coefficient affecté au contrôle de type correctif ; **c_k** =0 ou 1
  Concernant le nombre **s** de contrôles detectifs par risque, ses valeurs sont obtenues à partir de l'équation du modèle 3 et des valeurs maximales des paramètres connus qui sont listées ci-après : 6 pour **$G_{brute,}$** 2 pour **n_j,** 1 pour **b_j.** Ainsi, en tenant compte de l'équation du modèle 3, la valeur maximale de **s** est obtenue en divisant 6 par 2 ce qui donne une valeur entière 3. Par conséquent, le nombre **s** de contrôles detectifs est égal à 3 au maximum.
- S'agissant du nombre **t** de contrôles correctifs par risque, ses valeurs sont obtenues à partir de l'équation du modèle 3 et des valeurs maximales des paramètres connus qui sont listés ci-après : 6 pour **$G_{brute,}$** 2 pour **l_k,** 1 pour **c_k.** Ainsi, en tenant compte de l'équation du modèle 3, la valeur maximale de **t** est obtenue en divisant 6 par 2 ce qui donne une valeur entière 3. Par conséquent, le nombre **t** de contrôles correctifs est égal à 3 au maximum.

Ainsi, nous venons de calculer les deux facteurs permettant d'obtenir l'équation du troisième modèle que nous proposons pour calculer la criticité résiduelle des risques. Or d'après la formule existante **[22],** la criticité du risque est calculée en faisant le produit de la probabilité de survenance et de la gravité potentielle du risque. Par conséquent, pour le modèle 3, la criticité résiduelle est obtenue en effectuant le produit de la probabilité résiduelle et de la gravité résiduelle :

$$C_{résiduelle} = P_{résiduelle} * G_{résiduelle}$$

En remplaçant **$P_{résiduelle}$ et $G_{résiduelle}$** par leurs expressions, le modèle 3 se décline comme suit :

$$C_{résiduelle} = \left[[P_{brute} - \sum_{i=1}^{r} a_i * m_i \right] * \left[G_{brute} - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \right] \quad 4.1.3$$

Avec la contrainte r + s + t =3

Cette contrainte se justifie par le fait que P_{brute} et G_{brute} ont des valeurs maximales égales à 6, donc il faut impérativement le nombre total de contrôles préventifs, défectifs et correctifs ne dépassent pas 3 compte tenu de la structure de l'équation du modèle 3.

Le modèle 3 possède 11 paramètres

- **m_i, n_j, l_k**: coefficients affectés à la maturité des contrôles préventifs, detectifs, correctifs
- **a_i, b_j, c_k**: coefficients affectés aux contrôles de types préventif, detectif et correctif
- **r, s, t** : nombre de contrôles préventifs, detectifs et correctifs par risque
- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque

Les 10 avantages du modèle 3 sont déclinés comme suit :

- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'effort de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles sur les risques
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels
- *Gain de temps* moyen *de 12 min par risque lors de l'estimation des risques résiduels*
- *Taux de corrélation moyen avec les données de référence égal à 97.5%*
- *Une prise en compte des types de contrôles dans l'équation du modèle 3*

Les 3 limites du modèle 3 qui découlent des principes utilisés au niveau de ce chapitre et des tests qui seront décrits dans le chapitre 5 sont listées ci-après :

- *Réussite de quelques tests économétriques sur les quatorze recommandés*
- *Un modèle moins conviviale avec une équation ayant onze paramètres*
- Modèle instable car les taux de corrélation diffèrent selon les types de risque

d. Modèle 4

Le modèle 4 est basé sur la même approche que le modèle 3 dans la mesure où il tient compte de la maturité des contrôles et de leurs types. Cependant, le modèle 4 n'a pas les

mêmes coefficients affectés à la maturité des contrôles. En effet, les coefficients affectés à la maturité des contrôles qui sont utilisés pour ce modèle sont décrits ci-dessous:

Tableau 13: Coefficients affectés à la maturité des contrôles du modèle 4

Echelle de maturité des contrôles			
Valeur	**Descriptif**	**Signification**	**Coefficients affectés à la maturité des contrôles**
1	Inexistant	Le contrôle n'est pas défini	1
2	Informel	Le contrôle est défini mais elle n'est pas formalisée	2
3	Systématique	Le contrôle est défini et opérationnel	3
4	Intégré	Le contrôle est efficace, traçable et autoévalué	4
5	Optimisé	Le contrôle est managé et reporté et archivé	5

Selon cette échelle, les coefficients affectés à la maturité des contrôles ont la valeur 0, 1, 2, 3, 4 et 5. A chaque contrôle sera assignée une valeur du coefficient de maturité lors de l'évaluation des contrôles.

Pour le modèle 4, les coefficients affectés à la maturité des contrôles sont égaux aux valeurs des contrôles définis par le COSO, l'objectif visé étant de minimiser d'avantage les différences d'appréciation et résoudre le problème d'instabilité des modèles qui demeure un des défis majeurs à relever par notre modélisation.

La maturité globale des contrôles correspond à la somme des maturités des différents types de contrôles.

Maturité globale des contrôles = Maturité des contrôles préventifs+ Maturité des contrôles detectifs + Maturité de contrôles correctifs

En résumé : **Maturité globale des contrôles :**

$$\sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k$$

Maturité des contrôles préventifs

- **m_i:** coefficient affecté à la maturité du contrôle préventif ; **m_i** = 1, 2, 3, 4 et 5

- a_i: coefficient affecté au contrôle de type préventif ; a_i=0 ou 1
- **r:** nombre de contrôles préventifs ; r= 7 au maximum

Maturité des contrôles detectifs

- n_j**:** coefficient affecté à la maturité du contrôle detectif ; n_j= 1, 2, 3, 4 et 5
- b_j: coefficient affecté au contrôle de type detectif ; b_j=0 ou 1
- **s :** nombre de contrôles detectifs ; s= 7 au maximum

Maturité de contrôles correctifs :

- l_k**:** coefficient affecté à la maturité du contrôle correctif ; l_k= 1, 2, 3, 4 et 5
- c_k : coefficient affecté au contrôle de type correctif ; c_k=0 ou 1
- **t :** le nombre de contrôles correctifs ; t= 7 au maximum

Sachant que le modèle 4 prend également en compte la criticité brute des risques qui est obtenue à partir de la formule existante permettant de calculer la criticité du risque en effectuant le produit de la probabilité de survenance et de la gravité potentielle **[22].** La criticité brute est alors égale au produit de la probabilité brute et de la gravité brute.

$$C_{brute} = P_{brute} * G_{brute}$$

En définitive, la criticité résiduelle des risques calculée par le modèle 4 est obtenue en faisant la soustraction entre la criticité brute des risques et la maturité des contrôles préventifs, detectifs et correctifs. Ainsi, le modèle 4 se décline comme suit:

Criticité résiduelle= Criticité brute des risques – (Maturité des contrôles préventifs+ Maturité des contrôles detectifs + Maturité de contrôles correctifs)

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \qquad 4.1.4$$

Avec la contrainte avec **r + s + t =7**

La valeur de cette contrainte est obtenue à partir de l'équation du modèle 4 et des valeurs maximales des paramètres connus qui sont listées ci-après : 6 pour P_{brute} et G_{brute}, 5 pour m_i, n_j et l_k 1 pour a_i, b_j et c_k. Ainsi, en tenant compte de l'équation du modèle 4, la valeur maximale de cette contrainte est obtenue en divisant 36(6*6) par 5 ce qui donne une valeur entière égale 7 au maximum. Par conséquent, il est impératif que la somme du nombre de contrôles préventifs, défectifs et correctifs soit égal à 7, d'où la contrainte indiquée ci-dessus.

Le modèle 4 possède 11 paramètres

- $\mathbf{m_i}$, $\mathbf{n_j}$, $\mathbf{l_k}$: coefficients affectés à la maturité des contrôles préventifs, detectifs et correctifs
- $\mathbf{a_i}$, $\mathbf{b_j}$, $\mathbf{c_k}$: coefficients affectés aux contrôles préventifs, detectifs et correctifs
- **r, s, t** : nombre de contrôles préventifs, detectifs et correctifs par risque
- $\mathbf{P_{brute}}$: coefficient affecté à la probabilité de survenance brute du risque
- $\mathbf{G_{brute}}$: coefficient affecté à la gravité potentielle brute du risque

Les 12 avantages du modèle 4 sont déclinés comme suit :

- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'effort de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles sur les risques
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels
- *Gain de temps* moyen *de 15 min par risque lors de l'estimation des risques résiduels*
- *Taux de corrélation avec les données de référence égal à 98%*
- *Une prise en compte des types de contrôles dans l'équation du modèle 4*
- *Réussite de tous les quatorze tests économétriques recommandés*
- *Modèle stable car les taux de corrélation sont constants quel que soit le type de risque*

La seule limite du modèle 4 qui découle des principes utilisés au niveau de ce chapitre et tests qui seront décrits dans le chapitre 5 sont listées ci-après :

- *Un modèle moins conviviale avec une équation ayant onze paramètres*

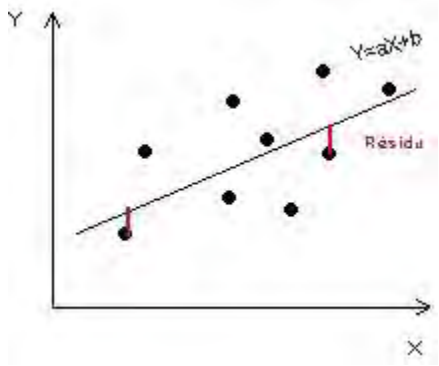
Remarque : Il faut noter que l'ensemble des échelles et coefficients utilisés dans les 3 premiers modèles sont définis par l'auteur, à l'exception du quatrième modèle ou l'on a considéré comme coefficients affectés à la maturité des controles, les valeurs relatives à la maturité des contrôles définies par le COSO **[24].**

IV.2 Equations de régressions linéaires

Dans le but de discrétiser les modèles mathématiques proposés, les équations de régressions linéaires y afférentes ont été définies. En effet, pour mettre en évidence l'existence d'une relation linéaire significative entre deux caractères quantitatifs continus X et Y, on peut chercher à formaliser la relation moyenne qui unit ces deux variables à l'aide de l'équation suivante **[110]**:

$$\mathbf{Y = f(X)} \text{ soit } \mathbf{Y = a.X + b}$$

Ainsi, la droite de régression de Y en fonction de X introduit l'hypothèse que les valeurs de Y dépendent de celles de X, cela signifie que la connaissance des valeurs de X permet de prévoir les valeurs de Y. Il s'agit donc d'un modèle de prévision et l'objectif est de minimiser l'erreur de prévision c'est-à-dire la distance entre les valeurs Yi observées et les valeurs Y*i estimés par la relation Y = aX+b. Les résidus seront la distance à la droite par rapport à l'axe Oy comme indiqué dans le schéma ci-dessous.



Droite exprimant Y en fonction de X

L'objectif visé est de chercher à exprimer la **dépendance** d'un caractère par rapport à un autre (X en fonction de Y). Il s'agit donc d'une modélisation à visée **prédictive** puisque l'on suppose que la connaissance de l'une des variables (appelée **variable indépendante**) permet d'estimer la valeur de l'autre variable (appelée **variable dépendante**). Dans le cas où il y a plusieurs variables indépendantes, l'équation de régression linéaire sera sous la forme :

Y= aX+ bZ+ … + C avec C la constante

Dans notre cas, nous avons 2 variables indépendantes, l'équation est donc sous la forme :

Y= aX+ bZ+ C avec C la constante

Les variables X ,Y et Z sont indiquées ci-dessous:

Y=CR

X=CB

Z= CM

En remplaçant Y, X et Z par leurs valeurs, on obtient

CR = a**CB+** b**CM+ C** avec C la constante

Par la suite, nous avons considéré le logarithme de ces variables pour les raisons suivantes :

- Le log permet de diminuer le volume des chiffres représentant une série, on la lisse mieux en quelque sorte. Sachant que le log s'applique sur des valeurs comprises dans l'intervalle] 0, +∞[, on pourra transformer l'ensemble des valeurs en log car toutes

nos valeurs sont strictement positifs. En effet, le log est une bijection de l'intervalle]0, +∞[vers] -∞, +∞[, tout réel peut s'écrire comme le log d'un autre réel positif **[101].**

- De plus, étant donné que certaines équations de nos modèles sont multiplicatives et d'autres sont additives, l'utilisation du log permet de faire passer la série multiplicative à série en additive **[102].** Ainsi, si le modèle est multiplicatif, on le log-linéarise pour pouvoir l'estimer plus facilement. De plus, il est plus facile de faire des régressions sur des séries additives.

Ainsi les variables indiquées ci-dessus deviennent :

CR=Log CR

CB=Log CB

CM=Log CM

Nous allons donc utiliser l'équation suivante pour traduire les modèles mathématiques initiaux et améliorés en équation de régressions linéaires:

logCR = a **logCB+** b log**CM+ C** avec C la constante

IV.2.1 Première équation de régressions linaires

A titre de rappel, les modèles mathématiques initiaux **4.1.1 et 4.1.2** sont basés sur les caractéristiques et la maturité des différents contrôles. Ils se déclinent comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i \qquad 4.1.1$$

Et

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i + cste \qquad 4.1.2$$

Les paramètres de ces modèles mathématiques initiaux sont décrits ci-après :

- **P** $_{brute}$: coefficient affecté à la probabilité de survenance brute du risque; **P** $_{brute}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G** $_{brute}$: coefficient affecté à la gravité potentielle brute du risque ; **G** $_{brute}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- $\mathbf{m_i}$**:** coefficient affecté à la maturité du contrôle i ; $\mathbf{m_i}$ pouvant prendre la valeur=0, 1 ou 2
- **n** le nombre de contrôles ; n pouvant être égal à 18 au maximum
- **Cste** : la constante

Pour écrire l'équation de régression linéaire correspondant aux modèles initiaux, il nous faut identifier la variable à expliquer ou endogène qui représente la criticité résiduelle des risques et les variables explicatives ou hexogènes permettant d'expliquer cette criticité résiduelle des risques. Il faut noter qu'il y aura toujours des variables qui ne seront pas prises en compte par les variables explicatives, ils vont alors concerner la constante de l'équation de régression linéaire qui sera définie **[111].**

Les variables et constantes de la première équation de régressions linéaires sont indiquées ci-dessous :

CR_i : Criticité résiduelle des risques, c'est la variable à expliquer

a : Coefficient affecté à la variable criticité brute des risques

CB_i : Criticité brute des risques, c'est l'une des variables explicatives

b : Coefficient affecté à la variable maturité des contrôles

CM_i : Maturité des contrôles, c'est l'une des variables explicatives

C : Constante

Ainsi, l'équation de régressions linéaire correspondant aux modèles mathématiques initiaux est déclinée ci-après :

$$\log(CR_i) = a\log(CB_i) - b\log(CM_i) + C \qquad \textbf{4.2.1}$$

IV.2.2 Seconde équation de régressions linaires

Dans le même ordre d'idées, les modèles mathématiques améliorés sont aussi traduites en équations de régressions linéaires. A titre de rappel, les modèles mathématiques améliorés **4.1.3** et **4.1.4** sont basés sur la maturité et les différents types de contrôles. Ces modèles sont déclinés ci-après :

$$\boldsymbol{C_{résiduelle} = \left[[P_{brute} - \sum_{i=1}^{r} a_i * m_i\right] * \left[G_{brute} - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k\right]} \qquad \textbf{4.1.3}$$

Et

$$\boldsymbol{C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k} \qquad \textbf{4.1.4}$$

Les paramètres de ces modèles mathématiques améliorés sont décrits ci-après :

- **m_i, n_j, l_k:** coefficients affectés à la maturité des contrôles préventifs, detectifs et correctifs ; m_i, n_j, l_k pouvant prendre la valeur=0, 1 et 2 pour le modèle 3 ou la valeur=1, 2, 3, 4 et 5 pour le modèle 4
- **a_i, b_j, c_k**: coefficients affectés aux contrôles préventifs, detectifs et correctifs ; a_i, b_j, c_k pouvant prendre les valeurs la valeur=0 ou 1
- **r, s, t** : nombre de contrôles préventifs, detectifs et correctifs; r, s, t pouvant être égal au nombre de 3 au maximum pour le modèle 3 et 7 au maximum pour le modèle 4
- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque ; **P brute** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque ; **G brute** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6

De la même façon, pour écrire l'équation de régression linéaire correspondant aux modèles améliorés, il nous faut identifier la variable à expliquer ou endogène qui représente la criticité résiduelle des risques et les variables explicatives ou hexogènes permettant d'expliquer cette criticité résiduelle des risques. Les variables qui ne seront pas prises en compte par les variables explicatives vont concerner dans la constante de l'équation de régression linéaire qui sera définie **[111].**

Les variables et constantes de la seconde équation de régressions linéaires sont indiquées ci-dessous :

CR_i : Criticité résiduelle des risques, c'est la variable à expliquer

a : Coefficient affecté à la variable criticité brute des risques

CB_i : Criticité brute des risques, c'est l'une des variables explicatives

b : Coefficient affecté à la variable maturité des contrôles préventifs

CP_i : Maturité des contrôles préventifs, c'est l'une des variables explicatives

c : Coefficient affecté à la variable maturité des contrôles detectifs

CD_i : Maturité des contrôles detectifs, c'est l'une des variables explicatives

d : Coefficient affecté à la variable maturité des contrôles correctifs

CC_i : Maturité des contrôles correctifs, c'est l'une des variables explicatives

$Cste$: Constante

Ainsi, l'équation de régressions correspondant aux modèles mathématiques améliorés est déclinée ci-après :

$$\log(CR_i) = alog(CB_i) - [blog(CP_i) + clog(CD_i) + dlog(CC_i)] + Cste \qquad \textbf{4.2.2}$$

Nous venons de proposer deux équations de régressions linéaires correspondant aux modèles mathématiques précédemment définis. Les coefficients et constantes de ces équations de régressions linéaires seront déterminés à l'aide de l'outil Eviews à travers les tests économétriques que nous allons détailler au niveau du prochain chapitre.

IV.3 Algorithmes

En prévision de l'implémentation des modèles proposés au niveau de l'outil R, les algorithmes y afférents ont été définis. Pour ce faire, nous avons traduit les équations des modèles initiaux et améliorés en algorithmes.

IV.3.1 Premier algorithme

A titre de rappel, les modèles mathématiques 1 et 2 sont basés sur la maturité et les différentes caractéristiques des contrôles, ils sont indiqués ci-dessous :

$$\boldsymbol{C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i} \qquad \textbf{4.1.1}$$

Et

$$\boldsymbol{C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i + cste} \qquad \textbf{4.1.2}$$

Les paramètres des modèles mathématiques initiaux sont décrits ci-après :

- **P** $_{\text{brute}}$: coefficient affecté à la probabilité de survenance brute du risque; **P** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G** $_{\text{brute}}$: coefficient affecté à la gravité potentielle brute du risque ; **G** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **m_i:** coefficient affecté à la maturité du contrôle i ; **m_i** pouvant prendre la valeur=0, 1 ou 2
- **n** le nombre de contrôles ; n pouvant être égal à 18 au maximum
- **Cste** : Constante

Sur cette base, nous avons défini le premier algorithme correspondant aux modèles mathématiques initiaux comme indiqué ci-après :

Algorithme 4.3.1 : Criticité résiduelle initiale

Entrées : P, G, M_i (i allant de 1 à N)

Sorties : CriticitéRési

Début

Pour i de 1 à N faire

CriticitéRési<- P*G - M_i

Fin Pour

Fin

NB: Pour le modèle 2, nous prenons en compte la valeur de la constante de l'équation et des coefficients affectés à la maturité des contrôles y afférents au niveau de l'algorithme indiqué ci-dessus.

Dans l'algorithme **4.3.1**, nous avons la criticité résiduelle initiale des risques qui prend en entrée :

- P correspondant au coefficient affecté à la probabilité de survenance brute des risques, les valeurs de P sont 0, 1, 2, 3, 4, 5 ou 6 compte tenu de l'échelle de probabilité de survenance brute définie précédemment.
- G correspondant au coefficient affecté à la gravité potentielle brute des risques, les valeurs de G sont 0, 1, 2, 3, 4, 5 ou 6 compte tenu de l'échelle de gravité potentielle brute définie précédemment.
- M_i (i allant de 1 à 18) correspondant au coefficient affecté à la maturité des contrôles, les valeurs de M sont 0, 1 et 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4
- ai, bj, ck: coefficients affectés aux contrôles compte tenu des coefficients de maturité définis

La sortie de l'algorithme **4.3.1** est une valeur représentant la criticité résiduelle des risques.

IV.3.2 Second algorithme

Dans la même optique, les modèles mathématiques améliorés ont également été traduites en algorithmes. En guise de rappel, les modèles mathématiques améliorés sont basés sur la maturité et les types de contrôles. Ils se déclinent comme suit :

$$C_{résiduelle} = \left[[P_{brute} - \sum_{i=1}^{r} a_i * m_i \right] * \left[G_{brute} - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \right] \quad 4.1.3$$

Et

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \qquad 4.1.4$$

Les paramètres de ces modèles mathématiques améliorés sont décrits ci-après :

- **m_i, n_j, l_k**: coefficients affectés à la maturité des contrôles préventifs, detectifs et correctifs ; m_i, n_j, l_k pouvant prendre la valeur=0, 1 et 2 pour le modèle 3 ou la valeur=1, 2, 3, 4 et 5 pour le modèle 4
- ai, bj, ck: coefficients affectés aux contrôles
- **a_i, b_j, c_k**: coefficients affectés aux contrôles préventifs, detectifs et correctifs ; a_i, b_j, c_k pouvant prendre les valeurs la valeur=0 ou 1
- **r, s, t** : nombre de contrôles préventifs, detectifs et correctifs ; r, s, t pouvant être égal au nombre de 3 au maximum pour le modèle 3 et 7 au maximum pour le modèle 4
- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque, P_{brute} pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque, G_{brute} pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6

Avant de définir les algorithmes optimisés correspondant aux modèles mathématiques améliorés, nous allons d'abord définir les trois fonctions algorithmiques y afférents. Ces trois fonctions algorithmiques sont relatives à la maturité des contrôles préventifs, à la maturité des contrôles detectifs et la maturité de contrôles correctifs ; elles sont décrites ci-après :

Algorithme 4.3.2. Maturité des contrôles préventifs

Fonction prévention (A, L, R :entier) : entier

Début

    Prévent <- 0

    Pour i de 1 à R faire

        Prévent <- Prévent + A* L

    Fin Pour

Retourne Prévent

Fin

Dans l'algorithme **4.3.2**, nous avons modélisé la maturité des contrôles préventifs. Il prend en entrée un vecteur A qui représente le coefficient affecté à la maturité des contrôles préventifs**,** un vecteur L qui représente le coefficient affecté aux contrôles préventifs et R qui représente le nombre de contrôles préventifs. Les valeurs de A, L er R sont indiquées ci-dessous :

- Les valeurs de A sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4
- ai, bj, ck: coefficients affectés aux contrôles, compte tenu des coefficients affectés à la maturité des contrôles préventifs
- Les valeurs de L sont 0 ou 1, compte tenu des coefficients affectés aux contrôles préventifs
- Les valeurs de R= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles préventifs

La sortie de cet algorithme correspond à une mesure représentant la maturité de contrôles préventifs.

Algorithme 4.3.3 Maturité des contrôles détectifs

Fonction détection (B, M, S : entier) : entier

Début

Détec <- 0

Pour i de 1 à S faire

Détec <- Détec + B* M

Fin Pour

Retourne Détec

Fin

Dans l'algorithme **4.3.3**, nous avons modélisé la maturité des contrôles detectifs. Il prend en entrée un vecteur B qui représente le coefficient affecté à la maturité des contrôles detectifs, un vecteur M qui représente le coefficient affecté aux contrôles detectifs et S qui représente le nombre de contrôles detectifs. Les valeurs de B, M et S sont indiquées ci-dessous :

- Les valeurs de B sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4, compte tenu des coefficients affectés à la maturité des contrôles detectifs
- Les valeurs de M sont 0 ou 1, compte tenu des coefficients affectés aux contrôles detectifs
- Les valeurs de S= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles detectifs

La sortie de cet algorithme est une mesure représentant la maturité de contrôles detectifs.

Algorithme 4.3.4 Maturité des contrôles correctifs

Fonction correction (C, N, T:) : entier

```
Début
    Corec <- 0
    Pour i de 1 à T faire
        Corec <- Corec + C * N
    Fin Pour
    Retourne Corec
Fin
```

Dans l'algorithme **4.3.4,** nous avons modélisé la maturité des contrôles correctifs. Il prend en entrée un vecteur C qui représente le coefficient affecté à la maturité des contrôles correctifs, un vecteur N qui représente le coefficient affecté aux contrôles préventifs et T qui représente le nombre de contrôles correctifs. Les valeurs de C, N et T sont indiquées ci-dessous :

- Les valeurs de C sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4 compte tenu des coefficients affectés à la maturité des contrôles correctifs
- Les valeurs de N sont 0 ou 1, compte tenu des coefficients affectés aux contrôles correctifs
- Les valeurs de T= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles correctifs

La sortie de cet algorithme constitue une mesure de la maturité de contrôles correctifs.

Ainsi nous venons de définir les trois fonctions algorithmiques permettant d'obtenir les algorithmiques optimisés correspondant aux modèles mathématiques améliorés. L'algorithme relatif au modèle 4 se décline comme suit :

Algorithme 4.3.5 Criticité résiduelle optimisée

Entrées : P, G, A, L, R, B, M, S, C, N, T

Sorties : Criticité

Précondition : R+S+T=7

Début

Retourne P*G – (prévention (A, L, R) – détection (B, M, S) – correction (C, N, T)

Fin

NB : pour le modèle 3 : la dernière instruction est la suivante :

Retourne (P - (prévention (A, L, R)) * (G– détection (B, M, S) – correction (C, N, T))

Dans l'algorithme **4.3.5**, nous avons calculé la criticité résiduelle des risques correspondant au modèle 4. Il prend en entrée :

- P : Probabilité de survenance brute des risques
- G : Gravité potentielle brute des risques
- un vecteur A : représente le coefficient affecté à la maturité des contrôles préventifs
- un vecteur L : représente le coefficient affecté aux contrôles préventifs,

- R qui représente le nombre de contrôles préventifs
- un vecteur B : représente le coefficient affecté à la maturité des contrôles detectifs
- un vecteur M : représente le coefficient affecté aux contrôles detectifs
- S qui représente le nombre de contrôles detectifs
- un vecteur C: représente le coefficient affecté à la maturité des contrôles correctifs
- un vecteur N : représente le coefficient affecté aux contrôles correctifs
- T qui représente le nombre de contrôles correctifs

La sortie de l'algorithme **4.3.5** représente une mesure représentant la criticité résiduelle optimisée. Elle doit vérifier la contrainte S+R+T=3 pour le modèle 3 et S+R+T=7 pour le modèle 4 pour les raisons évoquées en amont.

Conclusion

Dans ce chapitre, nous avons d'abord proposé quatre modèles mathématiques permettant de calculer les risques résiduels bancaires, à savoir les modèles 1 et 2 appelés modèles mathématiques initiaux qui sont basés sur la maturité et les caractéristiques des contrôles mais aussi les modèles 3 et 4 appelés modèles mathématiques améliorés qui sont basés sur la maturité et les types des contrôles. Pour discrétiser les modèles ainsi proposés, nous avons également définis les équations de régressions linéaires y afférentes. Dans le but d'implémenter les équations correspondants aux modèles mathématiques, les algorithmes y afférents ont été également définis. L'ensemble des modèles proposés seront testés en profondeur au niveau du dernier chapitre de ce document, l'objectif visé étant de les éprouver avant validation.

Chapitre V : Tests et Validation des modèles proposés

Introduction

Dans l'optique de valider les différents modèles mathématiques proposés, nous allons utiliser l'outil Eviews pour tester les équations de régressions linéaires et l'outil R pour tester les algorithmes y afférents. Dans un premier temps, divers tests économétriques seront réalisées sur les équations de régressions linéaires en utilisant les données d'apprentissage collectées au niveau des banques dans le but de les valider d'un point de vue statistique. Par la suite, les algorithmes proposés seront appliqués aux risques du système d'information avant détendre les tests aux autres risques bancaires, cela permettra de déterminer les taux de corrélation et les valeurs résiduelles entre les données de test collectées et les valeurs obtenues avec les modèles. Pour finir, une analyse comparative des différents modèles sera effectuée afin d'identifier les avantages et limites de chaque modèle en vue d'identifier le modèle retenu à l'issu de nos travaux.

V.1 Collecte des données de référence

Pour collecter les données de tests, nous avons collaboré avec des banques offrant les services bancaires classiques et des services monétiques (retraits et paiements par carte bancaire, E-Banking et M-Banking). Cet échantillon est représentatif dans la mesure où les autres banques ont approximativement les mêmes risques compte tenu de leur type de fonctionnement, des produits et services qu'elles mettent à la disposition de leurs clients mais également des normes et règlementations qui leur sont applicables. Nous tenons à préciser que le fait que les banques aient les mêmes typologies ne veut pas dire qu'elles ont le même niveau de risque. Si tel était le cas, cela voudrait dire que ces banques ont toutes le

même niveau de maturité de leurs dispositifs de management des risques et de contrôles interne, ce qui est pratiquement impossible. Cela se justifie d'ailleurs par la nature des données d'apprentissage collectées. En effet, pour un même risque, on a des niveaux de criticité brute des risques et de maturité des contrôles qui sont complètement différents.

Dans l'optique d'avoir des données représentatives, nous avons tenu compte du fait que le paysage bancaire de l'UEMOA est composé de quatre types d'acteurs à savoir les banques européennes, les banques panafricaines, les banques régionales et les banques nationales. Ainsi pour chacun de ces types, nous avons collecté les données semestrielles couvrant la période de test. Pour des raisons de confidentialité et compte tenu de la sensibilité des aspects liés au risque, nous ne divulguerons pas l'identité de ces banques. Etant donné que ces banques évaluent leurs risques résiduels de façon semestrielle, nous avons collecté les données de référence sur 4 semestres d'affilés de janvier 2016 à décembre 2017.

Pour ce faire, nous avons d'abord collecté un ensemble de données de référence parmi lesquelles, nous avons des données d'apprentissage pour lesquelles les résultats sont connus et des données de test dont les résultats sont inconnus. Par la suite, nous nous sommes focalisés sur les données d'apprentissage pour réaliser les quatorze tests économétriques préconisés au niveau d'Eviews. Pour finir, les modèles proposés ont été éprouvés avec les données de test sur R en vue déterminer les taux de corrélation l'erreur commise et les valeurs résiduelles.

A titre de rappel, le risque est tout évènement susceptible d'avoir un impact sur la réalisation des objectifs. Pour l'identifier, il faut procéder à l'analyse des objectifs des banques en utilisant une approche processus et en tenant compte des différentes collaborations et partenariats. L'identification des risques et contrôles ainsi que leur évaluation proprement dite se sont faites avec l'ensemble des acteurs concernés par les différents processus bancaires. La méthode utilisée est le RSCA workshop qui se déroule sous forme d'ateliers avec les acteurs listés au niveau de la matrice des interlocuteurs déclinée ci-dessous:

Tableau 14: Matrice des interlocuteurs au niveau des banques

Processus / Interlocuteurs	Marketing et Commercial	Conformité aux normes et reglementa-tions	Système d'information	Apres vente et Relation Clients	Finances et Comptabilité	Stratégie et Gouvernance	Ressources Humaines	Juridique et Contentieux	Audit et Contrôle	Nombre d'interven-tions
Adjoint au DG		x			x	x			x	4
SEGE		x			x	x		x	x	5
Conseiller Juridique		x						x		2

Directeur informatique		x	x	x	x	x	x		x	7
Agent informatique			x		x					2
Responsable Base de données		x	X						x	3
Directeur monétique	x	x	x	x	x	x	x	x	x	9
Agent monétique			x							2
Directeur Risques et conformité		x			x	x	x	x	x	6
Responsable Conformité		x	x					x	x	4
Risk Manager	x	x	x	x	x	x	x	x	x	9
Directeur Commercial	x	x		x	x	x	x		x	7
Responsable Commercial	x		x	x	x					4
Commercial	x		x	x						3
Chargé clientèle	x			x						2
Directeur RH		x			x	x	x	x	x	6
Responsable RH					x		x			3
Directeur Finances et comptabilité		x			x	x	x	x	x	6
Responsable trésorerie		x			x				x	3
Responsable Comptabilité		x			x				x	3
Nombre d'interlocuteur s dans le processus	6	14	9	7	15	9	8	9	13	88

V.2 Tests des équations de régressions linéaires

V.2.1 Présentation de l'outil Eviews

Eviews offre un vaste éventail de fonctionnalités pour la manipulation de données statistiques et l'analyse économétrique **[103].** C'est un outil permettant de travailler avec les séries temporelles, les données de panel ou les données longitudinales, etc. Avec Eviews, il est aisé de manipuler efficacement des données, de réaliser des analyses statistiques et économétriques, de générer des prévisions ou des simulations et de produire des graphiques de qualité publiable qui pourront être intégrés dans des articles ou des rapports. Dans le

milieu de la recherche, Eviews est très utile et fournit des résultats performants. Il peut être utilisé aussi bien en mode menu qu'en mode programmation.

V.2.2 Tests économétriques

a. Première équation de régressions linéaires

En guise de rappel, l'équation de régressions linéaires correspondant aux modèles mathématiques initiaux est déclinée ci-après :

$$\log(CR_i) = a\log(CB_i) - b\log(CM_i) + C \qquad \textbf{4.2.1}$$

Les variables et constantes de cette première équation de régressions linéaires sont indiquées ci-dessous :

CR_i : La criticité résiduelle des risques, c'est la variable à expliquer par l'équation

a : Le coefficient affecté à la variable criticité brute des risques

CB_i : La criticité brute des risques, c'est l'une des variables explicatives de l'équation

b : Le coefficient affecté à la variable maturité des contrôles

CM_i : La maturité des contrôles, c'est l'une des variables explicatives de l'équation

C: La constante

Pour tester cette première équation de régressions linéaires, nous l'avons appliqué à des données d'apprentissage provenant de différentes banques de la place. Au niveau de ces banques, les valeurs de **CB, CR et M** sont obtenues de la façon suivante :

L'identification des risques consiste à attribuer à chaque risque un libellé, une cause, une conséquence et un code spécifique. Quant à l'évaluation du risque brute, elle consiste à estimer la probabilité de survenance brute(**P_{brute}**), la gravité potentielle brute(**G_{brute}**) et la criticité brute(**CB**) qui est le produit des deux valeurs précédentes. Lors des séances d'évaluation, les banques quantifient chaque risque identifié en lui attribuant les coefficients affectés à sa probabilité de survenance brute et à sa gravité potentielle brute sur la base des échelles définies précédemment. Ainsi le produit de ces 2 coefficients permet d'obtenir les valeurs de **CB** collectées au niveau de ces banques.

L'identification des contrôles consiste à définir des règles appropriées de réduction des risques et des procédures adéquates à appliquer de façon efficace en vue d'apporter l'assurance que les niveaux de risques résiduels ne dépassent pas le niveau d'appétence au risque défini par le management. Evaluer un contrôle consiste à lui attribuer un coefficient affecté à la maturité du contrôle selon l'échelle de maturité définie précédemment. Ainsi, on obtient les valeurs de **CM** collectées au niveau des banques, **CM** est représenté par **M** au niveau du tableau 14.

Les valeurs de **CR** correspondent aux criticités résiduelles estimées par les banques lors des séances d'évaluation en utilisant la méthode RSCA. Ces valeurs sont estimées en combinant les données d'évaluation brute des risques à l'évaluation de la maturité des contrôles en vue d'obtenir le niveau de risque résiduel correspondant au niveau réel de l'exposition de la banque par rapport aux risques identifiés et évalués. Ainsi le produit de la probabilité de survenance résiduelle et de la gravité potentielle résiduelle permet d'obtenir les valeurs de **CR** collectées au niveau des banques.

Par ailleurs, face à la difficulté de collecter des données dans plusieurs banques à la fois, la problématique a été évoquée dans toutes les conférences auxquelles nous avons assisté dans le cadre de la publication de nos articles. Ainsi, les nombreuses suggestions qu'on a eues concouraient à la seule et même idée qui consistait à choisir un échantillon représentative qui tient compte de 3 aspects : 4 typologies des banques de l'UEMOA (européenne, panafricaine, régionale et nationale), les 3 pays concernés dans l'UEMOA (Sénégal, Burkina et Cote d'Ivoire) et les 4 semestres évalués par banque. Sur cette base, nous avons collaboré avec 4 banques provenant de 3 pays différents dont 2 au Sénégal, une au Burkina Faso et une autre en Côte D'ivoire.

L'ensemble des données d'apprentissage collectées sont indiquées dans le tableau ci-après:

Tableau 15:Données d'apprentissage collectées au niveau des 4 banques pour tester les modèles initiaux

DONNEES BANQUE 1				DONNEES BANQUE 2				DONNEES BANQUE 3				DONNEES BANQUE 4			
RISQUES	CR	CB	M	RISQUES	CR	CB	M	RISQUES	CR	CB	M	RISQUES	CR	CB	M
R1	1	4	3	R1	5	12	7	R1	15	24	9	R1	1	3	3
R2	2	5	3	R2	4	12	8	R2	12	24	12	R2	1	4	4
R3	2	5	3	R3	3	12	9	R3	18	30	12	R3	1	4	3
R4	1	6	5	R4	9	15	6	R4	16	30	14	R4	2	5	3
R5	2	6	4	R5	12	20	7	R5	20	36	14	R5	2	5	3
R6	1	6	4	R6	12	20	8	R6	1	6	5	R6	1	6	5
R7	2	6	4	R7	9	18	9	R7	3	9	6	R7	2	6	4
R8	2	6	4	R8	18	30	12	R8	3	10	7	R8	1	6	5
R9	2	6	4	R9	1	3	3	R9	5	10	5	R9	1	6	6
R10	1	6	5	R10	1	4	4	R10	6	12	6	R10	1	6	6
R11	2	6	4	R11	4	10	6	R11	5	12	7	R11	2	6	4
R12	2	8	6	R12	2	6	4	R12	4	12	8	R12	2	6	4
R13	2	8	6	R13	1	6	5	R13	3	12	9	R13	2	6	4
R14	3	9	6	R14	1	6	6	R14	9	15	6	R14	1	6	5
R15	4	9	5	R15	1	8	8	R15	9	16	7	R15	2	6	4
R16	4	9	5	R16	4	9	5	R16	10	18	8	R16	2	6	4
R17	3	10	7	R17	10	16	6	R17	9	18	9	R17	1	6	5
R18	5	10	5	R18	6	12	6	R18	10	20	10	R18	1	6	6
R19	4	10	6	R19	5	12	7	R19	15	24	9	R19	1	8	8
R20	4	10	6	R20	4	12	8	R20	15	24	10	R20	2	8	6
R21	3	10	7	R21	3	12	9	R21	20	30	11	R21	2	8	6
R22	3	10	7	R22	2	12	11	R22	18	30	12	R22	3	9	6
R23	2	10	8	R23	8	15	7	R23	2	6	4	R23	4	9	5
R24	3	10	7	R24	10	20	10	R24	1	6	5	R24	4	9	5
R25	4	10	6	R25	15	24	9	R25	4	9	5	R25	4	10	6
R26	6	12	6	R26	15	24	10	R26	4	10	6	R26	3	10	7
R27	5	12	7	R27	24	36	11	R27	4	10	6	R27	3	10	7
R28	4	12	8	R28	18	30	12	R28	5	12	7	R28	3	10	7
R29	3	12	9	R29	1	3	3	R29	4	12	8	R29	4	10	6
R30	5	12	7	R30	1	4	4	R30	3	12	9	R30	1	10	10
R31	4	12	8	R31	4	10	6	R31	2	12	10	R31	3	10	7
R32	3	12	9	R32	2	6	4	R32	8	15	7	R32	5	12	7
R33	2	12	10	R33	1	6	5	R33	8	16	8	R33	4	12	8
R34	3	12	9	R34	1	6	6	R34	9	18	9	R34	3	12	9
R35	2	12	10	R35	1	8	8	R35	8	18	10	R35	6	12	6
R36	1	12	10	R36	4	9	5	R36	9	20	11	R36	5	12	7
R37	4	12	8	R37	10	16	6	R37	16	24	8	R37	4	12	8
R38	3	12	9	R38	6	12	7	R38	15	24	9	R38	3	12	9
R39	4	12	8	R39	5	12	7	R39	20	30	10	R39	2	12	10
R40	3	12	9	R40	4	12	8	R40	20	30	11	R40	4	12	8
R41	3	12	9	R41	3	12	9	R41	24	36	12	R41	3	12	9
R42	2	12	10	R42	2	12	10	R42	2	6	4	R42	1	12	11
R43	2	12	10	R43	8	15	7	R43	2	6	4	R43	4	12	8
R44	1	12	11	R44	10	16	6	R44	3	10	7	R44	2	12	10
R45	4	12	8	R45	10	18	8	R45	2	8	6	R45	2	12	10
R46	9	15	6	R46	12	20	10	R46	2	8	6	R46	1	12	11
R47	8	15	7	R47	16	24	8	R47	3	10	7	R47	4	12	8
R48	8	15	7	R48	15	24	9	R48	2	10	8	R48	3	12	9
R49	6	15	9	R49	20	30	11	R49	3	12	9	R49	1	12	12
R50	4	15	11	R50	20	30	10	R50	2	12	10	R50	3	12	9

DONNEES BANQUE 1				DONNEES BANQUE 2				DONNEES BANQUE 3				DONNEES BANQUE 4			
RISQUES	CR	CB	M	RISQUES	CR	CB	M	RISQUES	CR	CB	M	RISQUES	CR	CB	M
R51	3	15	12	R51	24	36	12	R51	1	12	11	R51	4	12	8
R52	5	15	10	R52	1	6	6	R52	5	15	8	R52	9	15	6
R53	6	15	9	R53	2	6	4	R53	4	12	8	R53	8	15	7
R54	1	15	14	R54	2	6	4	R54	6	15	9	R54	8	15	8
R55	5	15	10	R55	3	10	7	R55	6	16	10	R55	6	15	9
R56	9	16	7	R56	2	8	6	R56	10	18	8	R56	6	15	9
R57	8	16	8	R57	2	8	6	R57	12	20	7	R57	5	15	10
R58	6	16	10	R58	3	10	7	R58	15	24	9	R58	6	15	9
R59	3	16	13	R59	3	10	7	R59	15	24	9	R59	5	15	10
R60	6	16	10	R60	4	12	8	R60	18	30	10	R60	5	15	10
R61	5	16	11	R61	3	12	9	R61	18	30	12	R61	6	15	9
R62	10	18	8	R62	1	12	11	R62	3	12	9	R62	10	16	6
R63	9	18	9	R63	6	15	9	R63	24	36	13	R63	10	16	6
R64	9	18	9	R64	6	16	10	R64	4	12	8	R64	6	16	10
R65	8	18	10	R65	10	18	8	R65	2	5	3	R65	5	16	11
R66	10	18	8	R66	15	20	5	R66	3	10	7	R66	3	16	13
R67	8	18	10	R67	16	24	8	R67	3	12	9	R67	9	18	9
R68	8	18	10	R68	15	24	9	R68	3	12	9	R68	12	18	7
R69	6	18	12	R69	20	30	10	R69	2	12	10	R69	10	18	8
R70	10	20	10	R70	18	30	12	R70	4	15	11	R70	10	18	8
R71	9	20	11	R71	3	12	9	R71	3	15	12	R71	8	18	11
R72	12	20	8	R72	2	5	3	R72	3	16	13	R72	6	18	12
R73	15	20	5	R73	1	8	8	R73	8	18	10	R73	8	18	10
R74	12	20	8	R74	1	9	9	R74	15	20	5	R74	12	20	7
R75	12	20	8	R75	1	10	10	R75	5	15	10	R75	12	20	8
R76	15	24	9	R76	3	10	7	R76	15	24	9	R76	10	20	10
R77	12	24	12	R77	3	12	9	R77	12	24	12	R77	12	20	10
R78	15	24	9	R78	1	12	12	R78	18	30	12	R78	15	20	5
R79	15	24	9	R79	4	12	8	R79	16	30	13	R79	8	20	12
R80	16	24	8	R80	6	15	9	R80	21	36	15	R80	6	20	14
R81	15	24	9	R81	5	15	10	R81	6	15	9	R81	15	24	9
R82	15	24	9	R82	3	16	13	R82	1	4	3	R82	15	24	9
R83	15	24	9	R83	8	18	10	R83	2	5	3	R83	16	24	8
R84	15	24	9	R84	15	20	6	R84	2	6	4	R84	15	24	9
R85	12	24	12	R85	2	6	4	R85	1	6	5	R85	12	24	12
R86	15	24	9	R86	2	6	4	R86	2	6	4	R86	15	24	9
R87	18	30	12	R87	3	10	7	R87	6	16	10	R87	15	24	10
R88	16	30	14	R88	2	8	6	R88	4	9	5	R88	20	30	10
R89	20	30	10	R89	2	8	6	R89	4	10	6	R89	20	30	10
R90	18	30	12	R90	3	10	7	R90	2	12	10	R90	18	30	12
R91	20	30	10	R91	2	10	8	R91	1	12	11	R91	20	30	10
R92	20	30	10	R92	3	12	9	R92	4	12	8	R92	20	30	10
R93	18	30	10	R93	2	12	10	R93	1	15	14	R93	18	30	12
R94	18	30	12	R94	1	12	11	R94	8	18	11	R94	18	30	12
R95	18	30	12	R95	8	15	8	R95	5	15	10	R95	16	30	14
R96	18	30	12	R96	4	12	8	R96	5	16	11	R96	24	36	12
R97	24	36	12	R97	6	15	9	R97	6	18	12	R97	24	36	12
R98	24	36	12	R98	0	6	6	R98	12	20	7	R98	24	36	11
R99	24	36	12	R99	2	6	4	R99	12	20	8	R99	24	36	12
R100	24	36	12	R100	6	16	10	R100	15	24	9	R100	24	36	12

Ces données d'apprentissage collectées ont été consignées en vue d'effectuer les différents tests économétriques sur Eviews. Les tests économétriques appliqués sur ces données d'apprentissage pour éprouver les modèles initiaux sont essentiellement la méthode des moindres carrées ordinaires, le coefficient de détermination, les tests de significativité et les tests de normalité des erreurs.

1. Méthode des moindres carrées

Les paramètres *(a et b)* de la première équation de régressions linéaires sont estimés par la méthode MCO (Moindres Carrées Ordinaires). Cette méthode a été utilisée parce que l'estimateur des MCO minimise la distance moyenne entre les points observés de leurs différentes coordonnées et la droite d'équation estimée. De plus, la méthode des moindres carrés permet d'obtenir un ajustement afin d'une série statistique double. C'est d'ailleurs la méthode qui donne le meilleur ajustement et c'est la raison pour laquelle, notre choix s'est porté sur elle. De manière spécifique,elle calcule pour chaque point du nuage, sa distance par rapport à une droite donnée puis à rendre minimale la somme de ces distances. Pour réaliser ces tests, nous avons appliqué la première équation de régressions linéaires aux données d'apprentissage collectées au niveau des banques sur 4 semestres d'affilés.

La première équation de régressions correspondant aux modèles mathématiques initiaux qui est définie dans le chapitre précédent est déclinée ci-après :

$$\log(CR_i) = a log(CB_i) - b log(CM_i) + C \qquad \textbf{4.2.1}$$

Les paramètres a et b sont à expliquer par l'équation de régression linéaire, il faut les estimer avec la méthode des moindres carrées et à partir des données d'apprentissage collectées au niveau des 4 banques.

L'exploitation d'Eviews avec les données collectées au niveau des banques sur 4 semestres donne les résultats suivants.

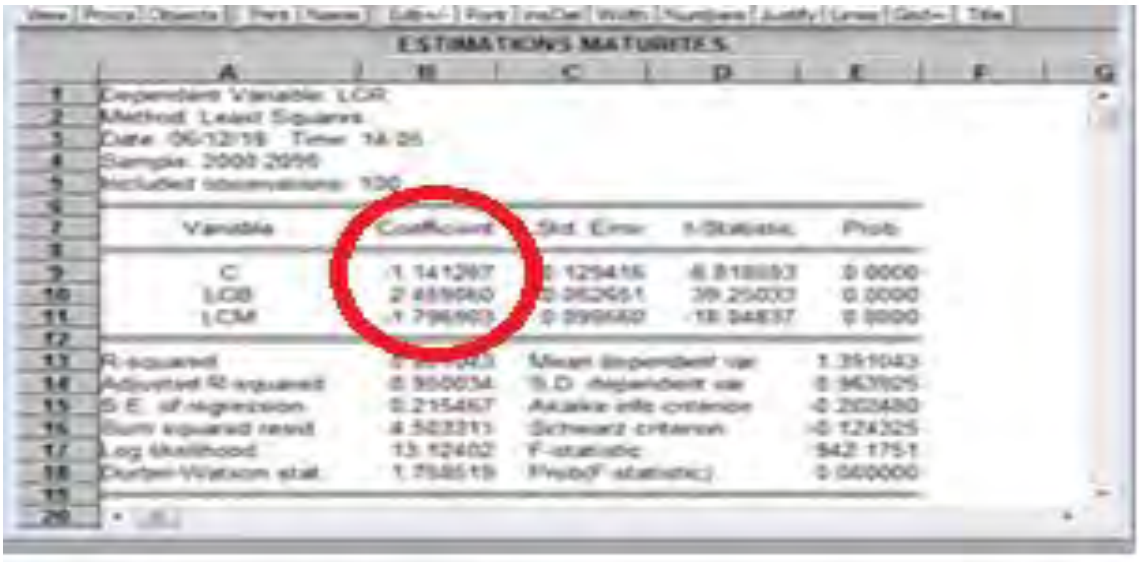
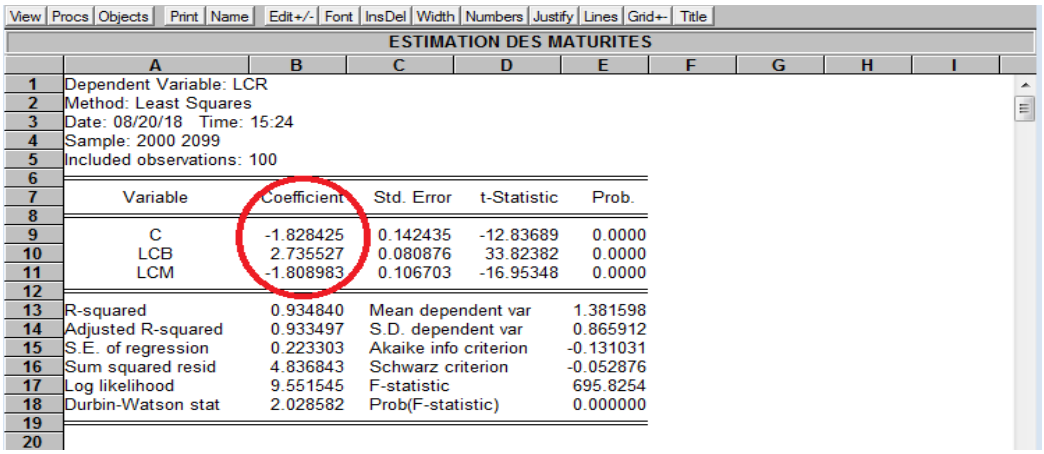


Figure 12 : Coefficients affectés aux variables de l'équation 1 et relatifs à la banque 1



View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+- | Title

ESTIMATION DES MATURITES

	A	B	C	D	E	F	G	H	I
1	Dependent Variable: LCR								
2	Method: Least Squares								
3	Date: 08/20/18 Time: 15:24								
4	Sample: 2000 2099								
5	Included observations: 100								
6									
7	Variable	Coefficient	Std. Error	t-Statistic	Prob.				
8									
9	C	-1.828425	0.142435	-12.83689	0.0000				
10	LCB	2.735527	0.080876	33.82382	0.0000				
11	LCM	-1.808983	0.106703	-16.95348	0.0000				
12									
13	R-squared	0.934840	Mean dependent var		1.381598				
14	Adjusted R-squared	0.933497	S.D. dependent var		0.865912				
15	S.E. of regression	0.223303	Akaike info criterion		-0.131031				
16	Sum squared resid	4.836843	Schwarz criterion		-0.052876				
17	Log likelihood	9.551545	F-statistic		695.8254				
18	Durbin-Watson stat	2.028582	Prob(F-statistic)		0.000000				
19									
20									

Figure 13: Coefficients affectés aux variables de l'équation 1 et relatifs à la banque 2

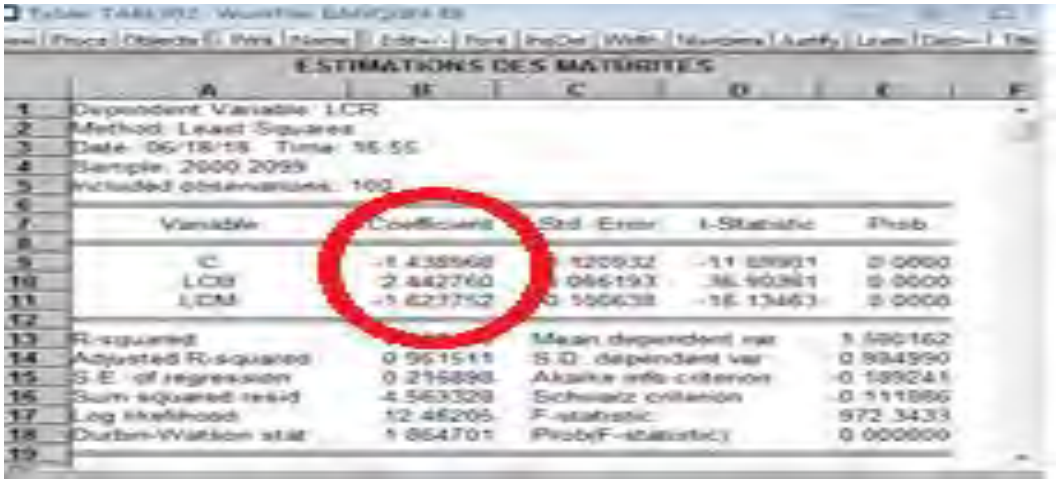


Figure 14: Coefficients affectés aux variables de l'équation 1 et relatifs à la banque 3

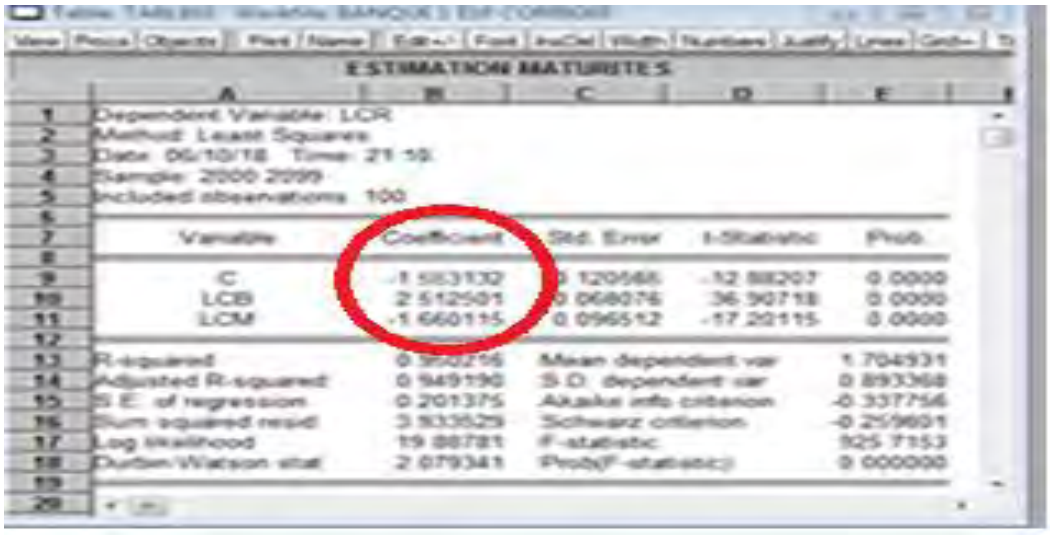


Figure 15: Coefficients affectés aux variables de l'équation 1 et relatifs à la banque 4

A la lecture de ces résultats obtenus avec Eviews, il en résulte que

a. Le coefficient $\boldsymbol{a}$ représentant le coefficient affecté à la variable criticité brute des risques possède une valeur positive pour les 4 semestres testés

b. Le coefficient $\boldsymbol{b}$ représentant le coefficient affecté à la variable maturité des contrôles possède une valeur négative pour les 4 semestres testés

c. La valeur **C** représentant la constante de l'équation est négative, elle correspond aux variables non prises en compte par les variables explicatives de l'équation de régressions linéaires à savoir la criticité brute des risques et la maturité des contrôles.

d. Sur les 4 semestres, les variables et constantes de l'équation sont approximativement égales

- **Interprétation économétriques**

a. Si la criticité brute augmente alors la criticité résiduelle augmente

b. Si la maturité des contrôles augmente alors la criticité résiduelle diminue

c. La négativité de la constante montre qu'elle est susceptible de contribuer à la diminution de la criticité résiduelle des risques

d. Les variables et constantes sont de même ordre pour les quatre banques ayant fournis des séries de données de même taille

- **Interprétation gestion des risques**

A titre indicatif, les 4 principes qui nous ont permis de définir les modèles initiaux correspondant à cette équation de régressions linéaires sont relatés ci-après **[24]** :

Principe 1
Un risque peut avoir un ou plusieurs contrôles. En effet, les contrôles sont définis et mis en œuvre dans le but de mitiger les risques. Ainsi, selon la nature du risque, un ou plusieurs contrôles y afférents peuvent être définis.

Principe 2
Les contrôles sont mis en œuvre pour maitriser les risques identifiés et évalués. En effet, suite à l'identification des risques, une première évaluation basée sur les échelles de probabilité de survenance brute et de gravité potentielle brute permet d'assigner à chaque risque, une valeur de criticité brute correspondant au niveau de criticité qui ne tient pas compte des contrôles effectivement mis en œuvre. Plus la criticité brute est élevée, plus le risque est critique.

Principe 3
Un contrôle a une seule maturité. Cette maturité correspond au niveau de mise en œuvre du contrôle, elle peut être inexistante, informelle, opérationnelle, intégrée ou optimisée.

Principe 4
Seuls, les contrôles matures peuvent réduire la probabilité de survenance brute et/ou la gravité potentielle brute des risques. Pour qu'un contrôle puisse considérablement réduire ou mitiger un risque, il faut qu'elle soit mature, cela signifie que sa maturité a un niveau opérationnel au minimum.

Nous pouvons donc conclure que les résultats obtenus concordent avec ces principes car il apparait que :

a. La criticité résiduelle diminue avec la maturité des contrôles. En effet, d'après la valeur du coefficient **b**, les contrôles ont un impact sur la probabilité de survenance brute et/ou la gravité potentielle brute des risques, ce qui est en accord avec les principes **4**.

b. Les résultats montrent que le risque possède plusieurs contrôles, ce qui est en accord avec les principes **1 et 3.**

c. La criticité résiduelle des risques $\boldsymbol{CR_i}$ est obtenue en faisant la soustraction entre la criticité brute des risques $\boldsymbol{CB_i}$ et la maturité globale des contrôles $\boldsymbol{CM_i}$, ce qui est en accord avec les principes **2 et 4**.

d. La négativité de la constante de l'équation montre qu'elle est susceptible de diminuer la criticité résiduelle des risques, ce qui est en accord avec le principe **2**

2. Coefficient de détermination

Le coefficient de détermination R mesure le degré de corrélation entre la variable à expliquer à savoir la criticité résiduelle des risques et les variables explicatives comme la criticité brute du risque et la maturité des contrôles. Ce coefficient permet de savoir si la variable à expliquer est réellement expliquée par les variables explicatives.

- si $0 < R^2$ <50%, il n'y a pas de corrélation entre la variable à expliquer et les variables explicatives
- si R^2 >50%, il y a corrélation entre la variable à expliquer et les variables explicatives

Pour effectuer ces tests, nous avons utilisé la même approche en appliquant la première équation de régressions linéaires aux données d'apprentissage collectées. Cette équation de régressions correspondant aux modèles mathématiques initiaux est déclinée ci-après :

$$\log(CR_i) = a\log(CB_i) - b\log(CM_i) + C \qquad \textbf{4.2.1}$$

L'exploitation d'Eviews avec les données collectées au niveau des banques sur 4 semestres donne les résultats suivants :

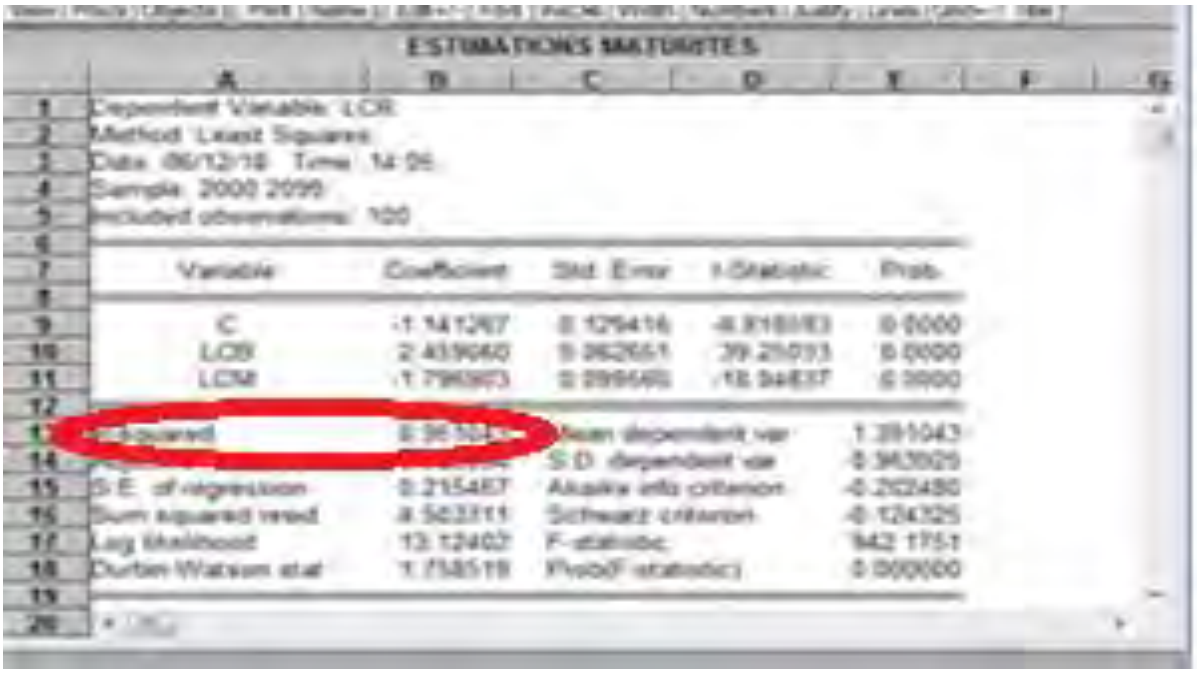


Figure 16:Coefficient de détermination obtenu avec l'équation 1 pour la banque 1

View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+- | Title

ESTIMATION DES MATURITES

Dependent Variable: LCR
Method: Least Squares
Date: 08/20/18 Time: 15:24
Sample: 2000 2099
Included observations: 100

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-1.828425	0.142435	-12.83689	0.0000
LCB	2.735527	0.080876	33.82382	0.0000
LCM	-1.808983	0.106703	-16.95348	0.0000

R-squared	0.934840	Mean dependent var	1.381598
Adjusted R-squared	0.933497	S.D. dependent var	0.865912
S.E. of regression	0.223303	Akaike info criterion	-0.131031
Sum squared resid	4.836843	Schwarz criterion	-0.052876
Log likelihood	9.551545	F-statistic	695.8254
Durbin-Watson stat	2.028582	Prob(F-statistic)	0.000000

Figure 17:Coefficient de détermination obtenu avec l'équation 1 pour la banque 2

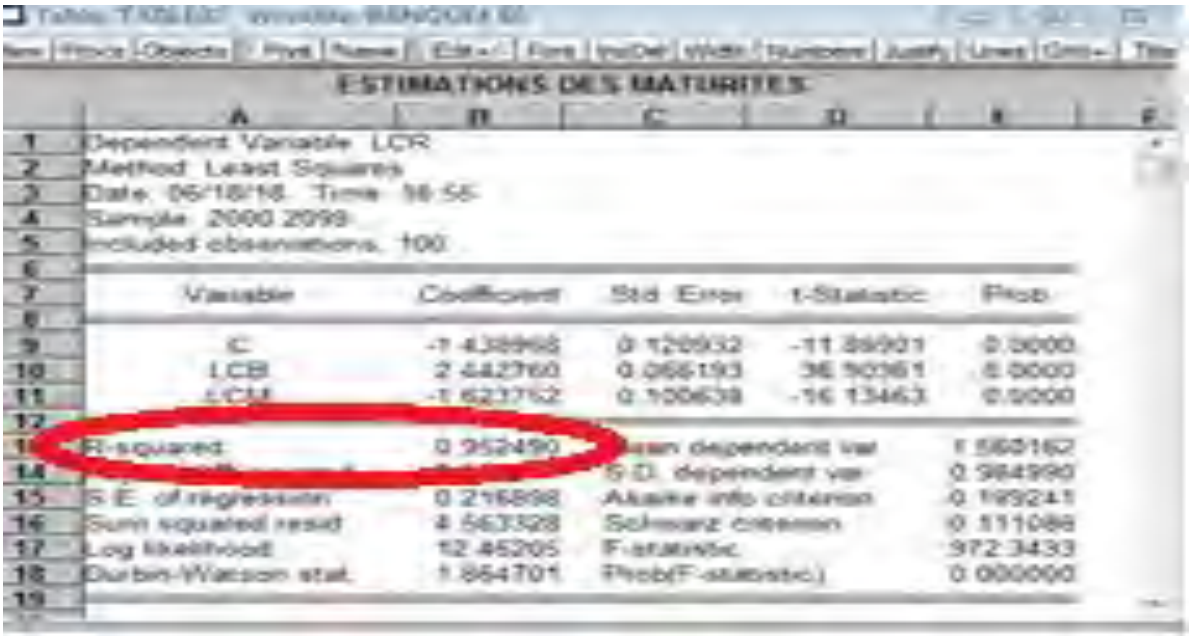


Figure 18:Coefficient de détermination obtenu avec l'équation 1 pour la banque 3

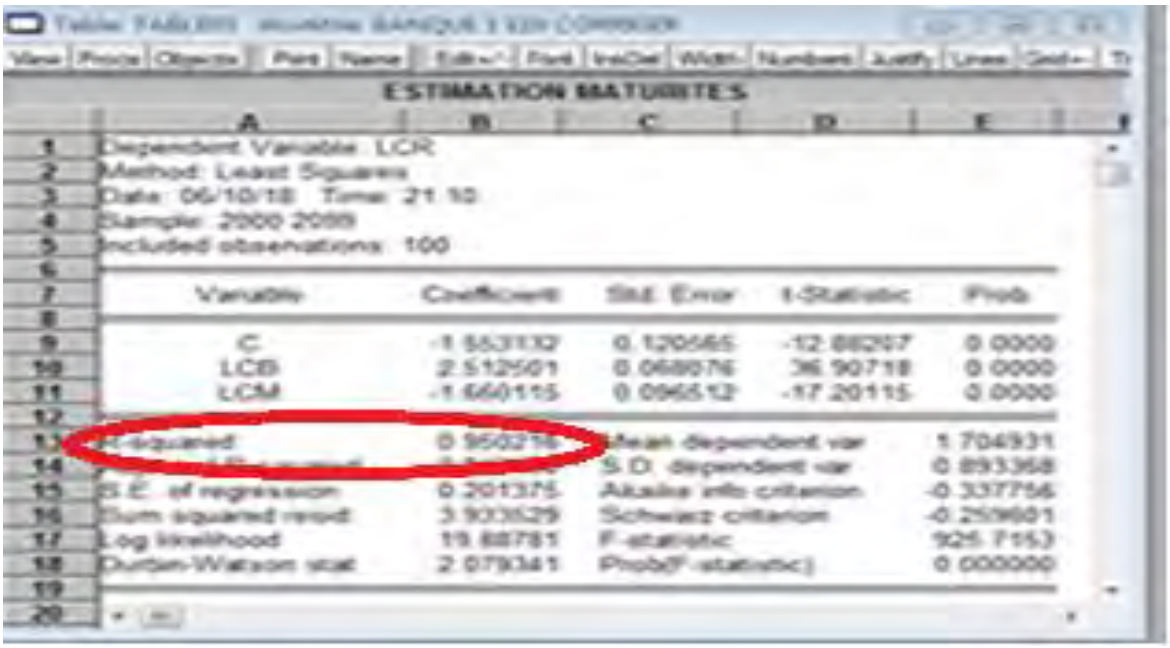


Figure 19:Coefficient de détermination obtenu avec l'équation 1 pour la banque 4

- **Interprétation des résultats**

Ainsi on obtient un coefficient de détermination égal à 0.95 pour 3 semestres et 0,93 pour un semestre.

Cela traduit que 93% ou 95% des criticités résiduelles sont expliquées par les criticités brutes et la maturité des contrôles. Ce qui signifie que la criticité brute et la maturité des contrôles sont des variables pertinentes qui permettent d'obtenir la criticité résiduelle des risques.

De plus, on constate que le coefficient est très élevé et dépasse largement le seuil de 50% permettant de statuer si le coefficient de détermination est correct ou pas ; ce résultat est donc satisfaisant.

3. **Tests de significativités**

Les hypothèses H_0 *et* H_1 relatives aux tests de significativité permettent d'expliquer le modèle par rapport à ses variables explicatives mais aussi de façon globale, ils sont indiqués ci-dessous :

$$H_{0(\,Premiere\ Hypothese)} : coefficient = 0$$
$$H_1(Deuxieme\ Hypothese : coefficient \neq 0$$

L'interprétation des coefficients relatifs à ces hypothèses est basée sur les valeurs de probabilité obtenues après estimation du modèle, elle est décrite ci-après :

- Si probabilité inférieure à 0,05 alors on accepte le coefficient H_1 cela signifie que la variable explicative concernée est significative.

- Si probabilité supérieure à 0,05 alors on accepte H_0 cela signifie que la variable explicative concernée n'est pas significative

Pour réaliser ces tests, nous avons aussi utilisé la même approche en appliquant la première équation de régressions linéaires aux données d'apprentissage collectées au niveau des 4 banques. Ainsi, nous avons effectué les deux types de tests de significativité suivants :

- **Test de Student** permettant de tester la significativité des variables explicatives, il permet de s'assurer que les variables explicatives ont une influence significative sur la variable à expliquer par l'équation.

- **Test de Fisher** permettant de tester la significativité globale de l'équation, il prend en compte la significativité de toutes les variables explicatives et permet de s'assurer que l'équation est globalement bonne.

A titre de rappel, la première équation de régression linéaire est déclinée ci-après :

$$\log(CR_i) = a log(CB_i) - b log(CM_i) + C \qquad \textbf{4.2.1}$$

- **Test de Student**

L'exploitation d'Eviews sur les 4 semestres d'affilés pour le test de Student donne les résultats suivants.

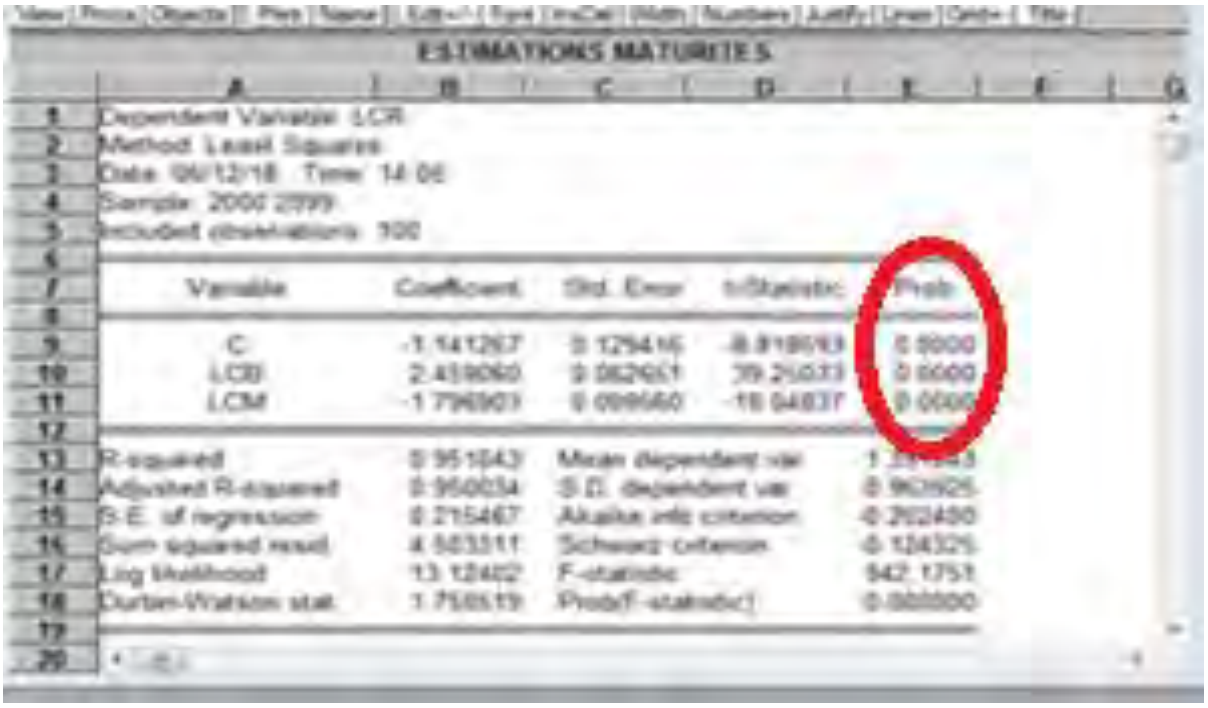


Figure 20:Test de Student: Résultats obtenus avec l'équation 1 pour la banque 1

View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+- | Title

ESTIMATION DES MATURITES

	A	B	C	D	E	F	G	H	I
1	Dependent Variable: LCR								
2	Method: Least Squares								
3	Date: 08/20/18 Time: 15:24								
4	Sample: 2000 2099								
5	Included observations: 100								
6									
7	Variable	Coefficient	Std. Error	t-Statistic	Prob.				
8									
9	C	-1.828425	0.142435	-12.83689	0.0000				
10	LCB	2.735527	0.080876	33.82382	0.0000				
11	LCM	-1.808983	0.106703	-16.95348	0.0000				
12									
13	R-squared	0.934840	Mean dependent var		1.381598				
14	Adjusted R-squared	0.933497	S.D. dependent var		0.865912				
15	S.E. of regression	0.223303	Akaike info criterion		-0.131031				
16	Sum squared resid	4.836843	Schwarz criterion		-0.052876				
17	Log likelihood	9.551545	F-statistic		695.8254				
18	Durbin-Watson stat	2.028582	Prob(F-statistic)		0.000000				
19									
20									
21									

Figure 21:Test de Student: Résultats obtenus avec l'équation 1 pour la banque 2

Figure 22:Test de Student: Résultats obtenus avec l'équation 1 pour la banque 3

Figure 23:Test de Student: Résultats obtenus avec l'équation 1 pour la banque 4

- **Interprétation des résultats**

D'après les résultats fournis par Eviews, la valeur de prob=00000 **s**ur les 4 semestres.

A l'issu de ce test, les résultats montrent que toutes les probabilités des variables explicatives sont largement inférieures à 5%. Nous pouvons en conclure que les variables explicatives concernées sont significatives. Elles ont donc une influence significative sur la variable à expliquer à savoir la criticité résiduelle des risques.

- **Test de Fisher**

L'exploitation d'Eviews sur les 4 semestres d'affilés pour le test de Fisher donne les résultats suivants.

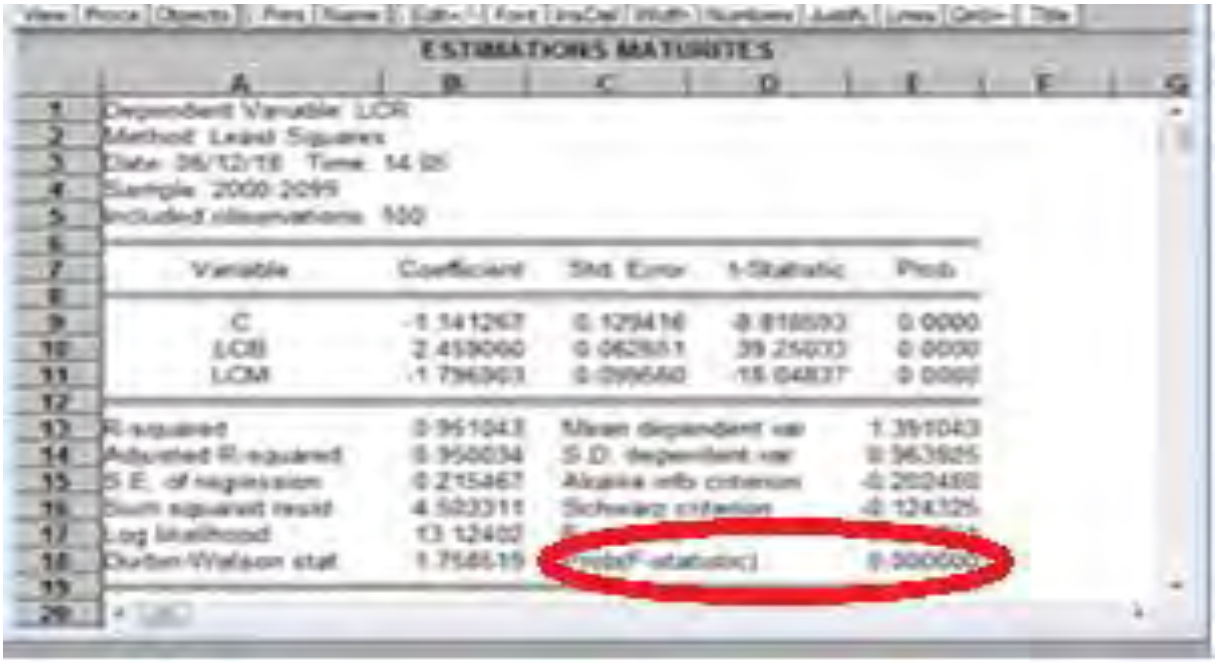


Figure 24:Test de Fisher: Résultats obtenus avec l'équation 1 pour la banque 1

View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+- | Title

ESTIMATION DES MATURITES

	A	B	C	D	E	F	G	H	I
1	Dependent Variable: LCR								
2	Method: Least Squares								
3	Date: 08/20/18 Time: 15:24								
4	Sample: 2000 2099								
5	Included observations: 100								
6									
7	Variable	Coefficient	Std. Error	t-Statistic	Prob.				
8									
9	C	-1.828425	0.142435	-12.83689	0.0000				
10	LCB	2.735527	0.080876	33.82382	0.0000				
11	LCM	-1.808983	0.106703	-16.95348	0.0000				
12									
13	R-squared	0.934840	Mean dependent var		1.381598				
14	Adjusted R-squared	0.933497	S.D. dependent var		0.865912				
15	S.E. of regression	0.223303	Akaike info criterion		-0.131031				
16	Sum squared resid	4.836843	Schwarz criterion		-0.052876				
17	Log likelihood	9.551545	F-statistic		695.8254				
18	Durbin-Watson stat	2.028582	Prob(F-statistic)		0.000000				
19									
20									

Figure 25:Test de Fisher: Résultats obtenus avec l'équation 1 pour la banque 2

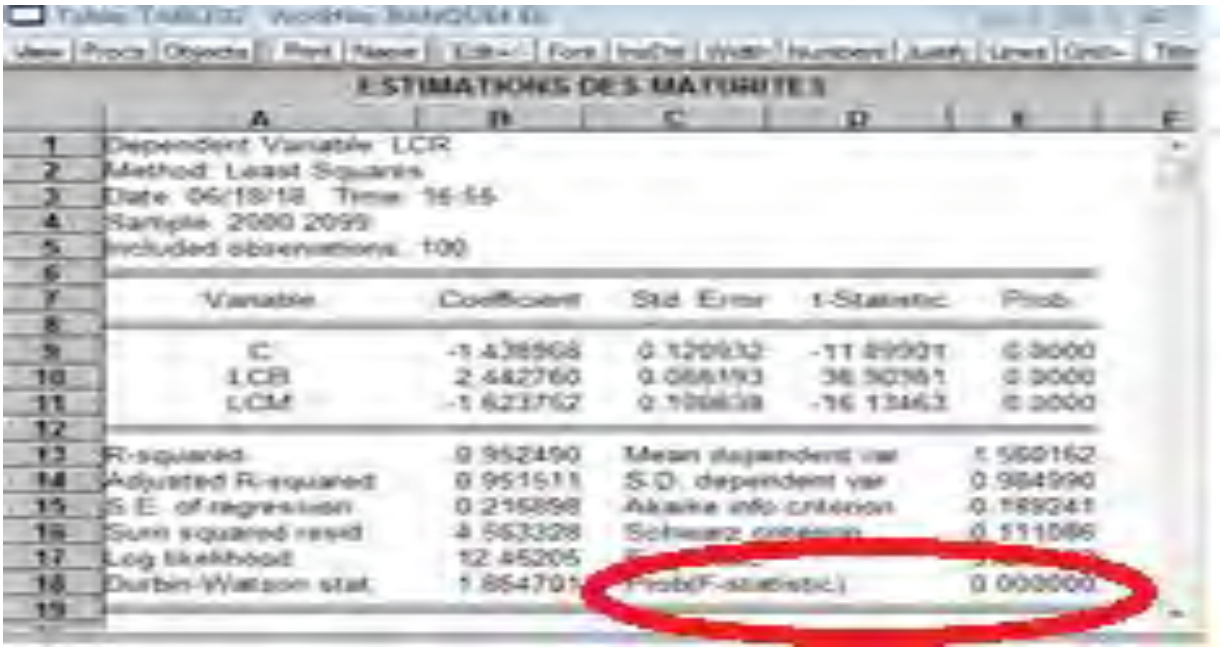


Figure 26:Test de Fisher: Résultats obtenus avec l'équation 1 pour la banque 3

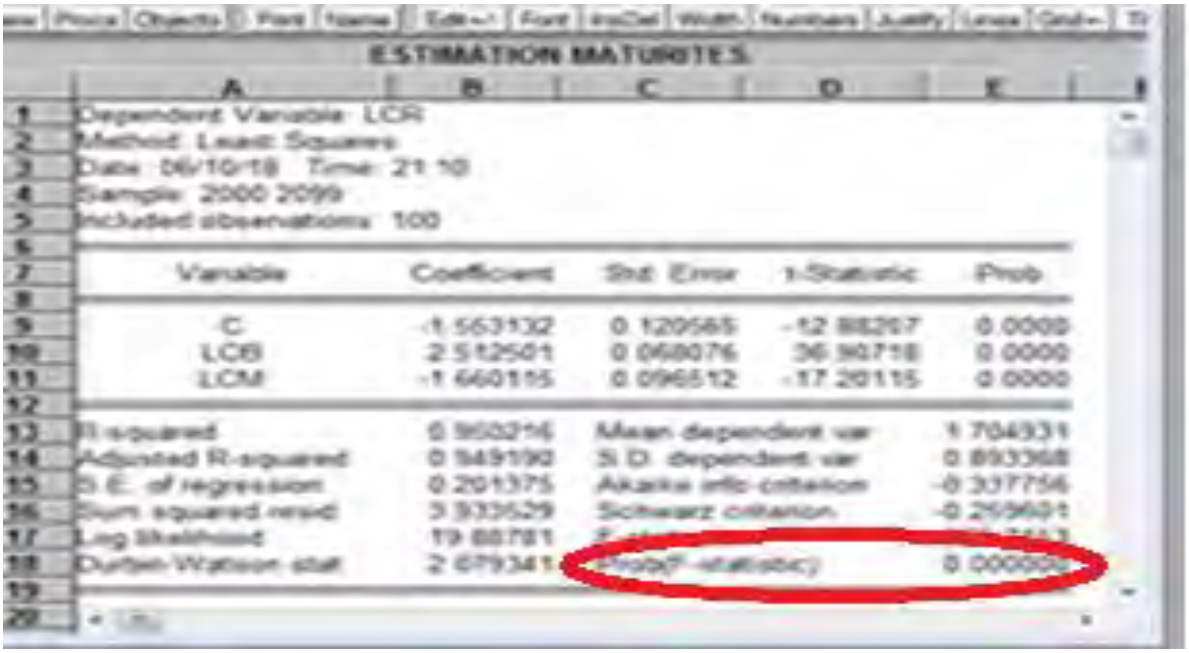


Figure 27:Test de Fisher: Résultats obtenus avec l'équation 1 pour la banque 4

- **Interprétation des résultats**

D'après les résultats fournis par Eviews, la valeur de prob F-Statistic=00000 sur les 4 semestres d'affilés, nous pouvons en conclure que l'équation est globalement significative car la valeur du prob (F-Statistic) est largement inférieure à 5%.

4. Test de normalité de Jarque Bera

Les tests de normalités des erreurs permettent de vérifier si les variables de l'équation suivent une loi normale selon les seuils décrits ci-après :

- Au seuil de 5%, on accepte l'hypothèse de normalité dès que la valeur de la probabilité est supérieure à 5%
- Au seuil de 5%, on rejette l'hypothèse de normalité dès que la valeur de la probabilité est inférieure ou égale à 5%

Les résultats du test de normalité des erreurs sur les 4 semestres d'affilés sont indiqués dans le tableau ci-dessous :

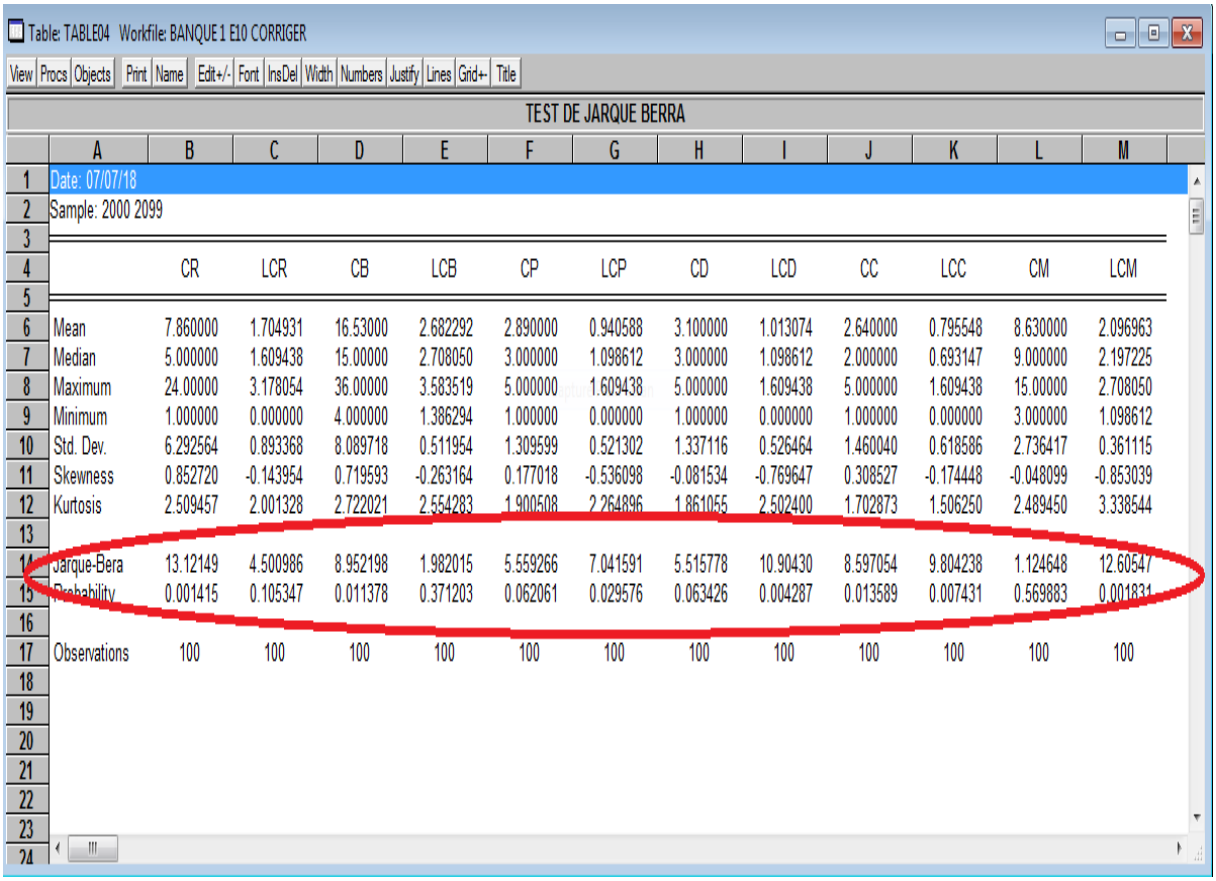


Table: TABLE04 Workfile: BANQUE 1 E10 CORRIGER

View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+ | Title

TEST DE JARQUE BERRA

Date: 07/07/18
Sample: 2000 2099

	CR	LCR	CB	LCB	CP	LCP	CD	LCD	CC	LCC	CM	LCM
Mean	7.860000	1.704931	16.53000	2.682292	2.890000	0.940588	3.100000	1.013074	2.640000	0.795548	8.630000	2.096963
Median	5.000000	1.609438	15.00000	2.708050	3.000000	1.098612	3.000000	1.098612	2.000000	0.693147	9.000000	2.197225
Maximum	24.00000	3.178054	36.00000	3.583519	5.000000	1.609438	5.000000	1.609438	5.000000	1.609438	15.00000	2.708050
Minimum	1.000000	0.000000	4.000000	1.386294	1.000000	0.000000	1.000000	0.000000	1.000000	0.000000	3.000000	1.098612
Std. Dev.	6.292564	0.893368	8.089718	0.511954	1.309599	0.521302	1.337116	0.526464	1.460040	0.618586	2.736417	0.361115
Skewness	0.852720	-0.143954	0.719593	-0.263164	0.177018	-0.536098	-0.081534	-0.769647	0.308527	-0.174448	-0.048099	-0.853039
Kurtosis	2.509457	2.001328	2.722021	2.554283	1.900508	2.264896	1.861055	2.502400	1.702873	1.506250	2.489450	3.338544
Jarque-Bera	13.12149	4.500986	8.952198	1.982015	5.559266	7.041591	5.515778	10.90430	8.597054	9.804238	1.124648	12.60547
Probability	0.001415	0.105347	0.011378	0.371203	0.062061	0.029576	0.063426	0.004287	0.013589	0.007431	0.569883	0.001831
Observations	100	100	100	100	100	100	100	100	100	100	100	100

Figure 28:Test de Jarque Bera: Résultats obtenus avec l'équation 1 pour la banque 1

Table: TABLE01 Workfile: POUR TEST

TEST DE NORMALITE

Date: 08/20/18
Sample: 2000 2099

	CR	LCR	CB	LCB	CP	LCP	CD	LCD	CC	LCC	CM	LCM
Mean	5.670000	1.381598	14.17000	2.553893	2.970000	0.971190	2.950000	0.971960	2.580000	0.778400	8.500000	2.087482
Median	4.000000	1.386294	12.00000	2.484907	3.000000	1.098612	3.000000	1.098612	2.000000	0.693147	9.000000	2.197225
Maximum	25.00000	3.218876	36.00000	3.583519	5.000000	1.609438	5.000000	1.609438	5.000000	1.609438	14.00000	2.639057
Minimum	1.000000	0.000000	4.000000	1.386294	1.000000	0.000000	1.000000	0.000000	1.000000	0.000000	3.000000	1.098612
Std. Dev.	4.888773	0.865912	6.286196	0.450515	1.306201	0.518084	1.258306	0.501144	1.415499	0.606141	2.572190	0.341470
Skewness	1.477145	0.016583	0.865639	-0.172870	0.055596	-0.635931	0.063821	-0.674807	0.362752	-0.156157	-0.102008	-0.813137
Kurtosis	5.084083	2.061220	3.689083?	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1.812603	1.536958	2.354467	3.202537
Jarque-Bera	54.46346	3.676703	14.47249	1.283148	5.503758	8.436612	4.589729	8.612394	8.067783	9.325128	1.909733	11.19078
Probability	0.000000	0.159079	0.000720	0.526463	0.063808	0.014724	0.100775	0.013485	0.017705	0.009442	0.384863	0.003715
Observations	100	100	100	100	100	100	100	100	100	100	100	100

Figure 29: Test de Jarque Bera: Résultats obtenus avec l'équation 1 pour la banque 2

Table: TABLE04 Workfile: BANQUE 3 E4

TEST DE JARQUE BERRA

Date: 07/07/18
Sample: 2000 2099

	CR	LCR	CB	LCB	CP	LCP	CD	LCD	CC	LCC	CM	LCM
Mean	6.240000	1.391043	13.72000	2.481619	2.470000	0.777821	2.660000	0.838030	2.550000	0.763359	7.680000	1.986829
Median	4.000000	1.386294	12.00000	2.484907	2.000000	0.693147	3.000000	1.098612	2.000000	0.693147	8.000000	2.079442
Maximum	24.00000	3.178054	36.00000	3.583519	5.000000	1.609438	5.000000	1.609438	5.000000	1.609438	13.00000	2.564949
Minimum	1.000000	0.000000	3.000000	1.098612	1.000000	0.000000	1.000000	0.000000	1.000000	0.000000	3.000000	1.098612
Std. Dev.	5.913723	0.963925	7.348579	0.536097	1.193035	0.522147	1.319780	0.556498	1.424001	0.609344	2.326310	0.337351
Skewness	1.293033	0.113102	1.105327	-0.180178	0.465927	-0.254267	0.325996	-0.341411	0.404749	-0.103405	-0.024509	-0.735605
Kurtosis	3.692159	1.919890	3.846870?	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1.816881	1.516556	2.411130	3.036386
Jarque-Bera	29.86178	5.074187	23.35076	0.619342	5.896567	5.834040	5.917113	7.277406	8.562750	9.347405	1.454880	9.024102
Probability	0.000000	0.079096	0.000009	0.733688	0.052430	0.054095	0.051894	0.026286	0.013824	0.009338	0.483144	0.010976
Observations	100	100	100	100	100	100	100	100	100	100	100	100

Figure 30:Test de Jarque Bera: Résultats obtenus avec l'équation 1 pour la banque 3

Table: TABLE03 Workfile: BANQUE4 E6

View | Procs | Objects | Print | Name | Edit+/- | Font | InsDel | Width | Numbers | Justify | Lines | Grid+ | Title

TEST DE JARQUE BERRA

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Date: 07/07/18												
2	Sample: 2000 2099												
3													
4		CR	LCR	CB	LCB	CP	LCP	CD	LCD	CC	LCC	CM	LCM
5													
6	Mean	7.360000	1.560162	15.44000	2.585489	2.680000	0.850070	2.850000	0.935195	2.680000	0.814643	8.210000	2.042553
7	Median	5.000000	1.609438	12.00000	2.484907	2.500000	0.895880	3.000000	1.098612	3.000000	1.098612	8.000000	2.079442
8	Maximum	24.00000	3.178054	36.00000	3.583519	5.000000	1.609438	5.000000	1.609438	5.000000	1.609438	14.00000	2.639057
9	Minimum	1.000000	0.000000	3.000000	1.098612	1.000000	0.000000	1.000000	0.000000	1.000000	0.000000	3.000000	1.098612
10	Std. Dev.	6.638608	0.984990	8.435519	0.569252	1.317175	0.546150	1.233988	0.505288	1.448650	0.615191	2.697904	0.374417
11	Skewness	1.111936	-0.069516	0.866106	-0.238738	0.365015	-0.337645	0.125208	-0.638301	0.249535	-0.245283	-0.078527	-0.776883
12	Kurtosis	3.145560	1.929374	3.027304	2.520783	2.035812	1.957882	2.070370	2.417589	1.707325	1.537806	2.251273	2.946033
13													
14	Jarque-Bera	20.69499	4.856538	12.50545	1.906803	6.094180	6.425112	3.862173	8.203813	8.000330	9.911110	2.438578	10.07126
15	Probability	0.000032	0.088189	0.001925	0.385428	0.047497	0.040254	0.144991	0.016541	0.018313	0.007044	0.295440	0.006502
16													
17	Observations	100	100	100	100	100	100	100	100	100	100	100	100
18													
19													
20													

Figure 31:Test de Jarque Bera: Résultats obtenus avec l'équation 1 pour la banque 4

On remarque que certaines variables ont une probabilité Jarque Bera inférieure à 5% sur les 4 semestres, ce qui n'est pas le cas pour d'autres variables. Par conséquent, toutes les variables ne suivent pas une loi normale. C'est la raison pour laquelle nous n'avons pas pu effectuer les autres tests économétriques recommandés avec cette première équation de régressions linéaires.

a. Seconde équation de régressions linéaires

La seconde équation de régression correspondant aux modèles mathématiques améliorés est déclinée ci-après :

$$\log(CR_i) = alog(CB_i) - [blog(CP_i) + clog(CD_i) + dlog(CC_i)] + Cste \qquad \textbf{4.2.2}$$

Les variables et constantes de cette équation de régressions linéaires sont indiquées ci-dessous :

CR_i : La criticité résiduelle des risques, est la variable à expliquer par le modèle

a : Le coefficient affecté à la variable criticité brute des risques

CB_i : La criticité brute des risques, est l'une des variables explicatives du modèle

b : Le coefficient affecté à la variable maturité des contrôles préventifs

CP_i : La maturité des contrôles préventifs, est l'une des variables explicatives du modèle

c : Le coefficient affecté à la variable maturité des contrôles detectifs

CD_i : La maturité des contrôles detectifs, est l'une des variables explicatives du modèle

d : Le coefficient affecté à la variable maturité des contrôles correctifs

CC_i : La maturité des contrôles correctifs, est l'une des variables explicatives

$Cste$: La constante

Les paramètres a et b sont à expliquer par l'équation de régression linéaire, il faut les estimer avec la méthode des moindres carrées à partir des données d'apprentissage collectées au niveau des banques.

1. **Collecte des données de référence**

Pour tester la seconde équation de régressions linéaires, nous avons adopté la même attitude que précédemment en appliquant l'équation concernée aux données d'apprentissage de différentes banques sur 4 semestres d'affilés.

Au niveau de ces banques, les valeurs de CB, CR, M, P, D et C sont obtenues de la façon suivante :

L'identification des risques consiste à attribuer à chaque risque un libellé, une cause, une conséquence et un code spécifique. Quant à l'évaluation du risque brute, elle consiste à estimer la probabilité de survenance brute(P_{brute}), la gravité potentielle brute(G_{brute}) et la criticité brute (CB) qui est le produit des deux valeurs précédentes. Lors des séances d'évaluation, les banques quantifient chaque risque identifié en lui attribuant les coefficients affectés à sa probabilité de survenance brute et sa gravité potentielle brute sur la base des échelles définies précédemment. Ainsi le produit de ces 2 coefficients permet d'obtenir les valeurs de CB collectées au niveau de ces banques.

Les valeurs de CR correspondent aux criticités résiduelles estimées par les banques lors des séances d'évaluation des risques résiduelles avec la méthode RSCA. Ces valeurs sont estimées en combinant les données d'évaluation brute des risques à l'évaluation de la maturité des contrôles en vue d'obtenir le niveau de risque résiduel correspondant au niveau réel de l'exposition de la banque par rapport aux risques identifiés et évalués. Ainsi le produit de la probabilité de survenance résiduelle et de la gravité potentielle résiduelle permet d'obtenir les valeurs de CR collectées au niveau des banques.

En ce qui concerne les variables P, D et C, ils sont propres au second modèle que nous proposons. A cet à effet, nous avons dû effectué un travail supplémentaire pour obtenir

leurs valeurs en tenant compte des coefficients affectés aux contrôles préventifs, detectifs, correctifs et à la maturité des différents types de contrôles définis précédemment. Ce travail consiste d'abord à identifier les types des contrôles à savoir les contrôles préventifs, detectifs et correctifs avant de leur attribuer les coefficients spécifiques à chacun et d'identifier les coefficients liés à leur niveau de maturité.

Par la suite, pour chaque contrôle, les coefficients liés à la typologie du contrôle et à la maturité du contrôle sont combinés pour obtenir les valeurs de P, D et C.

P correspond à la maturité des contrôles préventifs, il est obtenu en faisant le produit entre le coefficient affecté à la maturité du contrôle préventif et celui affecté au contrôle préventif.

D correspond à la maturité des contrôles detectifs, il est obtenu en faisant le produit entre le coefficient affecté à la maturité du contrôle detectif et celui affecté au contrôle detectif.

C correspond à la maturité des contrôles correctifs, il est obtenu en faisant le produit entre le coefficient affecté à la maturité du contrôle correctif et celui affecté au contrôle correctif.

Il faut noter qu'à ce niveau, nous avons rencontré d'énormes difficultés pour obtenir les données d'apprentissage relatives aux valeurs de P, D et C. La première difficulté réside dans le fait que le nouveau modèle que nous proposons possède des variables différentes de celles existantes au niveau des banques. Il a donc fallu assister aux séances d'évaluation des banques, expliquer notre modèle et l'appliquer séance tenante pour obtenir les données d'apprentissage qui permettront de tester ce second modèle. L'autre difficulté majeure est liée au fait que le nombre de risques sur lequel le nouveau modèle est testé dépend nécessairement du niveau de coopération de la banque mais aussi des criticités résiduelles qui ont variés d'un semestre à l'autre ; c'est d'ailleurs ce qui justifie la disparité entre le nombre de données d'apprentissage collectées d'une banque à l'autre pour tester ce modèle. L'ensemble des données collectées est indiqué ci-dessous :

Tableau 16:Données d'apprentissage collectées au niveau des 4 banques pour tester les modèles améliorés

DONNEES BANQUE 1						DONNEES BANQUE 2						DONNEES BANQUE 3						DONNEES BANQUE 4					
RISQUES	CR	CB	P	D	C	RISQUES	CR	CB	P	D	C	RISQUES	CR	CB	P	D	C	RISQUES	CR	CB	P	D	C
R1	5	8	1	1	1	R1	9	12	1	1	1	R1	11	14	1	1	1	R1	17	20	1	1	1
R2	6	10	2	1	1	R2	10	14	2	1	1	R2	12	16	2	1	1	R2	18	22	2	1	1
R3	7	12	2	2	1	R3	11	16	2	2	1	R3	13	18	2	2	1	R3	19	24	2	2	1
R4	8	14	3	2	1	R4	12	18	3	2	1	R4	14	20	3	2	1	R4	20	26	2	2	2
R5	9	12	1	1	1	R5	13	16	1	1	1	R5	15	18	1	1	1	R5	21	28	3	2	2
R6	9	16	4	2	1	R6	13	20	4	2	1	R6	15	22	4	2	1	R6	22	30	3	3	2
R7	10	14	2	1	1	R7	14	18	2	1	1	R7	16	20	2	1	1	R7	23	32	3	3	3
R8	10	18	5	2	1	R8	14	22	5	2	1	R8	16	24	5	2	1	R8	24	34	4	3	3
R9	11	16	2	2	1	R9	15	20	2	2	1	R9	17	22	2	2	1	R9	25	36	4	4	3
R10	11	20	5	3	1	R10	15	24	5	3	1	R10	17	26	5	3	1	R10	13	16	1	1	1
R11	12	18	2	2	2	R11	16	22	2	2	2	R11	18	24	2	2	2	R11	14	18	2	1	1
R12	12	22	5	3	2	R12	16	26	5	3	2	R12	18	28	5	3	2	R12	15	20	2	2	1
R13	13	20	3	2	2	R13	17	24	3	2	2	R13	19	26	3	2	2	R13	16	22	3	2	1
R14	13	24	5	4	2	R14	17	28	5	4	2	R14	19	30	5	4	2	R14	17	24	4	2	1
R15	14	22	3	3	2	R15	18	26	3	3	2	R15	20	28	3	3	2	R15	18	26	5	2	1
R16	14	26	5	4	3	R16	18	30	5	4	3	R16	20	32	5	4	3	R16	19	28	5	3	1
R17	15	24	3	3	3	R17	19	28	3	3	3	R17	21	30	3	3	3	R17	20	30	5	3	2
R18	15	28	4	4	5							R18	22	32	4	3	3						
R19	16	26	4	3	3							R19	23	34	4	4	3						
R20	16	30	4	5	5																		
R21	17	28	4	4	3																		
R22	17	32	5	5	5																		
R23	18	30	4	4	4																		
R24	19	32	5	4	4																		
R25	20	34	5	5	4																		
R26	21	36	5	5	5																		

Ces données d'apprentissage collectées ont été consignées en vue d'effectuer les différents tests de la seconde équation de régressions linéaires sur Eviews.

Par la suite, nous avons réalisé toute la panoplie de tests économétriques sur données collectées, les tests économétriques effectués pour éprouver les modèles améliorés sont : la méthode des moindres carrées ordinaires, le coefficient de détermination, les tests de significativité, les tests de normalité des erreurs, les tests d'hétéroscédasticité des erreurs, les tests de corrélation des erreurs, les tests de stabilité des paramètres. Pour finir, nous avons procédé à des tests de simulation, de prévision et de performance de cette seconde équation de régressions linéaires.

2. Méthode des moindre carrées

La méthode MCO (Moindres Carrées Ordinaires) utilisée est celle qui a été définie lors des tests réalisés avec la première équation de régressions linéaires.

La seconde équation de régressions linéaires correspondant aux modèles mathématiques améliorés est déclinée ci-après :

$$\log(CR_i) = alog(CB_i) - [blog(CP_i) + clog(CD_i) + dlog(CC_i)] + Cste \qquad \textbf{4.2.2}$$

L'exploitation d'Eviews avec les données d'apprentissage collectées au niveau des banques sur 4 trimestres d'affilés donne les résultats suivants.

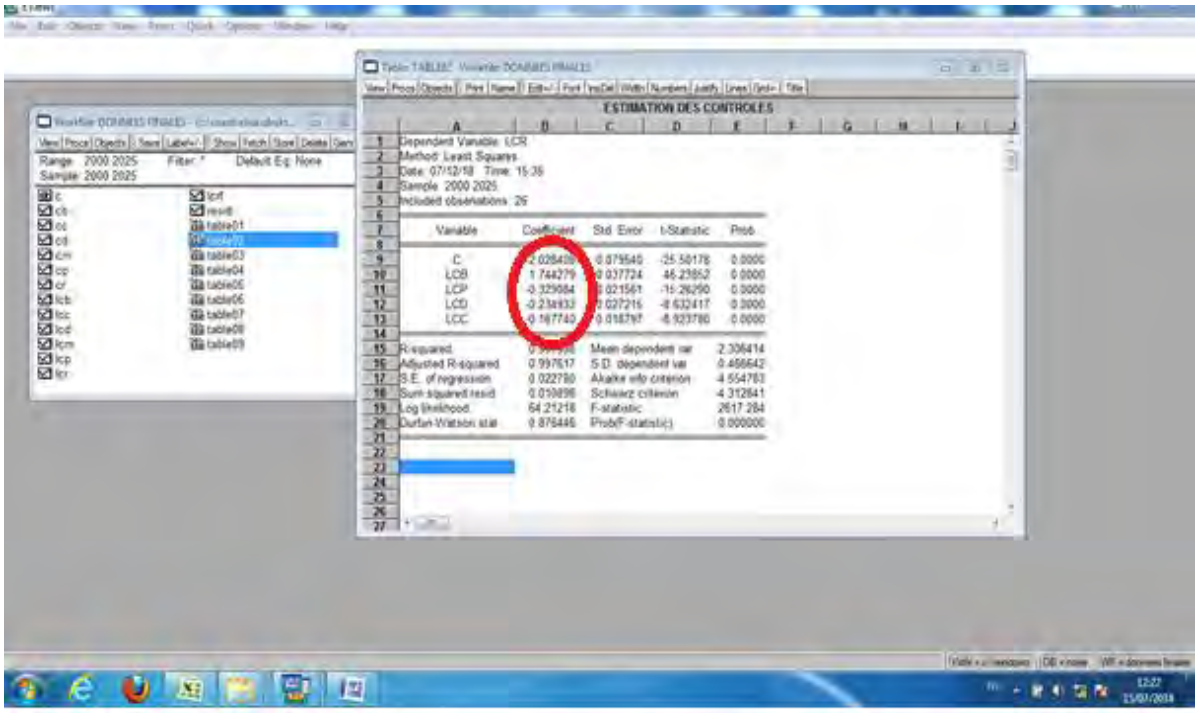


Figure 32:Coefficients affectés aux variables de l'équation 2 et relatifs à la banque 1

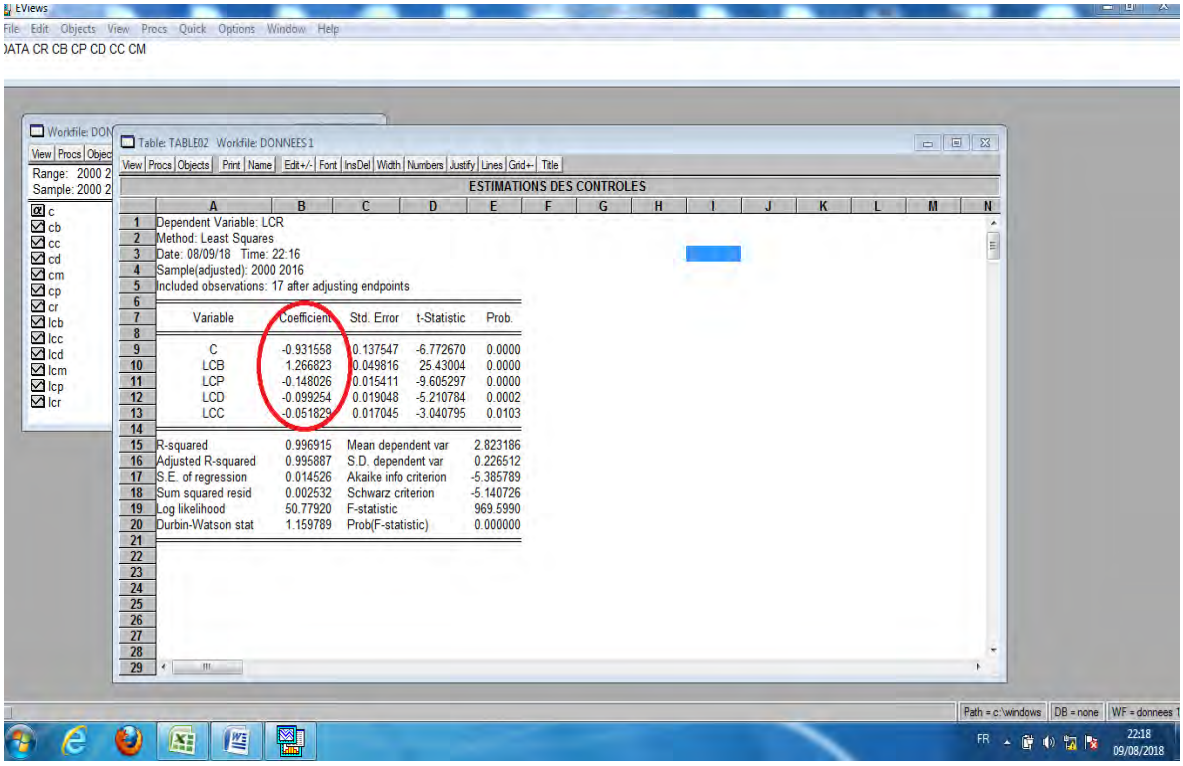


Figure 33:Coefficients affectés aux variables de l'équation 2 et relatifs à la banque 2

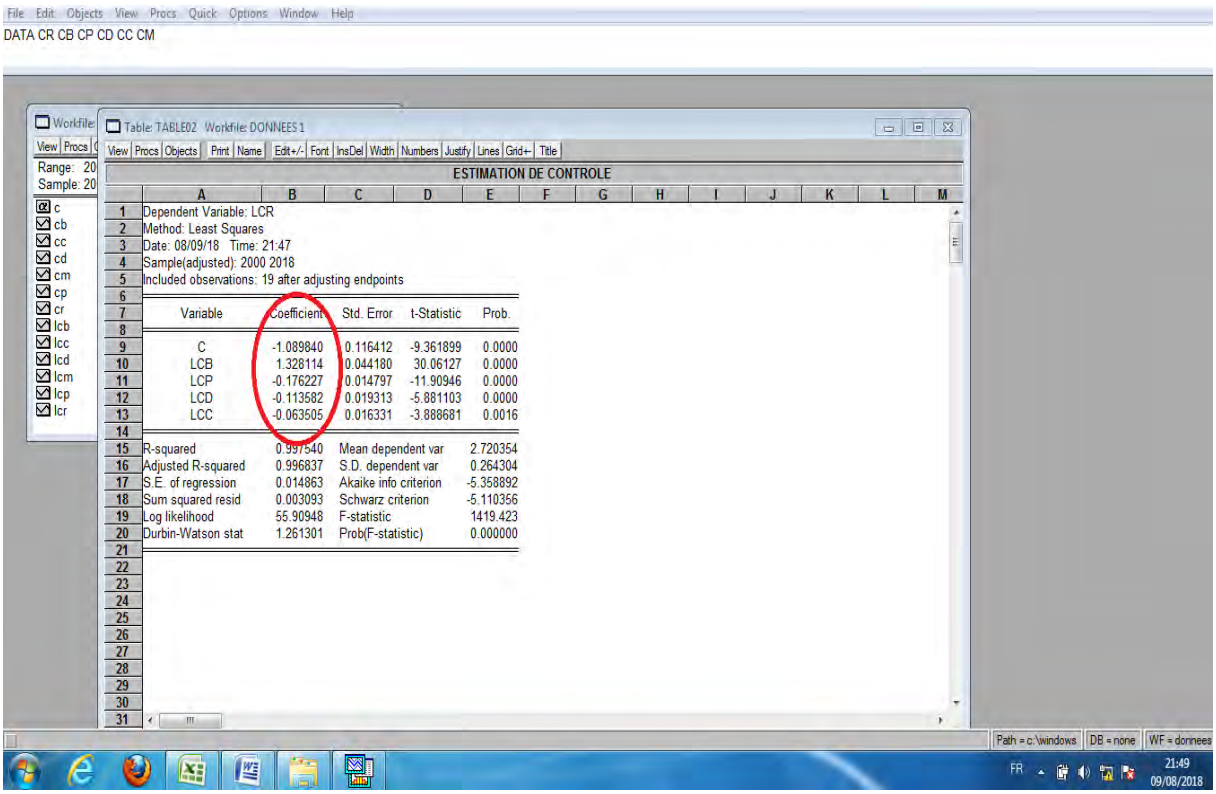


Figure 34:Coefficients affectés aux variables de l'équation 2 et relatifs à la banque 3

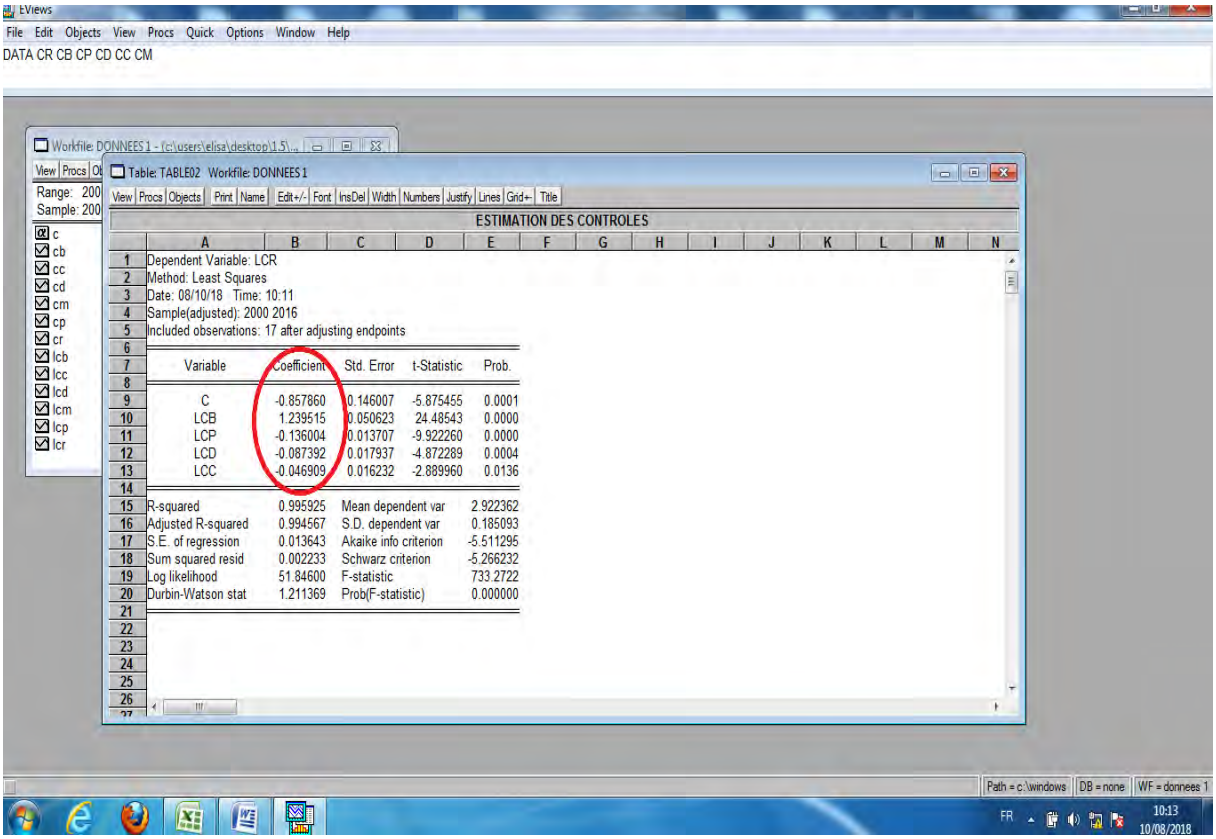


Figure 35:Coefficients affectés aux variables de l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

A la lecture de ces résultats obtenus avec Eviews, il découle que

a. Le coefficient $\boldsymbol{a}$ représentant le coefficient affecté à la variable criticité brute des risques possède une valeur positive pour les 4 semestres.

b. Le coefficient $\boldsymbol{b}$ représentant le coefficient affecté à la variable maturité des contrôles préventifs possède une valeur négative pour les 4 semestres.

c. Le coefficient $\boldsymbol{c}$ représente le coefficient affecté à la variable maturité des contrôles detectifs possède une valeur négative pour les 4 semestres.

d. Le coefficient *d* représente affecté à la variable maturité des contrôles correctifs possède une valeur négative pour les 4 semestres.

e. La valeur $Cste$ représentant la constante de l'équation est négative, elle correspond aux variables non prises en compte par les variables explicatives de l'équation de régression linéaire à savoir la criticité brute des risques et la maturité des contrôles préventifs, detectifs et correctifs

f. Les semestres 2 et 4 ont des variables et constantes de même ordre

- **Interprétation économétriques**

a. Si la criticité brute augmente alors la criticité résiduelle augmente
b. Si la maturité des contrôles préventifs augmente alors la criticité résiduelle diminue
c. Si la maturité des contrôles detectifs augmente alors la criticité résiduelle diminue
d. Si la maturité des contrôles correctifs augmente alors la criticité résiduelle diminue
e. La négativité de la constante montre qu'elle est susceptible de contribuer à la diminution de la criticité résiduelle des risques
f. Les variables et constantes sont de même ordre pour les deux banques ayant fournis des séries de données de même taille

- **Interprétation gestion des risques**

En guise de rappel, les 7 principes qui nous ont permis de définir ce modèle sont relatés ci-après **[24]:**

Principe 1
Un risque peut avoir un ou plusieurs contrôles. En effet les contrôles sont définis et mis en œuvre dans le but de mitiger les risques. Ainsi, selon la nature du risque, un ou plusieurs contrôles y afférents peuvent être définis.

Principe 2
Les contrôles sont mis en œuvre pour maitriser les risques identifiés et évalués. En effet suite à l'identification des risques, une première évaluation basée sur les échelles de probabilité de survenance brute et de gravité potentielle brute permet d'assigner à chaque risque, une valeur de criticité brute correspondant au niveau de criticité qui ne tient pas compte des contrôles effectivement mis en œuvre. Plus la criticité brute est élevée, plus le risque est critique.

Principe 3
Un contrôle possède une seule valeur maturité et un type. En effet la maturité correspond au niveau de mise en œuvre du contrôle, elle peut être inexistante, informelle, systématique, intégré ou optimisé. Quant au type de contrôle, elle fait référence à la nature proprement dite du contrôle qui peut être soit préventif, détectif ou correctif.

Principe 4
Seuls, les contrôles matures peuvent réduire la probabilité brute et/ou la gravité brute des risques. Pour qu'un contrôle puisse considérablement réduire ou mitiger un risque, il faut qu'elle soit mature, cela signifie que sa maturité a un niveau opérationnel au minimum.

Principe 5
Les contrôles préventifs contribuent à faire baisser la probabilité de survenance brute du risque(Pbrute). Par définition, ces contrôles sont définis pour agir en amont et empêcher que le risque se produise.

Principe 6
Les contrôles détectifs contribuent à faire baisser la gravité potentielle brute du risque (G_{brute}). En effet, l'utilité de ce type de contrôle repose sur la communication du risque avéré.

Principe 7
Les contrôles correctifs contribuent à faire baisser la gravité potentielle brute du risque (G_{brute}). En effet, ce sont des contrôles qui sont définis dans le but de prendre en charge le risque détecté.
Nous pouvons en conclure que les résultats obtenus concordent avec ces principes, car il apparait que :

a. La criticité résiduelle diminue avec la maturité des contrôles, ce qui est en accord avec le principe 4.

b. Les résultats montre que le risque possède plusieurs contrôles de types différents à savoir $\boldsymbol{CP_i}$: maturité des contrôles préventifs, $\boldsymbol{CD_i}$: Maturité des contrôles detectifs et $\boldsymbol{CC_i}$: Maturité des contrôles correctifs, ce qui est en accord avec les principes **1 et 3.**
c. D'après les valeurs des coefficients **b, c et d**, les contrôles préventifs, detectifs et correctifs ont un impact sur la probabilité de survenance brute et/ou la gravité potentielle brute des risques, ce qui est en accord avec les principes **5, 6 et 7**.
d. La Criticité résiduelle des risques $\boldsymbol{CR_i}$ est obtenue en faisant la soustraction entre la criticité brute des risques $\boldsymbol{CB_i}$ et les maturités des différents types de contrôles ($\boldsymbol{CP_i}$: Maturité des contrôles préventifs, $\boldsymbol{CD_i}$: Maturité des contrôles detectifs et $\boldsymbol{CC_i}$: Maturité des contrôles correctifs). Ce qui est en accord avec les principes **2, 5, 6 et 7**.
e. La négativité de la constante de l'équation montre qu'elle est susceptible de diminuer la criticité résiduelle des risques, ce qui est en accord avec le principe **2**

3. Coefficient de détermination

Le coefficient de détermination R est le même que celui utilisé précédemment. Pour effectuer ces tests, nous avons utilisé la même approche en appliquant la seconde équation de régressions linéaires aux données d'apprentissage collectées. La seconde équation de régressions correspondant aux modèles mathématiques améliorés est déclinée ci-après :

$$\log(CR_i) = alog(CB_i) - [blog(CP_i) + clog(CD_i) + dlog(CC_i)] + Cste \qquad \textbf{4.2.2}$$

L'exploitation d'Eviews avec les données d'apprentissage collectées sur les 4 semestres donne les résultats suivants:

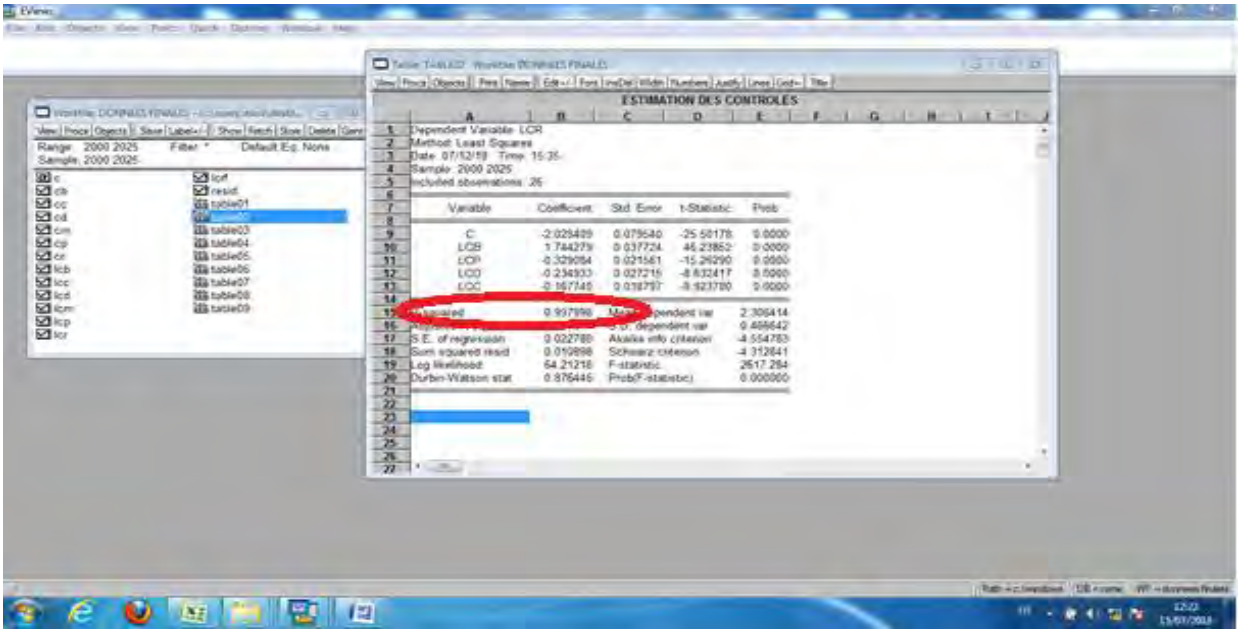


Figure 36:Coefficient de détermination obtenu avec l'équation 2 et relatif à la banque 1

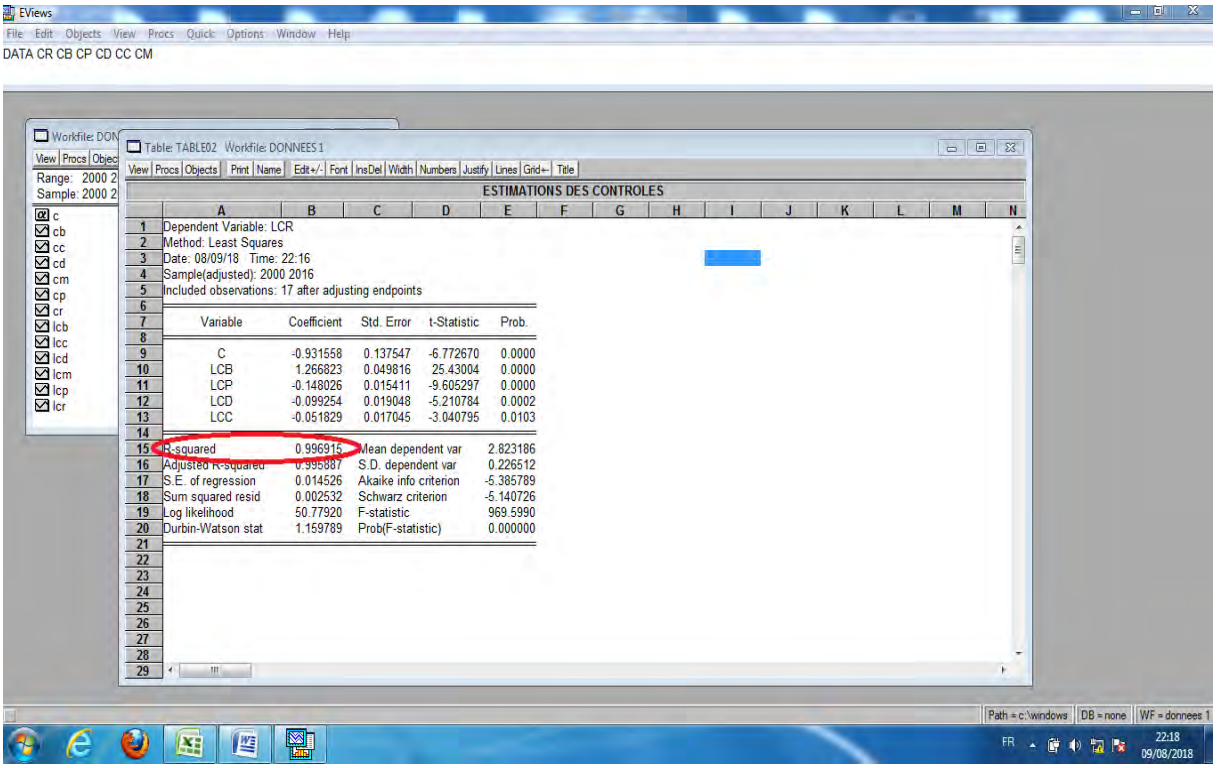


Figure 37:Coefficient de détermination obtenu avec l'équation 2 et relatif à la banque 2

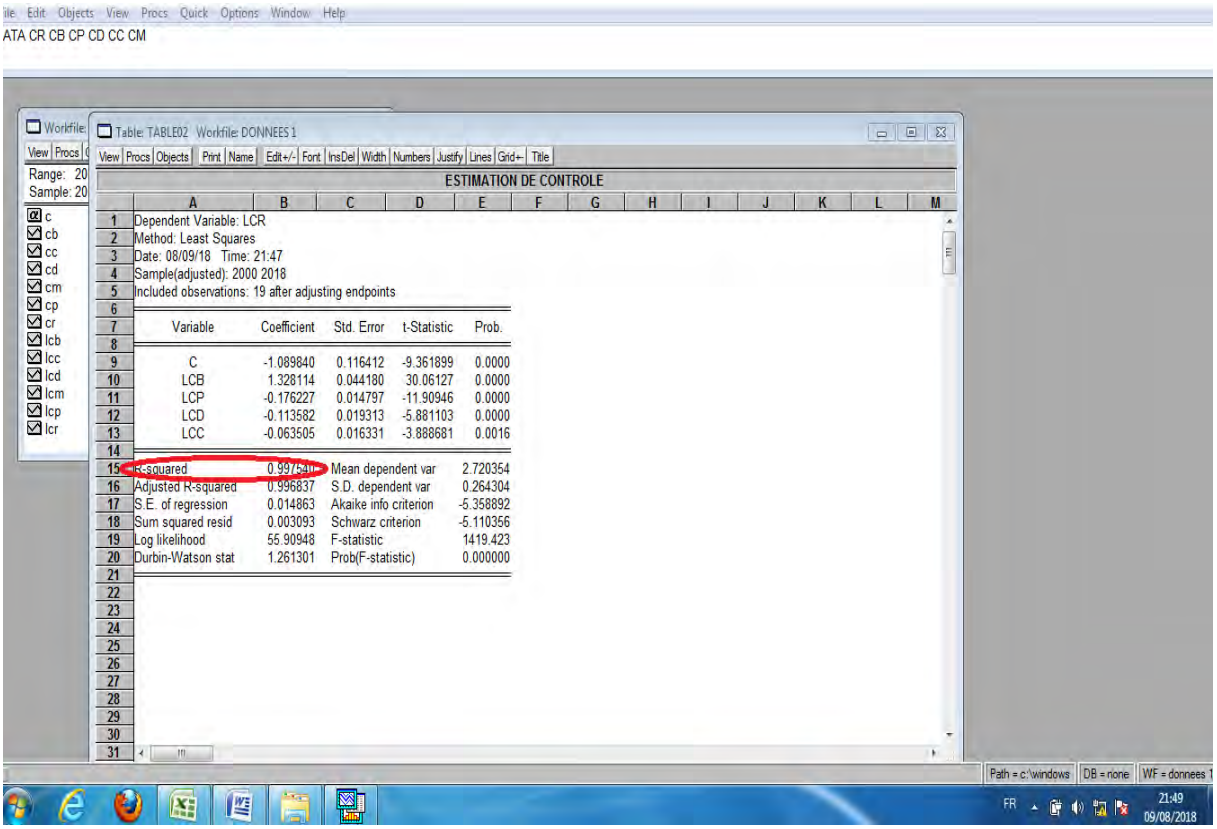


Figure 38:Coefficient de détermination obtenu avec l'équation 2 et relatif à la banque 3

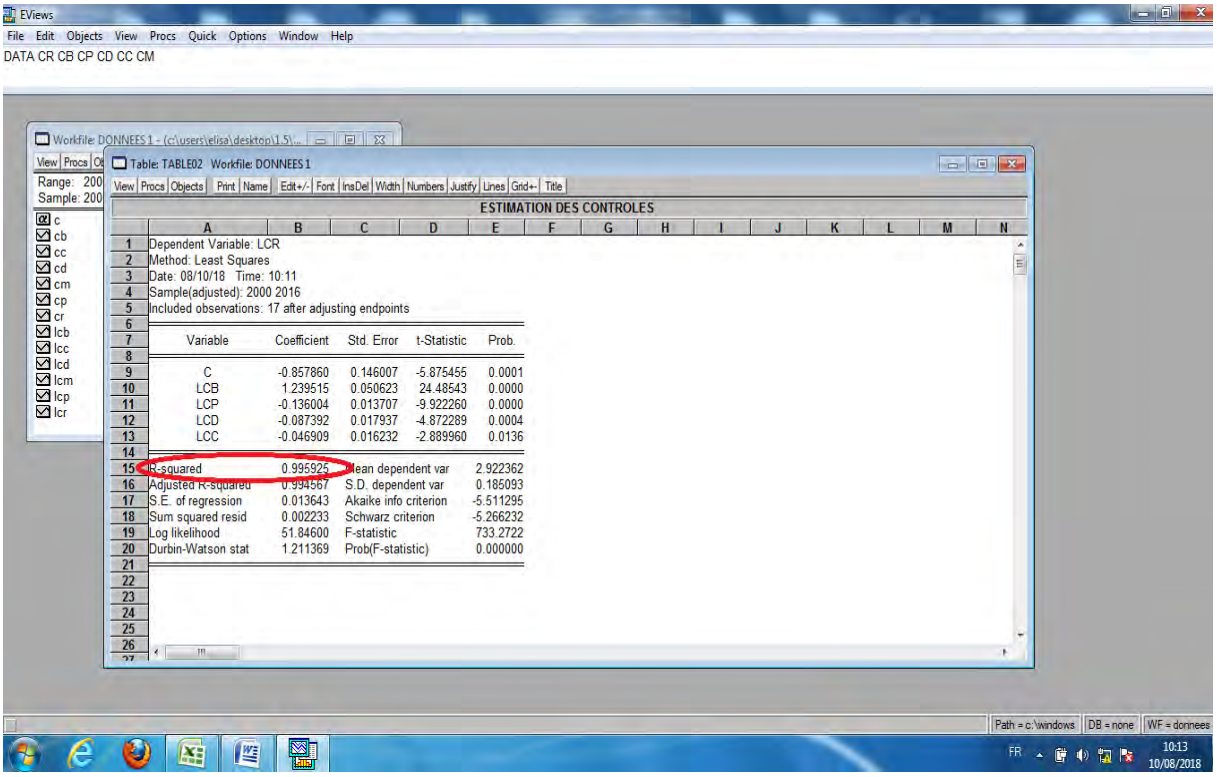


Figure 39:Coefficient de détermination obtenu avec l'équation 2 et relatif à la banque 4

Interprétation des résultats

On obtient un coefficient de détermination égal à 0.99 donc $R^2 = 0{,}99$ sur les 4 semestres d'affilés. Cela traduit que 99% des criticités résiduelles sont expliquées par les criticités brutes, la maturité des contrôles préventifs, la maturité des contrôles detectifs et la maturité des contrôles correctifs. Ce qui signifie que la criticité brute, la maturité des contrôles préventifs, la maturité des contrôles detectifs et la maturité des contrôles correctifs sont des variables pertinentes permettant d'obtenir la criticité résiduelles des risques. De plus, on constate un coefficient élevé qui dépasse largement le seuil de 50% permettant de statuer si le coefficient de corrélation est correct ou pas. Ce résultat est donc satisfaisant.

4. **Tests de significativités**

Les hypothèses H_0 et H_1 sont également celles utilisées précédemment.

Pour réaliser ces tests, nous avons aussi utilisé la même approche en appliquant la seconde équation de régressions linéaires aux données d'apprentissage collectées. Ainsi, nous effectuerons les deux types de tests de significativité suivants :

- **Test de Student** permettant de tester la significativité des variables explicatives, il permet de s'assurer que les variables explicatives ont une influence significative sur la variable à expliquer par l'équation.

- **Test de Fisher** permettant de tester la significativité globale de l'équation, il prend en compte la significativité de toutes les variables explicatives et permet de s'assurer que l'équation est globalement bonne.

A titre de rappel, la seconde équation de régressions linéaires est déclinée ci-après :

$$\log(CR_i) = alog(CB_i) - [blog(CP_i) + clog(CD_i) + dlog(CC_i)] + Cste \qquad \textbf{4.2.2}$$

- **Test de Student**

L'exploitation d'Eviews avec les données de 4 semestres d'affilés pour le test de Student donne les résultats suivants.

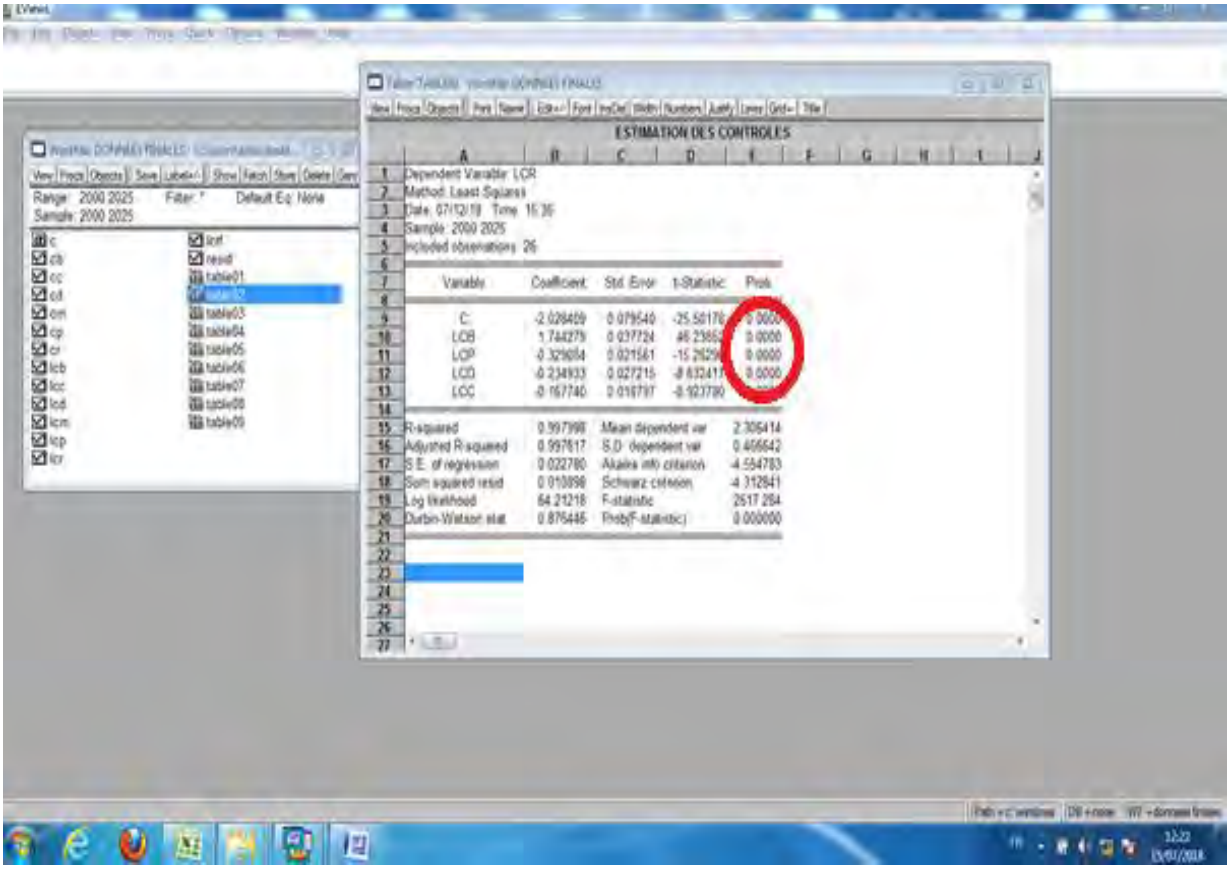


Figure 40: Test de Student: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

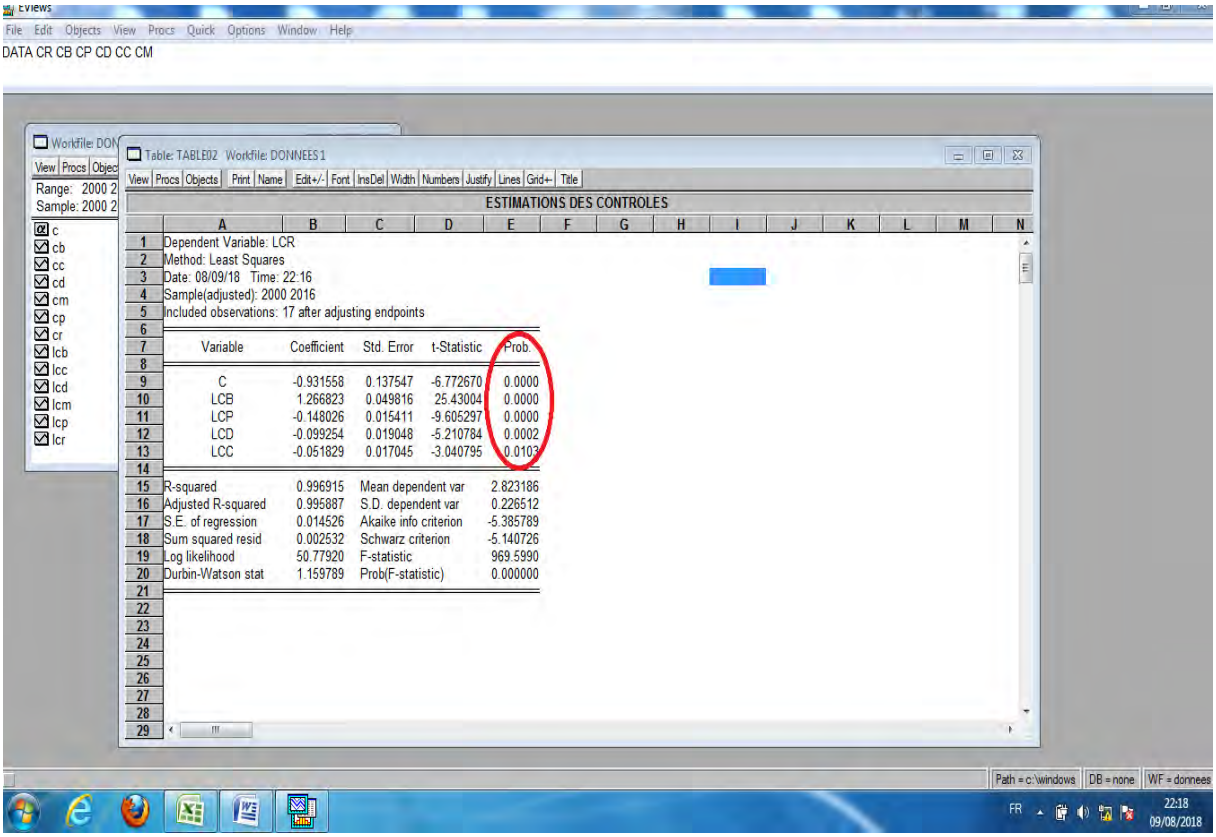


Figure 41:Test de Student: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

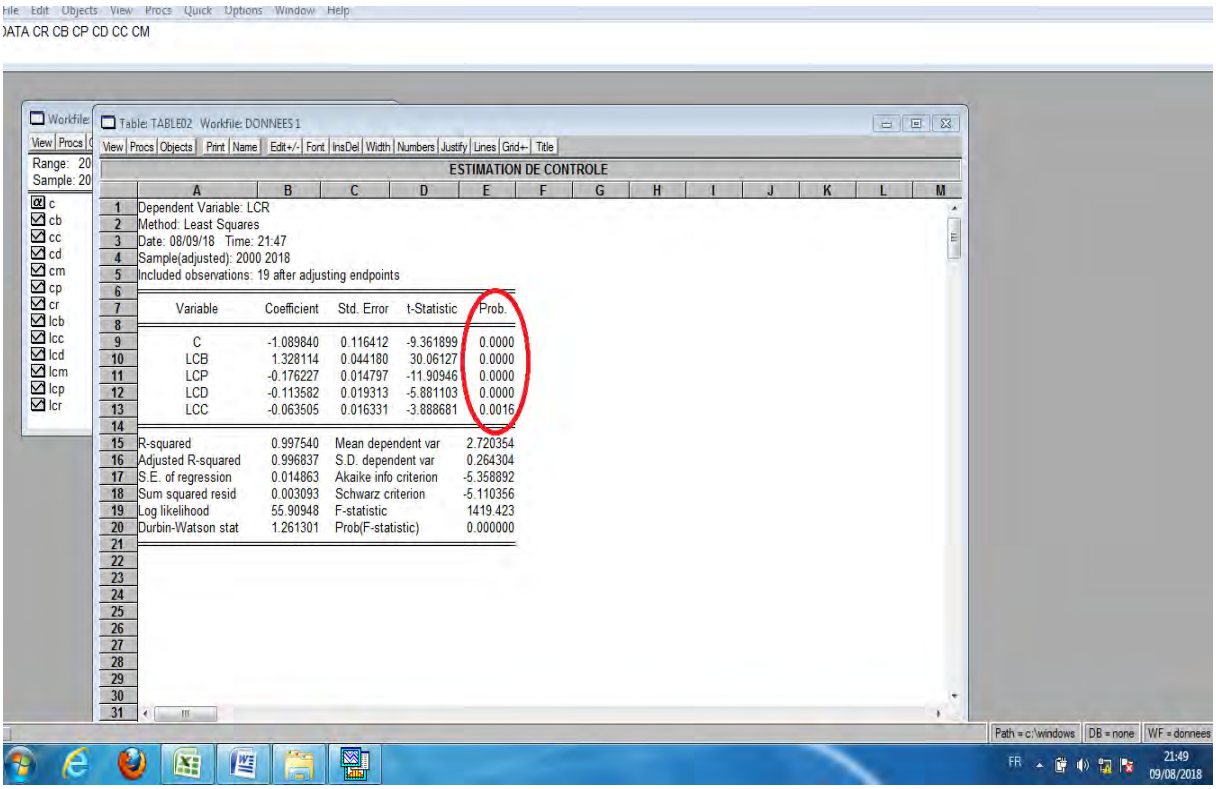


Figure 42:Test de Student: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

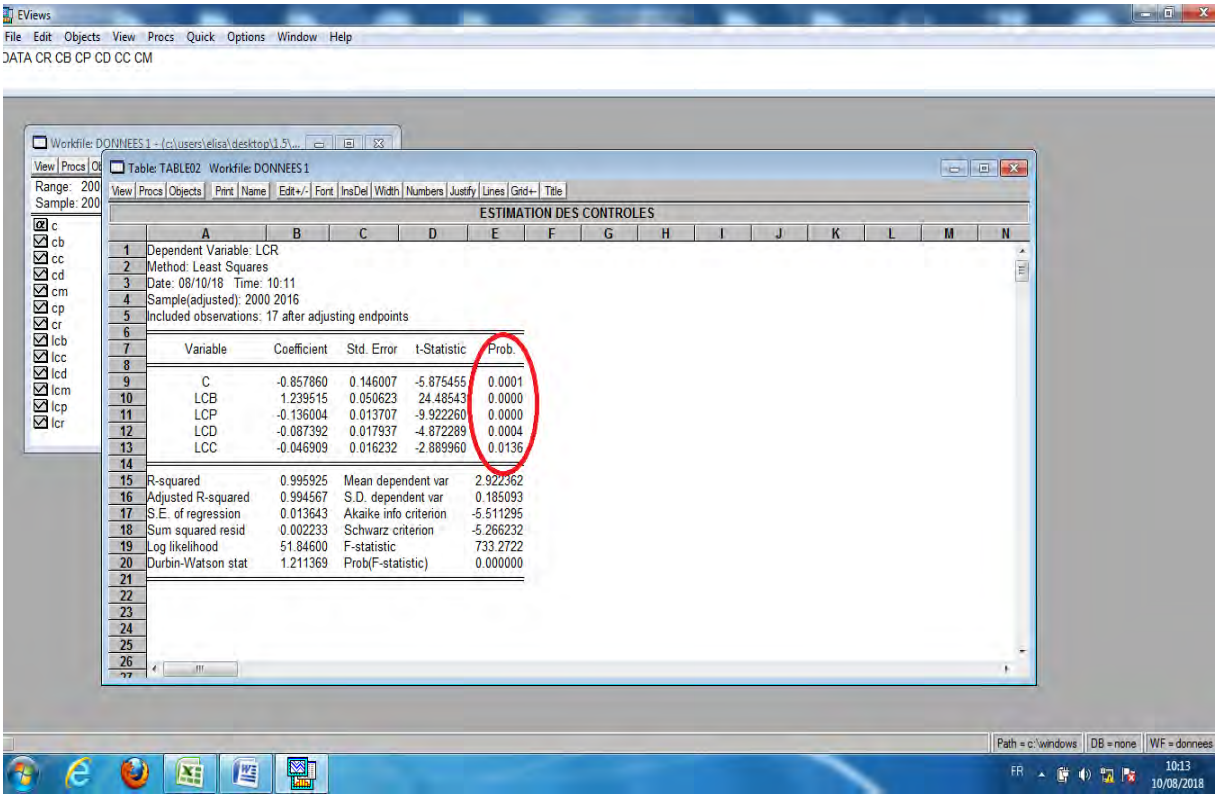


Figure 43:Test de Student: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

D'après les résultats fournis par Eviews, la valeur de prob=00000 sur 4 semestres d'affilés.

A l'issue de ce test, les résultats montrent que toutes les probabilités des variables explicatives sont largement inférieures à 5%, nous pouvons en conclure que les variables explicatives concernées sont significatives. Elles ont donc une influence significative sur la variable à expliquer à savoir la criticité résiduelle des risques.

- **Test de Fisher**

L'exploitation d'Eviews donne les résultats suivants sur les 4 trimestres d'affilés pour le test de Fisher.

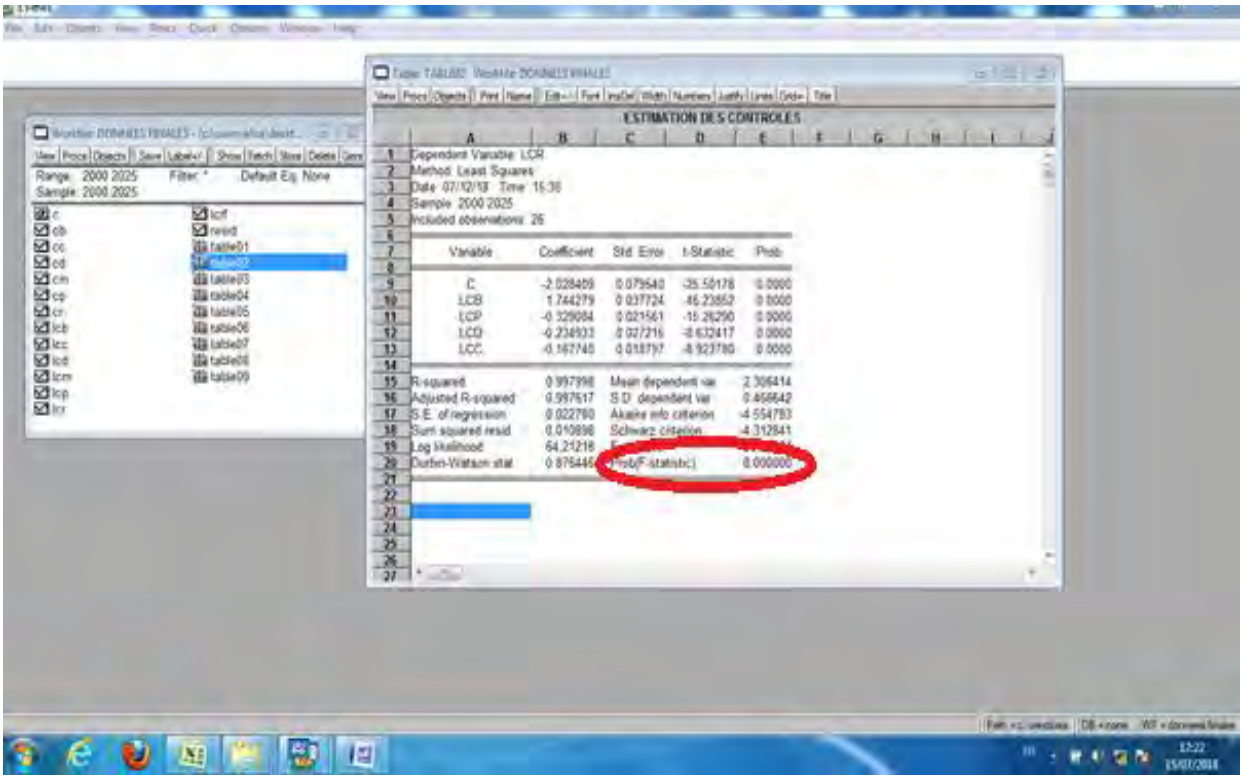


Figure 44:Test de Fisher: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

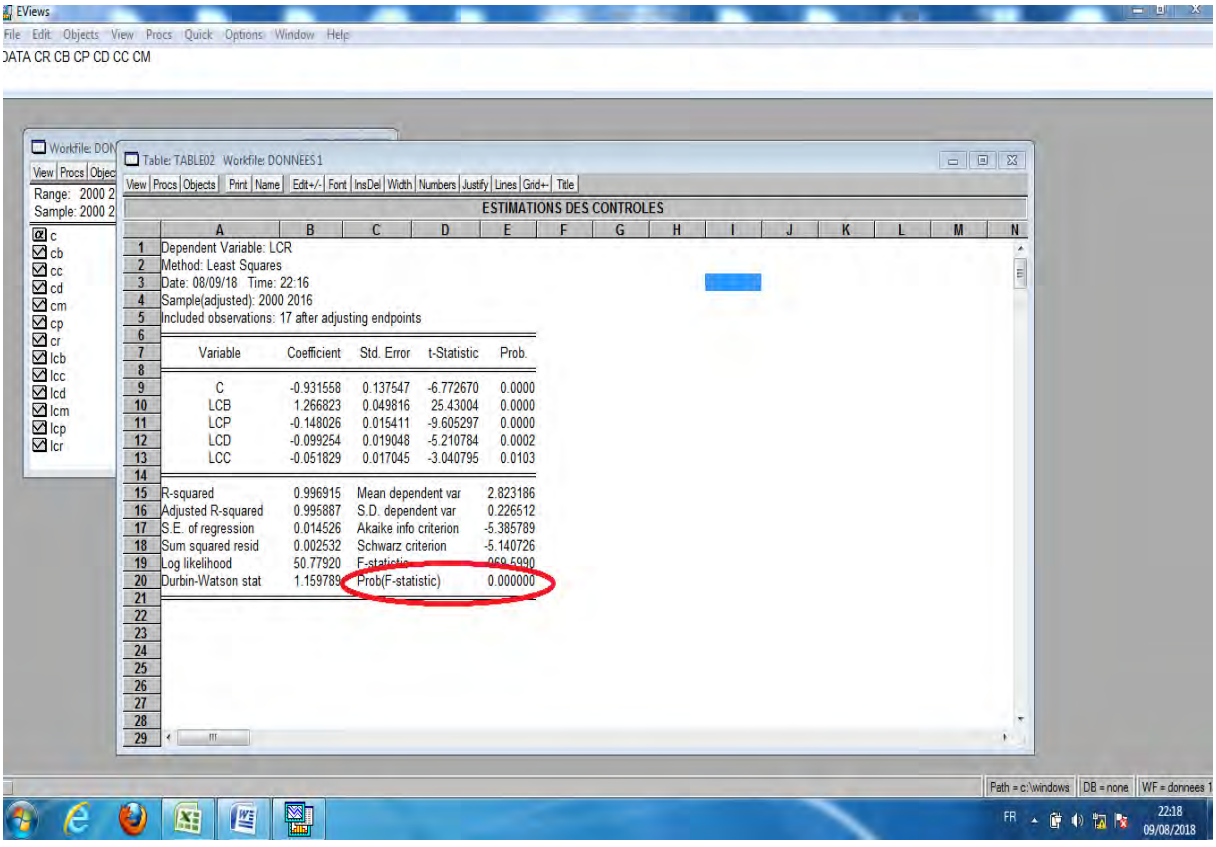


Figure 45:Test de Fisher: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

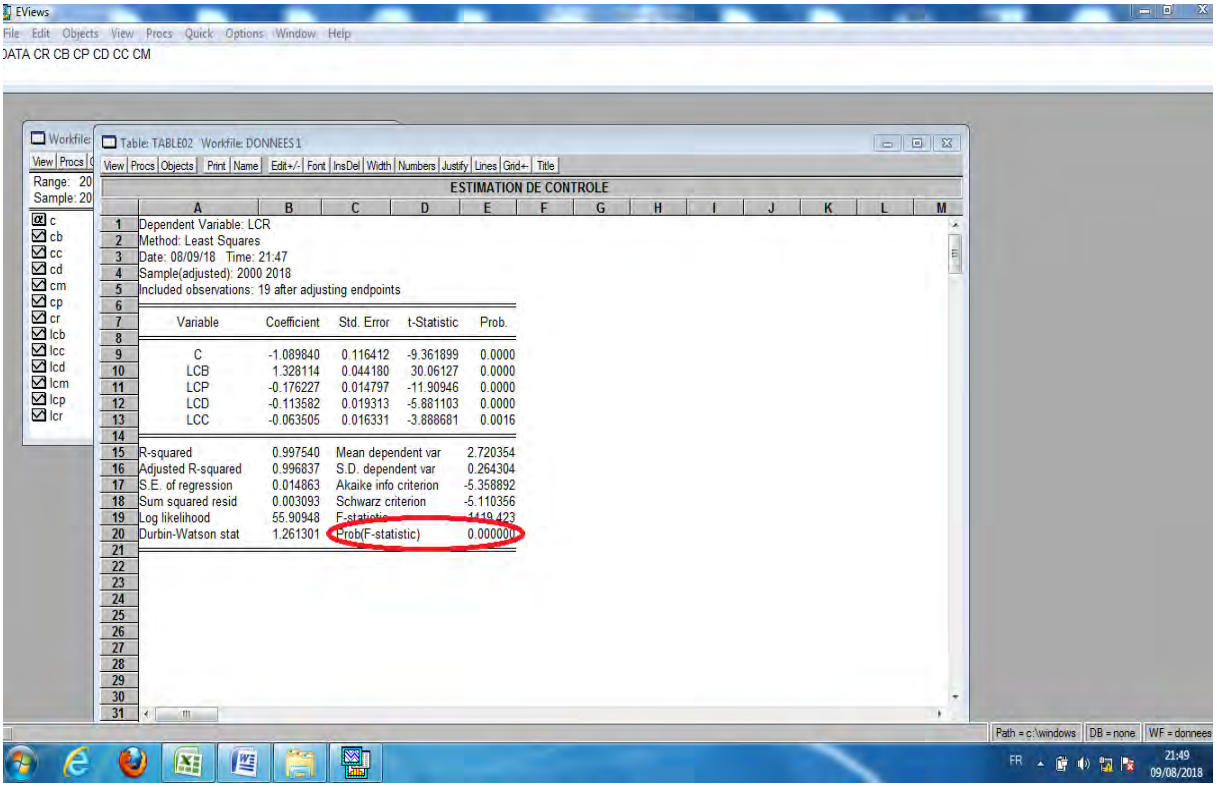


Figure 46:Test de Fisher: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

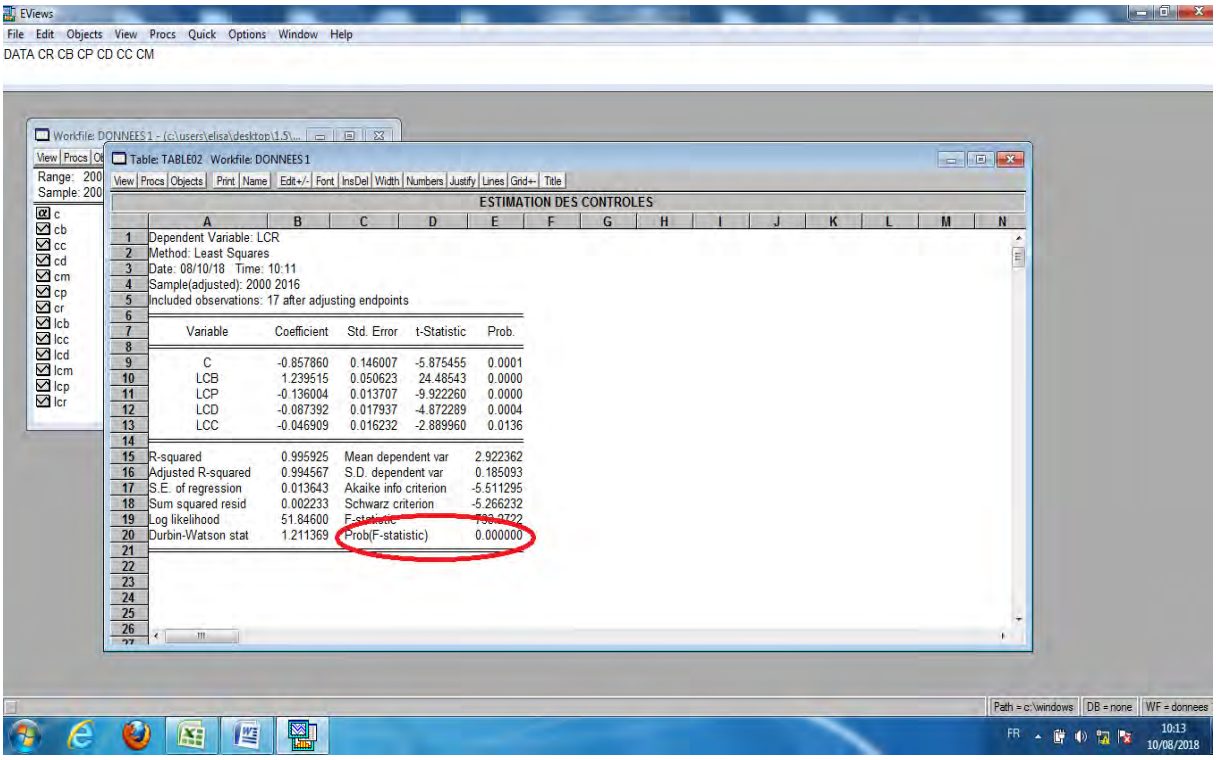


Figure 47:Test de Fisher: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

D'après les résultats fournis par Eviews, la valeur de prob F-Statistic=00000 sur 4 semestres d'affilés. Nous pouvons conclure que l'équation est globalement significative car la valeur du prob (F-Statistic) est largement inférieure à 5%.

5. Test de normalité de Jarque Bera

Les tests de normalités des erreurs permettent de vérifier si les variables de l'équation suivent une loi normale selon les seuils utilisés précédemment.

Les résultats du test de normalité des erreurs sur les 4 semestres d'affilés sont indiqués dans le tableau ci-dessous.

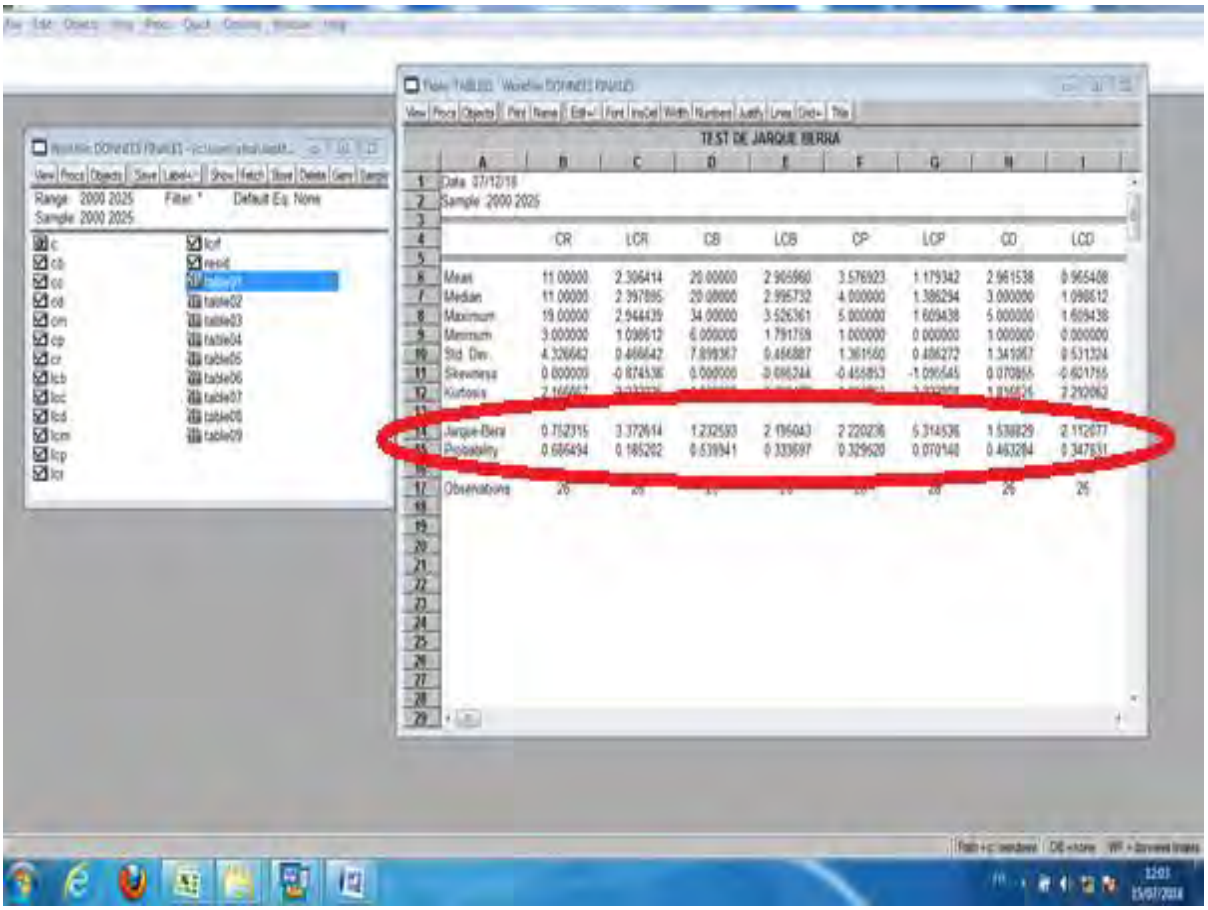


Figure 48:Test de Jarque Bera: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

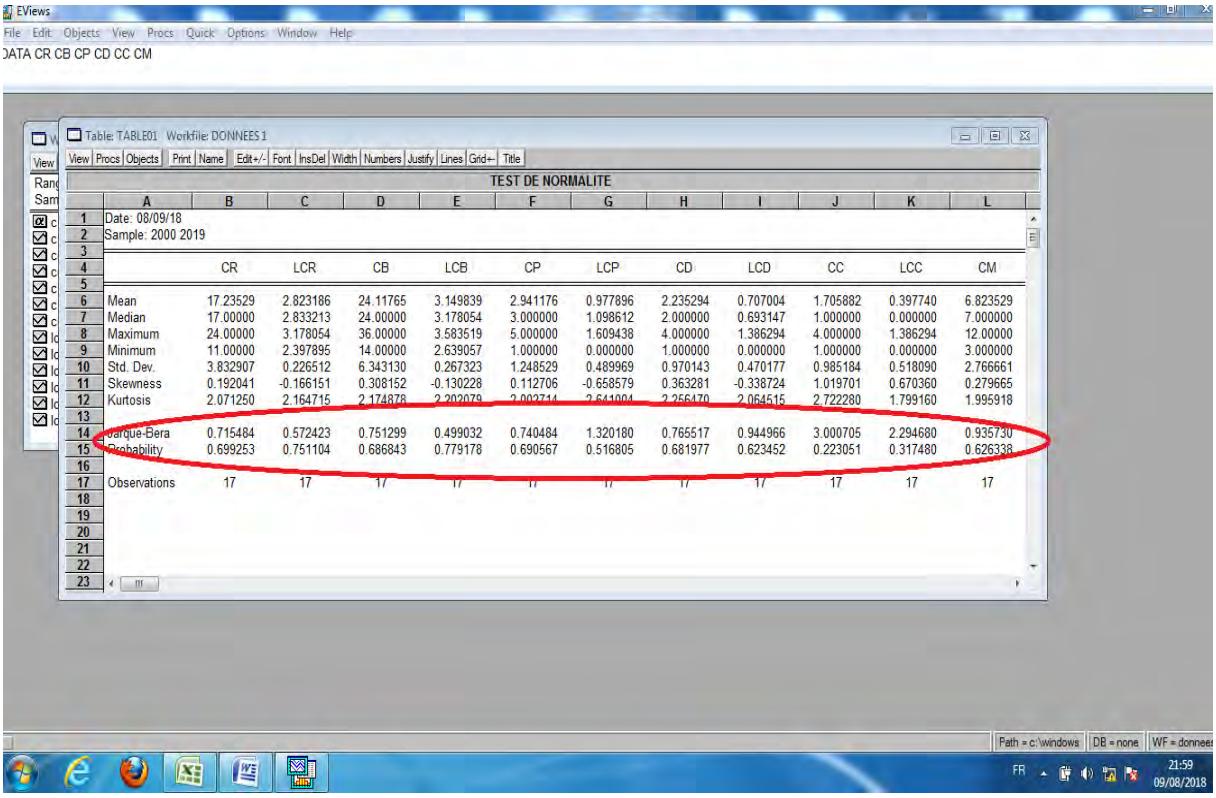


Figure 49:Test de Jarque Bera: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

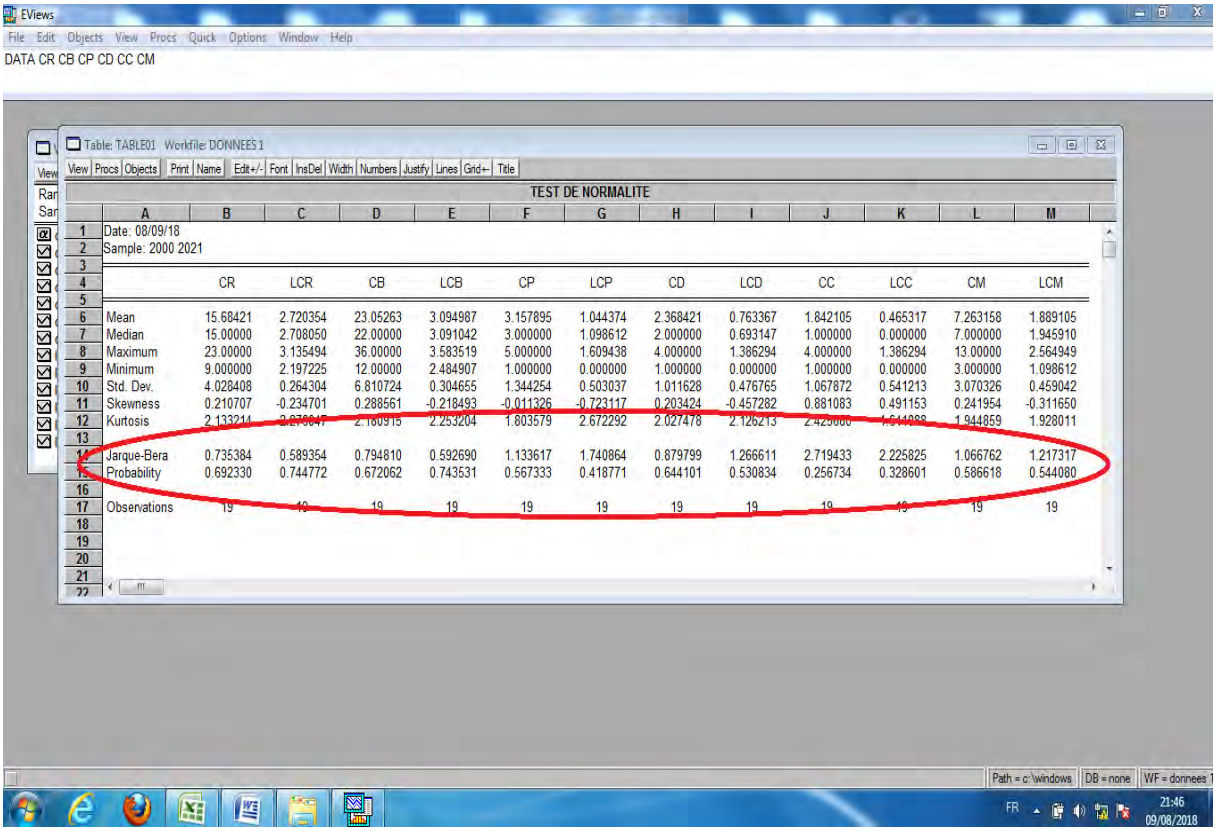


Figure 50:Test de Jarque Bera: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

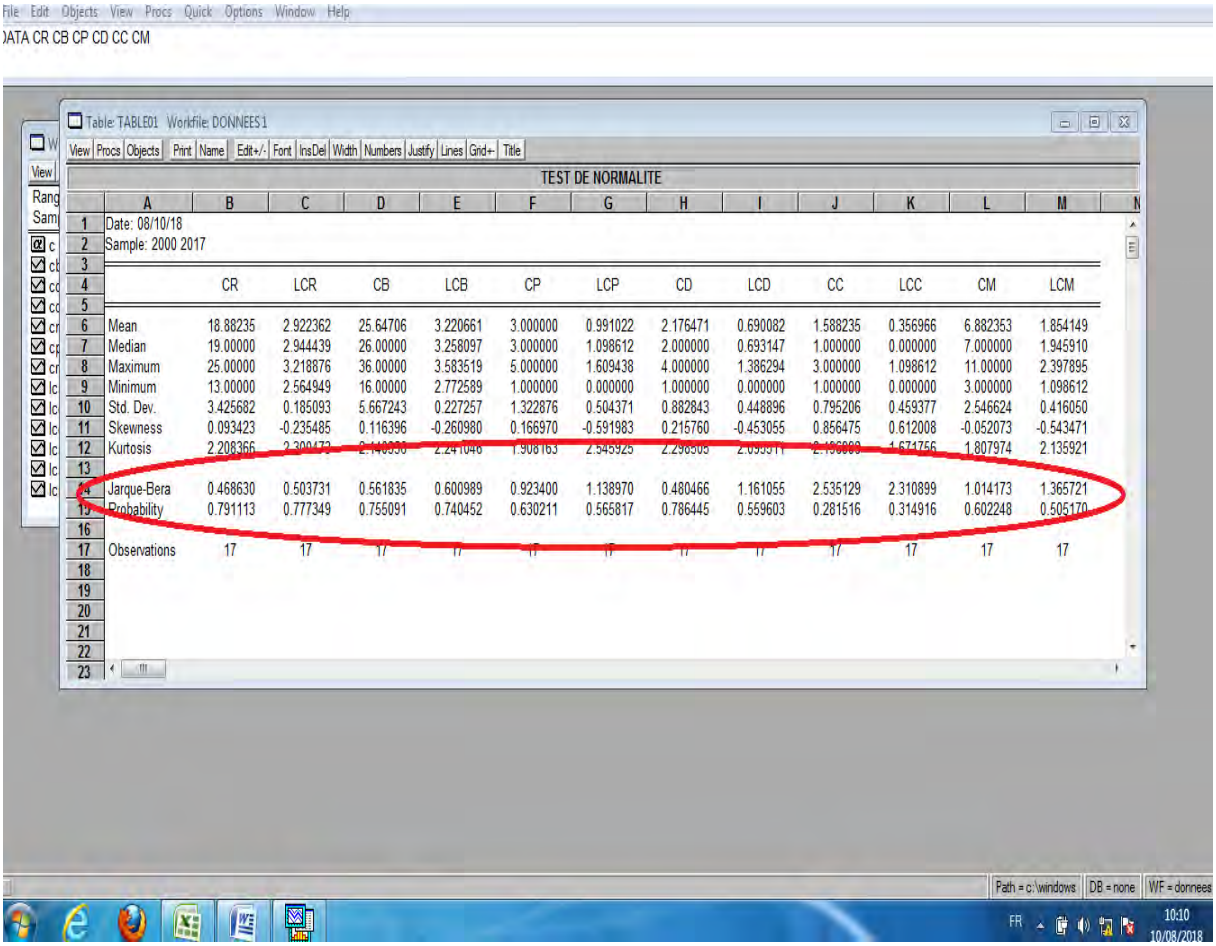


Figure 51:Test de Jarque Bera: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

On remarque que toutes les variables ont une probabilité supérieure à 5% sur 4 semestres d'affilés, par conséquent ils suivent une loi normale. C'est la raison pour laquelle nous avons pu réaliser les autres tests économétriques recommandés.

6. Tests d'hétéroscédasticité des erreurs

Les tests d'hétéroscédasticité des erreurs permettent d'apprécier le comportement de l'équation par rapport aux erreurs. Il s'agit essentiellement du test de White et du test d'Arch.

- **Test de White**

Le test de White permet de savoir si le modèle est homoscédastique ou hétéroscédastique en tenant compte de la régression du carré du résidu. Il existe deux hypothèses :

$$H_0 : modéle\ homoscédastique$$

$$H_1 : modéle\ hétéroscédastique$$

- Le modèle est homoscédastique si prob est supérieur à 5%
- Le modèle est hétéroscédastique si prob est inférieur ou égal à 5%

Les résultats obtenus avec Eviews sur les 4 semestres testés sont indiqués ci-dessous :

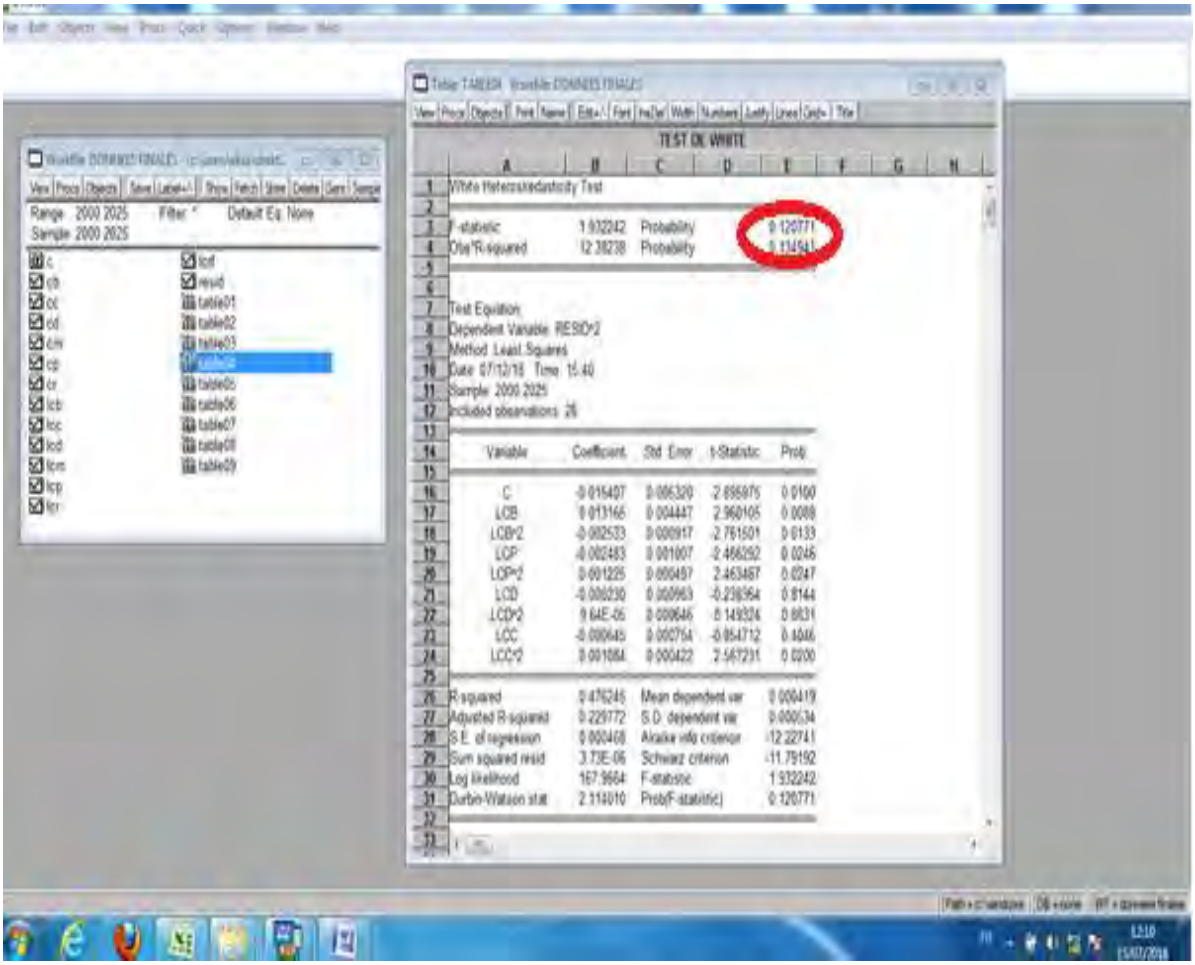


Figure 52:Test de White: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

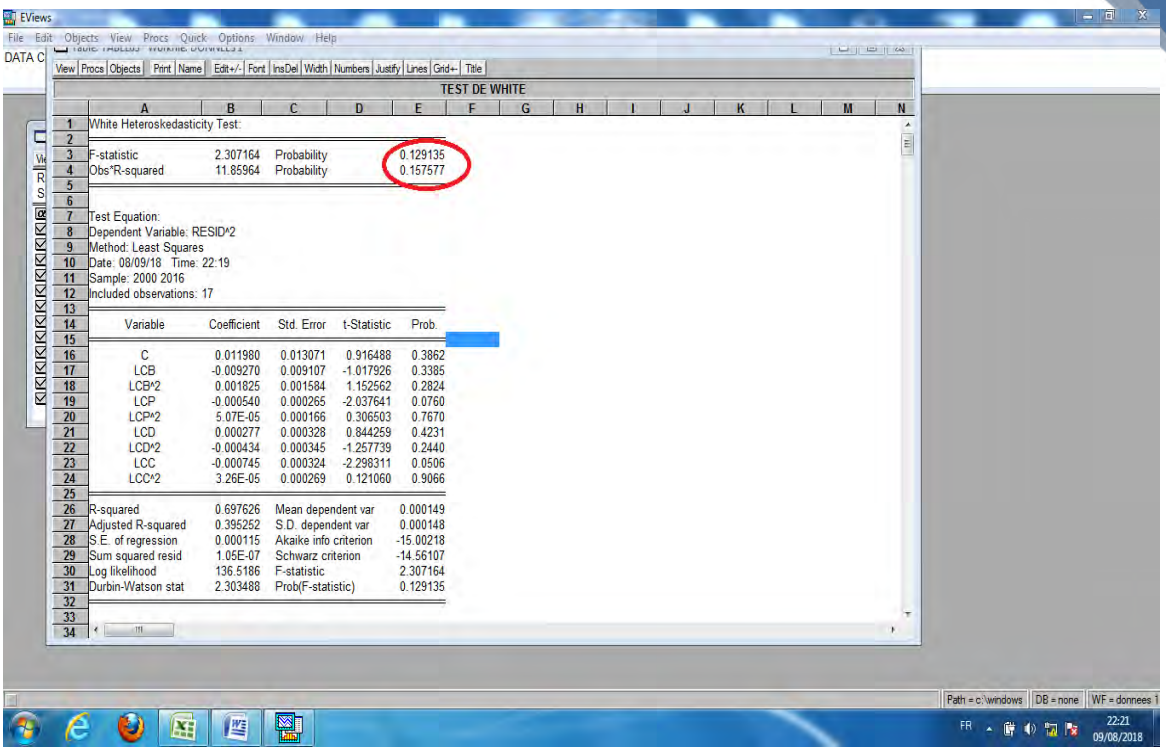


Figure 53:Test de White: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

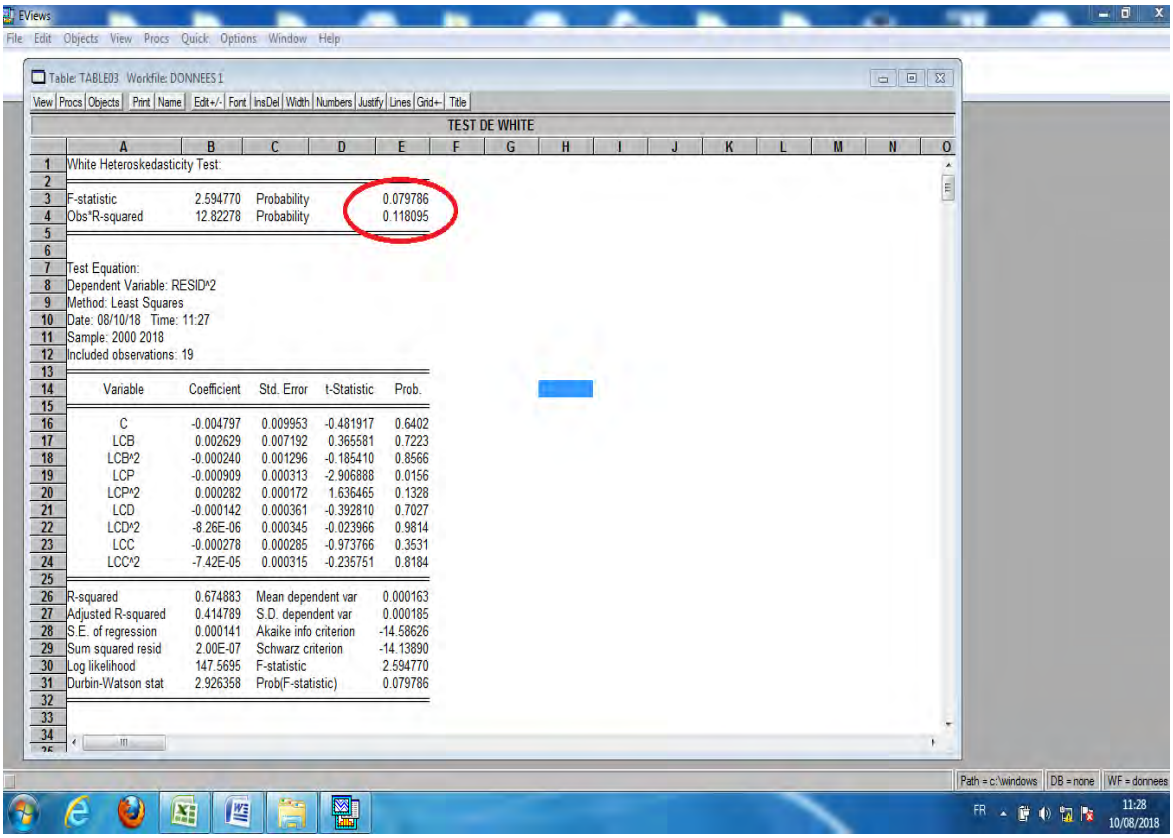
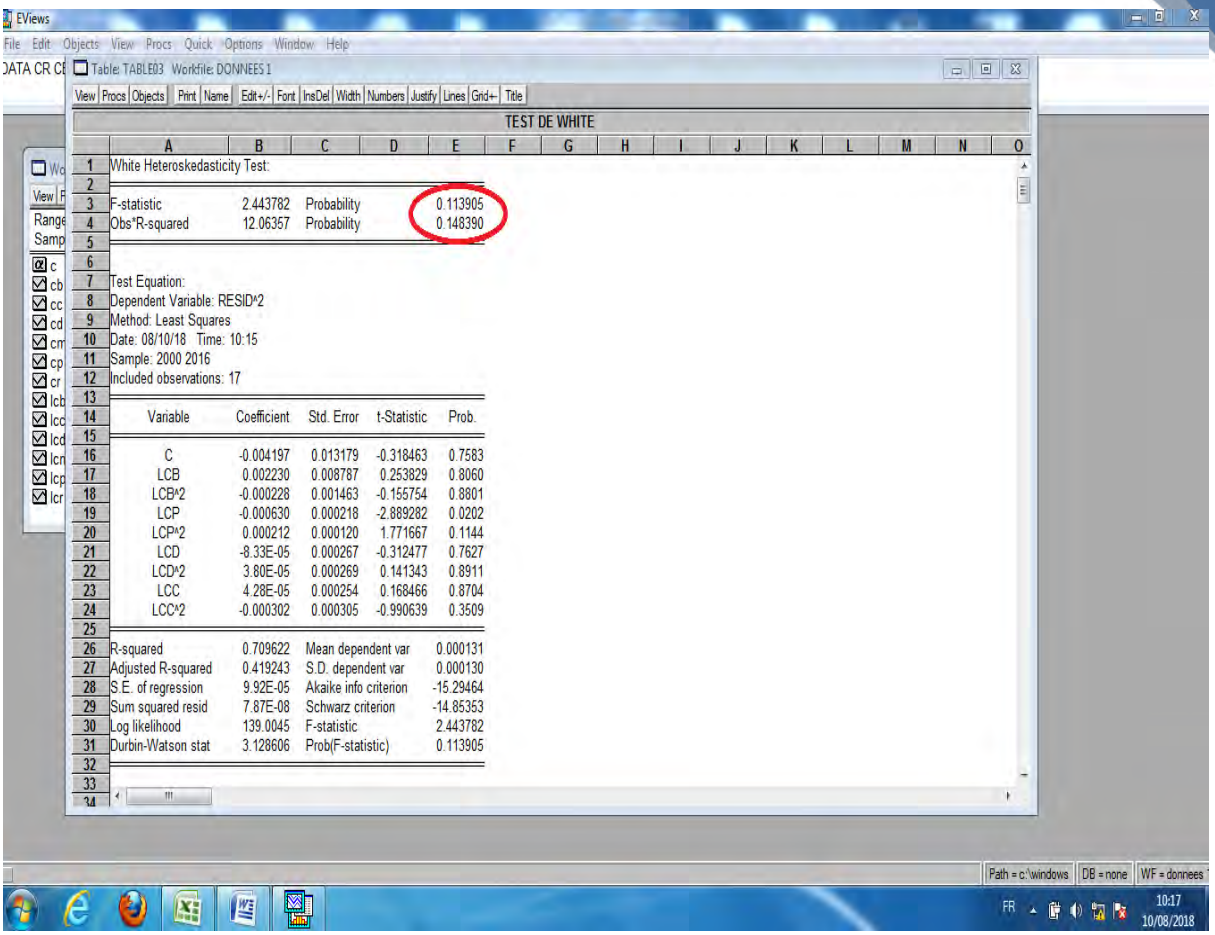


Figure 54:Test de White: Résultats obtenus avec l'équation 2 et relatifs à la banque 3



TEST DE WHITE

White Heteroskedasticity Test:

F-statistic	2.443782	Probability	0.113905
Obs*R-squared	12.06357	Probability	0.148390

Test Equation:
Dependent Variable: RESID^2
Method: Least Squares
Date: 08/10/18 Time: 10:15
Sample: 2000 2016
Included observations: 17

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.004197	0.013179	-0.318463	0.7583
LCB	0.002230	0.008787	0.253829	0.8060
LCB^2	-0.000228	0.001463	-0.155754	0.8801
LCP	-0.000630	0.000218	-2.889282	0.0202
LCP^2	0.000212	0.000120	1.771667	0.1144
LCD	-8.33E-05	0.000267	-0.312477	0.7627
LCD^2	3.80E-05	0.000269	0.141343	0.8911
LCC	4.28E-05	0.000254	0.168466	0.8704
LCC^2	-0.000302	0.000305	-0.990639	0.3509

R-squared	0.709622	Mean dependent var	0.000131
Adjusted R-squared	0.419243	S.D. dependent var	0.000130
S.E. of regression	9.92E-05	Akaike info criterion	-15.29464
Sum squared resid	7.87E-08	Schwarz criterion	-14.85353
Log likelihood	139.0045	F-statistic	2.443782
Durbin-Watson stat	3.128606	Prob(F-statistic)	0.113905

Figure 55:Test de White: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

Les valeurs de prob sont supérieures à 5% sur les données d'apprentissage couvrant 4 semestres. Par conséquent, on accepte l'hypothèse d'homoscédasticité des erreurs. Cela signifie que les estimations obtenues par la méthode des moindres carrées sont optimales. Ce qui confirme l'estimation des paramètres (a, b, c et d) de l'équation obtenus avec les MCO.

- **Régression du carré du résidu sur LCB et LCB^2**

Suite à la réalisation de ce test, les résultats obtenus sur les données de 4 semestres sont indiqués ci-dessous :

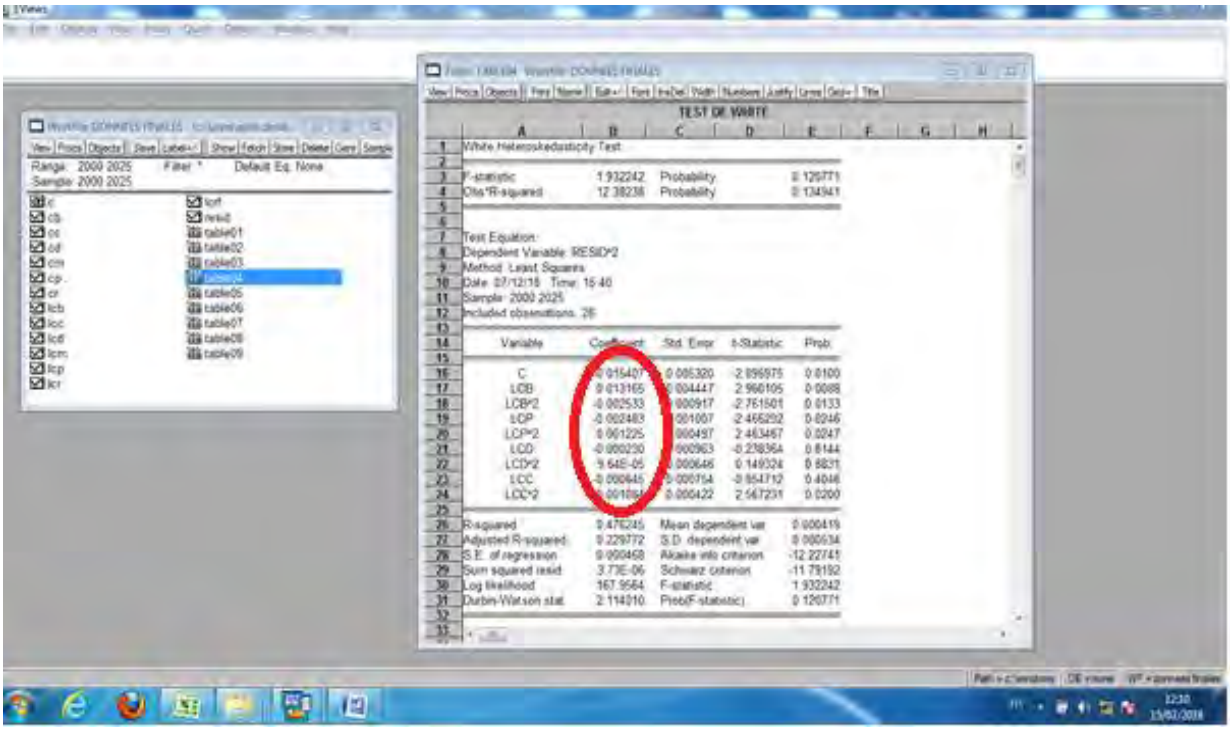


Figure 56:Régression du carré du résidu: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

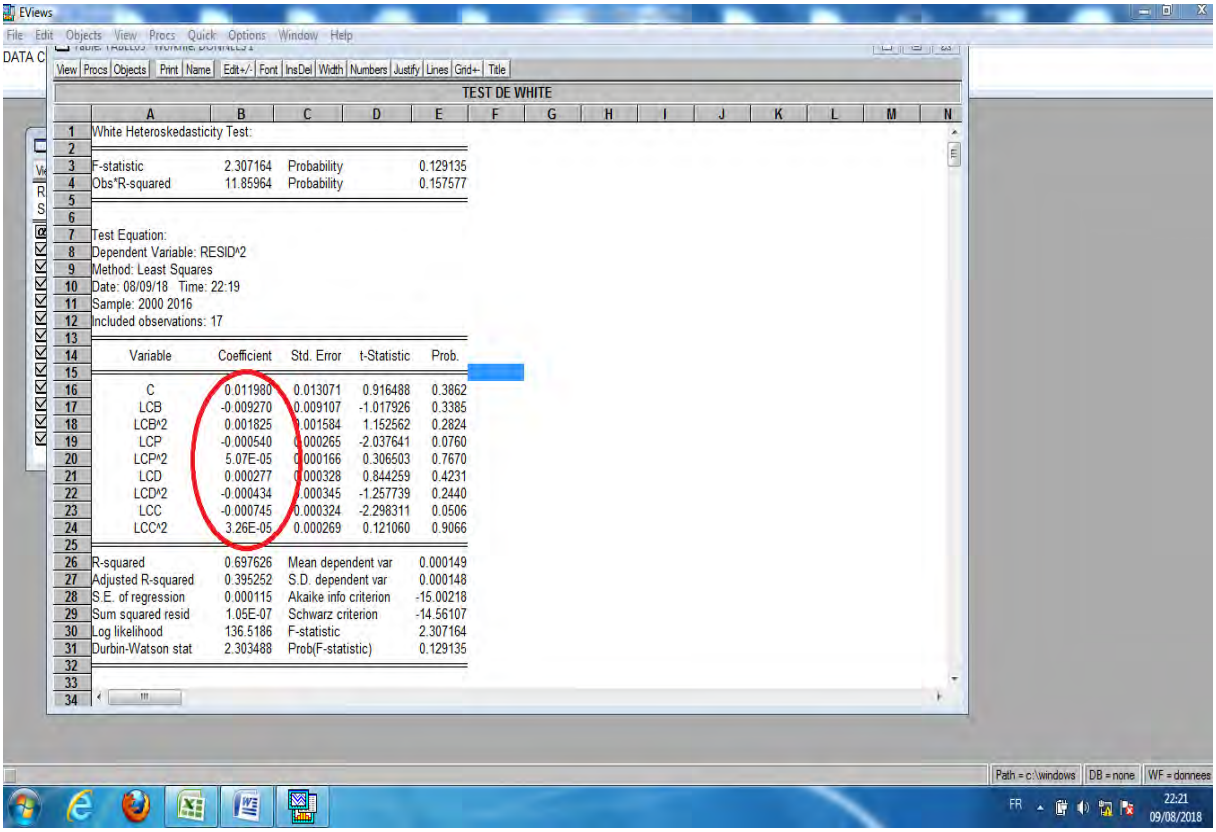


Figure 57:Régression du carré du résidu: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

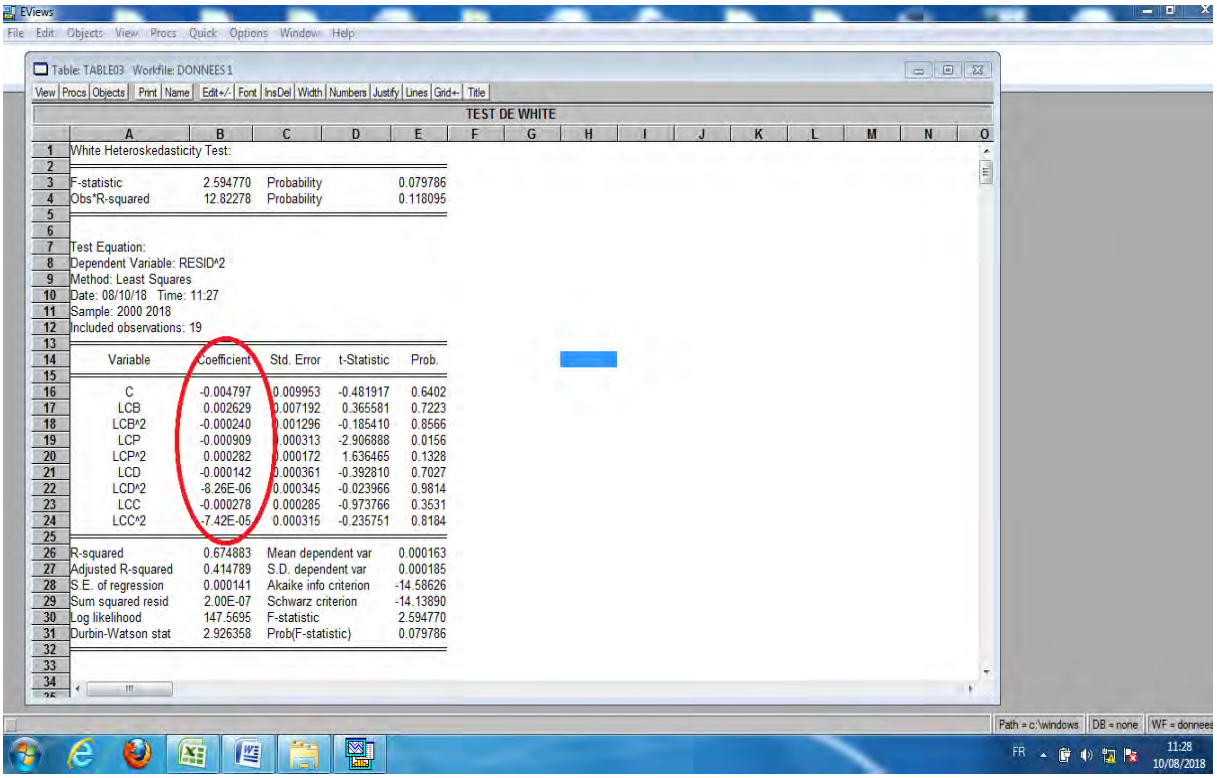


Figure 58:Régression du carré du résidu: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

.

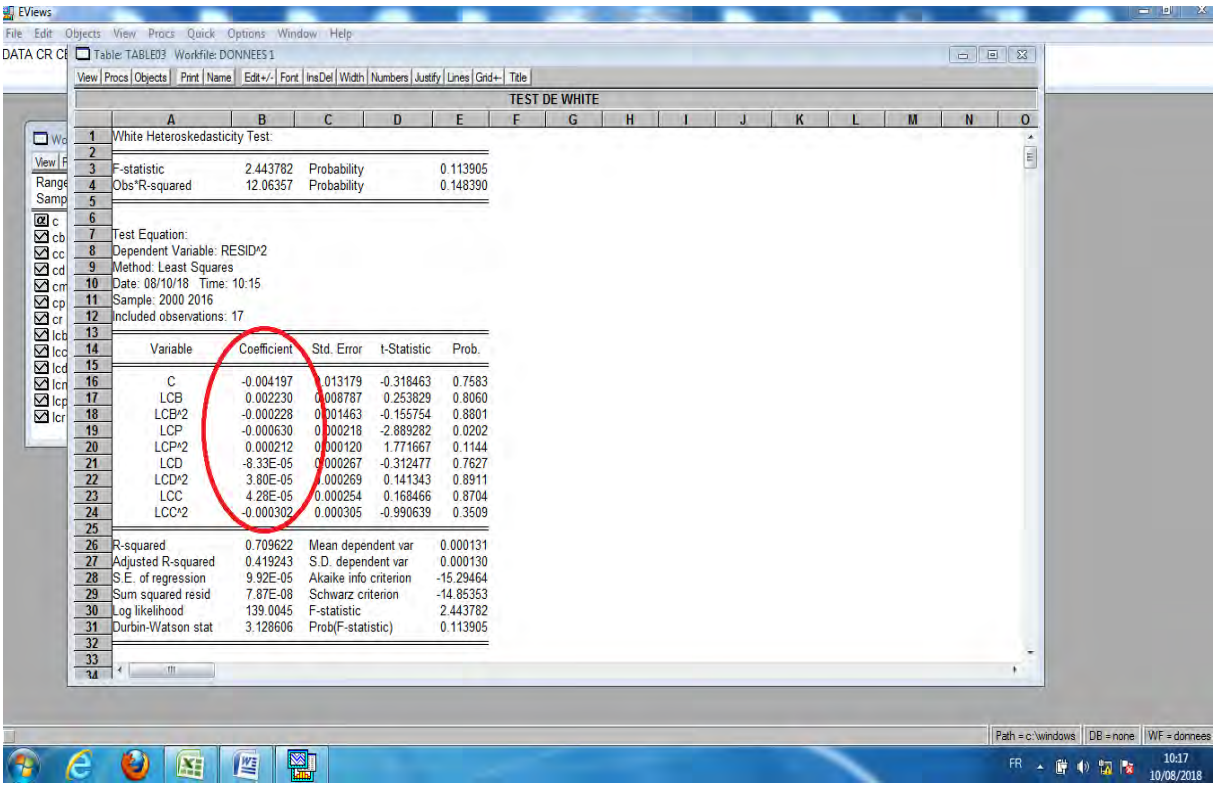


Figure 59:Régression du carré du résidu: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

Tous les coefficients du modèle sont significativement égaux à zéro sur les 4 semestres d'affilés, donc l'hypothèse d'homoscédasticité des erreurs est acceptée.

7. Test d'ARCH

Le test d'Arch permet de savoir si les erreurs de l'équation sont homocédastiques ou hétéroscédastiques en tenant compte de la régression autorégressive. Les deux hypothèses sont les suivants :

$$H_0 : erreur\ homocédastiques$$

$$H_1 : erreurs\ \ hétéroscédastique$$

- Les erreurs sont homocédastiques si prob supérieur à 5%
- Les erreurs sont hétéroscédastiques si prob est inférieur ou égales à 5%

Les résultats obtenus avec Eviews sont indiqués ci-après :

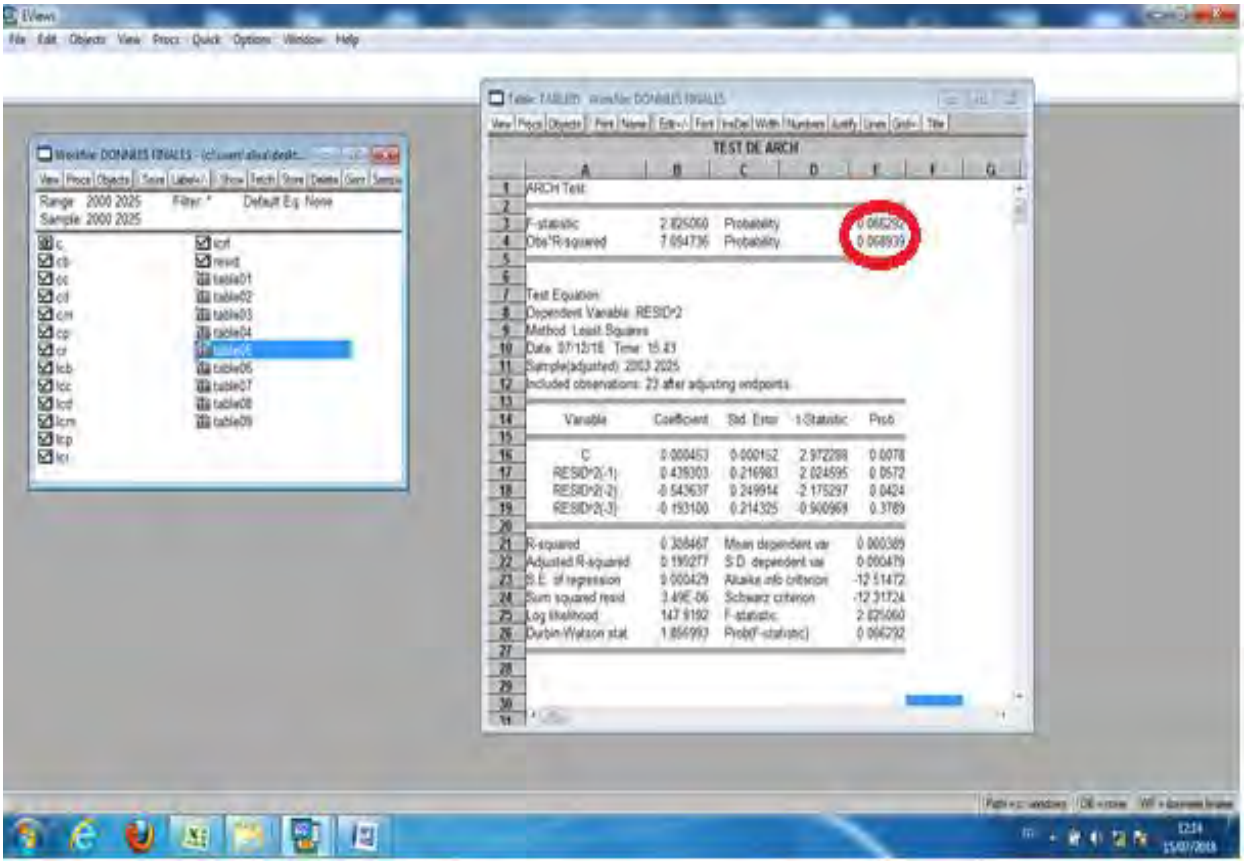


Figure 60:Test d'Arch: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

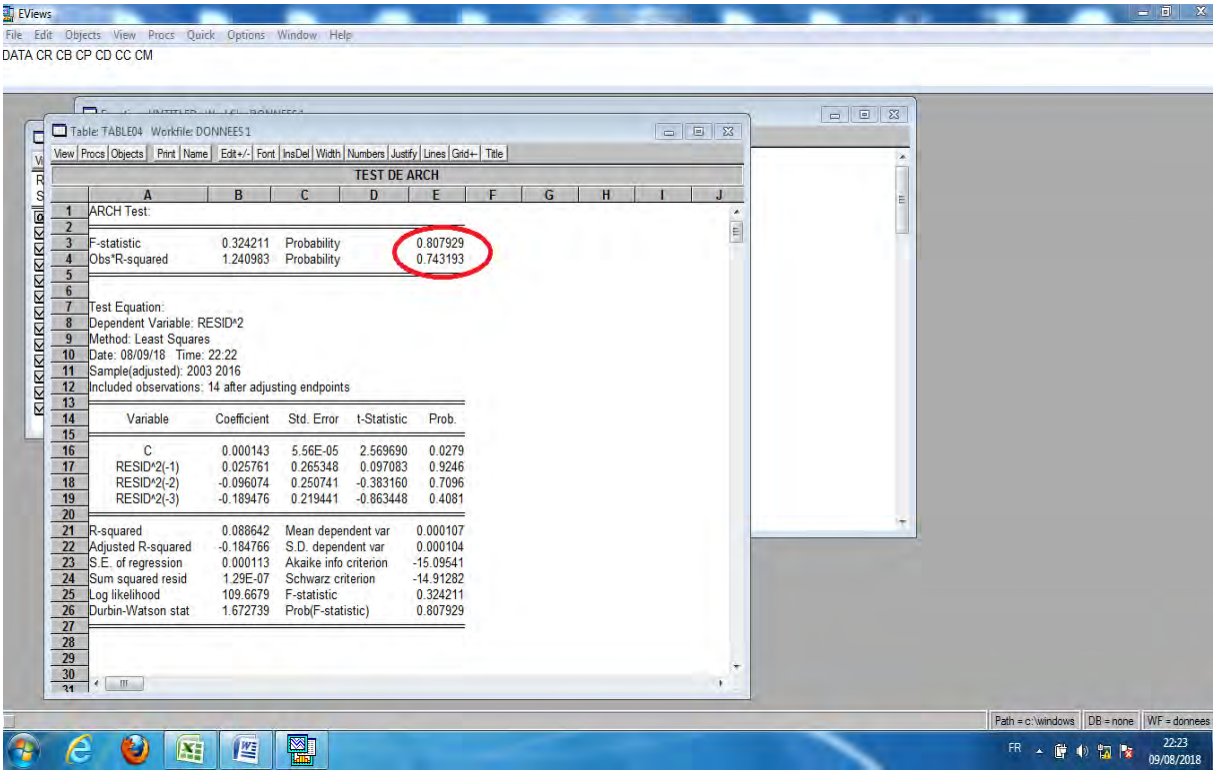


Figure 61:Test d'Arch: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

.

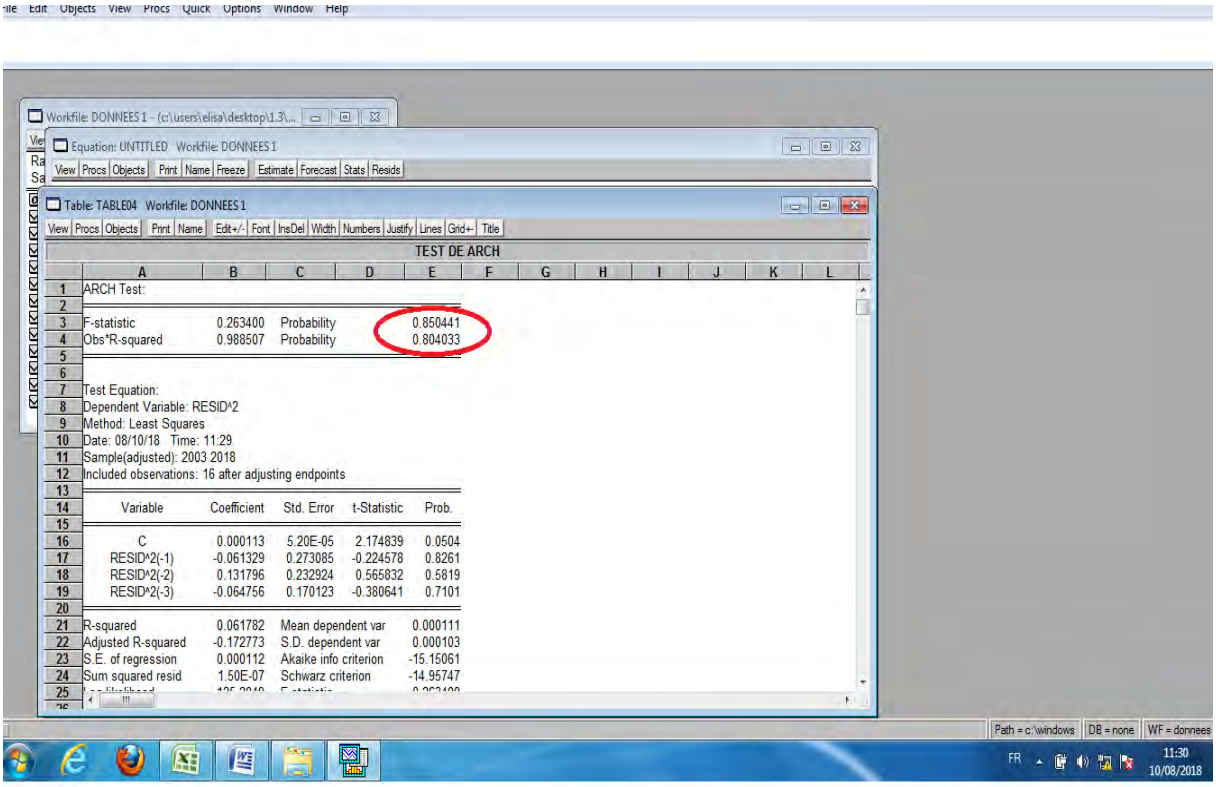


Figure 62:Test d'Arch: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

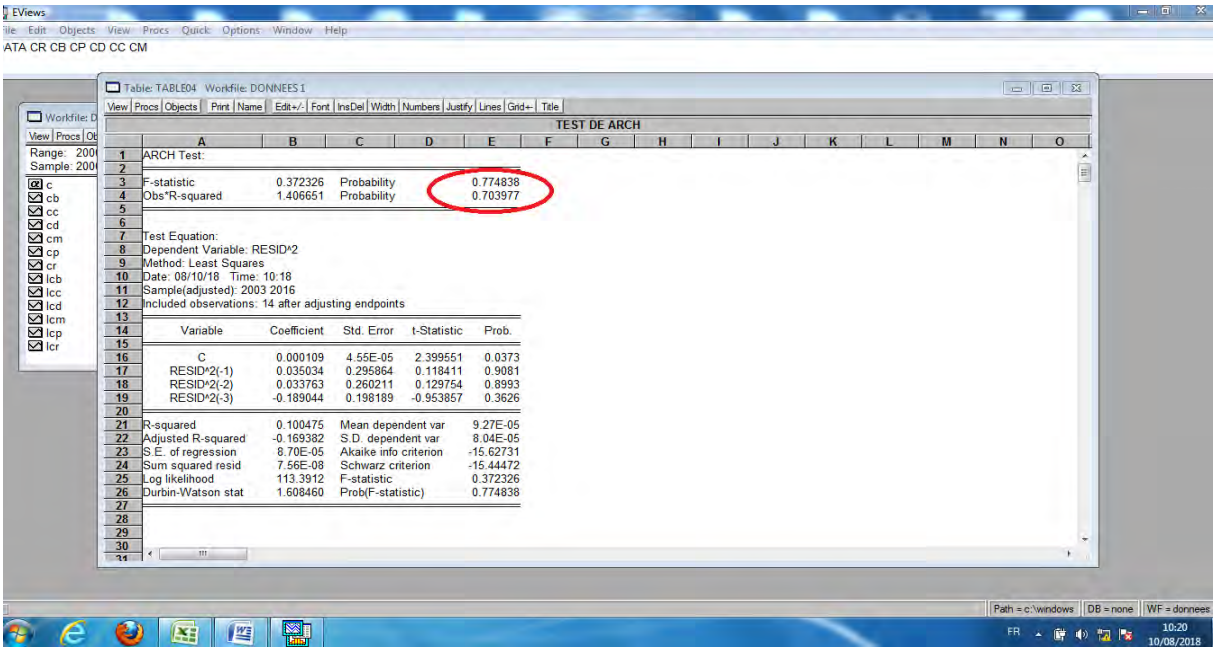


Figure 63:Test d'Arch: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

Les probabilités sont supérieures à 5% sur les 4 semestres d'affilés, donc on accepte l'hypothèse d'homoscédasticité des erreurs, on peut conclure que les estimations des paramètres de l'équation (a, b, c et d) obtenues par les MCO sont optimales.

- **Régression autorégressive**

Les résultats obtenus suite à la réalisation de ce test sont indiqués ci-dessous :

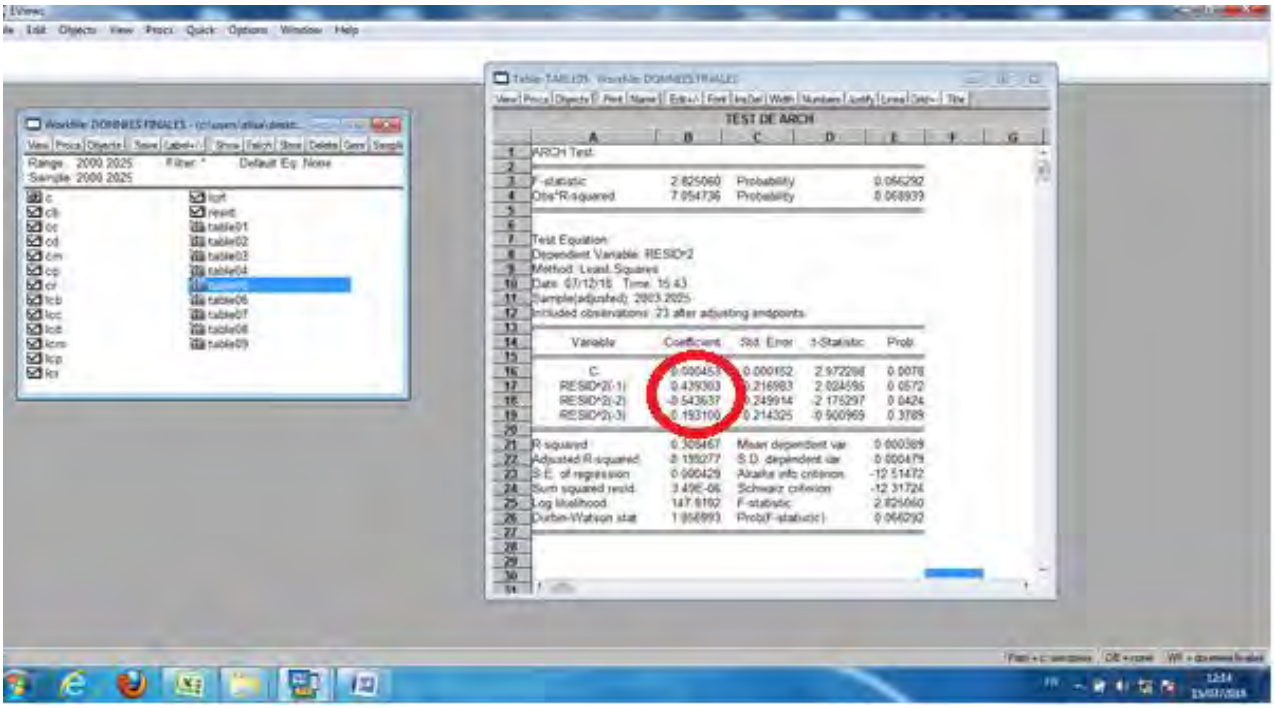


Figure 64:Régression autorégressive: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

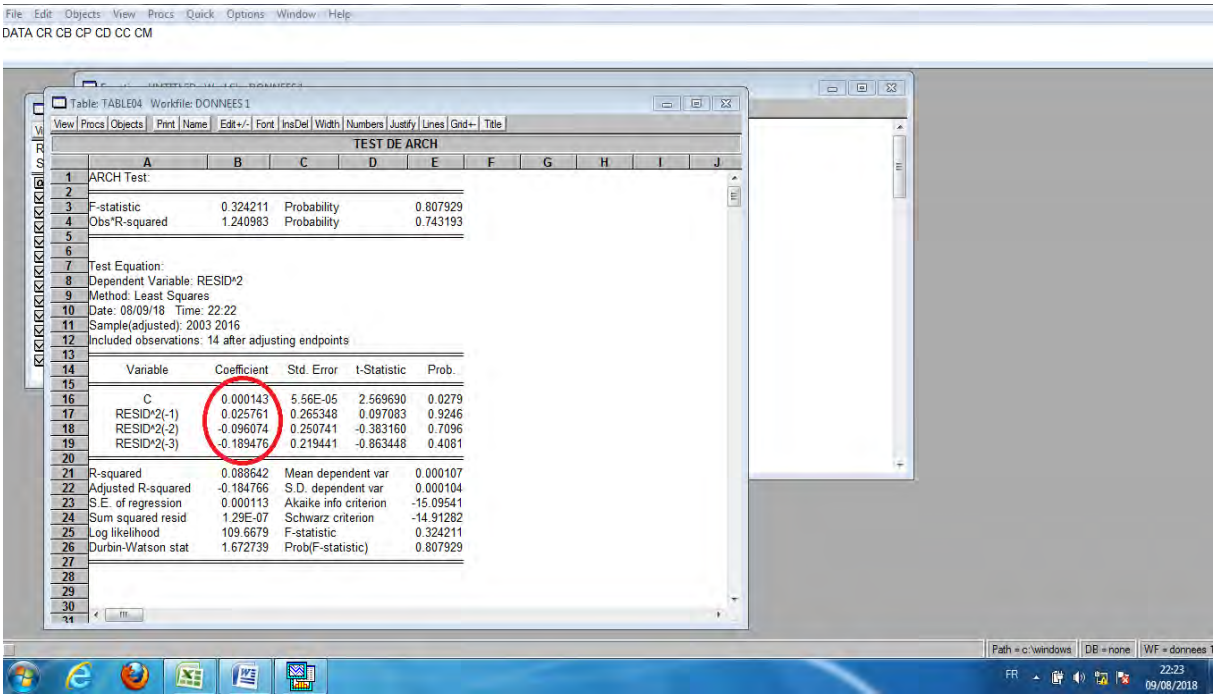


Figure 65:Régression autorégressive: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

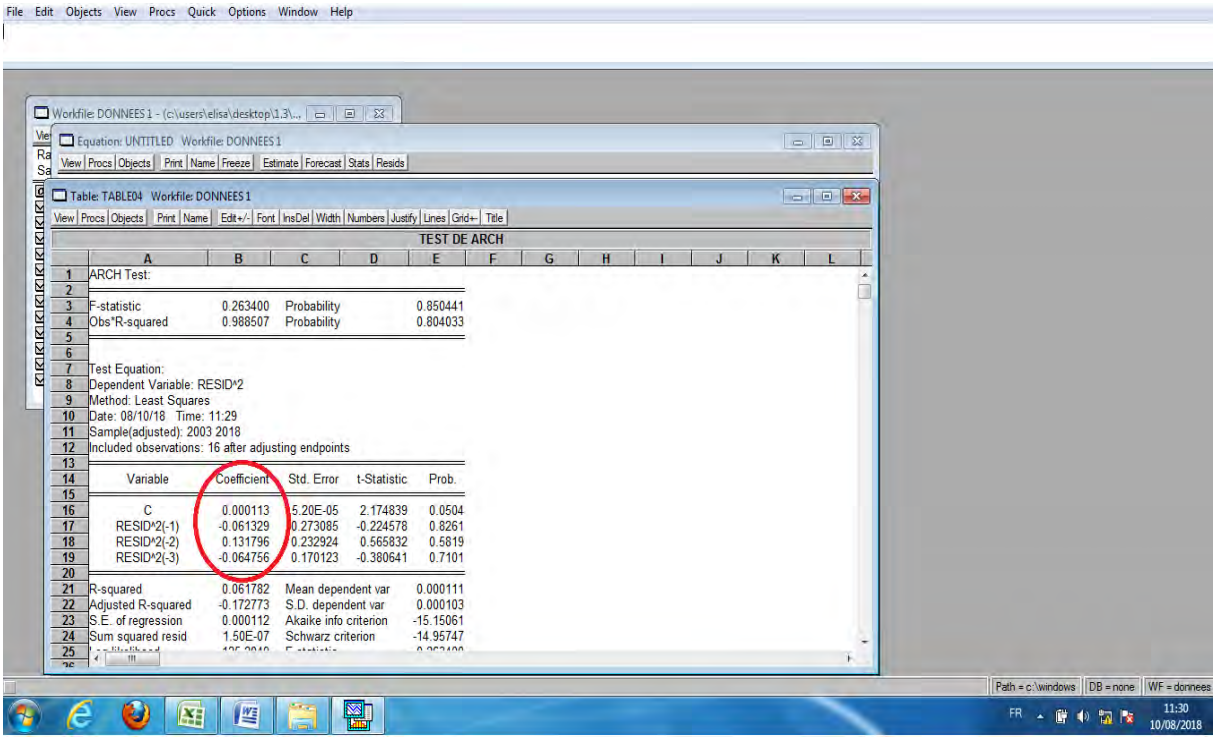


Figure 66:Régression autorégressive: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

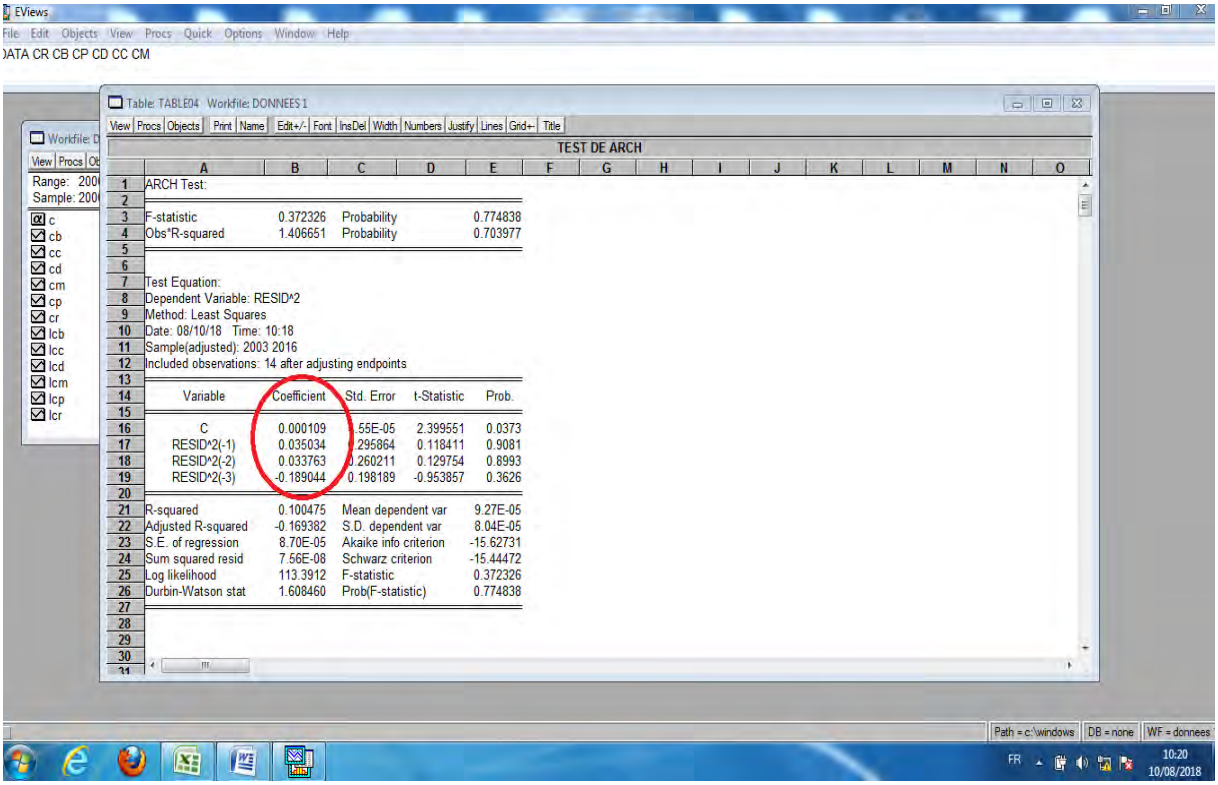


Figure 67:Régression autorégressive: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

Le coefficient a_1, a_2, a_3 obtenus sur les 4 semestres d'affilés sont significativement égaux à zéro, l'hypothèse d'homoscédasticité des erreurs est donc acceptée.

8. Test de Durbin Watson

Le test de Durbin Watson permet de vérifier s'il y a corrélation entre les erreurs à travers l'existence d'un potentiel lien entre les erreurs. L'idéal serait qu'il n'y ait pas de corrélation des erreurs. Les deux hypothèses de ce test sont.

$$H_0 : erreurs\ non\ corrélées$$

$$H_1 : erreurs\ correlées$$

A l'issu des tests, les coefficients de Durbin Watson obtenus sont indiqués ci-dessous :

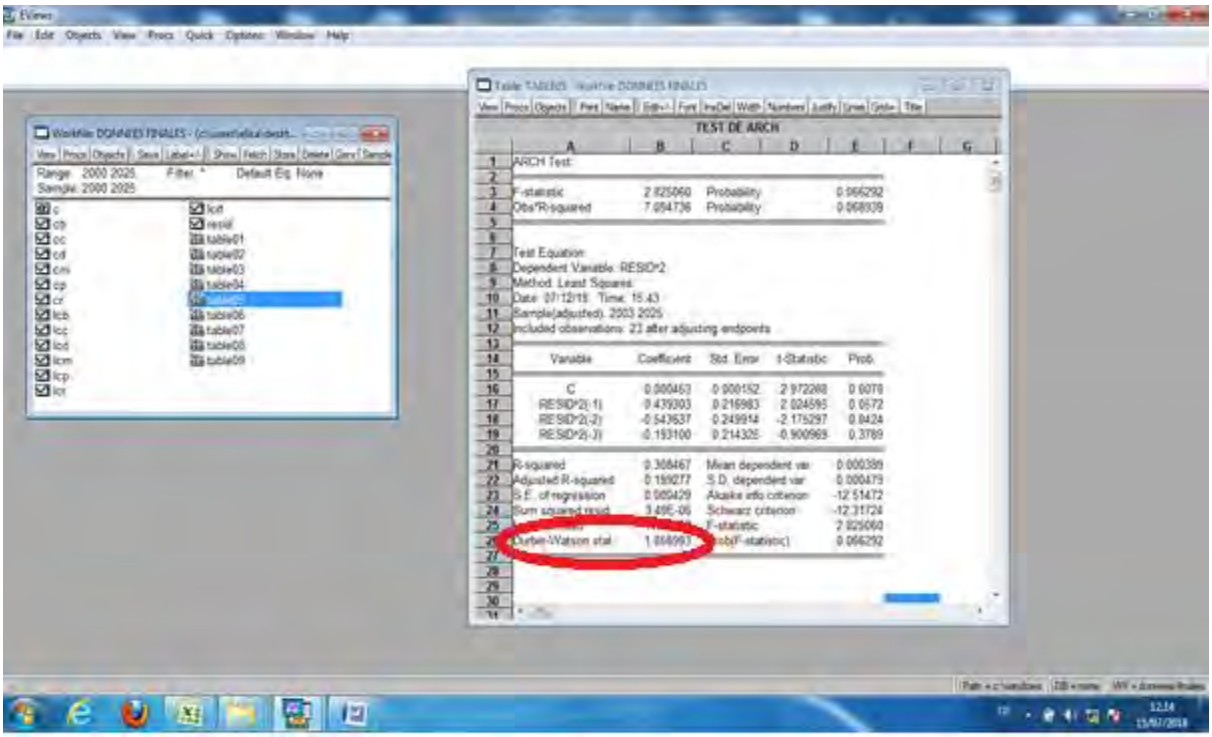


Figure 68:Test de Durbin Watson: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

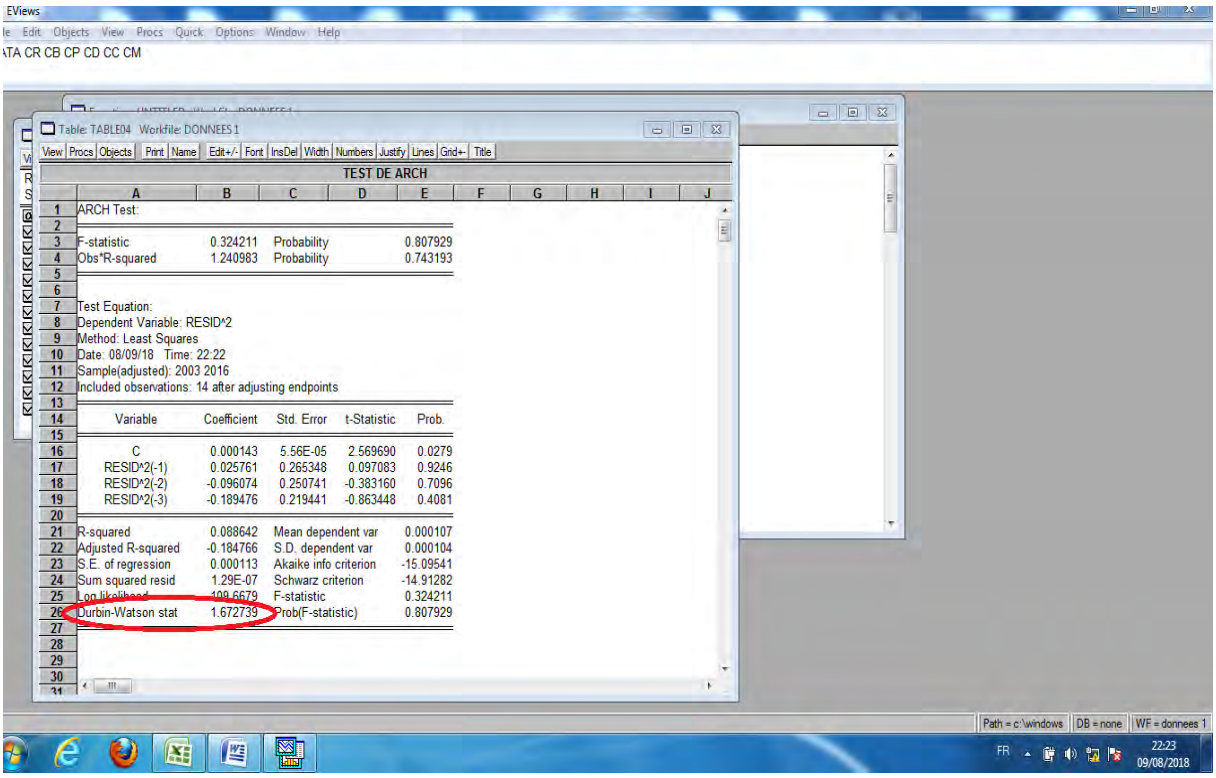


Figure 69:Test de Durbin Watson: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

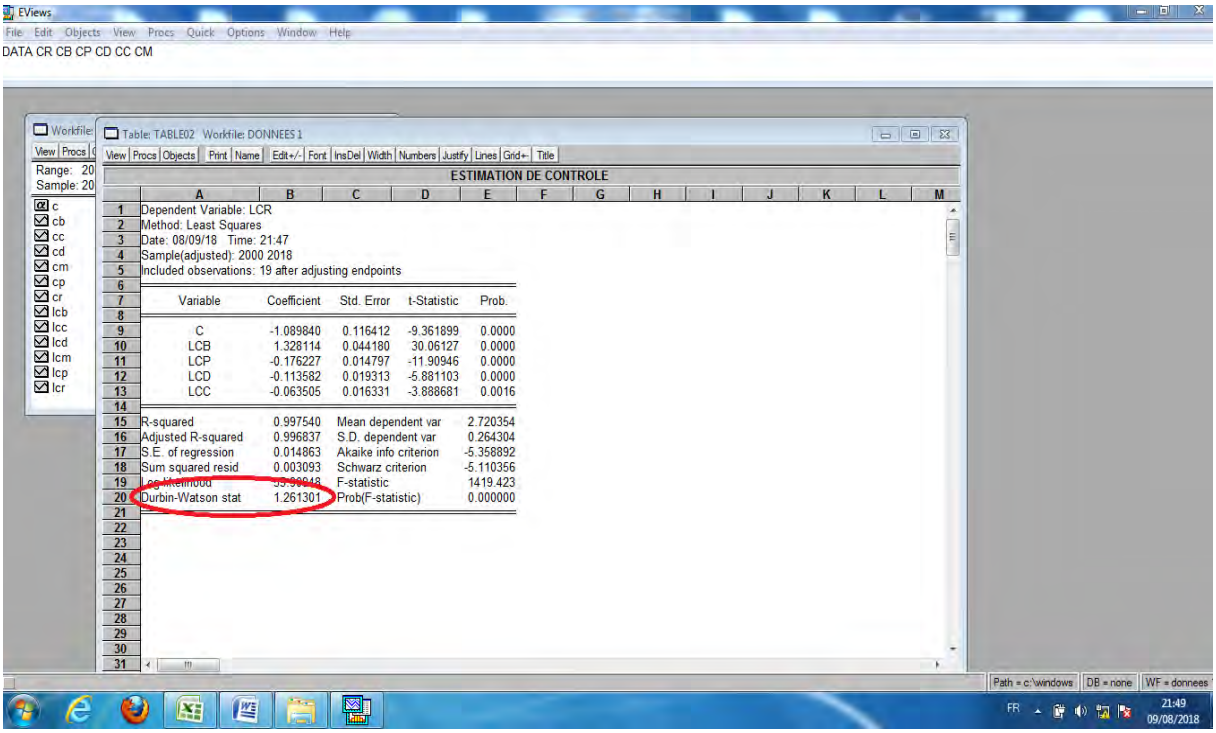


Figure 70:Test de Durbin Watson: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

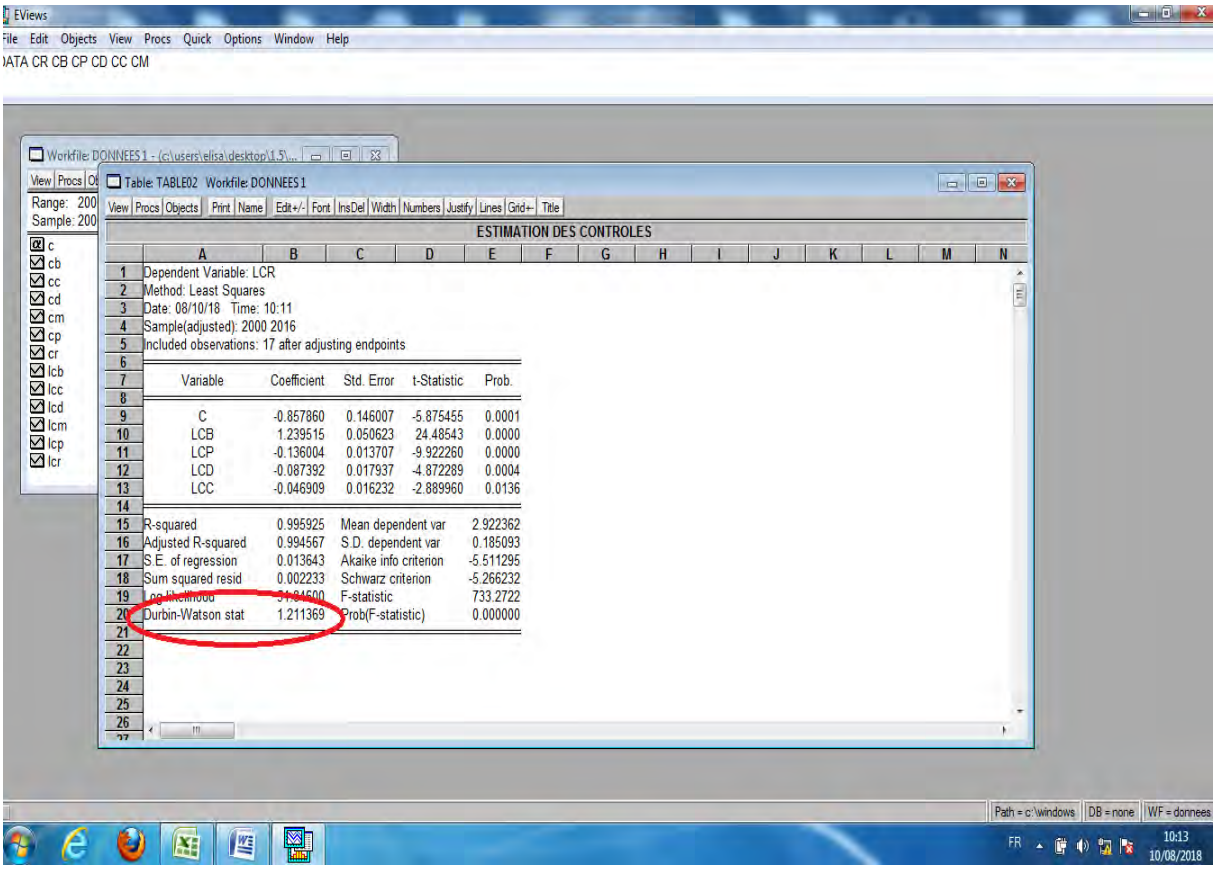


Figure 71:Test de Durbin Watson: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

En tenant compte des coefficients obtenus avec ce test et des intervalles y afférents au niveau du tableau de correspondance, on remarque qu'il n'y a aucune corrélation des erreurs sur les 4 semestres d'affilés. Donc on peut conclure que les erreurs de cette équation ne sont pas corrélées.

9. Test de de Ramsey

Le test de Ramsey permet de s'assurer de la spécification de l'équation proposée en vérifiant qu'elle est bien spécifique, qu'elle répond aux besoins et qu'elle résout le problème soulevé. Les hypothèses y afférentes sont les suivantes :

- Si probabilité est supérieure 5%, on accepteH_0, le modèle est bien spécifié
- Si probabilité est inférieure à 5%, on n'accepte pas H_0 , le modèle est mal spécifié

Les résultats obtenus sur les 4 semestres d'affilés avec Eviews sont indiqués ci-après :

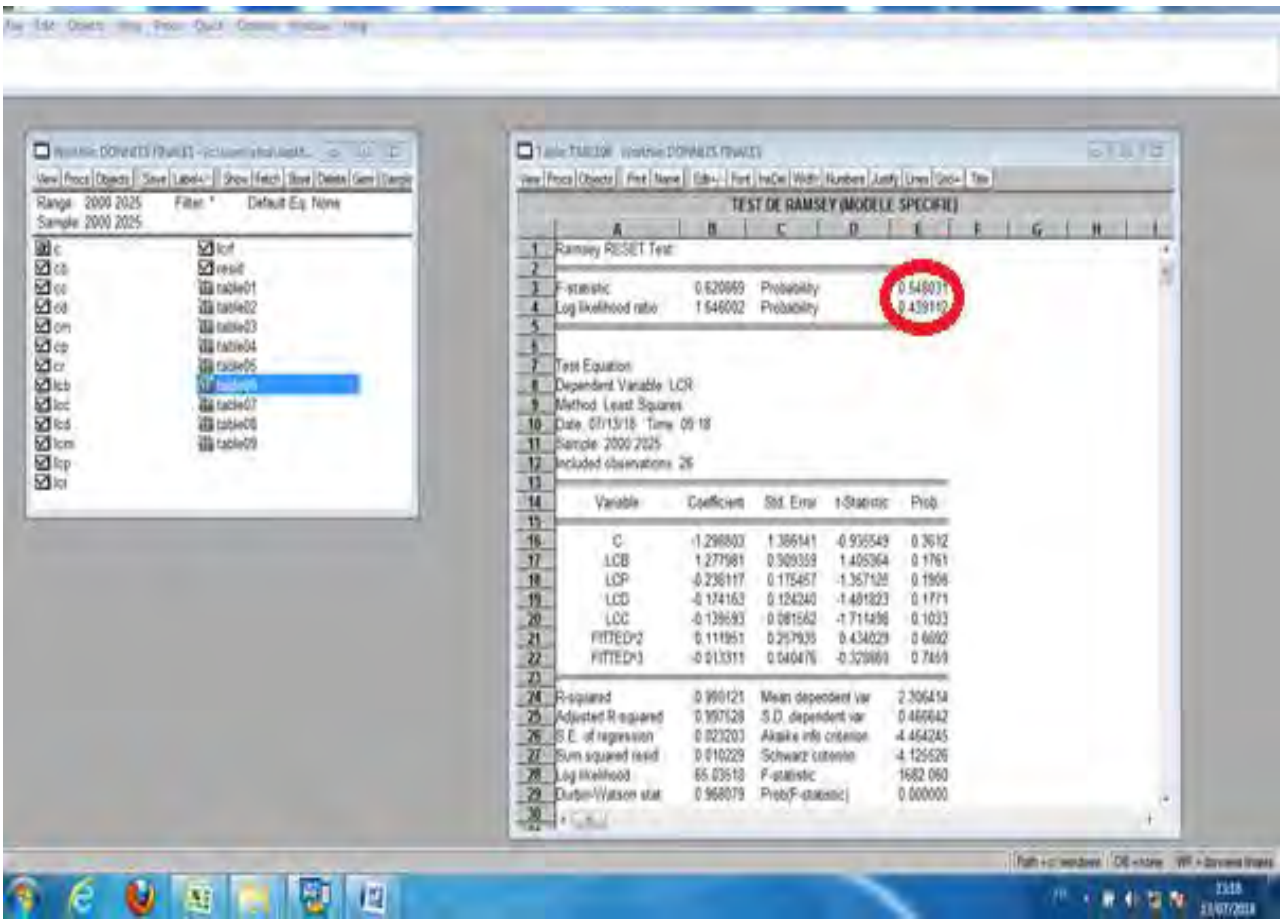


Figure 72:Test de Ramsey: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

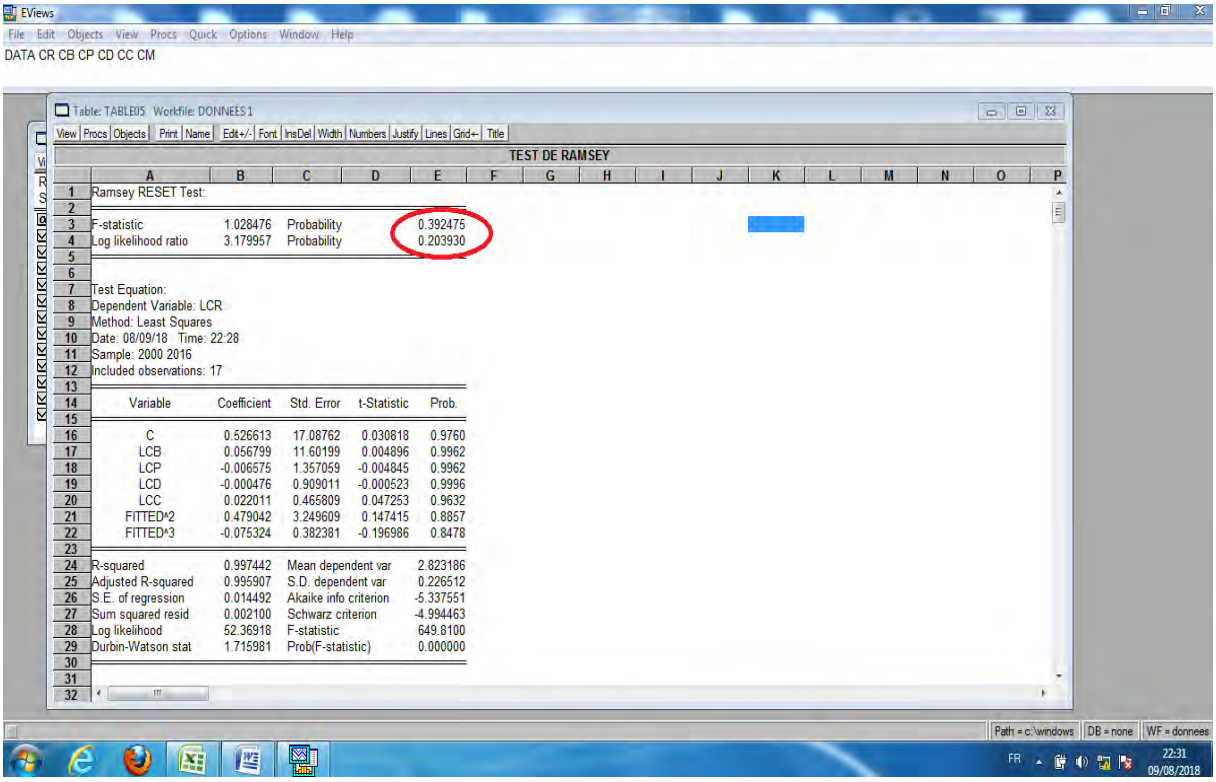


Figure 73:Test de Ramsey: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

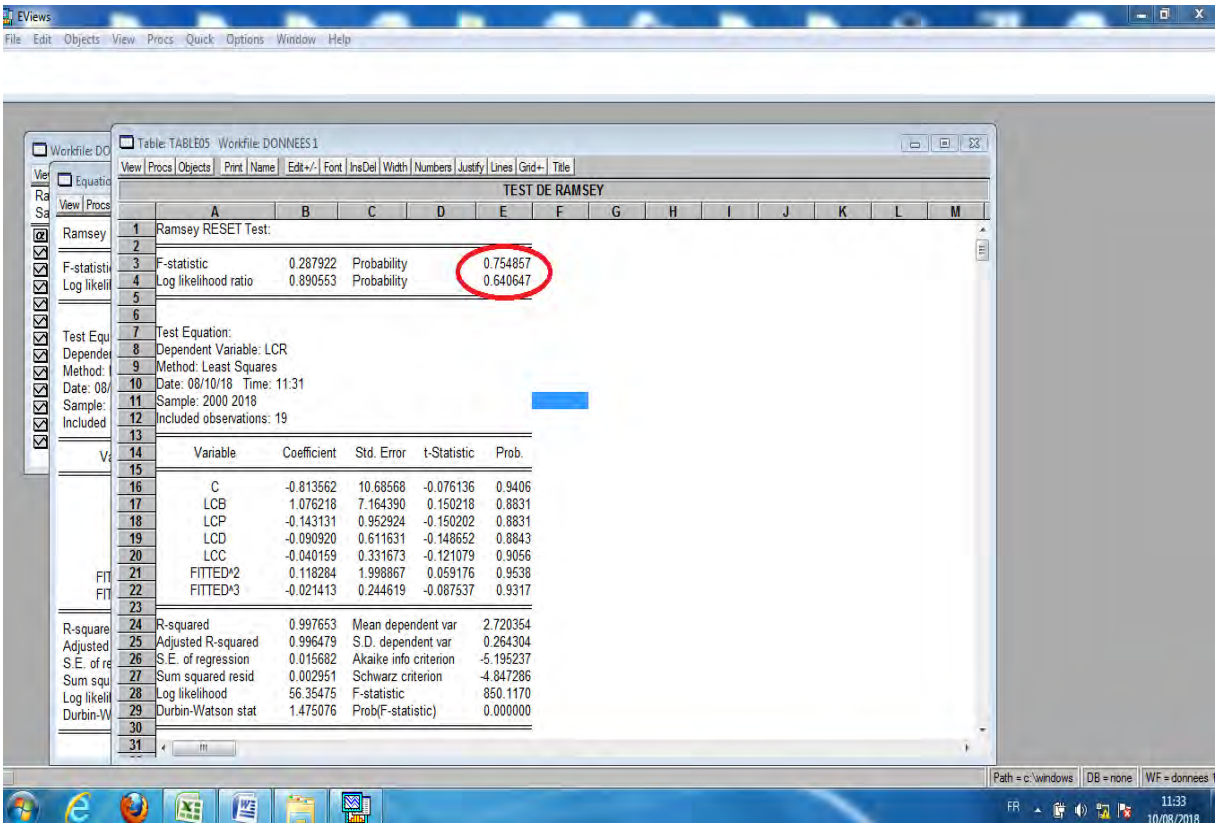


Figure 74:Test de Ramsey: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

.

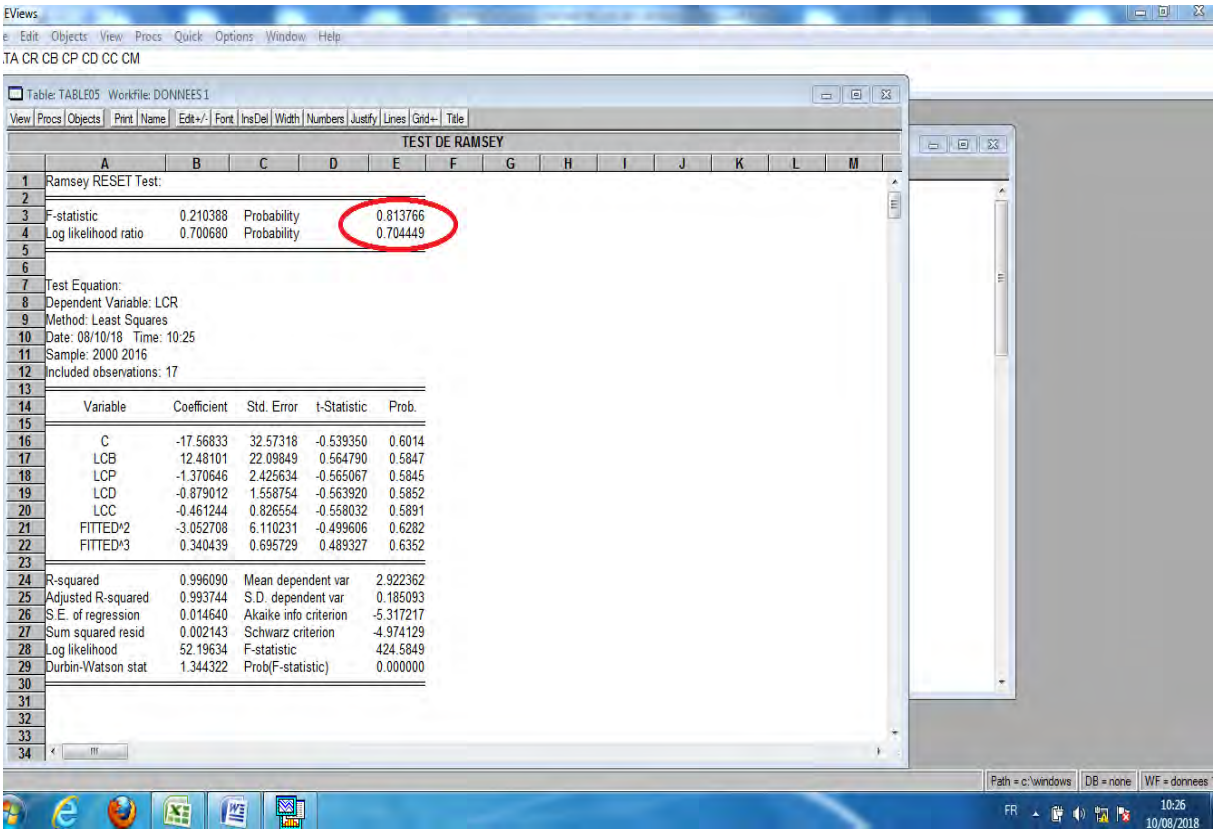


Figure 75:Test de Ramsey: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

D'après les résultats indiqués dans le tableau ci-dessus, les valeurs de F-statistic sont supérieures à 5% sur les 4 semestres d'affilés, cela signifie que l'équation de régression linéaire est bien spécifiée.

10. Test de stabilité des paramètres (test de Show)

Le test de Show permet de s'assurer de la stabilité des paramètres de l'équation en vérifiant si ses paramètres sont stables. Les hypothèses concernées sont les suivantes :

- Si probabilité est supérieure 5%, on accepte H_0 , donc les paramètres sont stables
- Si probabilité est inférieure à 5%, on n'accepte pas H_0, donc les paramètres non stables

Les résultats obtenus sur les 4 semestres d'affilés avec Eviews sont indiqués ci-après :

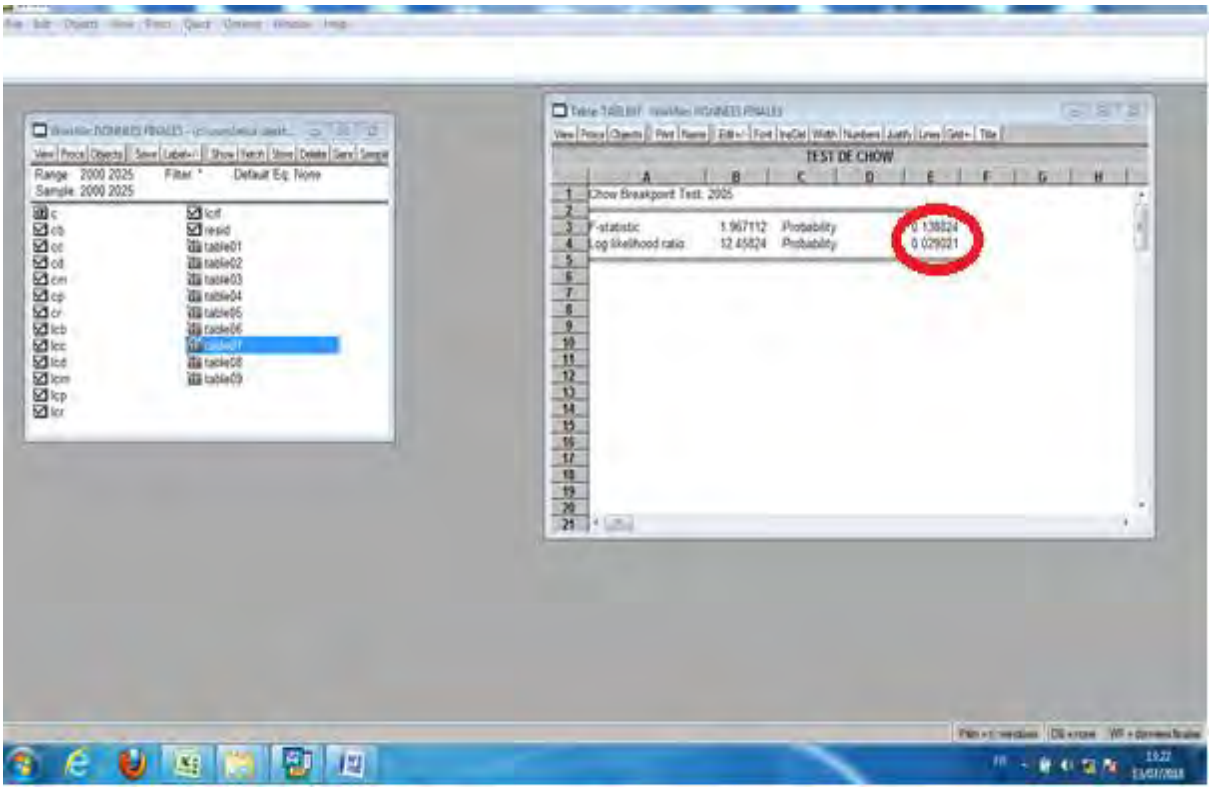


Figure 76:Test de Show: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

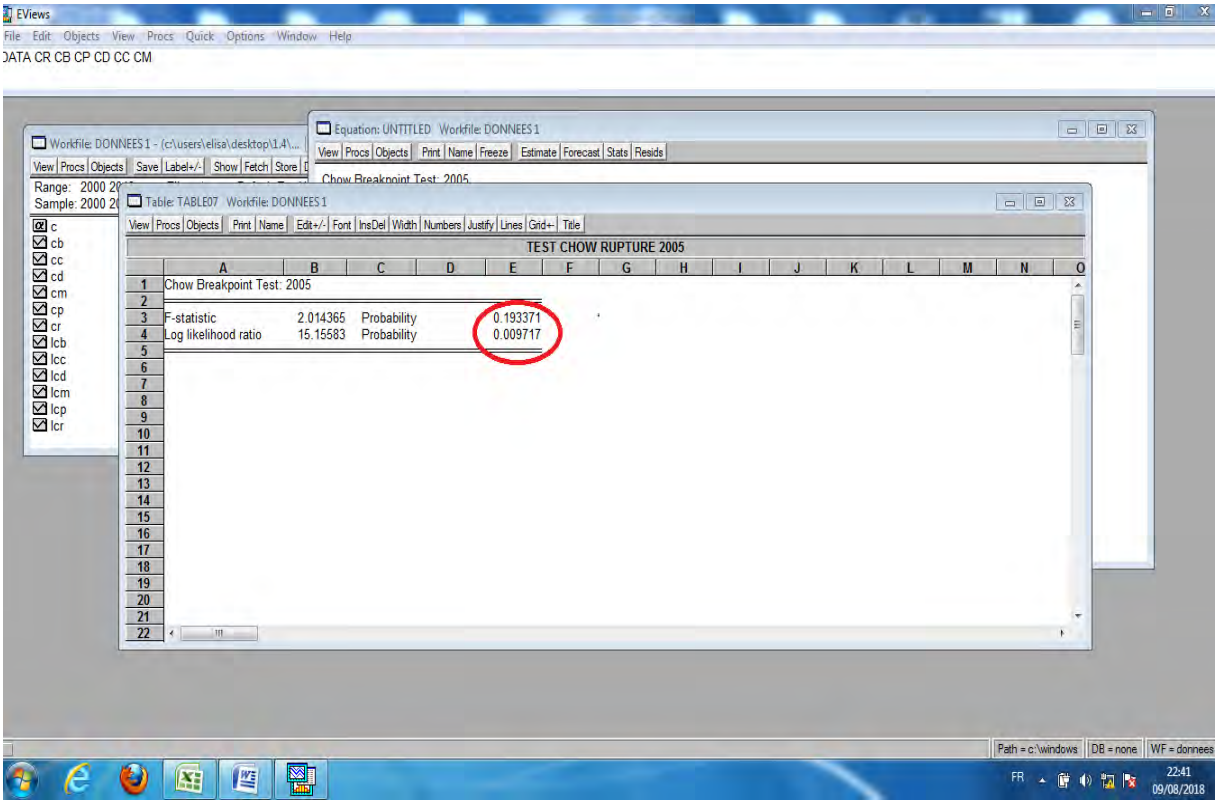


Figure 77:Test de Show: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

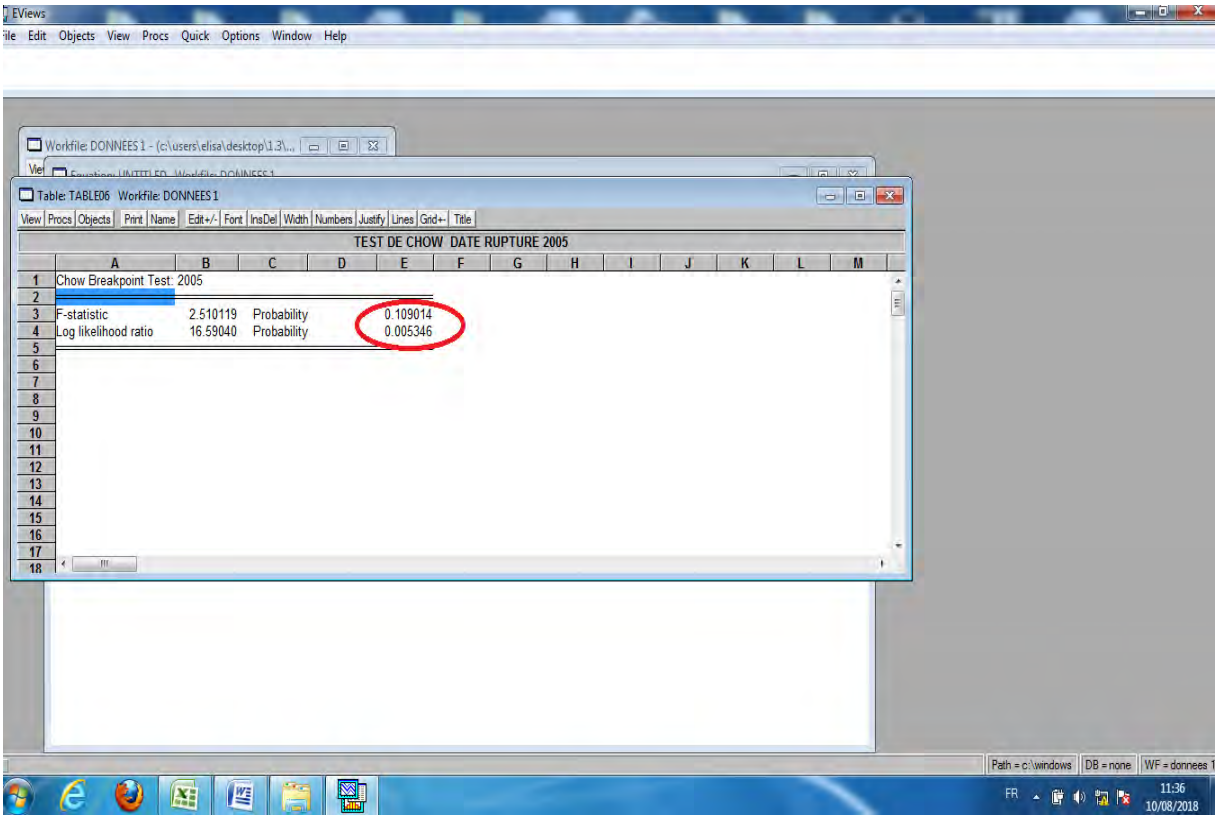


Figure 78:Test de Show: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

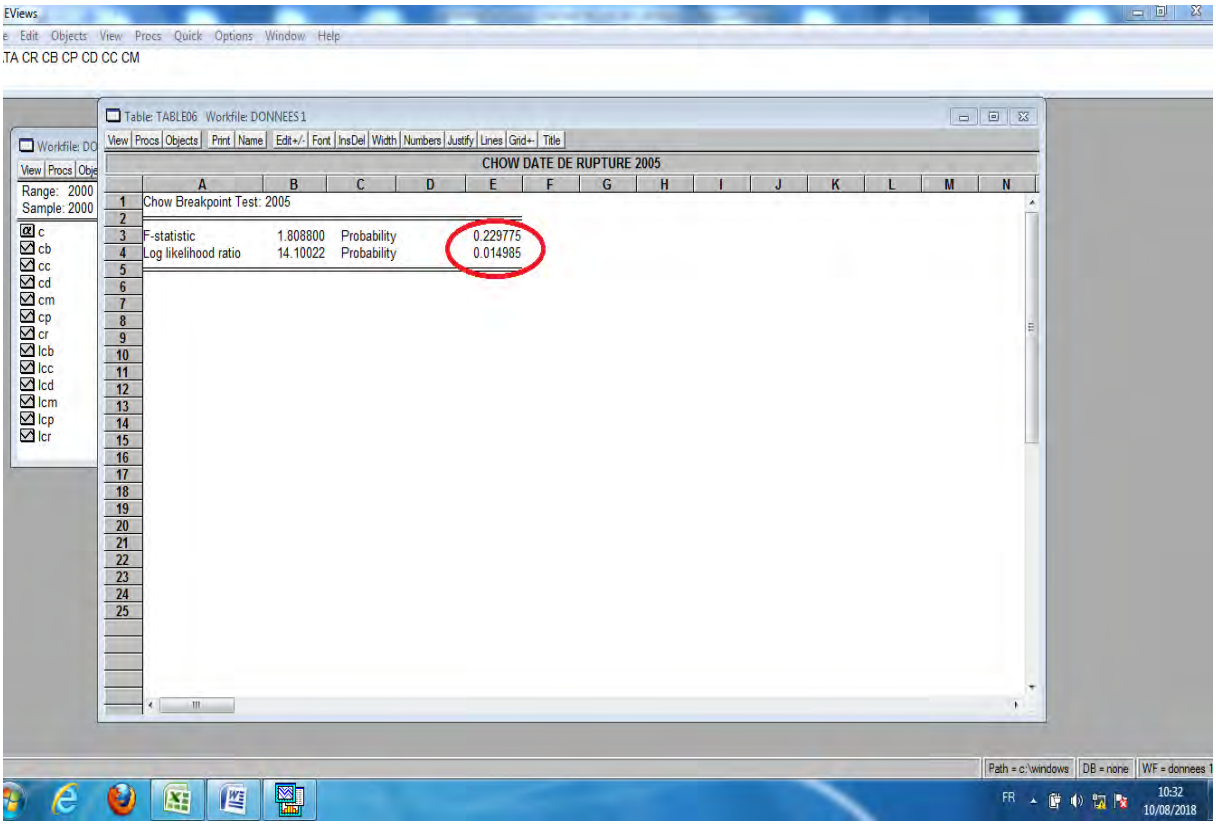


Figure 79:Test de Show: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

Après estimation, on remarque que pour chaque semestre, l'une des probabilités supérieure est à 5%, dans ce cas on accepte H_0 , cela signifie que l'équation est stable. En ce qui concerne l'autre probabilité inférieure à 5%, elles dénotent l'existence d'instabilités. Les spécificités de ces instabilités seront élucidées avec la réalisation des tests de CUSUM et CUSUM CARRE.

11. Test de CUSUM et CUSUM CARRE

Ces tests permettent de caractériser les instabilités de l'équation à travers la détection des instabilités structurelles et ponctuelles.

Pour ce test, les deux règles de décision sont les suivantes :

- Si la courbe ne coupe pas les bornes du corridor alors le modèle est stable
- Si la courbe coupe les bornes du corridor alors le modèle est instable, dans ce cas, la courbe indique la période d'instabilité

a. Test de CUSUM

Ce test permet de détecter les instabilités structurelles de l'équation. Les résultats obtenus sur les 4 semestres d'affilés avec Eviews sont indiqués ci-après :

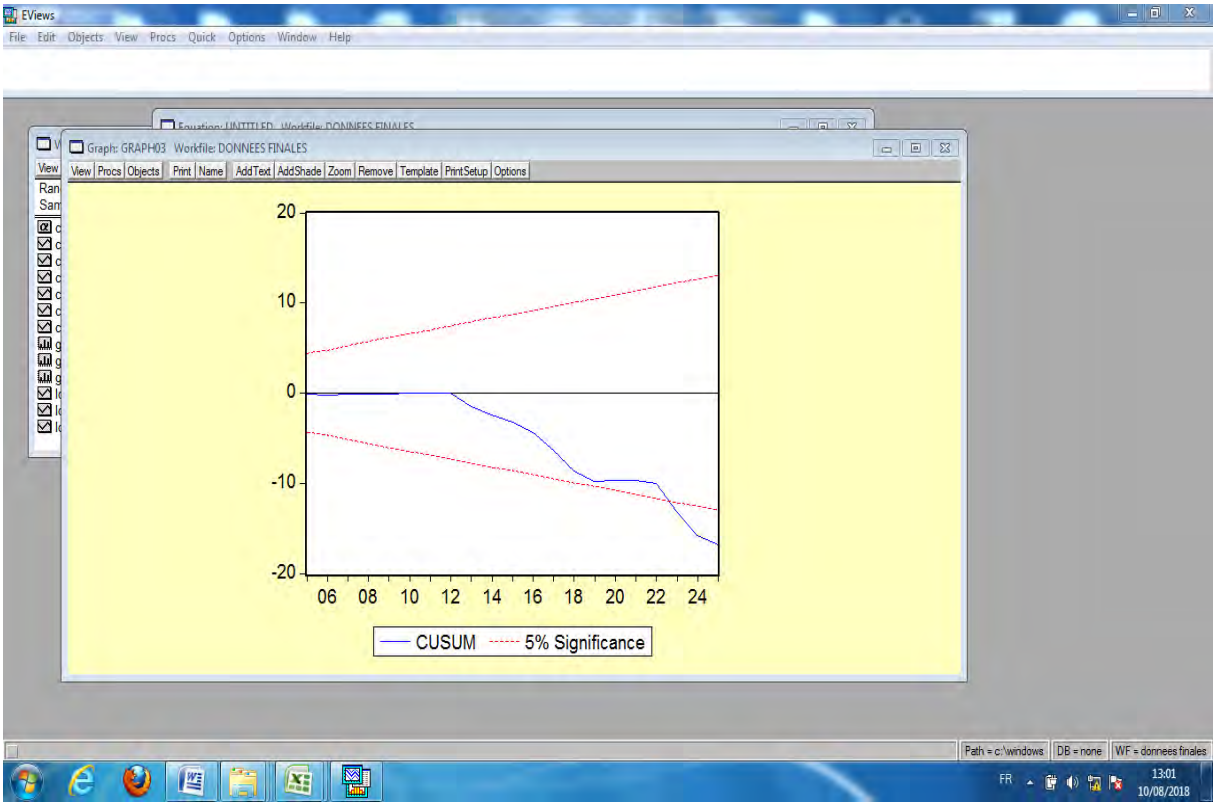


Figure 80:Test de CUSUM: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

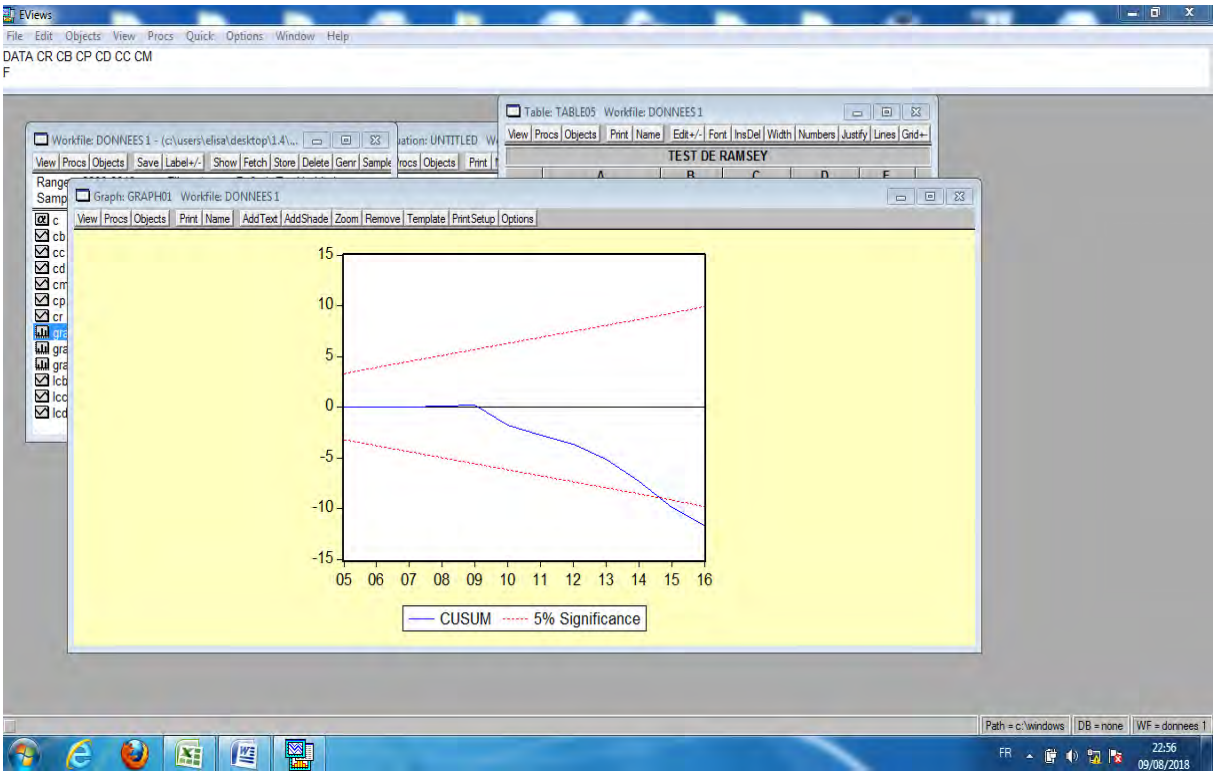


Figure 81:Test de CUSUM: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

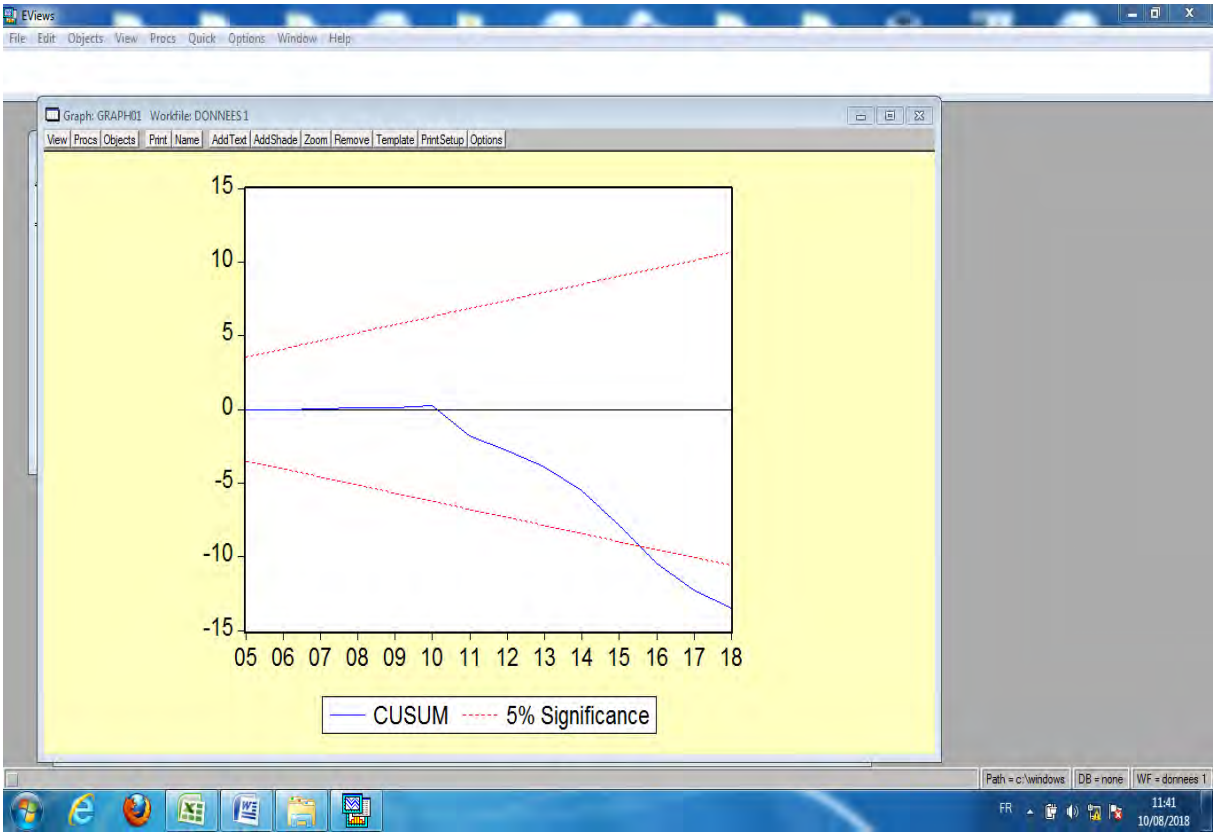


Figure 82:Test de CUSUM: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

Figure 83:Test de CUSUM: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

Interprétation des résultats

A la lecture de ces graphiques, on remarque que la courbe représentant les données sort du corridor sur les deux dernières valeurs de la série. Cela dénote des instabilités structurelles de l'équation pour ces valeurs.

b. Test de CUSUM CARRE

Ce test permet de détecter les instabilités ponctuelles de l'équation. Les résultats obtenus sur les 4 semestres d'affilés avec Eviews sont indiqués ci-après :

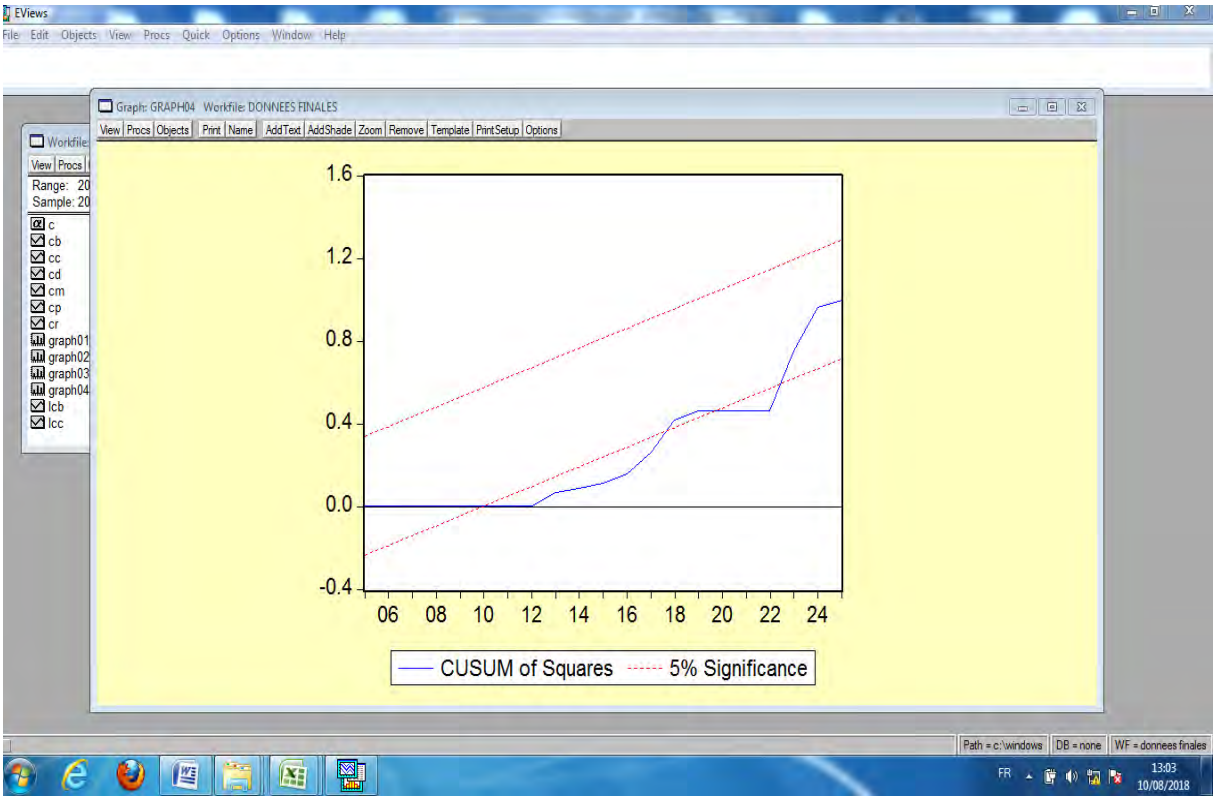


Figure 84:Test de CUSUM CARRE: Résultats obtenus avec l'équation 2 et relatifs à la banque 1

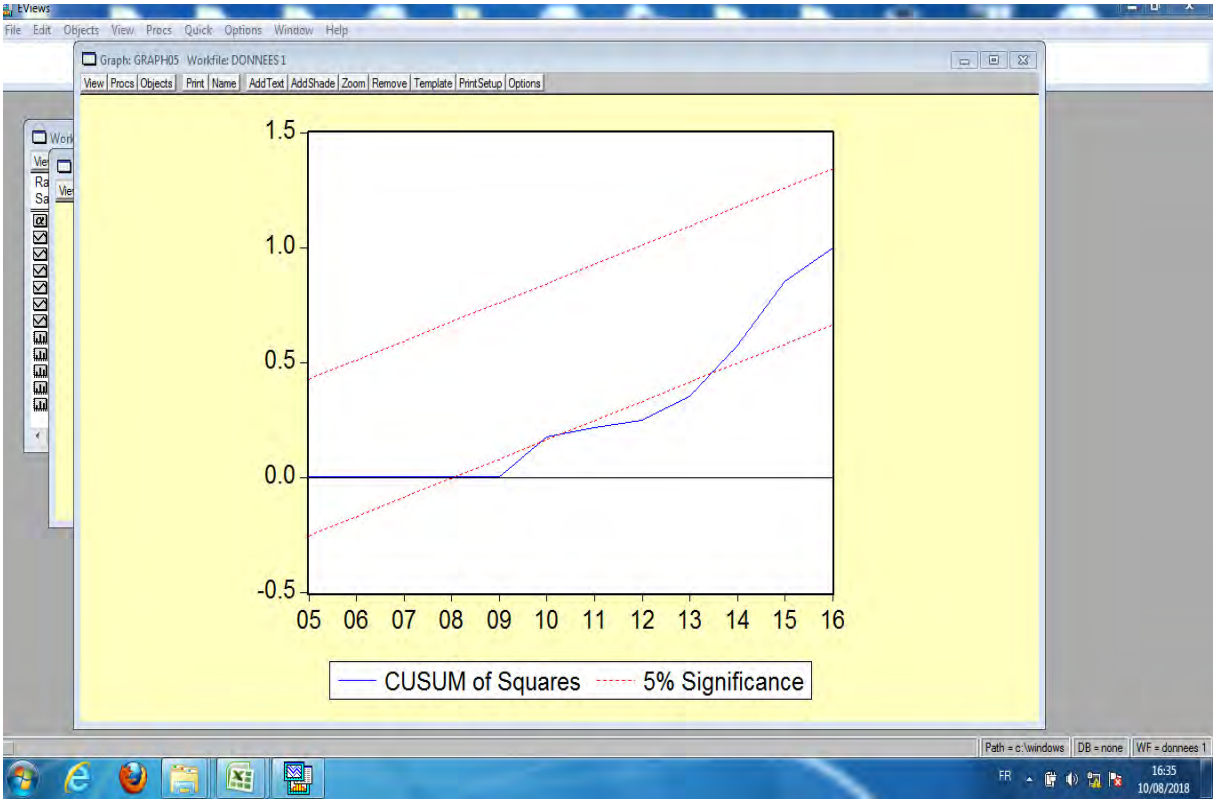


Figure 85:Test de CUSUM CARRE: Résultats obtenus avec l'équation 2 et relatifs à la banque 2

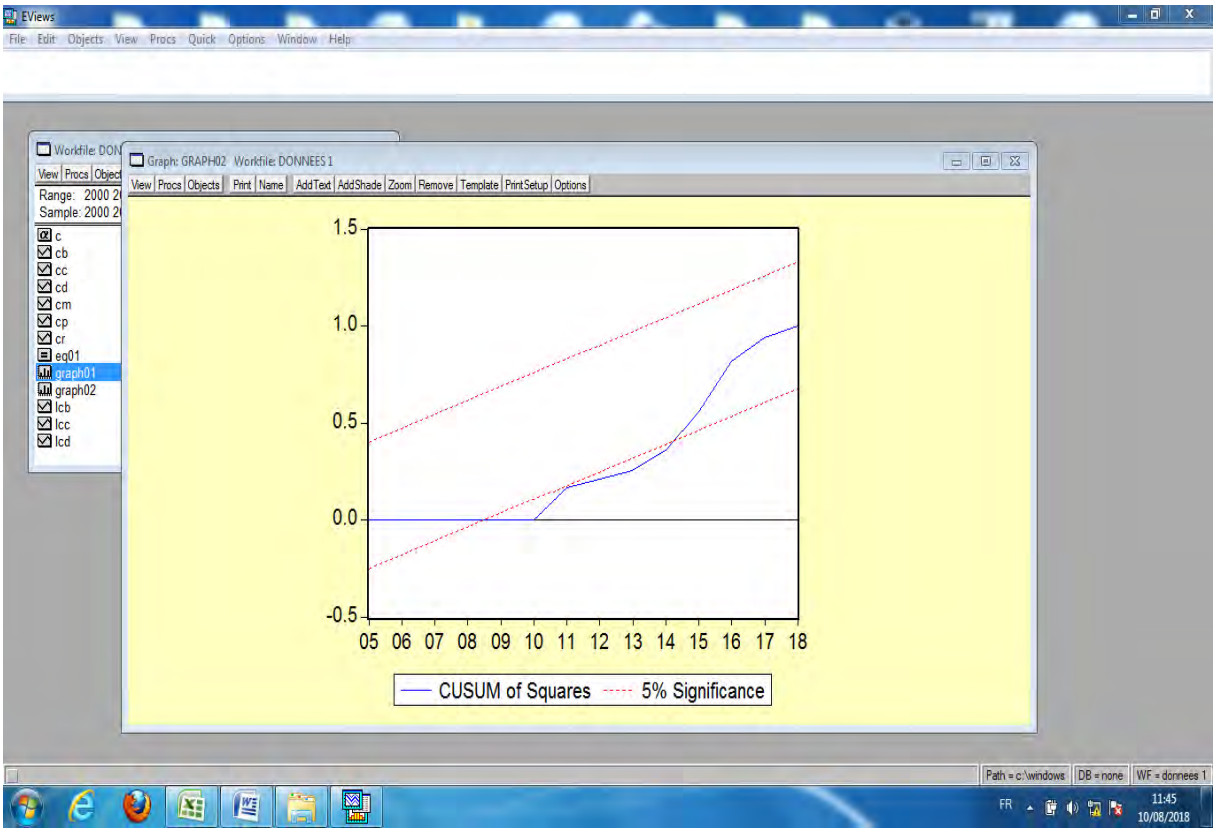


Figure 86:Test de CUSUM CARRE: Résultats obtenus avec l'équation 2 et relatifs à la banque 3

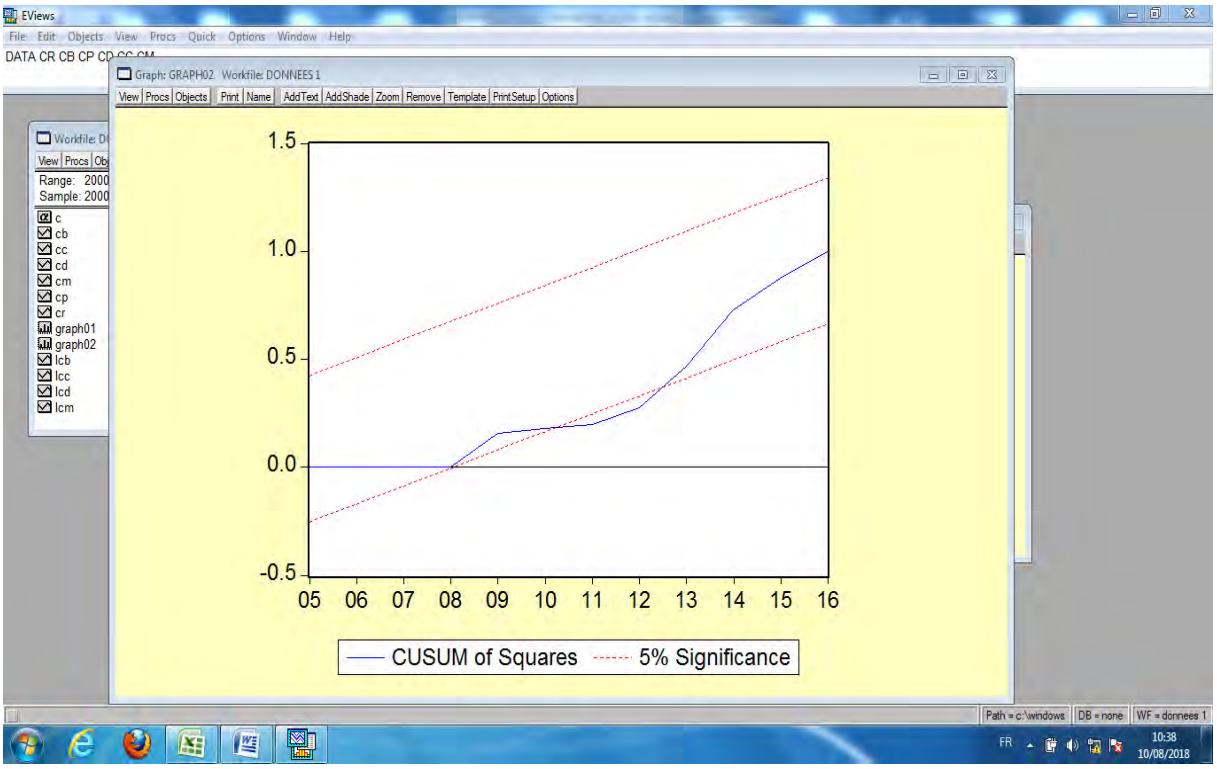


Figure 87:Test de CUSUM CARRE: Résultats obtenus avec l'équation 2 et relatifs à la banque 4

- **Interprétation des résultats**

A la lecture de ces graphiques, on remarque que la partie instable de la courbe représentant les dernières données de la série est redirigée dans le corridor, cela signifie que les instabilités structurelles de l'équation sont corrigées avec le temps. Les instabilités ponctuelles détectées s'expliquent par les estimations erronées constatées pour ces valeurs.

V.2.3 Simulation de l'équation améliorée par les MCO

Nous avons également effectué les simulations de l'équation en vue de faire une comparaison entre les données estimées correspondant aux données collectées au niveau des banques et les données ajustées correspondants aux valeurs obtenues avec l'équation. Les résultats obtenus avec Eviews sur 4 semestres d'affilés sont indiqués ci-après :

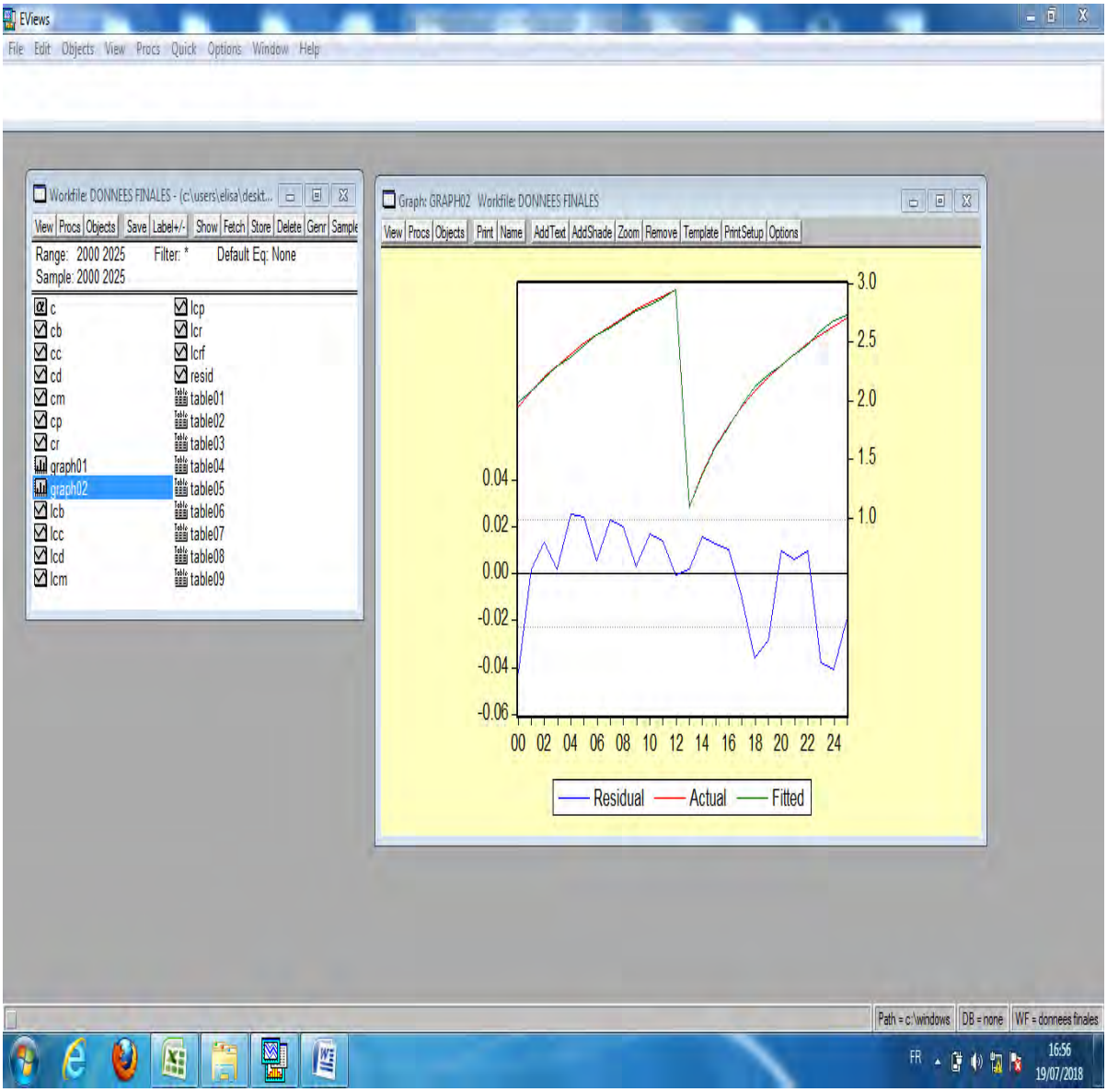


Figure 88:Simulation de l'équation 2: Résultats obtenus avec la banque 1

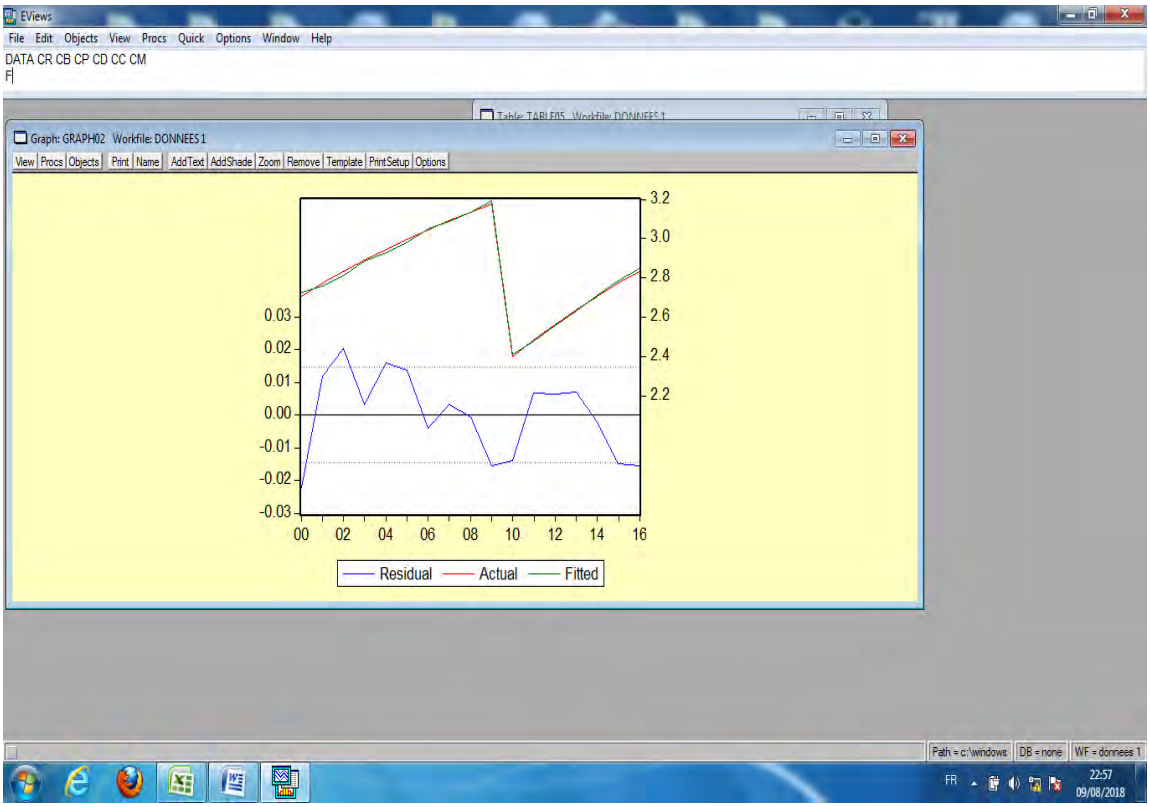


Figure 89:Simulation de l'équation 2: Résultats obtenus avec la banque 2

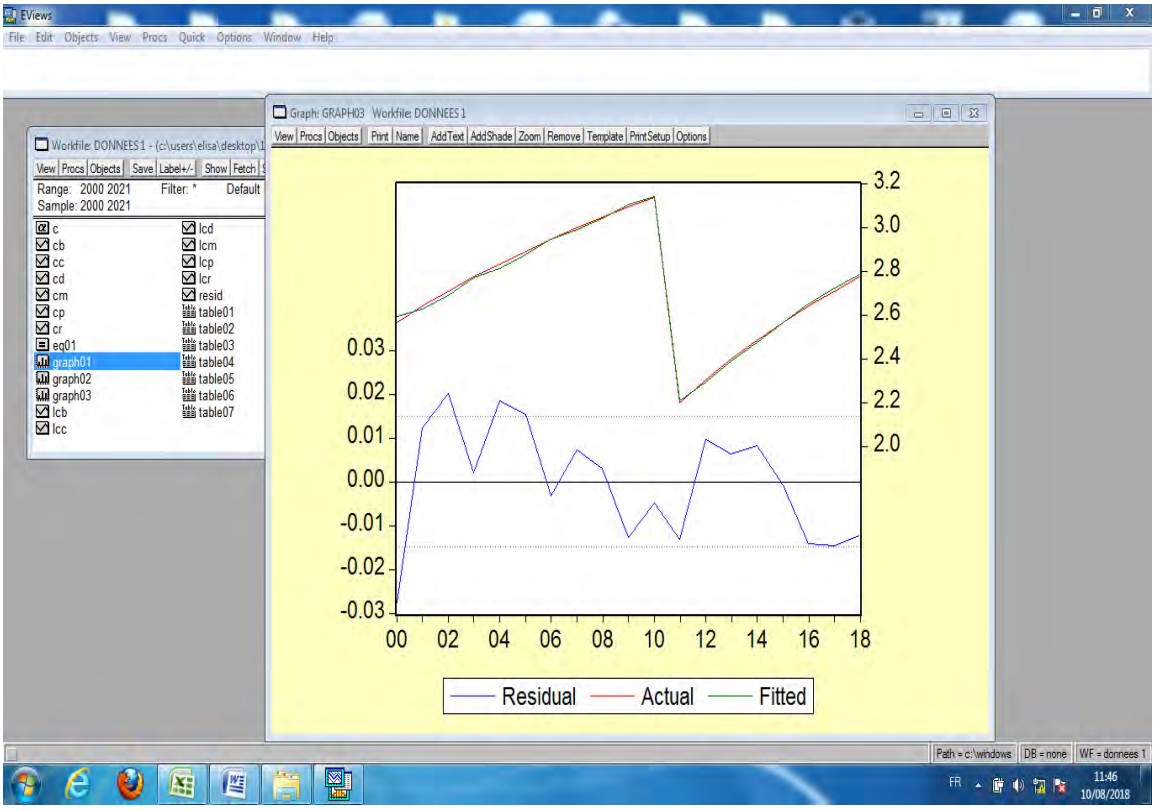


Figure 90:Simulation de l'équation 2: Résultats obtenus avec la banque 3

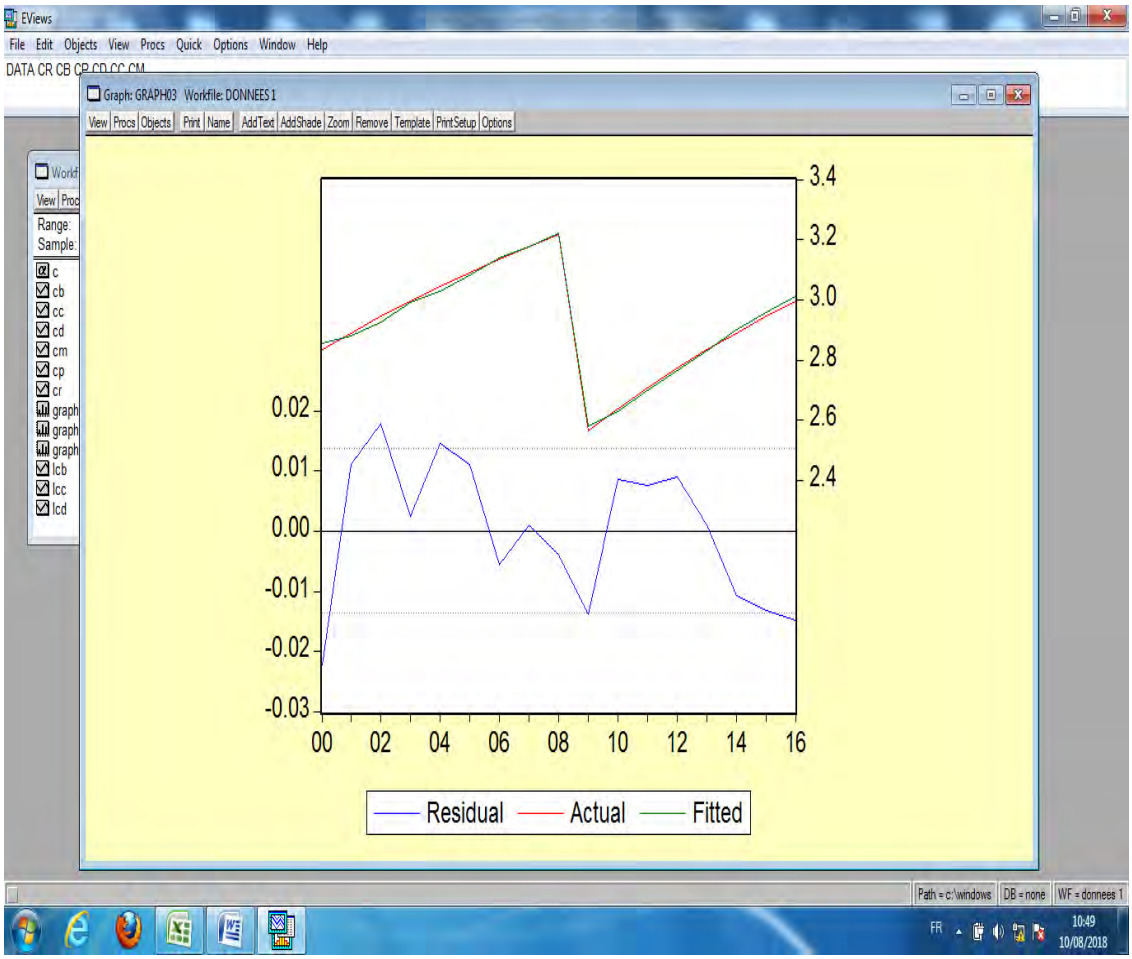


Figure 91:Simulation de l'équation 2: Résultats obtenus avec la banque 4

Interprétation des résultats

Après simulation, il apparait que les courbes des données observées (actual) et ajustées (fitted) sont proches sur les 4 semestres d'affilés, cela signifie que l'erreur commise est faible. Cette erreur sera quantifiée à l'aide des critères de prévisions. Nous pouvons donc conclure que le modèle a des chances d'avoir un bon pouvoir prédictif car il reproduit fidèlement le passé. Par ailleurs, on note également le défaut de lissage des données non logarisées (residual), ce qui confirme l'avantage de l'utilisation du logarithme que nous avons adopté dès le début de notre modélisation.

V.2.4 Prévision de l'équation améliorée par les MCO

A ce niveau, nous avons effectué d'abord effectué une prévision basée sur les valeurs. Les résultats obtenus avec Eviews sur 4 semestres d'affilés sont indiqués ci-après :

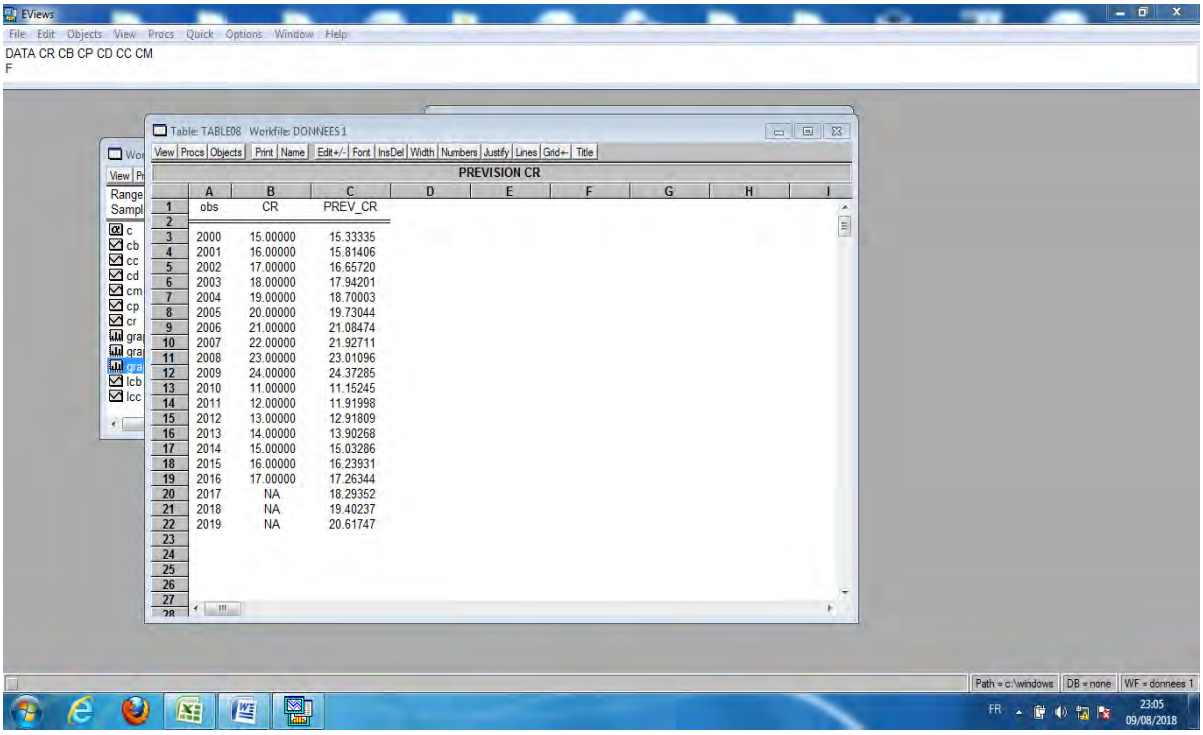


Figure 92: Prévision en valeurs de l'équation 2: Résultats obtenus avec la banque 1

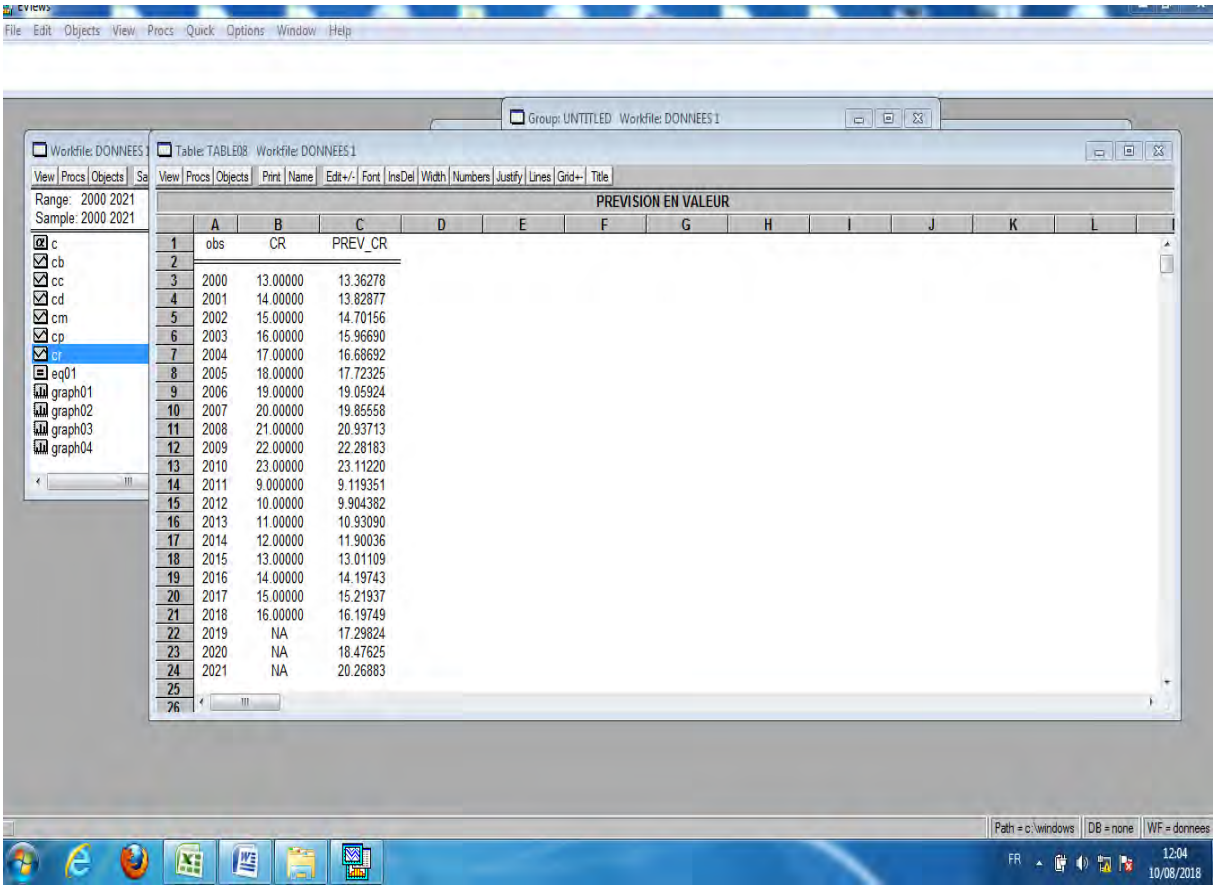


Figure 93: Prévision en valeurs de l'équation 2: Résultats obtenus avec la banque 2

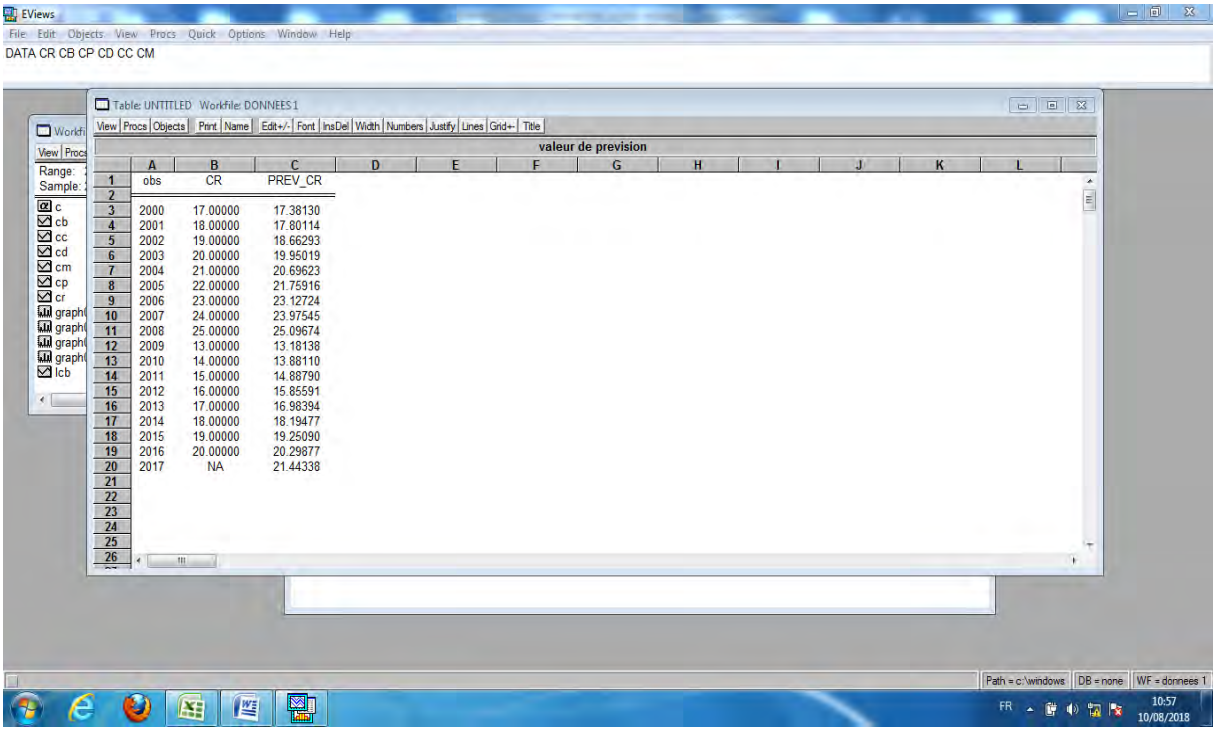


Figure 94:Prévision en valeurs de l'équation 2: Résultats obtenus avec la banque 3

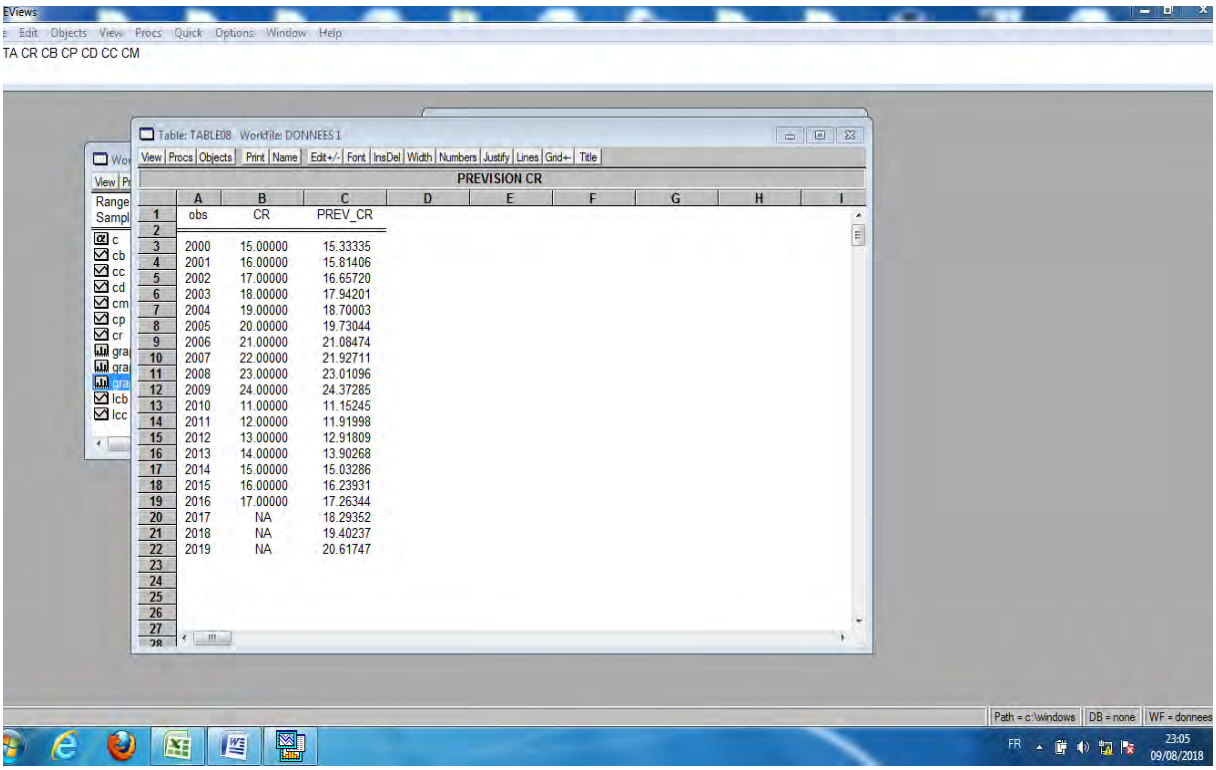


Figure 95:Prévision en valeurs de l'équation 2: Résultats obtenus avec la banque 4

Par la suite, dans le but de mieux interpréter ces valeurs, nous avons procédé à une représentation graphique de ces prévisions sur les 4 semestres testés. Les résultats obtenus avec Eviews sont indiqués ci-après :

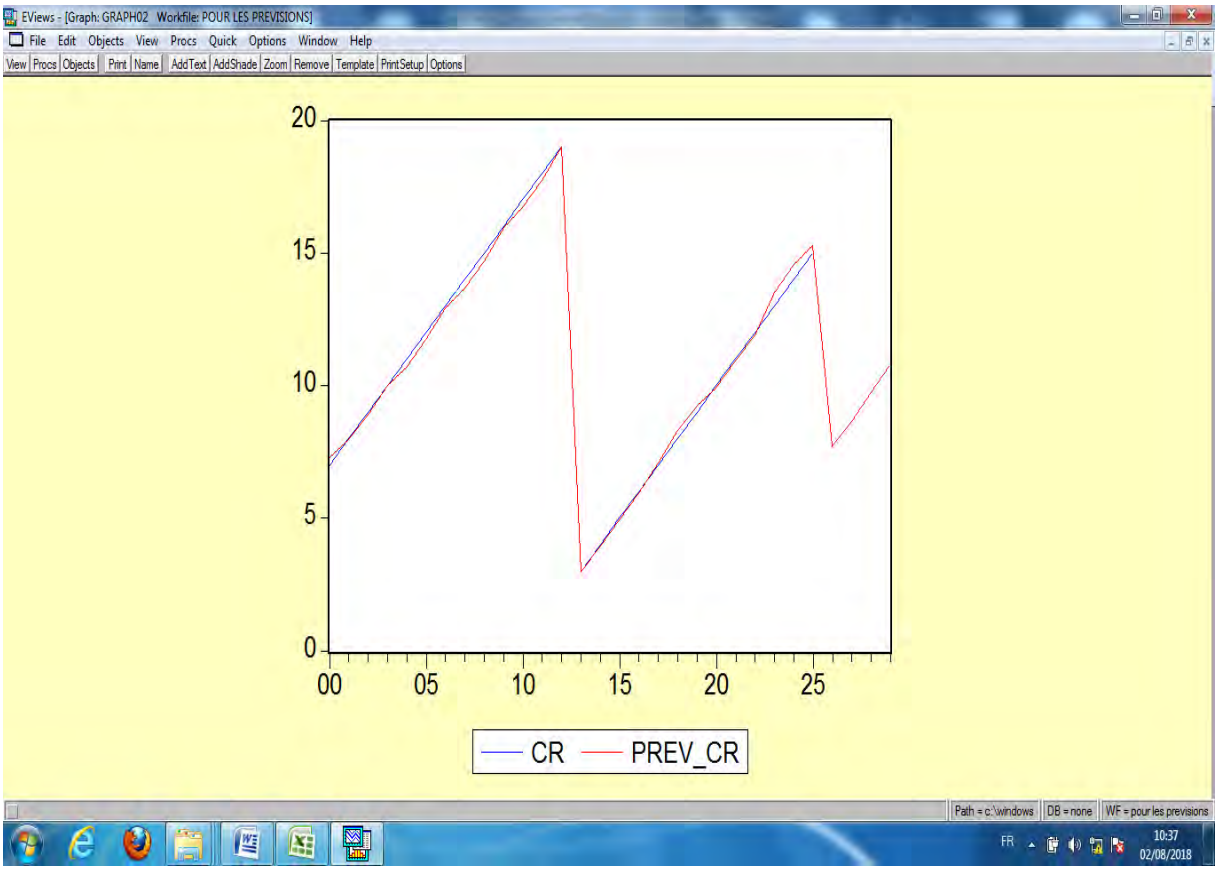


Figure 96: Prévision graphique de l'équation 2: Résultats obtenus avec la banque 1

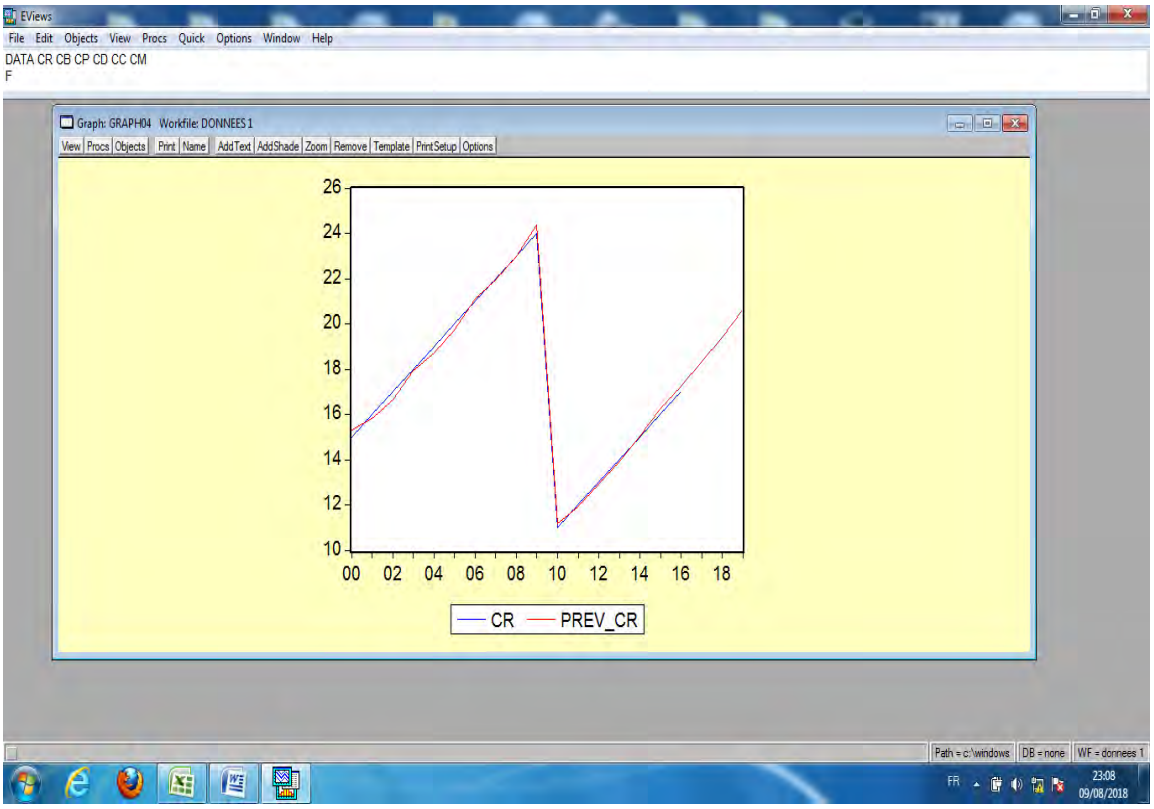


Figure 97:Prévision graphique de l'équation 2: Résultats obtenus avec la banque 2

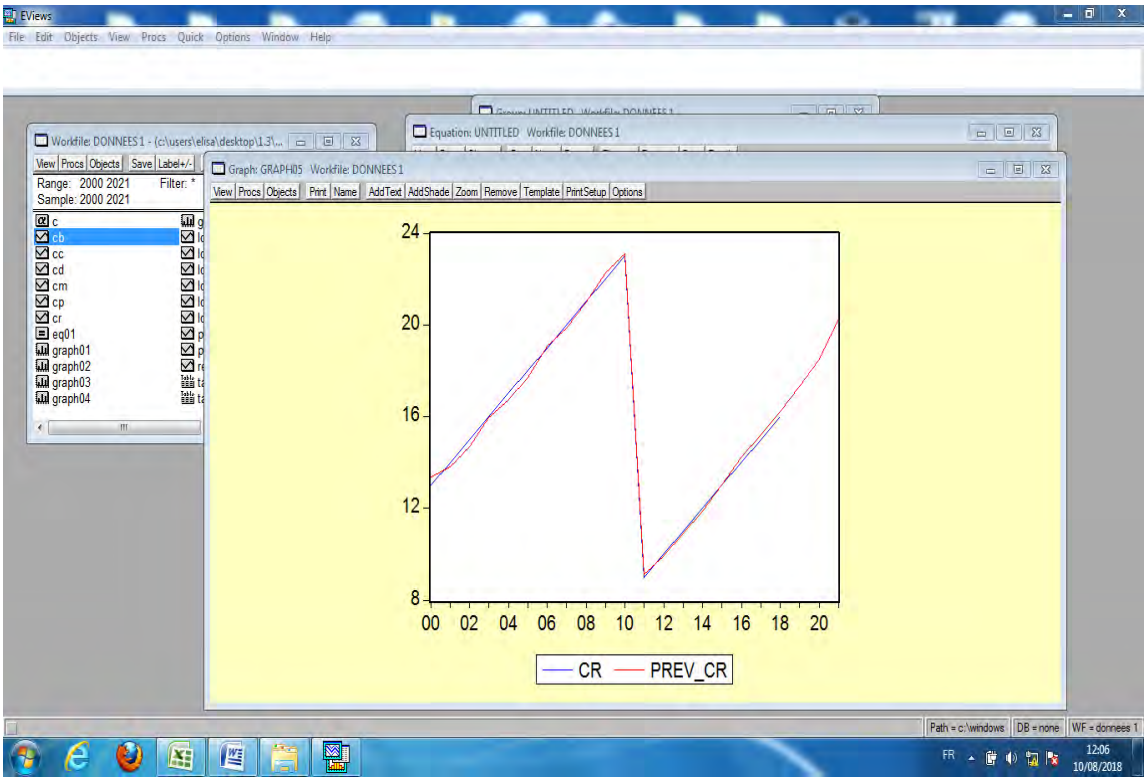


Figure 98:Prévision graphique de l'équation 2: Résultats obtenus avec la banque 3

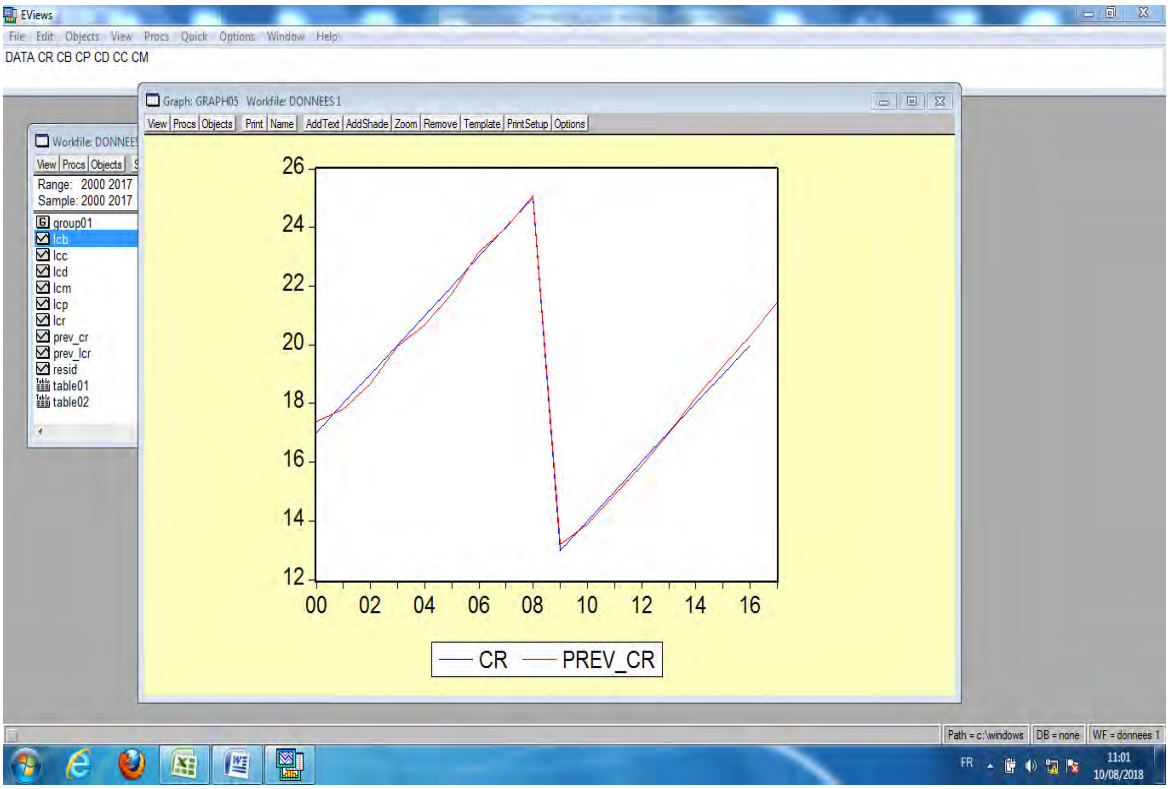


Figure 99:Prévision graphique de l'équation 2: Résultats obtenus avec la banque 4

Interprétation des résultats

A la lecture de ces graphiques, on remarque que les deux types de prévisions suivent la tendance des valeurs actuelles. Ce qui est permet de conclure que les prévisions sont correctes.

Pour finir, nous avons utilisé les critères de prévision MAPE (Mean Absolute Precetenge Errror) et U de Theil(Theil Inequality Coefficient) pour apprécier les performances prévisionnelles de l'équation. Les résultats obtenus avec Eviews sont indiqués ci-après :

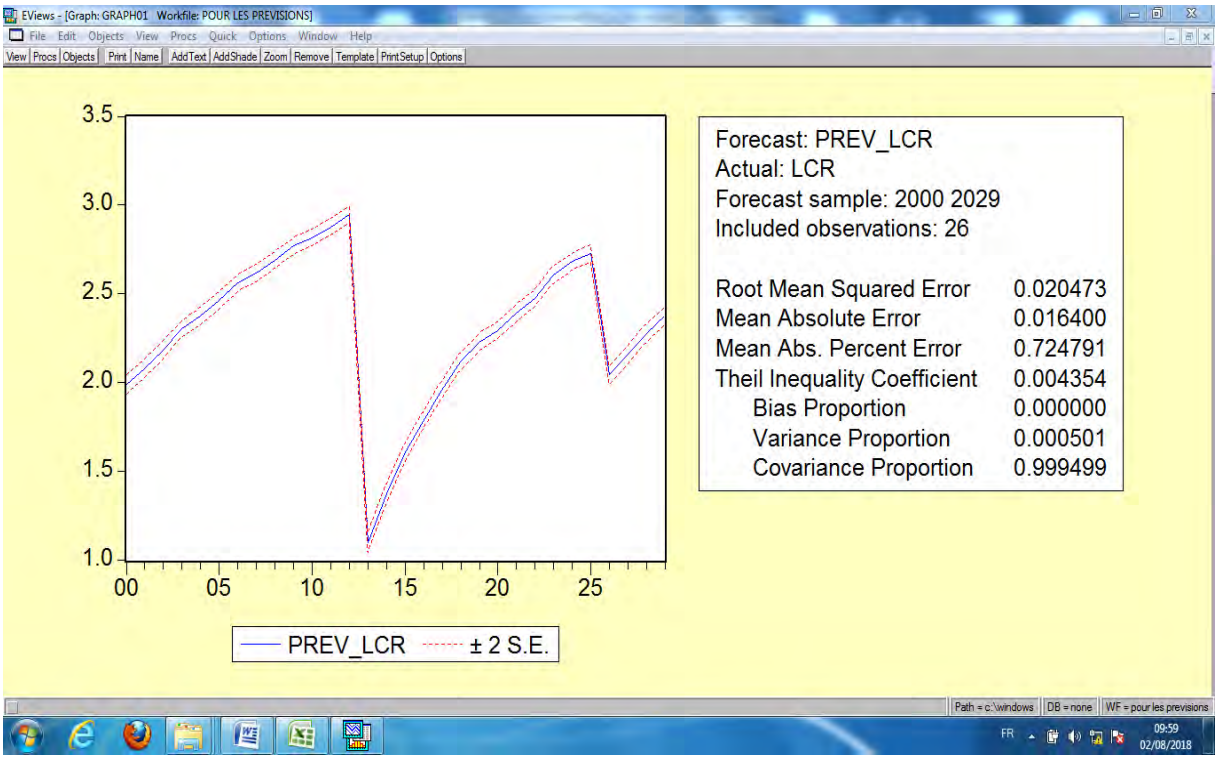


Figure 100: Performance de l'équation 2: Résultats obtenus avec la banque 1

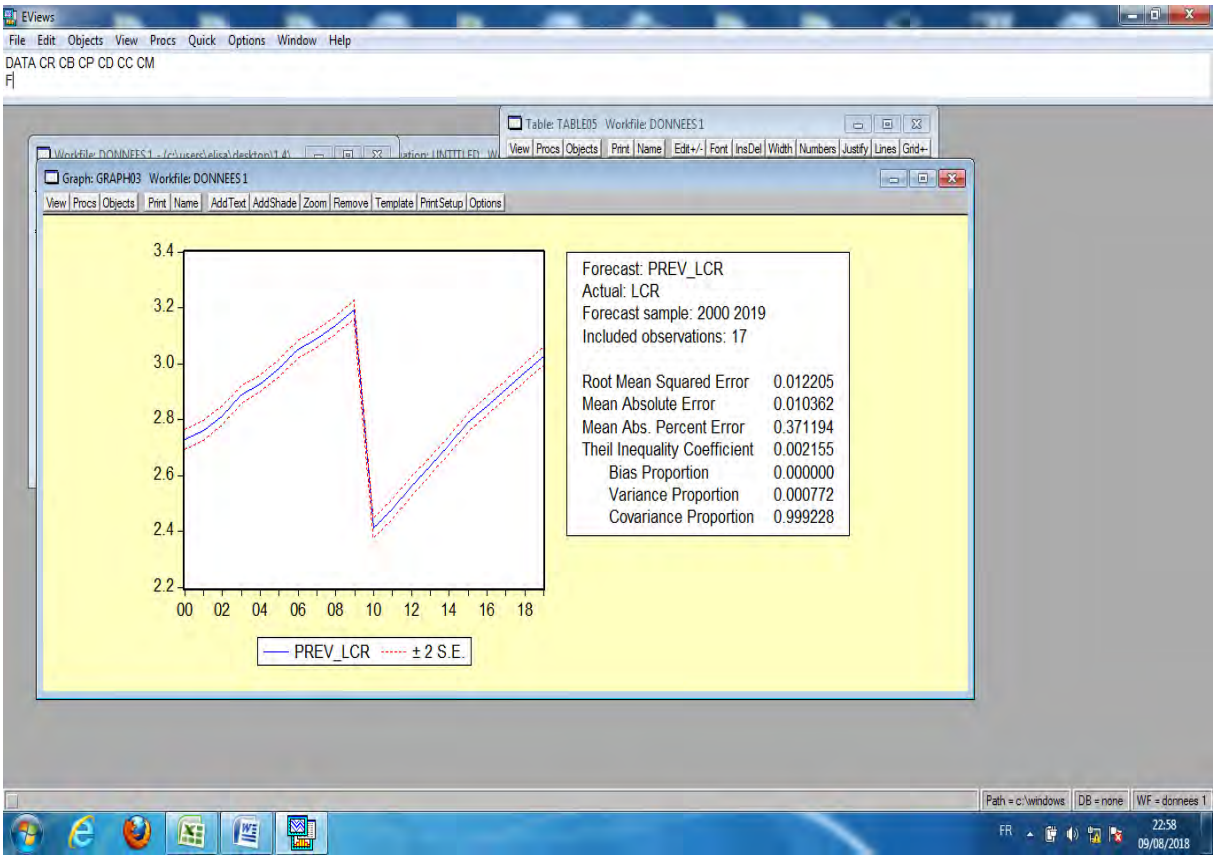


Figure 101: Performance de l'équation 2: Résultats obtenus avec la banque 2

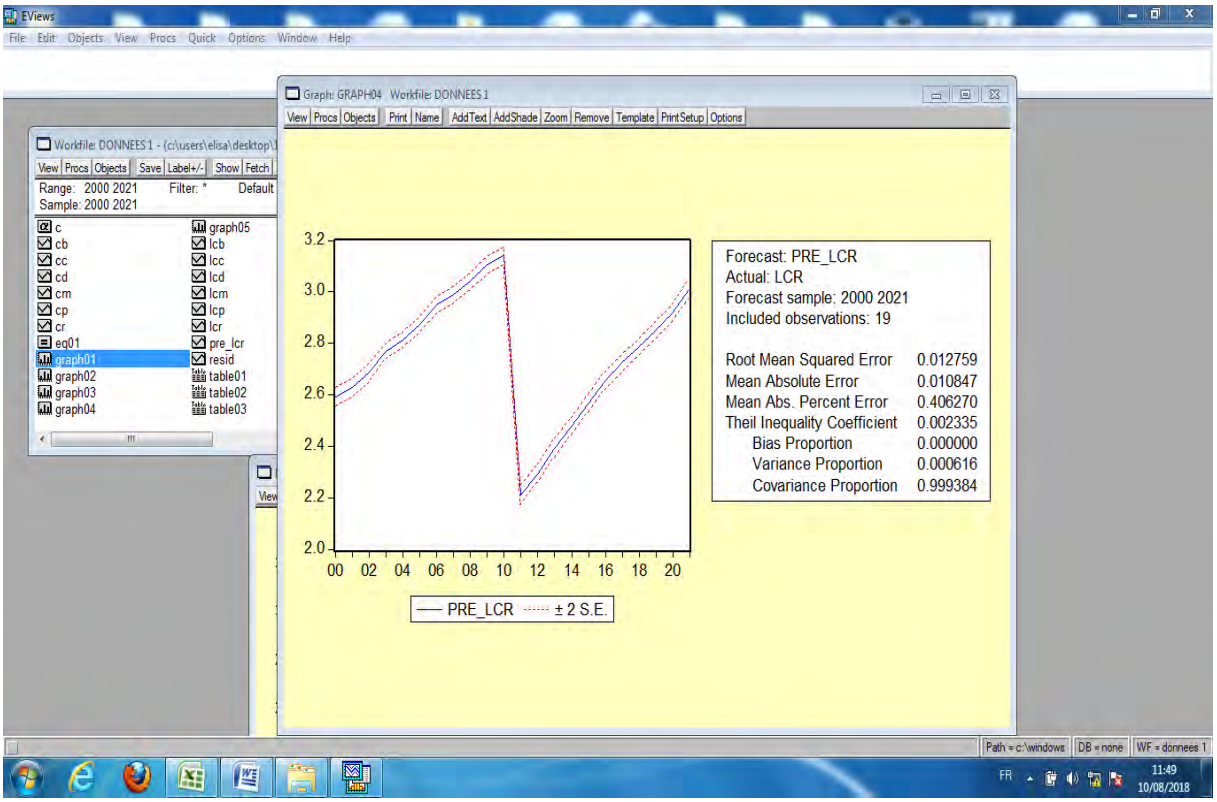


Figure 102: Performance de l'équation 2: Résultats obtenus avec la banque 3

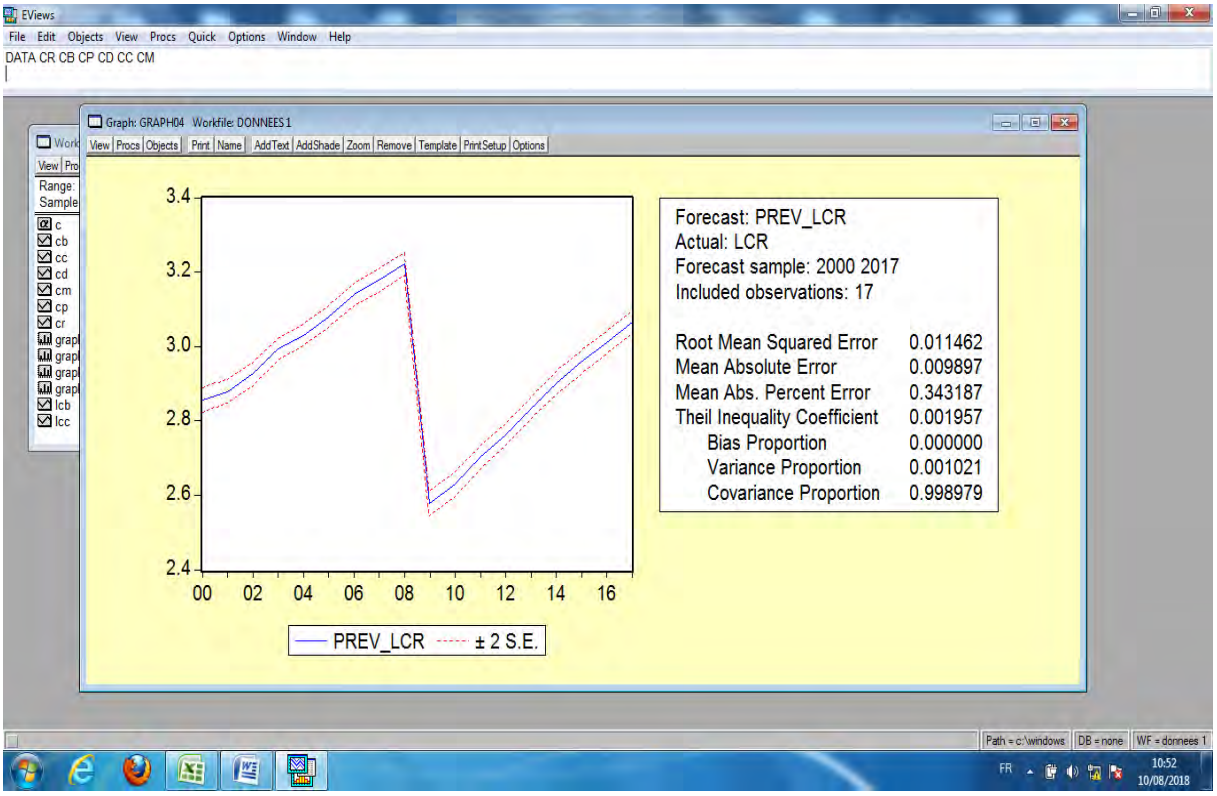


Figure 103: Performance de l'équation 2: Résultats obtenus avec la banque 4

- **Interprétation des résultats**

A l'issu de ces tests, on obtient des erreurs absolues moyennes en pourcentage qui sont inférieures à 1% et des valeurs du critère U de Theil qui sont proches de 0. Ce qui permet de conclure que l'équation a de bonnes performances prévisionnelles.

Ainsi, la réussite de l'ensemble des tests économétriques recommandés sur Eviews nous permet d'aborder les tests qui seront effectués sur R avec les données de tests collectées.

V.3 Tests des modèles et algorithmes

V.3.1 Présentation de l'outil R

L'outil R est un logiciel de statistiques crée par Ross Ihaka & Robert Gentleman. Il est à la fois un langage informatique et un environnement de travail. Les commandes sont exécutées grâce à des instructions codées dans un langage relativement simple, les résultats sont affichés sous forme de texte et les graphiques sont visualisés directement dans une fenêtre spécifique. Ce logiciel sert à manipuler des données, à tracer des graphiques et à faire des analyses statistiques sur ces données **[104].** La bibliothèque tikz permet de créer des schémas. Il n'est pas nécessaire de faire des captures avec cette bibliothèque. Par ailleurs, dans la bibliothèque Igraph, la fonction plot permet de visualiser les graphes, le résultat d'une simulation, etc. Ce flux de la visualisation peut être redirigé dans un fichier tikz. De plus, Igraph est une bibliothèque qui contient plusieurs fonctions de manipulations des graphes. Il existe une version utilisable dans R mais aussi une version utilisable avec le langage Python et le langage C.

V.3.2 Application des équations des modèles

Dans le but de tester les modèles mathématiques initiaux et améliorés, nous avons appliqué les équations et algorithmes y afférents à tous les risques bancaires. Pour cela, nous avons d'abord assigné à chaque risque, sa probabilité de survenance brute et sa gravité potentielle brute en utilisant les échelles de gravité et de probabilité précédemment définies. Par la suite, nous avons identifié le nombre de contrôles propres à chaque risque et affecté à chaque contrôle la valeur du coefficient affecté à sa maturité en utilisant ce qui a été défini en amont.

a. Tests et résultats des modèles 1 et 2

Nous avons d'abord appliqué les équations des modèles 1 et 2 aux risques et contrôles avant de comparer les valeurs obtenues aux données de test collectées au niveau des banques. Le modèle 1 se décline comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i \qquad 4.1.1$$

Les paramètres de ce modèle sont décrits ci-après :

- **P** $_{\text{brute}}$: coefficient affecté à la probabilité de survenance brute du risque; **P** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G** $_{\text{brute}}$: coefficient affecté à la gravité potentielle brute du risque ; **G** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- $\mathbf{m_i}$**:** coefficient affecté à la maturité du contrôle i ; $\mathbf{m_i}$ pouvant prendre la valeur=0, 1 ou 2
- **n** le nombre de contrôles ; n pouvant prendre les valeurs entières comprises entre 0 et 18 au maximum

Nous avons également appliqué les équations du modèle 2 aux risques et contrôles avant de comparer les valeurs obtenues aux données de test collectées en amont. Le modèle 2 se décline comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{n} m_i + cste \qquad 4.1.2$$

Les paramètres de ce modèle sont décrits ci-après :

- **P** $_{\text{brute}}$: coefficient affecté à la probabilité de survenance brute du risque; **P** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G** $_{\text{brute}}$: coefficient affecté à la gravité potentielle brute du risque ; **G** $_{\text{brute}}$ pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- $\mathbf{m_i}$**:** coefficient affecté à la maturité du contrôle i ; $\mathbf{m_i}$ pouvant prendre la valeur=0, 1 ou 2
- **n** le nombre de contrôles ; n pouvant prendre les valeurs entières comprises entre 0 et 18 au maximum
- **Cste** : la constante

Suite à l'implémentation des algorithmes relatifs aux modèles 1 et 2 au niveau de l'outil R, les valeurs obtenues ont été comparées aux données de test qui ont été collectées au niveau des banques. Dans le but d'avoir une représentation graphique permettant de visualiser cette comparaison, les graphes dessinés avec le logiciel R sont représentés ci-dessous :

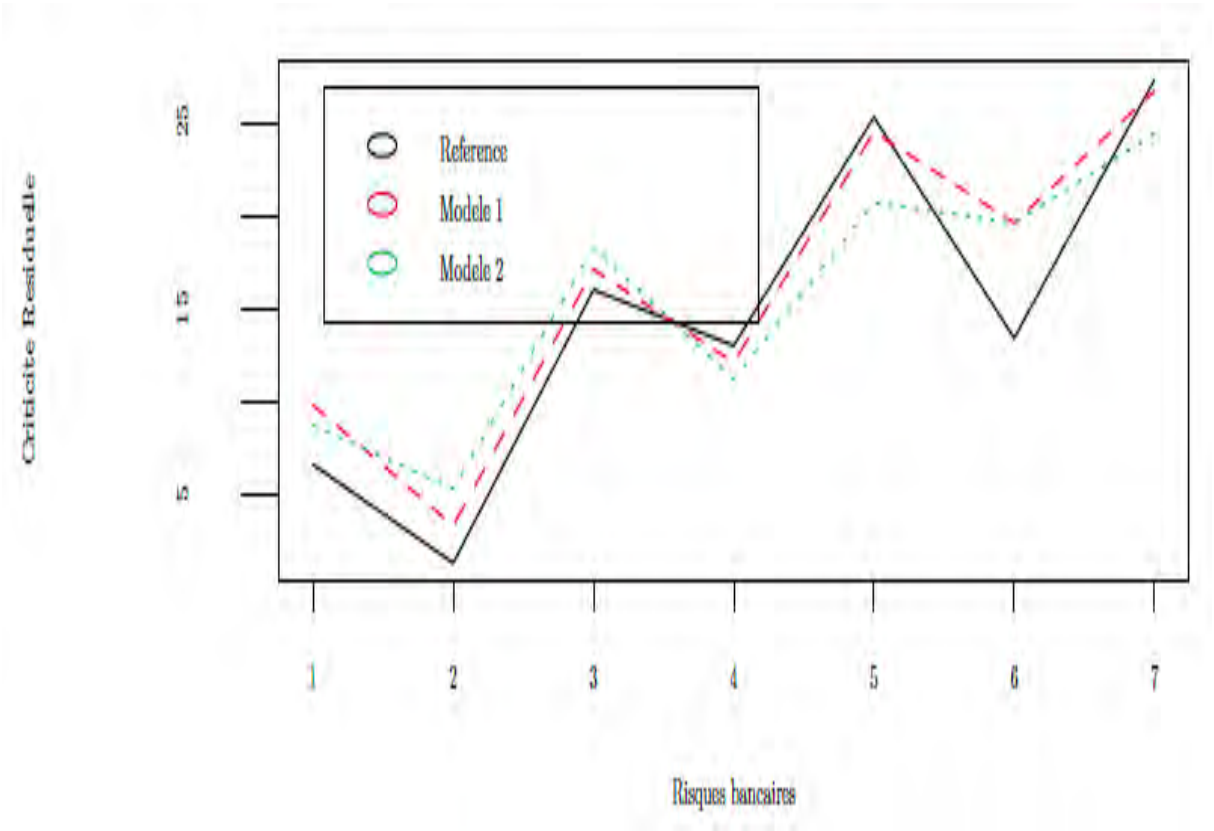


Figure 104:Comparaison entre les modèles initiaux et les données de test par risques bancaires

- **Résultats et Interprétations**

A la lecture de ce graphique, on remarque que les différences entre les valeurs obtenues avec les modèles 1 et 2 et celles des données de test sont relativement faibles et diffèrent selon les catégories de risques. Cela signifie que les deux modèles sont instables. Ce qui conforte les résultats obtenus lors des tests économétriques où nous n'avons pas pu dérouler toute la batterie de tests recommandés et permettant de valider les modèles à cause du défaut de normalité des erreurs. Nous pouvons donc en déduire que ces deux modèles ont en commun cette limite malgré l'existence d'une constante qui tient compte des différentes caractéristiques d'un contrôle au niveau du modèle 2.

Nous avons également testé les modèles améliorés en appliquant les équations et algorithmes y afférents à tous les risques bancaires. Pour cela, nous avons d'abord assigné à chaque risque sa probabilité de survenance brute et gravité potentielle brute en utilisant les échelles précédemment définies. Par la suite, nous avons identifié le nombre de contrôles propres à chaque risque et assigné à chaque contrôle le coefficient affecté à sa maturité sur la base des coefficients définis en amont. Enfin, nous avons comparé les valeurs obtenues aux données de test collectées en amont.

b. Tests et résultats des modèles 3 et 4

Nous avons appliqué les équations du modèle 3 aux risques et contrôles avant de comparer les valeurs obtenues avec les valeurs de test collectées en amont. Le modèle 3 se décline comme suit :

$$C_{résiduelle} = \left[[P_{brute} - \sum_{i=1}^{r} a_i * m_i \right] * \left[G_{brute} - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \right] \quad 4.1.3$$

Les paramètres de ce modèle sont décrits ci-après :

- **m_i, n_j, l_k**: coefficient affecté à la maturité des contrôles préventifs, détectif et correctif ; m_i, n_j, l_k pouvant prendre la valeur=0, 1 ou 2
- **a_i, b_j, c_k**: coefficients affectés aux contrôles préventifs, detectifs et correctifs ; a_i, b_j, c_k pouvant prendre les valeurs la valeur=0 ou 1
- **r, s, t** : nombre de contrôles préventifs, détectif et correctifs ; r, s, t pouvant prendre les valeurs entières comprises entre 0 et 3 au maximum
- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque, **P_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque, **G_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6

Nous avons également appliqué les équations du modèle 4 aux risques et contrôles avant de comparer les valeurs obtenues aux données de tests collectées en amont. Le modèle 4 se décline comme suit :

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \quad 4.1.4$$

Les paramètres de ce modèle sont décrits ci-après :

- **m_i, n_j, l_k**: coefficient affecté à la maturité des contrôles préventifs, detectifs et correctifs ; m_i, n_j, l_k pouvant prendre la valeur=1, 2, 3, 4 ou 5
- **a_i, b_j, c_k**: coefficients affectés aux contrôles préventifs, detectifs et correctifs ; a_i, b_j, c_k pouvant prendre les valeurs la valeur=0 ou 1
- **r, s, t** : nombre de contrôles préventifs detectifs et correctifs ; r, s, t pouvant prendre les valeurs entières comprises entre 0 et 7 au maximum
- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque, **P_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque, **G_{brute}** pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6

Par la suite, les algorithmes relatifs aux modèles 3 et 4 ont été implémentés au niveau du logiciel R. Dans le but d'avoir une représentation graphique, les valeurs obtenues avec les modèles améliorés et celles relatives aux données de test ont été comparées. Cette comparaison est illustrée à travers le graphe dessiné avec le logiciel R indiqué ci-dessous :

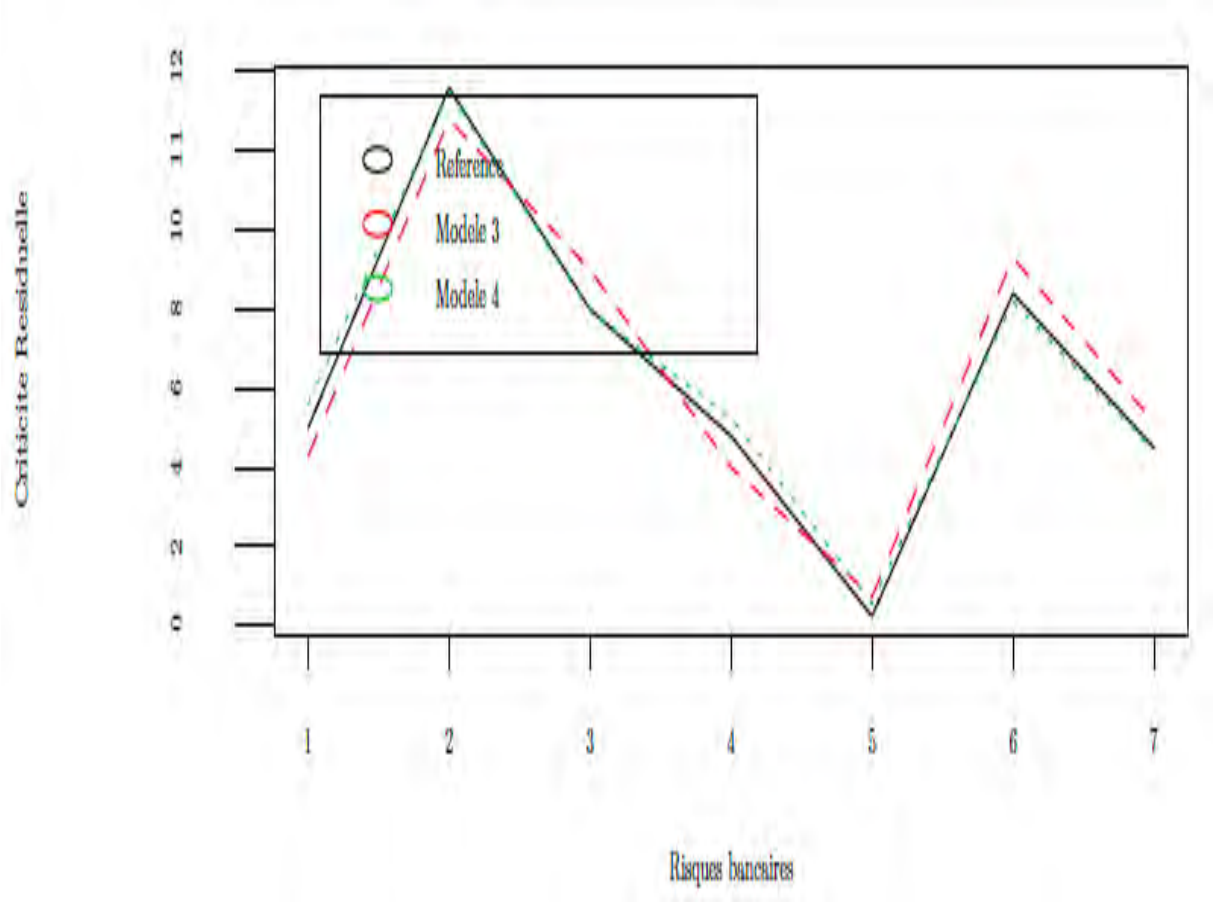


Figure 105: Comparaison entre les modèles améliorés et les données de test par risques bancaires

- **Résultats et Interprétations**

En analysant le contenu du graphique ci-dessus, on remarque que les différences entre les valeurs obtenues avec les modèles 3 et 4 et celles des valeurs de test sont faibles avec le modèle 3 mais très faibles avec le modèle 4. Cela signifie que les valeurs obtenues avec le modèle 4 correspondent mieux aux données de test. Nous pouvons en déduire que le modèle 4 est meilleur et plus stable que le modèle 3 d'autant plus qu'il bénéficie des avantages du troisième modèle tout en ayant un apport supplémentaire à savoir la possibilité de tester plus de contrôles (7 au lieu de 3 pour le modèle 3). De plus, ceci est en parfait accord avec la réussite de tous les tests économétriques recommandés par ce modèle, cela avait permis de valider le modèle 4 d'un point de vue économétrique.

V.3.3 calcul des taux de corrélation

a. Application sur les risques du système d'information

En vue d'éprouver les 4 modèles proposés, on se propose de calculer les taux de corrélation entre les valeurs obtenues avec les modèles et les données de test collectées sur la base des spécificités suivantes propres au système d'information **[34]:**

- Les composants du système d'information (Matériel, Logiciel, Réseaux, Bases de données, Application, Information et Site)
- Les critères de sécurité de l'information (Authentification, Traçabilité, Intégrité, Confidentialité, Non répudiation, Disponibilité et Anonymat)
- Les phases SDLC (Initialisation, Conception, Implémentation, Vérification et Maintenance)
- Les types de vulnérabilités SI (Environnement interne, Collaborations et Partenariat, Non-conformité, Fraude interne et externe, Accès physique et logique, autres)
- Les types d'attaques SI (Ingénierie Social, Vols de données, Codes malveillants Logiciels espions, Attaques réseaux, Attaques web, Attaques physiques et Cryptanalyse, autres)

Pour tester les modèles sur les spécificités du système d'information citées ci-dessus et indépendamment des risques qu'ils contiennent, nous avons d'abord procédé à la classification des risques du système d'information par types de composants SI, par critères de sécurité de l'information, par phases SDLC, par types de vulnérabilités SI et par types d'attaques SI. Par la suite, pour chaque spécificité, nous avons identifié le nombre de contrôles avant de calculer la maturité moyenne de ces contrôles et d'appliquer les équations des quatre modèles. Les valeurs ainsi obtenues avec les modèles ont été comparées aux données de test collectées au niveau des banques en vue de déterminer les taux de corrélation. Les taux de corrélation obtenus par spécificités du système d'information sont indiqués dans Le tableau récapitulatif ci-dessous :

Tableau 17: Taux de corrélation par risques du système d'information

Spécificités Système d'Information	**TAUX DE CORRELATION AVEC LE MODELE 1**	**TAUX DE CORRELATION AVEC LE MODELE 2**	**TAUX DE CORRELATION AVEC LE MODELE 3**	**TAUX DE CORRELATION AVEC LE MODELE 4**
Composants SI	94%	95%	97%	98%
Critères de sécurité	96%	96%	98%	99%
Phases SDLC	95%	96%	98%	99%
Vulnérabilités SI	95%	96%	98%	98%
Attaques SI	95%	96%	98%	98%
MOYENNE	**95%**	**96%**	**98%**	**98%**

- **Résultats et Interprétations**

Le taux de corrélation moyen entre les données des modèles et les données collectées est égal à 95% pour le modèle 1, 96% pour le modèle 2, 98% pour le modèle 3 et 98% pour le modèle 4. Nous pouvons en déduire que les modèles 3 et 4 ont les meilleurs taux de corrélation par risques SI.

Dans l'optique d'étendre les tests des quatre modèles aux autres processus de la banque, nous avons décidé d'appliquer les équations y afférentes à tous les risques bancaires en tenant compte des spécificités suivants **[12]:**

- Les types processus bancaires (Marketing et Commercial, Conformité aux normes et règlementations, Système d'information, Apres Vente et Relation Client, Finances et Comptabilité, Gouvernance et Stratégie, Ressources Humaines, Juridique et Contentieux, Audit et Contrôle)
- Les types de risques bancaires (Crédit, Stratégique, Liquidité, Marché, Politique, Opérationnel et Contentieux)

b. Application des modèles sur les risques bancaires par processus

Pour tester les modèles proposés sur tous les risques bancaires selon leurs processus et indépendamment des risques qu'ils contiennent, nous avons d'abord procédé à la classification des risques bancaires par processus. Ensuite, pour chaque processus, nous avons identifié le nombre de risques bancaires et le nombre de contrôles par risque avant de calculer la maturité moyenne de ces contrôles et d'appliquer les équations des modèles. Enfin, nous avons comparé les valeurs obtenues avec les modèles aux données de test collectées en calculant leurs taux de corrélation par processus comme illustré ci-dessous :

Tableau 18:Taux de corrélation par risques relatifs aux processus bancaires

PROCESSUS	TAUX DE CORRELATION AVEC LE MODELE 1	TAUX DE CORRELATION AVEC LE MODELE 2	TAUX DE CORRELATION AVEC LE MODELE 3	TAUX DE CORRELATION AVEC LE MODELE 4
Marketing et Commercial	94%	98%	96%	99%
Conformité aux normes et réglementations	94%	97%	95%	99%
Système d'information	95%	96%	96%	99%
Apres Vente et Relation Client	95%	98%	95%	99%
Finances et Comptabilité	93%	98%	95%	99%

Gouvernance et Stratégie	94%	98%	95%	99%
Ressources Humaines	95%	98%	95%	98%
Juridique et Contentieux	94%	98%	95%	99%
Audit et Contrôle	95%	98%	95%	98%
MOYENNE	**94%**	**98%**	**95%**	**98%**

- **Résultats et Interprétations**

Le taux de corrélation moyen entre les données des modèles et les données collectées est égal à 94% pour le modèle 1, 98% pour le modèle 2, 95% pour le modèle 3 et 98% pour le modèle 4. Nous pouvons en déduire que les modèles 2 et 4 ont les meilleurs taux de corrélation par risques processus.

c. Application des modèles sur les risques bancaires par types

En vue de tester les modèles proposés sur tous les risques bancaires selon leurs types et indépendamment des risques qu'ils contiennent, nous avons d'abord procédé à la classification des risques bancaires par type. Ensuite, pour chaque type de risques bancaires, nous avons identifié le nombre de contrôles par risque avant de calculer la maturité moyenne de ces contrôles et d'appliquer les équations des modèles. Enfin, nous avons comparé les valeurs obtenues avec les modèles aux données de test collectées en calculant leurs taux de corrélation par type de risques bancaires comme illustré ci-dessous :

Tableau 19:Taux de corrélation par type de risques bancaires

TYPES	TAUX DE CORRELATION AVEC LE MODELE 1	TAUX DE CORRELATION AVEC LE MODELE 2	TAUX DE CORRELATION AVEC LE MODELE 3	TAUX DE CORRELATION AVEC LE MODELE 4
Crédit	94%	96%	95%	98%
Stratégique	90%	98%	96%	98%
Liquidité	95%	95%	95%	98%
Marché	92%	98%	95%	99%
Politique	93%	98%	95%	98%
Opérationnel	96%	98%	95%	99%
Contentieux	97%	98%	95%	98%
MOYENNE	**94%**	**98%**	**95%**	**98%**

Résultats et Interprétations

Le taux de corrélation moyenne entre les données des modèles et les données de test collectées est égal à 94% pour le modèle 1, 98% pour le modèle 2, 95% pour le modèle 3 et 98% pour le modèle 4. Nous pouvons en déduire que les modèles 2 et 4 ont les meilleurs taux de corrélation par types de risques.

Par ailleurs, compte tenu des résultats obtenus à l'issu des trois tests effectuées (risques système d'information, risques bancaires par processus et risques bancaires par types), nous pouvons conclure que :

- Le modèle 4 a un taux de corrélation qui s'élève à 98% aussi bien pour les risques du système d'information que pour les risques bancaires par processus ou par type. De plus, tous les tests économétriques sont réussis avec ce modèle d'où sa stabilité. Il est donc indiqué pour le calcul des risques résiduels de toutes les catégories de risques.
- Le modèle 3 a un taux de corrélation avec la référence qui est égal à 98% lorsqu'il s'agit des risques du système d'information, il serait donc mieux adapté au calcul des risques résiduels du système d'information ; cependant, il est instable.
- Les modèles 2 a un taux de corrélation qui est égal à 98% lorsqu'il s'agit des risques bancaires par processus et par types. il serait donc le mieux adapté à ces types de risques. Cependant, il est instable aussi.
- Le modèle 1 a le plus faible taux de corrélation avec la référence comparé aux autres modèles. De plus, il est instable ; il n'est donc pas très indiqué.

V.3.4 Analyse des valeurs résiduels

Dans le but d'éprouver les modèles proposés, nous nous sommes intéressés aux valeurs résiduelles entre les valeurs relatives aux modèles proposés et les données de test collectées en amont au niveau des banques.

a. Valeurs résiduelles entre les modèles initiaux et les données de référence

Les valeurs résiduelles correspondent à la différence entre les valeurs obtenues avec les modèles et les données de test collectées. Pour ce faire, nous allons considérer le graphique combiné schématisant les données de test et les valeurs obtenues avec les modèles 1 et 2.

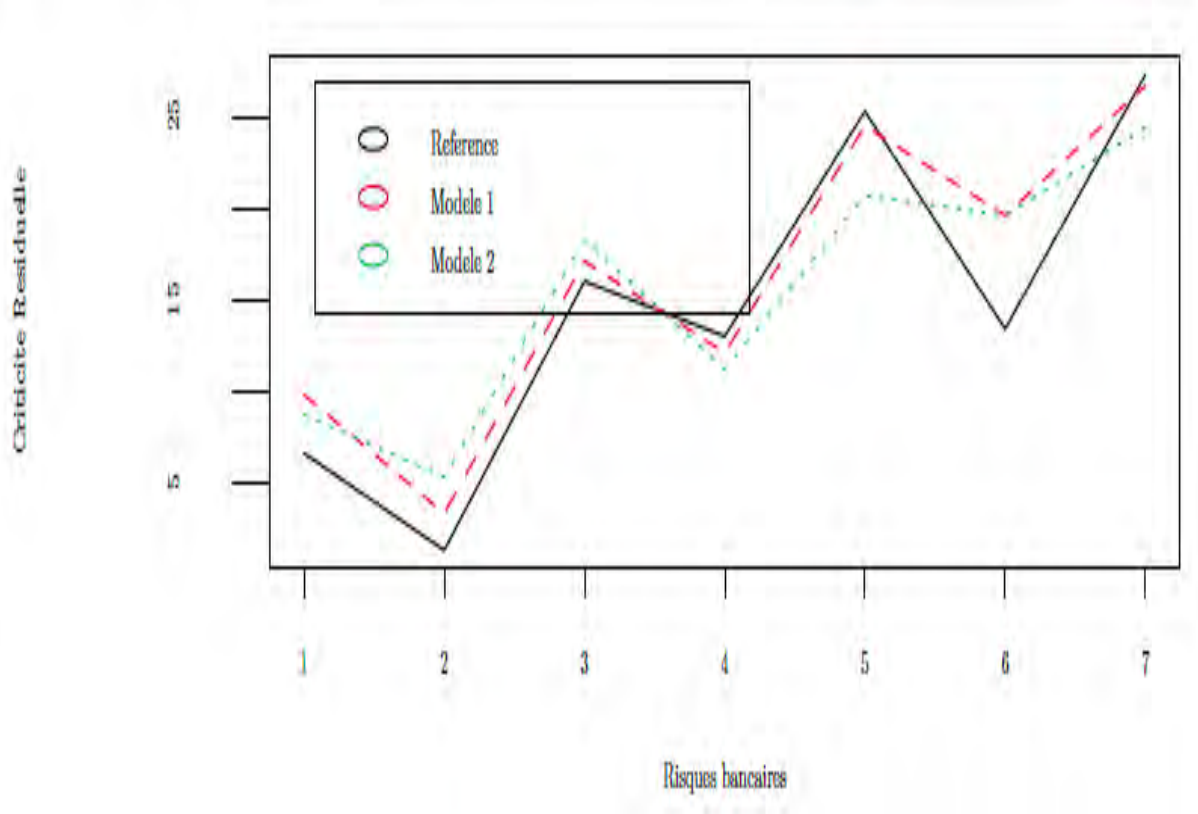


Figure 106: Comparaison entre les modèles initiaux et les données de test par risques bancaires

Résultats et Interprétations

- La plupart des valeurs relatives au modèle 1 et 2 sont supérieures ou inferieures aux données de test. Cela signifie que la plupart des valeurs résiduelles entre les valeurs des modèles initiaux et les données de test sont positives ou négatives.
- Quelques valeurs obtenues avec les modèles initiaux correspondent aux données collectées, cela signifie que peu de valeurs résiduelles sont égales à zéro.

Nous pouvons donc conclure que les modèles initiaux couvrent le spectre des valeurs de référence. Pour l'échantillon de test utilisé, on note des écarts entre les valeurs relatives aux modèles initiaux et les données de test, cela montre l'instabilité induite par le défaut réussite des tests économétriques réalisés en amont pour ces modèles.

b. Valeurs résiduelles entre les modèles améliorés et les données de référence

Pour analyser ces valeurs résiduelles, nous allons considérer le graphique combiné schématisant les données de test et les valeurs des modèles 3 et 4.

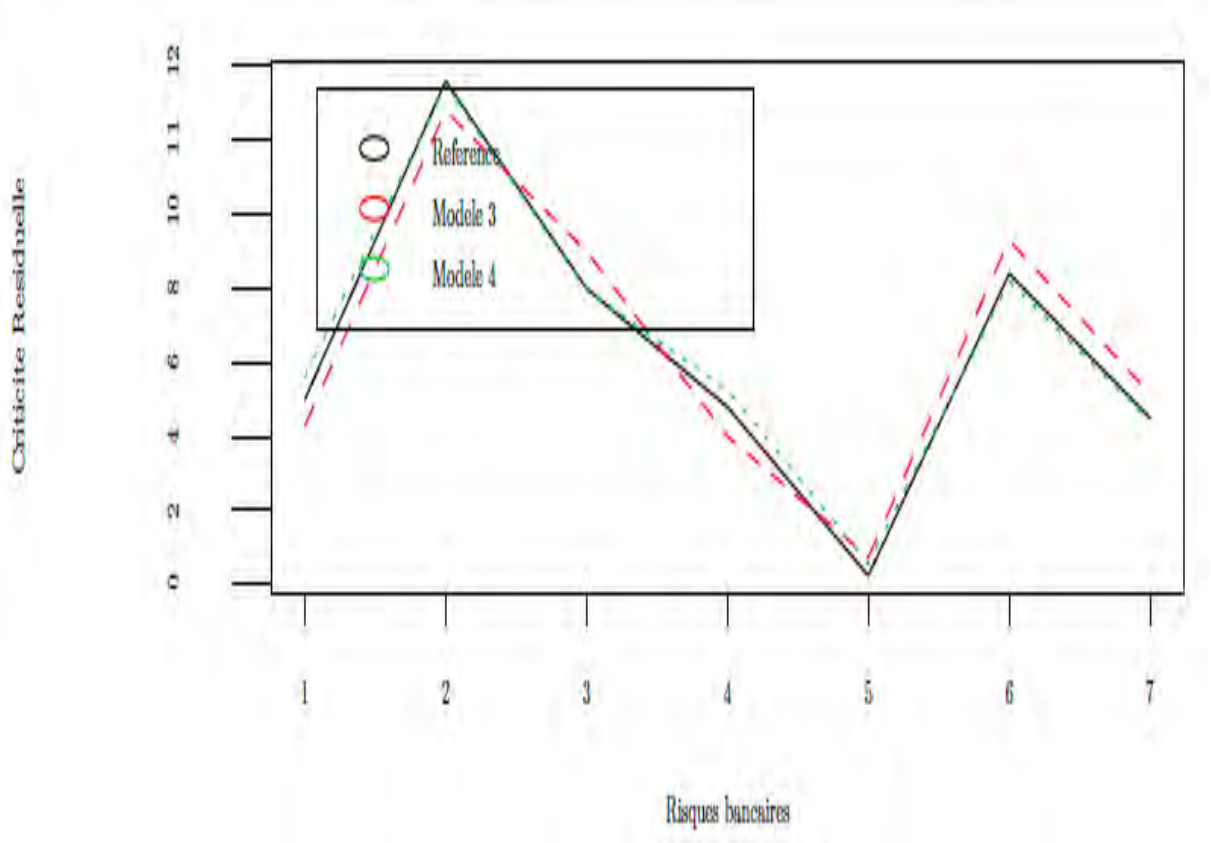


Figure 107: Comparaison entre les modèles améliorés et les données de test par risques bancaires

Résultats et Interprétations

- Plusieurs valeurs relatives aux modèles 3 et 4 sont supérieures ou inferieures aux données de test. Cela signifie que plusieurs valeurs résiduelles entre les valeurs les modèles améliorés et les données de test sont positives ou négatives.
- Beaucoup valeurs obtenues avec les modèles améliorés correspondent aux données collectées. Cela signifie que beaucoup de valeurs résiduelles sont égales à zéro.

Nous pouvons donc conclure que les modèles améliorés couvrent tout le spectre des valeurs de test. En plus, les valeurs y afférentes sont plus proches des données de test que celles des modèles initiaux. Pour l'échantillon de test utilisé, on note des écarts minimes entre les valeurs relatives au modèle 4 et les données de test. Cela montre la stabilité du modèle 4 qui a été prouvée lors des tests économétriques réalisés en amont.

En définitive, nous pouvons conclure que le modèle 4 a le meilleur taux de corrélation quel que soit la nature des risques concernés, de plus il est stable et se caractérise par la réussite de tous les tests économétriques. Par conséquent il constitue la meilleure modélisation des risques résiduels bancaires.

V.4 Comparaison des modèles proposés

V.4.1 Corrélation, homogénéité, paramètres et variables

A l'issu des tests effectués sur les différents modèles proposés au niveau des logiciels R et Eviews, les résultats sont globalement satisfaisants. En effet, les taux de corrélation entre les modèles et les données varient de 94% à 98%, le modèle 4 demeure le meilleur. Pour mieux cerner les spécificités de chaque modèle, nous avons dressé le tableau comparatif suivant :

Tableau 20: Comparaison des spécificités des quatre modèles proposés

MODELES	Taux de corrélation moyen pour les risques SI	Taux de corrélation moyen pour les risques bancaires	Stabilité	Nombre de paramètres	Nombre de constante
MODELE 1	**95%**	**94%**	**NON**	**4**	**0**
MODELE 2	**96%**	**98%**	**NON**	**4**	**1**
MODELE 3	**98%**	**95%**	**NON**	**11**	**0**
MODELE 4	**98%**	**98%**	**OUI**	**11**	**0**

En analysant les taux de corrélation moyens, on remarque que :

- Les taux de corrélation obtenus avec les modèles 1, 2 et 3 sont différents selon la catégorie de risques, cela signifie que les modèles 1, 2 et 3 ne sont pas stables.
- Les taux de corrélation obtenus avec le modèle 4 sont les mêmes quel que soit la catégorie de risques, cela signifie que le modèle 4 stable.
- Le modèle 1 a un taux de corrélation moyen égal à 94.5% avec la référence alors que le modèle 2 un taux de corrélation moyen égal à 97 % avec la référence cela signifie que le modèle 2 correspondrait mieux à la référence que le modèle 1.
- Le modèle 3 a un taux de corrélation moyen égal à 97.5% avec la référence alors que le modèle 4 un taux de corrélation moyen égal à 98 % avec la référence cela signifie que le modèle 4 est plus conforme à la référence.

En analysant les autres éléments de comparaison, il s'avère qu'il y a moins de paramètres pour les modèles initiaux que pour les modèles améliorés et que le modèle 2 est le seul à avoir une valeur constante. Les modèles initiaux seraient donc plus conviviaux que les modèles améliorés cependant ils ont les plus faibles taux de corrélation avec la référence et ne sont pas stables. C'est la raison pour laquelle, nous recommandons le modèle 4 pour le calcul des risques résiduels bancaires.

V.4.2 Résultats des tests économétriques

Avant la réalisation des tests évoqués ci-dessus, toute la panoplie de tests économétriques recommandés avait été déroulée sur les deux équations de régressions linéaires correspondantes aux modèles mathématiques initiaux et améliorés. Pour mieux cerner l'impact des résultats obtenus avec les tests, nous avons dressé un tableau comparatif en tenant compte des quatorze critères tests préconisés :

Tableau 21: Résultats des tests économétriques sur les modèles de régressions linéaires

Tests économétriques	**Objectifs**	**Première équation de régressions linéaires**	**Seconde équation de régressions linéaires**
Estimation des paramètres par la méthode des MCO	Déterminer les variables et constante du modèle	OK	OK
Coefficient de détermination	Mesurer le degré de corrélation entre la variable à expliquer et les variables explicatives du modèle	OK	OK
Test de Student	S'assurer que les variables explicatives ont une influence significative sur la variable à expliquer par le modèle	OK	OK
Test de Fisher	S'assurer que le modèle est globalement bon	OK	OK
Test de Jarque-Bera	Permet de vérifier que les variables de l'équation suivent une loi normale	KO	OK
Test de white	Permet d'apprécier le comportement du modèle par rapport aux erreurs en tenant compte de la régression du carré du résidu	NA	OK
Test d'ARCH	Permet d'apprécier le comportement du modèle par rapport aux erreurs en tenant compte de la régression autorégressive	NA	OK
Test de Durbin Watson	Permet de vérifier qu'il n'y a pas de corrélation des erreurs	NA	OK
Test de Ramsey	Permet de vérifier que le modèle est bien spécifié	NA	OK
Test de Show	Permet de vérifier que les paramètres du modèle sont stables	NA	OK

Tests de Cusum et Cusum carré	Permettent de caractériser les instabilités structurelles et les instabilités ponctuelles du modèle	NA	OK
Simulation du modèle	Permet de savoir si le modèle a un bon pouvoir prédictif	NA	OK
Prévision du modèle	Permet de conclure que les prévisions du modèle sont correctes	NA	OK
Performance du modèle	Permet de conclure que le modèle a de bonnes performances prévisionnelles	NA	OK

En analysant le tableau ci-dessus, on remarque que :

- Pour la première équation de régressions linéaires, 3 des 14 tests économétriques sont réussis. Cela signifie que les variables et constantes de cette équation ont été déterminés, qu'il existe une forte corrélation entre la variable à expliquer et les variables explicatives du modèle. De plus, toutes les variables explicatives de ce modèle sont significatives et l'équation est globalement correcte. Cependant l'échec du troisième test prouve que les variables du modèle ne suivent pas une loi normale, c'est la raison pour laquelle les autres tests économétriques n'ont pas pu être réalisés.
- Concernant la seconde équation de régressions linéaires, tous les tests économétriques préconisés ont été réussis. Cela signifie que les variables et constantes de cette équation ont été déterminées, qu'il existe une forte corrélation entre la variable à expliquer et les variables explicatives de l'équation. De plus toutes les variables explicatives sont significatives et l'équation est globalement correcte. Par ailleurs, les variables du modèle suivent une loi normale, cela prouve la normalité des erreurs et nous permet de poursuivre la réalisation des autres tests économétriques. Ainsi, la réussite des tests de White et Arch nous permet de conclure que les estimations des paramètres de l'équation par la méthode des moindres carrées sont optimales. Par ailleurs, le fait que les tests de Durbin Watson, Ramsey et Show soient également réussis permet de conclure qu'il n'y a pas de corrélation des erreurs, que le l'équation est bien spécifiée et qu'elle est stable. Les résultats obtenus avec les tests de Cusum et Cusum Carré nous ont permis de conclure que les instabilités structurelles de l'équation sont corrigées avec le temps et que les instabilités ponctuelles sont dues aux erreurs marginales sur les données collectées au niveau des banques. Pour finir, les résultats obtenus avec les simulations et prévisions permettent de conclure que cette seconde équation a un bon pouvoir prédictif et qu'elle a de bonnes performances prévisionnelles. Par conséquent, l'équation de régressions linéaires correspondant aux modèles mathématiques améliorés est la meilleure.

V.5 Avantages des modèles proposés

V.5.1 Avantages divers

Les modèles proposés permettent d'obtenir la criticité résiduelle des risques à travers une appréciation optimale de la maturité des contrôles et une automatisation du processus d'estimation de leur impact sur les risques brutes sans pour autant passer par d'innombrables séances de travail. Les principes de base définis en amont pour proposer les quatre modèles ainsi que les résultats des tests effectués sur les modèles nous ont permis d'identifier les avantages communs listés ci-après :

- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'efforts de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles sur les risques
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels

L'apport du deuxième modèle par rapport au premier modèle est indiqué ci-dessous :

- Le taux de corrélation moyen entre les valeurs du modèle et les données de test est passé de 94.5% à 97%.

Les apports du troisième modèle par rapport au deuxième modèle sont :

- Le taux de corrélation moyen entre les valeurs du modèle et les données de test est passé de 97% à 97.5%
- Les types de contrôles (préventif, detectif et correctif) sont prises en compte dans l'équation du modèle 3

Le quatrième modèle a eu un apport considérable dans la mesure où il a permis de corriger les limites des précédents modèles. Ses avantages sont listés ci-après :

- Le taux de corrélation entre les valeurs du modèle et les données de test est passé de 97% pour le modèle 3 à 98% pour le modèle 4.
- Les types de contrôles (préventif, detectif et correctif) sont aussi prises en compte dans l'équation du modèle 4
- La réussite de tous les quatorze tests économétriques recommandés
- La stabilité car les taux de corrélation sont constants quel que soit le type de risques

Les apports des différents modèles qui sont relatifs au gain de temps moyen seront explicités dans le prochain paragraphe.

V.5.2 Gain de temps moyen

De toute évidence, les équations des modèles proposés permettent de gagner du temps dans l'estimation des risques résiduels. Dans l'optique de mieux apprécier l'utilité de notre modélisation, nous nous sommes proposés de mesurer le gain de temps moyen obtenu grâce à nos modèles de la façon suivante. Nous nous sommes munis de chronomètre lors des séances d'évaluation des risques résiduels avec la méthode RSCA afin de mesurer la durée totale nécessaire pour estimer l'ensemble des risques résiduels. Ensuite, nous avons divisé cette durée par le nombre de risques et de sessions en vue d'obtenir le temps moyen d'estimation d'un risque résiduel avec la méthode RSCA, cette durée est appelée Y. Par la suite, cet exercice est répété pour chaque modèle proposée et la durée totale nécessaire à l'estimation de tous les risques résiduels est consignée à la fin de la séance. Le temps moyen nécessaire à l'estimation d'un risque résiduel avec un modèle donné correspond la durée totale divisée par le nombre de risques, cette durée est appelée X. Le gain de temps moyen par risque avec ce modèle est obtenu en faisant la soustraction entre Y et X. L'ensemble des gains de temps moyen obtenus grâce aux modèles proposés sont indiqués ci-après:

Tableau 22:Gain de temps moyen obtenu avec les différents modèles

Nombre de risques	**Gain moyen de temps obtenu avec le modèle 1**	**Gain de temps moyen obtenu avec le modèle 2**	**Gain de temps moyen obtenu avec le modèle 3**	**Gain de temps moyen obtenu avec le modèle 4**
1	10 minutes	10 minutes	12 minutes	15 minutes
50	8 heures	8 heures	10 heures	12.5 heures
100	16 heures	16 heures	20 heures	25 heures
150	24 heures	24 heures	30 heures	37.5 heures
200	32 heures	32 heures	40 heures	50 heures
250	40 heures	40 heures	50 heures	62.5heures
300	48 heures soit 6 jours/hommes	48 heures soit 6 jours/hommes	60 heures soit 7.5 jours/hommes	75 heures soit 9 jours/hommes

Comme illustré dans le tableau ci-dessus, les modèles initiaux permettent à chaque évaluateur de gagner 48 heures dans l'évaluation résiduelle de 300 risques. Sachant qu'une journée de travail est étalé sur 8 heures, le gain de temps moyen équivaut à 6 jours/ homme par évaluateur. Quant aux modèles améliorés, ils permettent de gagner beaucoup plus de temps soit 7.5 jours/hommes avec le modèle 3 et 9 jours/hommes pour le modèle 4 lors de l'évaluation de 300 risques résiduels soit une augmentation qui varie entre 1.5 et 3

jours/hommes par rapport aux modèles initiaux. Sachant que les évaluations se font durant des séances de travail nécessitant la participation de plusieurs collaborateurs ; dans le cas où le nombre d'évaluateurs est égale à 10, ce gain de temps moyen est alors multiplié par 10. Ainsi, on obtient 60 jours/hommes gagnés avec les modèles initiaux et 90 jours/hommes gagnés avec le modèle 4. Ce gain de temps est considérable pour les banques et permet d'éviter la perte de temps pour chacun des différents évaluateurs. De plus, ce gain de temps moyen pourra être utilisé pour définir et déployer de nouveaux contrôles en vue de mieux maitriser les différentes types de risques dans un secteur bancaire en profonde mutation et caractérisé des clients de plus en plus exigeants.

V.6 Contribution de nos travaux

Dans le cadre de cette thèse, nous avons d'abord décrit les concepts et définitions propres à la gestion des risques et au contrôle interne dans le but de lever toutes équivoques et de s'accorder sur les terminologies qui seront utilisées tout au long de nos travaux comme illustré au niveau du chapitre 1. En nous appuyant sur une étude bibliographique couvrant aussi bien le management des risques informatiques que le management des risques bancaires et en tenant compte de notre expertise et de l'expérience de nos interlocuteurs dans les différentes banques avec lesquelles nous avons collaboré dans le cadre de nos travaux, nous avons déclinée les différentes typologies de risques bancaires. Nous avons également fait un focus sur les actions de maitrise de ces risques qui permettent de ramener les risques résiduels à un niveau acceptable comme indiqué dans le chapitre 2.

Nous nous sommes également appesantis sur les méthodologies permettant d'obtenir les risques résiduels qui représentent le niveau de risque qui subsiste après la mise en œuvre de l'ensemble des controles. Par la suite, nous avons décliné les spécificités et limites des principales méthodologies utilisées ; il s'agit notamment de la méthode outillée et de la méthode RSCA. En ce qui concerne la méthode RSCA qui demeure la plus utilisée, elle se compose de plusieurs étapes préliminaires, à savoir, la définition des objectifs de processus, l'identification des risques liés à chaque processus, l'évaluation brute des risques identifiés et l'évaluation de la maturité des contrôles mis en œuvre. Nous avons analysé en profondeur ses différentes variantes et avons constaté que cette méthode présente un certain nombre de limites à savoir : une perte de temps, un investissement personnel et un certain niveau d'expertise de la part des évaluateurs mais aussi de potentiels erreurs d'estimation du risque résiduel. Nous nous sommes alors penchés sur les récents travaux visant à alléger la méthode RSCA notamment celle qui propose une soustraction entre les risques inhérents et les contrôles implémentés pour obtenir les risques résiduels**.** Cependant il n'y a pas de précision dans la manière de soustraire et les valeurs des modèles ne sont pas comparées aux données de référence. Nous avons alors entrepris de proposer des modèles permettant de calculer les risques résiduels et d'effectuer différents tests en vue d'éprouver les modèles proposés avant de les valider comme expliqué dans le chapitre 3.

Dans l'optique de proposer les modèles permettant de calculer les risques résiduels bancaires, nous avons d'abord identifié les 10 caractéristiques spécifiques à un contrôle s et défini 4 principes découlant d'une exploitation documentaire rigoureuse avant de proposer les modèles initiaux qui sont basés sur les caractéristiques et la maturité des contrôles. Pour définir les paramètres des équations relatifs à ces modèles, nous avons proposé des coefficients affectés à la probabilité de survenance brute des risques, à la gravité potentielle brute des risques et à la maturité des contrôles. Nous obtenons alors les modèles mathématiques 1 et 2 qui seront d'abord traduits en équations de régressions linéaires puis en algorithmes comme indiqué dans le chapitre 4. Par la suite, nous avons souhaité appliquer toute la batterie de tests économétriques préconisés à ces modèles au niveau d'Eviews en utilisant les données d'apprentissage collectées au niveau des banques. Cependant, suite à la réussite de 3 tests économétriques sur les quatorze recommandés, nous n'avons pas pu réaliser les autres tests économétriques compte tenu du défaut de normalité des erreurs. Cela ne nous a pas empêché d'implémenter les algorithmes relatifs à ces modèles au niveau de logiciel R et déterminer le taux moyen de corrélation entre les données de test collectées au niveau des banques et les valeurs obtenues avec ces modèles initiaux. Le taux moyen de corrélation s'est révélé être égal à 94.5% pour le modèle 1 et 97% pour le modèle 2. Ces résultats ont fait l'objet de publications dans **[107] et [108].** Il faut noter que ces résultats étaient assez satisfaisants mais ne nous permettait pas de conclure sur la validité de ces modèles initiaux comme indiqué dans le chapitre 5. Ainsi, suite à l'analyse de ces résultats obtenus lors de l'ensemble des tests réalisés sur les modèles initiaux, les axes d'amélioration de notre modélisation étaient d'une part, proposer de nouveaux modèles pour lesquels tous les tests économétriques seront réussis dans le but de faire des simulations et des prévisions et d'autre part, stabiliser ces nouveaux modèles tout en obtenant une meilleure corrélation avec les données de test collectées .

Compte tenu des limites des modèles initiaux, nous avons décidé de changer d'approche lors la définition des modèles améliorés, ainsi ces modèles seront basés sur les typologies et la maturité des contrôles. Pour ce faire, nous avons commencé par identifier les 3 typologies de contrôles et défini 7 principes de base qui en tiennent compte. Pour définir les paramètres des équations relatifs à ces modèles améliorés, nous avons également proposé des coefficients affectés à la probabilité de survenance brute des risques, à la gravité potentielle brute des risques, à la maturité et au type de contrôles. Nous obtenons alors les modèles mathématiques 3 et 4 qui seront d'abord traduits en équations de régressions linéaires puis en algorithmes comme indiqué dans le chapitre 4. Par la suite, divers tests économétriques ont été réalisés sur ces modèles au niveau d'Eviews en utilisant les données d'apprentissage collectées au niveau des banques. Les résultats étaient très satisfaisants avec la réussite de l'ensemble des tests économétriques recommandés. Il faut noter qu'à ce niveau, nous avons rencontré d'énormes difficultés pour obtenir les données d'apprentissage notamment les valeurs spécifiques aux typologies des contrôles.

En effet, les modèles améliorés contiennent des paramètres différents de ceux existants au niveau des banques. Il a donc fallu assister aux séances d'évaluation des banques, expliquer les principes de ces nouveaux modèles et les appliquer séance tenante pour obtenir les données d'apprentissage y afférentes. En dépit de cette difficulté, cette démarche a eu des avantages pour les banques à travers la classification de leurs différents types de risques et une meilleure visibilité sur leurs typologies de contrôles. En ce qui nous concerne, l'avantage réside dans le fait que nous ayons pu collecter des données réelles qui nous ont permis d'éprouver ces modèles améliorés avant validation. Pour finir nous avons implémenté les algorithmes relatifs à ces modèles au niveau de l'outil R et déterminé le taux moyen de corrélation entre les données de tests collectées au niveau des banques et les valeurs obtenues avec ces modèles. Ce taux est égal à 97.5% pour le modèle 3 et 98% pour le modèle 4**.** Il faut noter que pour le modèle 4, le taux de corrélation obtenu est le même aussi bien pour les risques du système d'information que pour tous les risques bancaires par processus ou par type. Ces résultats ont d'ailleurs fait l'objet de publications dans [**105], [106] et [109].** De plus, le modèle 4 est stable et offre le meilleur gain de temps moyen, ce qui est très satisfaisant et permet de conclure sur la validité de ce modèle comme indiqué au niveau du chapitre 5.

En définitive, tous les objectifs visés par l'amélioration des modèles initiaux ont été atteints avec les modèles optimisés dites améliorés et plus particulièrement avec le modèle 4. En effet, les trois premiers modèles ont les avantages communs listés ci-après :

- Une seule séance de travail pour l'estimation de la criticité résiduelle du risque
- Une diminution des compromis en cas de désaccord entre les évaluateurs
- Peu d'expertise et d'efforts de la part des évaluateurs grâce au modèle
- Elimination des différences d'appréciation de l'impact des contrôles des controles
- Evaluation optimale de la maturité des contrôles par les évaluateurs
- Allègement et facilitation de l'estimation des risques résiduels
- Réduction du taux d'erreur dans l'estimation des risques résiduels

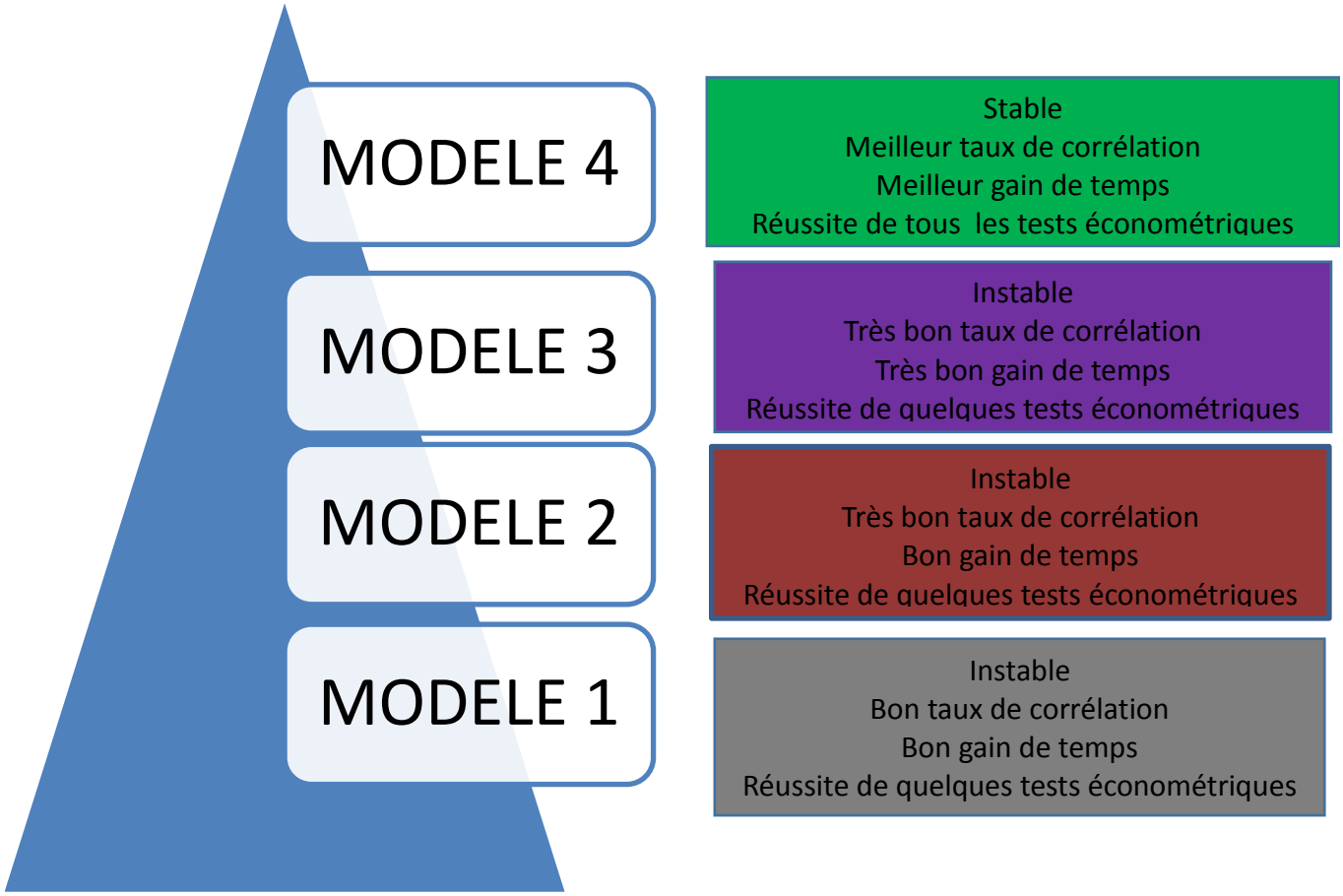
Le quatrième modèle a eu un apport considérable dans la mesure où il a permis de corriger toutes les limites des précédents modèles. Ses avantages supplémentaires sont listés ci-après :

- Le gain de temps moyen lors de l'estimation des risques résiduels est passé de 10min à 15 min par risque
- Le taux de corrélation entre les valeurs du modèle 4 et les données de test est passé de 94.5% à 98%
- Les types de contrôles (préventif, detectif et correctif) sont prises en compte dans l'équation du modèle 4
- La réussite de tous les quatorze tests économétriques recommandés dans Eviews
- La stabilité car les taux de corrélation sont constants quel que soit le type de risques

Le récapitulatif des spécificités propres à chacun des quatre modèles proposés est illustré dans le schéma ci-dessous :

Figure 108: Récapitulatif des spécificités des quatre modèles proposés

Le schéma décliné ci-dessous, nous indique que le modèle 4 est stable, possède le meilleur taux de corrélation moyen et le meilleur gain de temps moyen. De plus, tous les tests économétriques se sont déroulés avec succès. Cela prouve que ce modèle est valide. Pour toutes ces raisons, nous recommandons l'utilisation du modèle 4 pour le calcul des risques résiduels bancaires.



Dans le cadre de cette thèse les articles ci-après ont été publiés :

1. M.Ndaw, G.Mendy and S.Ouya, A quantification model of internal control impact on banking risks using FMECA, IEEE, 5th World Congress on Information and Communication Technologies (WICT), Marrakech, 2015

2. M.Ndaw, G.Mendy and S.Ouya, Modeling the impact of controls on information system risks, World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, Londres, 2016

3. M.Ndaw, G.Mendy and S.Ouya, Improving the quantification model of internal control impact on banking risks using FMECA, World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, Paris, 2016

4. M.Ndaw, G.Mendy, S.Ouya and D.Seck: Quantify the Maturity of Internet Banking Security Measures in WAEMU Banks, 1st EAI International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas EAI, INTERSOL, DAKAR, APRIL 11–12, 2017

5. M.Ndaw, G.Mendy and S.Ouya, Modeling the Effect of Security Measures on Electronic Payment Risks, 13th International Conference on Information Assurance and Security (IAS), Marrakech, 2018

Conclusion

Dans le but d'approfondir les tests et d'éprouver les modèles proposés, nous nous sommes proposés de dérouler toute la batterie de tests économétriques recommandés sur les deux équations de régressions linéaires correspondants aux modèles mathématiques initiaux et améliorés. A l'issu de ces tests, il s'avère que tous les tests sont réussis pour la seconde équation de régressions linéaire. Nous avons également procédé à l'implémentation des algorithmes relatifs aux quatre modèles mathématiques au niveau du logiciel R. Suite aux résultats obtenus sur les risques du système d'information puis sur les autres risques bancaires, il est apparu que le modèle 4 a le meilleur taux de corrélation avec les données de test qui s'élève à 98%. Par ailleurs, les résultats des tests effectués montrent que quel que soit le niveau de probabilité de survenance des risques, le niveau de gravité potentielle des risques, le niveau de maturité des contrôles et les typologies de risques et de controles au niveau des banques avec lesquelles nous avons collaboré, les résultats sont très satisfaisants pour le modèle 4. Nous avons clôturé ce chapitre par une déclinaison des différents avantages des modèles, une analyse comparative des modèles et une synthèse de la contribution de nos travaux dont la recommandation préconise l'utilisation du modèle 4 pour le calcul des risques résiduels bancaires. Nous estimons donc avoir atteint l'objectif final visé par nos travaux qui était de proposer un modèle de calcul du risque résiduel qui tiennent compte de la réalité des banques et qui sont facilement applicables.

Chapitre 6 : Mise en œuvre opérationnelle des modèles proposés

Introduction

Dans l'optique d'accompagner et de faciliter la tâche au personnel des banques, il est nécessaire d'exposer la façon de collecter les données et d'utiliser les modèles mathématiques et algorithmiques proposés pour le calcul de la criticité résiduelle des risques bancaires. Ce chapitre s'inscrit dans ce cadre et permet de décrire de manière spécifique la mise en œuvre des modèles proposées.

6.1 Mise en pratique du modèle mathématique

A titre de rappel, nous avons retenu le modèle 4 pour le calcul de la criticité résiduelle des risques bancaires. Ce modèle se décline comme suit.

$$C_{résiduelle} = P_{brute} * G_{brute} - \sum_{i=1}^{r} a_i * m_i - \sum_{j=1}^{s} b_j * n_j - \sum_{k=1}^{t} c_k * l_k \qquad 4.1.4$$

Les paramètres de ce modèle sont décrits ci-après :

- **P_{brute}** : coefficient affecté à la probabilité de survenance brute du risque, P_{brute} pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **G_{brute}** : coefficient affecté à la gravité potentielle brute du risque, G_{brute} pouvant prendre la valeur 1, 2, 3, 4, 5 ou 6
- **a_i, b_j, c_k**: coefficients affectés aux contrôles préventifs, detectifs et correctifs ; a_i, b_j, c_k pouvant prendre les valeurs la valeur=0 ou 1
- **m_i, n_j, l_k**: coefficients affectés à la maturité des contrôles préventifs, detectifs et correctifs ; m_i, n_j, l_k pouvant prendre la valeur=0, 1 et 2 pour le modèle 3 ou la valeur=1, 2, 3, 4 et 5 pour le modèle 4
- **r, s, t** : nombre de contrôles préventifs, detectifs et correctifs ; r, s, t pouvant être égal au nombre de 3 au maximum pour le modèle 3 et 7 au maximum pour le modèle 4

Pour utiliser ce modèle, il faut collecter au niveau de la banque, les valeurs de **P_{brute}, G_{brute}, a_i, b_j, c_k, m_i, n_j, l_k, r, s et t** de la façon suivante :

Pour les valeurs de **P_{brute} et G_{brute}**, il faut identifier et évaluer l'ensemble des risques de la banque. L'identification des risques consiste à attribuer à chaque risque un libellé, une cause, une conséquence et un code spécifique. Quant à l'évaluation du risque brute, elle consiste à estimer la probabilité de survenance brute**(P_{brute})** et la gravité potentielle brute**(G_{brute})** avec les échelles décrites ci-dessous :

Tableau 23: Echelle de la Probabilité de Survenance brute du risque

Echelle de la Probabilité de Survenance brute du risque	
Coefficient	**Signification**
1	Très peu probable
2	Peu probable
3	Probable
4	Très probable
5	Certain
6	Très Certain

Selon cette échelle, les coefficients affectés à la probabilité de survenance brute du risque ont la valeur 1,2, 3, 4, 5 et 6. Ainsi, lors de l'évaluation de la probabilité de survenance brute de chaque risque, le coefficient approprié est assigné au risque concerné.

La gravité potentielle brute du risque est définie comme étant une estimation des impacts potentiels du risque sur la réalisation des objectifs de la banque. L'échelle utilisée pour évaluer la gravité brute potentielle des risques est déclinée ci-après:

Tableau 24:Echelle de la Gravité potentielle brute du risque

Echelle de la Gravité potentielle brute du risque	
Coefficient	**Signification**
1	Très peu grave
2	Peu grave
3	Grave
4	Très grave
5	Situation de crise
6	Crise majeure

Selon cette échelle, les coefficients affectés à la gravité potentielle brute du risque ont les valeurs 1, 2, 3, 4, 5 ou 6. Ainsi, lors de l'évaluation de la gravité potentielle brute de chaque risque, le coefficient approprié est assigné au risque concerné.

Concernant les valeurs de $\mathbf{a_i}$, $\mathbf{b_j}$, $\mathbf{c_k}$, elles sont obtenues comme suit :
Le coefficient affecté aux controles préventifs ($\mathbf{a_i}$) dépend essentiellement du fait que le contrôle soit préventif ou non. Ainsi, si le contrôle est préventif, le coefficient qui lui est affecté est égal à 1, dans le cas échéant, le coefficient qui lui est affecté est égal à 0 comme indiqué dans le tableau ci-dessous.

Tableau 25: Coefficients affectés aux contrôles préventifs

Echelle des contrôles préventifs		
Descriptif	**Signification**	**Coefficients affectés aux contrôles préventifs**
préventif	Le contrôle agit sur la probabilité de survenance du risque brute	1
non préventif	Le contrôle n'a pas d'effet sur la probabilité de survenance du risque brut	0

Les coefficients affectés aux controles de type detectif et correctif indiqués ci-après :

Tableau 26: Coefficients affectés aux contrôles detectifs

Echelle des contrôles detectifs		
Descriptif	**Signification**	**Coefficients affectés aux contrôles detectifs**
détectif	Le contrôle agit sur la gravité potentielle du risque	**1**
non détectif	Le contrôle n'a pas d'effet sur la gravité potentielle du risque	**0**

Le coefficient affecté aux controles detectifs **(b_j)**dépend du fait que le contrôle est détectif ou non. Ainsi si le contrôle est détectif, le coefficient qui lui est affecté est égal à 1, dans le cas échéant, le coefficient qui lui est affecté est égale à 0 comme indiqué dans le tableau ci-dessus.

Tableau 27: Coefficients affectés aux contrôles correctifs

Echelle des contrôles correctifs		
Descriptif	**Signification**	***Coefficients affectés aux contrôles correctifs***
correctif	Le contrôle agit sur la gravité potentielle du risque	1
non correctif	Le contrôle n'a pas d'effet sur la gravité potentielle du risque	0

Le coefficient affecté aux controles correctifs **(c_k)** dépend du fait que le contrôle est correctif ou non. Ainsi si le contrôle est correctif, le coefficient qui lui est affecté est égale à 1, dans le cas échéant, le coefficient qui lui est affecté est égale à 0 comme indiqué dans le tableau ci-dessus.

Pour obtenir les valeurs de **m_i, n_j, l_k,** il faut associer à chaque type de contrôle, son niveau de maturité comme indiquée ci-dessous.

$\mathbf{m_i}$ correspond au coefficient affecté à la maturité du contrôle préventif

$\mathbf{n_j}$ correspond au coefficient affecté à la maturité du contrôle detectif

$\mathbf{l_k}$ correspond au coefficient affecté à la maturité du contrôle correctif

L'identification des contrôles consiste à définir des règles appropriées de réduction des risques et des procédures adéquates à appliquer de façon efficace en vue d'apporter l'assurance que les niveaux de risques résiduels ne dépassent pas le niveau d'appétence au risque défini par le management. Evaluer un contrôle consiste à lui attribuer un coefficient affecté à la maturité du contrôle selon l'échelle de maturité définie ci-après.

Tableau 28: Coefficients affectés à la maturité des contrôles du modèle 4

Echelle de maturité des contrôles			
Valeur	**Descriptif**	**Signification**	**Coefficients affectés à la maturité des contrôles**
1	Inexistant	Le contrôle n'est pas défini	1
2	Informel	Le contrôle est défini mais elle n'est pas formalisée	2
3	Systématique	Le contrôle est défini et opérationnel	3
4	Intégré	Le contrôle est efficace, traçable et autoévalué	4
5	Optimisé	Le contrôle est managé et reporté et archivé	5

Il faut également identifier les valeurs de **r**, **s, t** représentants respectivement le nombre de contrôles préventifs, detectifs et correctifs par risque.

Pour mettre en œuvre ce modèle, il suffit d'appliquer l'équation sur Excel en utilisant les données collectées.

6.2 Mise en pratique du modèle algorithmique

L'algorithme correspondant au modèle 4 est indiqué ci-dessous :

Algorithme 4.3.5 Criticité résiduelle optimisée

Entrées : P, G, A, L, R, B, M, S, C, N, T

Sorties : Criticité

Précondition : R+S+T=7

Début

Retourne P*G – (prévention (A, L, R) – détection (B, M, S) – correction (C, N, T)

Fin

NB : pour le modèle 3 : la dernière instruction est la suivante :

Retourne (P - (prévention (A, L, R)) * (G– détection (B, M, S) – correction (C, N, T))

Dans l'algorithme **4.3.5**, nous avons calculé la criticité résiduelle des risques correspondant au modèle 4. Il prend en entrée :

- P : Probabilité de survenance brute des risques
- G : Gravité potentielle brute des risques
- un vecteur A : représente le coefficient affecté à la maturité des contrôles préventifs
- un vecteur L : représente le coefficient affecté aux contrôles préventifs,
- R qui représente le nombre de contrôles préventifs
- un vecteur B : représente le coefficient affecté à la maturité des contrôles detectifs
- un vecteur M : représente le coefficient affecté aux contrôles detectifs
- S qui représente le nombre de contrôles detectifs
- un vecteur C: représente le coefficient affecté à la maturité des contrôles correctifs
- un vecteur N : représente le coefficient affecté aux contrôles correctifs
- T qui représente le nombre de contrôles correctifs

La sortie de l'algorithme **4.3.5** représente une mesure représentant la criticité résiduelle optimisée. Elle doit vérifier la contrainte S+R+T=3 pour le modèle 3 et S+R+T=7 pour le modèle 4 pour les raisons évoquées en amont.

Les trois fonctions algorithmiques qui apparaissent dans l'instruction sont relatives à la maturité des contrôles préventifs, à la maturité des contrôles detectifs et la maturité de contrôles correctifs ; elles sont décrites ci-après :

Algorithme 4.3.2. Maturité des contrôles préventifs

Fonction prévention (A, L, R :entier) : entier

```
Début
        Prévent <- 0
        Pour i de 1 à R faire
                Prévent <- Prévent + A* L
        Fin Pour
        Retourne Prévent
Fin
```

Dans l'algorithme **4.3.2**, nous avons modélisé la maturité des contrôles préventifs. Il prend en entrée un vecteur A qui représente le coefficient affecté à la maturité des contrôles préventifs**,** un vecteur L qui représente le coefficient affecté aux contrôles préventifs et R qui représente le nombre de contrôles préventifs. Les valeurs de A, L er R sont indiquées ci-dessous :

- Les valeurs de A sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4
- ai, bj, ck: coefficients affectés aux contrôles, compte tenu des coefficients affectés à la maturité des contrôles préventifs
- Les valeurs de L sont 0 ou 1, compte tenu des coefficients affectés aux contrôles préventifs
- Les valeurs de R= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles préventifs

La sortie de cet algorithme correspond à une mesure représentant la maturité de contrôles préventifs.

Algorithme 4.3.3 Maturité des contrôles détectifs

```
Fonction détection (B, M, S : entier) : entier
Début
    Détec <- 0
    Pour i de 1 à S faire
        Détec <- Détec + B* M
    Fin Pour
    Retourne Détec
Fin
```

Dans l'algorithme **4.3.3**, nous avons modélisé la maturité des contrôles detectifs. Il prend en entrée un vecteur B qui représente le coefficient affecté à la maturité des contrôles detectifs, un vecteur M qui représente le coefficient affecté aux contrôles detectifs et S qui représente le nombre de contrôles detectifs. Les valeurs de B, M et S sont indiquées ci-dessous :

- Les valeurs de B sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4, compte tenu des coefficients affectés à la maturité des contrôles detectifs
- Les valeurs de M sont 0 ou 1, compte tenu des coefficients affectés aux contrôles detectifs
- Les valeurs de S= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles detectifs

La sortie de cet algorithme est une mesure représentant la maturité de contrôles detectifs.

Algorithme 4.3.4 Maturité des contrôles correctifs

Fonction correction (C, N, T:) : entier

Début

Corec <- 0

Pour i de 1 à T faire

Corec <- Corec + C * N

Fin Pour

Retourne Corec

Fin

Dans l'algorithme **4.3.4,** nous avons modélisé la maturité des contrôles correctifs. Il prend en entrée un vecteur C qui représente le coefficient affecté à la maturité des contrôles correctifs, un vecteur N qui représente le coefficient affecté aux contrôles préventifs et T qui représente le nombre de contrôles correctifs. Les valeurs de C, N et T sont indiquées ci-dessous :

- Les valeurs de C sont 0, 1 ou 2 pour le modèle 3 et 1, 2, 3, 4 et 5 pour le modèle 4 compte tenu des coefficients affectés à la maturité des contrôles correctifs
- Les valeurs de N sont 0 ou 1, compte tenu des coefficients affectés aux contrôles correctifs
- Les valeurs de T= 0 à 3 au maximum pour le modèle 3 et 0 à 7 au maximum pour le modèle 4, compte tenu du nombre de contrôles correctifs

La sortie de cet algorithme constitue une mesure de la maturité de contrôles correctifs.

Ainsi, nous venons de décliner les trois fonctions algorithmiques ainsi que la fonction principale permettant d'obtenir la criticité résiduelle avec le modèle 4. Pour utiliser ce modèle algorithmique, il suffit d'implémenter les algorithmes y afférents dans langage de programmation de votre choix.

Conclusion

Ce chapitre nous permis d'expliquer la façon de mettre en œuvre les modèles mathématiques et algorithmiques proposés pour le calcul des risques résiduels bancaires. Cela permettra aux banques d'être efficaces et efficients dans l'estimation de leurs risques résiduels. Ces niveaux de risques résiduels devront être comparés à l'appétence au risque définie par la banque en vue de trancher sur l'efficacité ou non des dispositifs de maitrise émis en place.

Conclusion générale

Depuis plusieurs années, les banques ont adopté une démarche de gestion des risques rigoureuse même si l'on note encore des disparités dans le niveau maitrise de ces risques. Le niveau de maturité des contrôles face aux risques dépend de plusieurs facteurs, tels que les activités de contrôle déployées ou la culture du risque **[11].** L'évolution des modes de vie et du pouvoir d'achat a contribué à renforcer et à favoriser l'émergence de banques éthiques. En effet, la clientèle est mieux informée, plus exigeante et de plus en plus procédurière, ce qui est à l'origine de l'implantation dans les banques, d'une solide culture juridique, du renforcement des règles de déontologie, du respect aux accords de Bale **[112]** et de la conformité aux normes et réglementations en vigueur. A cela s'ajoute, la problématique de la sécurisation des moyens de paiement électronique compte tenu de l'importance grandissante des grands réseaux internationaux du paiement par carte en l'occurrence Visa et Mastercard mais aussi des opérateurs non-bancaires comme les opérateurs télécoms. En effet, l'arrivée de nouvelles solutions comme le portemonnaie électronique et surtout le paiement par téléphone mobile font que le système d'information bancaire est de plus en plus vulnérable. D'où la nécessité de maitriser également ces nouveaux risques susceptibles d'être à l'origine différents types de fraudes pouvant avoir des conséquences néfastes pour les banques et les clients. Dans ce contexte, la direction du système d'information joue un rôle majeur dans la démarche de gestion des risques bancaires. Et ce, par le biais de contributions indirectes en particulier dans les domaines de la formation et de la sécurité informatique mais également de façon directe à travers le traitement de ses propres risques liés aux systèmes d'information **[29**]. Le rôle de la direction du système d'information dans la démarche de gestion des risques est proportionnel au niveau de maturité de l'entreprise en matière de gestion des risques. En effet, elle agit souvent comme un moteur dans la mise en place d'une démarche globale de gestion des risques. Les moyens par lesquels la direction du système d'information peut participer à la démarche de gestion des risques sont nombreux, il s'agit notamment de la création d'applications informatiques destinées à diminuer certains risques, de la vérification du bon fonctionnement de la gestion intégrée des risques , de la mise en place d'outils anti-fraude, de l'élaboration des indicateurs de type conformité aux normes sécuritaires informatiques et du développement d'outils consacrés à la gestion des risques.

Il est difficile de maitriser tous les risques bancaires, car les problématiques actuelles sont nombreuses et complexes dans un contexte d'enjeux et d'évolutions. Toutefois, les banques devraient relever le défi d'un contrôle interne mature et efficace malgré le caractère manuel de certaines tâches. Parmi les tâches manuelles, on peut citer l'estimation de la criticité

résiduelle des risques qui nécessite beaucoup de séances de travail et un certain niveau d'expertise de la part des évaluateurs. Il appartient aux administrateurs de la banque de déterminer le niveau de risque qu'il est prêt à accepter que l'on appelle appétence au risque. Le management, quant à lui, est responsable de la conception, de la mise en œuvre et de la supervision des dispositifs de contrôle interne et de gestion des risques. Dans ce contexte, les risques doivent être évalués de manière continue et les activités de contrôle doivent être conçues pour répondre aux risques spécifiques de l'entité concernée au niveau de la banque. Pour faire face à ce défi tant organisationnel que méthodologique, les banques utilisent le plus souvent la méthode RSCA basée sur l'AMDEC qui permet de faire une analyse des modes de défaillance, de leurs effets et leurs criticités.
Tout au début de nos travaux de thèse, nous nous sommes très vite rendu compte de la nécessité de procéder à une exploitation documentaire rigoureuse des normes relatives à la gestion des risques et au contrôle interne. Il s'agit essentiellement du COSO 1,2 3 et ERM mais aussi de l'ISO 31000 et l'ISO 27005. Il s'est avéré que ces normes restent très ouvertes sur la manière d'estimer les risques résiduels, d'où les nombreuses difficultés rencontrées et les taux d'erreurs constatés dans l'estimation des risques résiduels au niveau des banques. Il fallait donc définir les principes de base de notre modélisation afin de cadrer un certain nombre d'aspects essentiels pour éviter au maximum les erreurs d'appréciation tout en gardant la souplesse des normes. De cette analyse minutieuse a découlé un état de l'art élaboré avec soin qui a permis de mettre en exergue la diversité des contrôles bancaires, les spécificités des risques résiduels bancaires, la méthode outillée et la méthode RSCA..

De manière concrète, lors de l'estimation des risques résiduels, la probabilité de survenance brute et la gravité potentielle brute des différents risques sont estimées puis combinés aux niveaux de maturité des contrôles en vue de déterminer la criticité résiduelle des risques. Cette estimation se fait au cours de plusieurs sessions de travail avec des évaluateurs de profil différents et nécessite un consensus en cas de désaccord. La RSCA demeure la méthode la plus utilisée, elle possède trois approches principales, à savoir l'approche workshop, l'approche questionnaire et l'approche hybride qui constitue une synthèse des deux premières. Cependant, cette méthode est manuelle, fastidieuse et comporte un certain nombre de limites à savoir: une perte de temps, un investissement personnel de la part des intervenants, un certain niveau d'expertise et de potentiels erreurs d'estimation. Les récents travaux relatifs au RSCA ayant pour but d'alléger cette démarche proposent une soustraction entre les risques inhérents et les contrôles implémentés pour obtenir les risques résiduels **[93],** cependant il n'y a pas de précision sur la manière de soustraire et les valeurs obtenues avec cette approche ne sont pas comparées aux données de référence.

Nos travaux de recherche ont donc porté sur la modélisation des risques résiduels à travers l'évaluation de l'impact des contrôles mis en œuvre au niveau des banques sur les risques brutes. Pour ce faire, nous avons proposé quatre modèles mathématiques à savoir deux modèles initiaux basés sur les caractéristiques et la maturité des contrôles et deux autres modèles améliorés qui sont axés sur la maturité et les types de contrôles. Par la suite, les modèles mathématiques initiaux et améliorés sont traduites en équations de régressions linéaires ; les algorithmes y afférentes ont également été définis dans le but de les éprouver avant validation. Au niveau du logiciel Eviews, les deux équations de régressions linéaires ont été éprouvées à travers l'exécution des tests économétriques recommandés en utilisant

les données d'apprentissage collectées au niveau des banques. Les résultats sont très satisfaisants avec la réussite de tous ces tests pour la seconde équation de régressions linéaires; cela a permis de valider cette équation d'un point de vue économétrique. Dans l'optique d'approfondir les tests, les algorithmes correspondants aux modèles mathématiques ont également été implémentés au niveau du logiciel R avant d'être appliqués sur les risques du système d'information et sur tous les autres risques bancaires. Les résultats obtenus sont également très satisfaisants avec un taux de corrélation moyen avec les données de test égal à 98% pour le modèle 4.

Par ailleurs, face à la difficulté de collecter des données d'apprentissage et de test dans plusieurs banques à la fois, nous avons contourné le problème en collaborant avec 4 banques provenant de 3 pays différents, ces banques étant de profils différents et ayant des niveaux de maitrise de risques différents. Ainsi, les données d'apprentissage permettront de tester les équations de régressions linéaires au niveau de l'outil Eviews avant d'implémenter les algorithmes concernés au niveau de l'outil R. Les résultats obtenus à l'issu des tests réalisés ont été satisfaisants aussi bien sur Eviews que sur R. De plus, pour la collecte des données de référence dans 3 des 4 banques(deuxième banque du Sénégal, la banque au Burkina Faso et la banque en Côte d'Ivoire), nous n'étions pas présents aux séances de travail effectuées avec les collaborateurs des banques concernées. Cela veut dire que nous avons pris le risque de considérer des données collectées en notre absence sur la base des explications que nous leur avons fournies à distance et moyennant une charte de confidentialité très contraignante que nous avons dû signer juste pour obtenir des données réelles. Cela dénote de l'applicabilité et de la facilité d'utilisation de nos modèles. Ces résultats sont donc probants, c'est d'ailleurs la raison pour laquelle ils ont été validés dans des conférences d'audience internationale dans un domaine aussi sensible.

De manière synthétique, les résultats obtenus révèlent que le modèle 4 est le meilleur d'autant plus que tous les tests économétriques sont réalisés avec succès, il est stable et possède le meilleur taux de corrélation avec les données de test collectées auprès des banques ayant des spécificités différentes. Globalement, les modèles proposés ont un certain nombre d'avantages à savoir la facilitation du calcul de la criticité résiduelle des risques mais aussi le gain de temps moyen considérable qui pourra être mis à profit par les banques pour améliorer leurs dispositifs de contrôle interne. Dans nos travaux futurs, nous préconisons aussi de traiter en perspectives, l'existence de corrélation entre les types de contrôles, cela nous permettra certainement de réduire les variables d'entrées du modèle 4 dont le nombre important constitue la seule limite de ce modèle. Nous envisageons également d'étendre les tests à des secteurs différents de la banque et nous projetons d'implémenter un outil de gestion intégré des risques en vue d'automatiser tout le processus de gestion et de pilotage des risques. .

Depuis plusieurs années, les banques ont adopté une démarche de gestion des risques rigoureuse même si l'on note encore des disparités dans le niveau maitrise de ces risques. Le niveau de maturité des contrôles face aux risques dépend de plusieurs facteurs, tels que les

activités de contrôle déployées ou la culture du risque **[11].** L'évolution des modes de vie et du pouvoir d'achat a contribué à renforcer et à favoriser l'émergence de banques éthiques. En effet, la clientèle est mieux informée, plus exigeante et de plus en plus procédurière, ce qui est à l'origine de l'implantation dans les banques, d'une solide culture juridique, du renforcement des règles de déontologie, du respect aux accords de Bale **[112]** et de la conformité aux normes et réglementations en vigueur. A cela s'ajoute, la problématique de la sécurisation des moyens de paiement électronique compte tenu de l'importance grandissante des grands réseaux internationaux du paiement par carte en l'occurrence Visa et Mastercard mais aussi des opérateurs non-bancaires comme les opérateurs télécoms. En effet, l'arrivée de nouvelles solutions comme le portemonnaie électronique et surtout le paiement par téléphone mobile font que le système d'information bancaire est de plus en plus vulnérable. D'où la nécessité de maitriser également ces nouveaux risques susceptibles d'être à l'origine différents types de fraudes pouvant avoir des conséquences néfastes pour les banques et les clients. Dans ce contexte, la direction du système d'information joue un rôle majeur dans la démarche de gestion des risques bancaires. Et ce, par le biais de contributions indirectes en particulier dans les domaines de la formation et de la sécurité informatique mais également de façon directe à travers le traitement de ses propres risques liés aux systèmes d'information **[29**]. Le rôle de la direction du système d'information dans la démarche de gestion des risques est proportionnel au niveau de maturité de l'entreprise en matière de gestion des risques. En effet, elle agit souvent comme un moteur dans la mise en place d'une démarche globale de gestion des risques. Les moyens par lesquels la direction du système d'information peut participer à la démarche de gestion des risques sont nombreux, il s'agit notamment de la création d'applications informatiques destinées à diminuer certains risques, de la vérification du bon fonctionnement de la gestion intégrée des risques , de la mise en place d'outils anti-fraude, de l'élaboration des indicateurs de type conformité aux normes sécuritaires informatiques et du développement d'outils consacrés à la gestion des risques.

Il est difficile de maitriser tous les risques bancaires, car les problématiques actuelles sont nombreuses et complexes dans un contexte d'enjeux et d'évolutions. Toutefois, les banques devraient relever le défi d'un contrôle interne mature et efficace malgré le caractère manuel de certaines tâches. Parmi les tâches manuelles, on peut citer l'estimation de la criticité résiduelle des risques qui nécessite beaucoup de séances de travail et un certain niveau d'expertise de la part des évaluateurs. Il appartient aux administrateurs de la banque de déterminer le niveau de risque qu'il est prêt à accepter que l'on appelle appétence au risque. Le management, quant à lui, est responsable de la conception, de la mise en œuvre et de la supervision des dispositifs de contrôle interne et de gestion des risques. Dans ce contexte, les risques doivent être évalués de manière continue et les activités de contrôle doivent être conçues pour répondre aux risques spécifiques de l'entité concernée au niveau de la banque. Pour faire face à ce défi tant organisationnel que méthodologique, les banques utilisent le plus souvent la méthode RSCA basée sur l'AMDEC qui permet de faire une analyse des modes de défaillance, de leurs effets et leurs criticités.
Tout au début de nos travaux de thèse, nous nous sommes très vite rendu compte de la nécessité de procéder à une exploitation documentaire rigoureuse des normes relatives à la gestion des risques et au contrôle interne. Il s'agit essentiellement du COSO 1,2 3 et ERM mais aussi de l'ISO 31000 et l'ISO 27005. Il s'est avéré que ces normes restent très ouvertes sur la manière d'estimer les risques résiduels, d'où les nombreuses difficultés rencontrées et

les taux d'erreurs constatés dans l'estimation des risques résiduels au niveau des banques. Il fallait donc définir les principes de base de notre modélisation afin de cadrer un certain nombre d'aspects essentiels pour éviter au maximum les erreurs d'appréciation tout en gardant la souplesse des normes. De cette analyse minutieuse a découlé un état de l'art élaboré avec soin qui a permis de mettre en exergue la diversité des contrôles bancaires, les spécificités des risques résiduels bancaires, la méthode outillée et la méthode RSCA..

De manière concrète, lors de l'estimation des risques résiduels, la probabilité de survenance brute et la gravité potentielle brute des différents risques sont estimées puis combinés aux niveaux de maturité des contrôles en vue de déterminer la criticité résiduelle des risques. Cette estimation se fait au cours de plusieurs sessions de travail avec des évaluateurs de profil différents et nécessite un consensus en cas de désaccord. La RSCA demeure la méthode la plus utilisée, elle possède trois approches principales, à savoir l'approche workshop, l'approche questionnaire et l'approche hybride qui constitue une synthèse des deux premières. Cependant, cette méthode est manuelle, fastidieuse et comporte un certain nombre de limites à savoir: une perte de temps, un investissement personnel de la part des intervenants, un certain niveau d'expertise et de potentiels erreurs d'estimation. Les récents travaux relatifs au RSCA ayant pour but d'alléger cette démarche proposent une soustraction entre les risques inhérents et les contrôles implémentés pour obtenir les risques résiduels **[93],** cependant il n'y a pas de précision sur la manière de soustraire et les valeurs obtenues avec cette approche ne sont pas comparées aux données de référence.

Nos travaux de recherche ont donc porté sur la modélisation des risques résiduels à travers l'évaluation de l'impact des contrôles mis en œuvre au niveau des banques sur les risques brutes. Pour ce faire, nous avons proposé quatre modèles mathématiques à savoir deux modèles initiaux basés sur les caractéristiques et la maturité des contrôles et deux autres modèles améliorés qui sont axés sur la maturité et les types de contrôles. Par la suite, les modèles mathématiques initiaux et améliorés sont traduites en équations de régressions linéaires ; les algorithmes y afférentes ont également été définis dans le but de les éprouver avant validation. Au niveau du logiciel Eviews, les deux équations de régressions linéaires ont été éprouvées à travers l'exécution des tests économétriques recommandés en utilisant les données d'apprentissage collectées au niveau des banques. Les résultats sont très satisfaisants avec la réussite de tous ces tests pour la seconde équation de régressions linéaires; cela a permis de valider cette équation d'un point de vue économétrique. Dans l'optique d'approfondir les tests, les algorithmes correspondants aux modèles mathématiques ont également été implémentés au niveau du logiciel R avant d'être appliqués sur les risques du système d'information et sur tous les autres risques bancaires. Les résultats obtenus sont également très satisfaisants avec un taux de corrélation moyen avec les données de test égal à 98% pour le modèle 4.

Par ailleurs, face à la difficulté de collecter des données d'apprentissage et de test dans plusieurs banques à la fois, nous avons contourné le problème en collaborant avec 4 banques provenant de 3 pays différents, ces banques étant de profils différents et ayant des niveaux de maitrise de risques différents. Ainsi, les données d'apprentissage permettront de

tester les équations de régressions linéaires au niveau de l'outil Eviews avant d'implémenter les algorithmes concernés au niveau de l'outil R. Les résultats obtenus à l'issu des tests réalisés ont été satisfaisants aussi bien sur Eviews que sur R. De plus, pour la collecte des données de référence dans 3 des 4 banques(deuxième banque du Sénégal, la banque au Burkina Faso et la banque en Côte d'Ivoire), nous n'étions pas présents aux séances de travail effectuées avec les collaborateurs des banques concernées. Cela veut dire que nous avons pris le risque de considérer des données collectées en notre absence sur la base des explications que nous leur avons fournies à distance et moyennant une charte de confidentialité très contraignante que nous avons dû signer juste pour obtenir des données réelles. Cela dénote de l'applicabilité et de la facilité d'utilisation de nos modèles. Ces résultats sont donc probants, c'est d'ailleurs la raison pour laquelle ils ont été validés dans des conférences d'audience internationale dans un domaine aussi sensible.

De manière synthétique, les résultats obtenus révèlent que le modèle 4 est le meilleur d'autant plus que tous les tests économétriques sont réalisés avec succès, il est stable et possède le meilleur taux de corrélation avec les données de test collectées auprès des banques ayant des spécificités différentes. Globalement, les modèles proposés ont un certain nombre d'avantages à savoir la facilitation du calcul de la criticité résiduelle des risques mais aussi le gain de temps moyen considérable qui pourra être mis à profit par les banques pour améliorer leurs dispositifs de contrôle interne. Dans nos travaux futurs, nous préconisons aussi de traiter en perspectives, l'existence de corrélation entre les types de contrôles, cela nous permettra certainement de réduire les variables d'entrées du modèle 4 dont le nombre important constitue la seule limite de ce modèle. Nous envisageons également d'étendre les tests à des secteurs différents de la banque et nous projetons d'implémenter un outil de gestion intégré des risques en vue d'automatiser tout le processus de gestion et de pilotage des risques. .

Bibliographie

[1] Rapport annuel de la commission Bancaire, Union Economique et Monétaire Ouest Africaine, 2010

[2] F.Gbongué, Quels outils pour le pilotage technique des risques des banques subsahariennes francophones dans le cadre de Bâle II, Financial Afrik, January 18th, 2015

[3] Management des risques selon COSO, CHAPITRE 4, IIA

[4] B.Ki-ZERBO, Objectifs COSO: Le nouveau COSO et ses 17 principes fondateurs pour un contrôle interne efficient, IFACI, juin-juillet 2013

[5] Dr. Patchin Curtis and M.Carey, Deloitte & Touche LLP, Risk Management in Practice, COSO, October 2012

[6] Circulaire N°03/2011/CB/C relative à l'organisation du contrôle interne du système de contrôle interne dans les établissements de l'UEMOA

[7] R.BERNARD, Reglementation: Les evolutions de la regulation et de la supervision bancaire, Rappel historique et problématiques post crise, AFRITAC, Avril 2011

[8] Basel Committee on Banking Supervision, Consultative Document Identification and measurement of step-in risk, Issued for comment, March 2016

[9] Gomes et C. Wilkins. « Le point sur les normes de liquidité de Bâle III », Revue du système financier, Banque du Canada, 2013

[10] L.Lipol and J.Haq, Risk Analysis Method: FMEA/FMECA in the Organizations, University of Boras, Sweden, 2011

[11] D.CHELLY et S.SEBELOUE, les métiers du risque et du contrôle Bancaire, Optimindwinter, 2014

[12] Les métiers du secteur de la banque, Référentiel des métiers cadres du secteur de la banque, APEC, Edition 2012

[13] Produits et services pour la monétique, le M2M et l'efficacité énergétique, KORTEX PSI, Paris 2016

[14] C.VANTET, La monétique: Les transactions bancaires, Novembre 2008

[15] Circulaire N°07 relative à l'organisation du système de contrôle interne des établissements de crédit de l'UEMOA et de la CEMAC

[16] D. Weese, Overview of risk assessment methods and applications, Executive Director of AMGEC, June 2006

[17] Diagramme D'ISHIKAWA = diagramme CAUSE-EFFET, National Agency for innovation and Research, Luxinnovation

[18] La methodologie AMDEC, CRTA, Novembre 2004

[19] AMDEC, Exemple, BAC PRO, MSMA

[20] Diagramme D'ISHIKAWA = diagramme CAUSE-EFFET, National Agency for innovation and Research, Luxinnovation

[21] Les outils: 5M, QQOQCP, AMDEC, Journées Nationales de Prévention, La demarche d'évaluation des risques professionnels, Inserm, DRH/BCPR, JNP- 2014

[22] L.Bélanger, J.Brouillard et A.Buteau, Identification et Evaluation des risques: Guide de prévention, ISBN: 978-2-89618-050-9, ASSTSAS, 2015

[23] Guidance on Monitoring Internal Control Systems, Committee of Sponsoring Organizations of the Treadway Commission, 2, pp. 7-8, Volume I: Executive Summary, 2009

[24] Le management des risques de l'entreprise: Cadre de reference, Committee of Sponsoring Organizations of the Treadway Commission, p. 333 de la version française du COSO de 1992 , 2004

[25] J.Harvey, Introduction to managing risk, Topic Gateway series no. 28, Technical Information Service, Last reviewed, February 2008

[26] Les activités de controle, le controle interne, IIA

[27] M.Riffat, A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5, Process Assessment Model (PAM) GIAC (GCCC), Gold Certification, April 2015

[28] Analyse et gestion des risques dans les grandes entreprises, Impacts et rôle pour la DSI, Institut d'Etudes et de Recherche pour la Sécurité des Entreprises, CIGREF, 2017

[29] Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information: un levier exceptionnel de création de valeur et de croissance, IBM, 2008

[30] J.Rasmussen, Proactive Risk Management in a Dynamic Society. HURECON, Risk Center, University of Karlstad, 2000

[31] P.PEROTIN, Les Progiciels de gestion intégrée, instrument de l'intégration organisationnelle: Etude d'un cas, Université Montpellier II, Septembre 2004

[32] Towards a better approach of the risk management: from the ontological modeling of the accidental process to decision aided interactive system, HAL Id: tel-00338938, Institut National Polytechnique de Lorraine - INPL, 2008

[33] M.Monperrus, La mesure des modèles par les modèles : une approche générative. HAL Id: tel-00514492, Software Engineering, Université Rennes 1, 2008

[34] W.Jouve, Approche déclarative pour la génération de canevas logiciels dédiés à l'informatique ubiquitaire, HAL Id: tel-00402605, Software Engineering, Bordeaux I, 2009

[35] MEHARI : Guide de développement d'une base de connaissance d'analyse de risques. CLUSIF, 2012

[36] Guidance for Industry Quality Risk Management, US Department of Health and Human Services Food and Drug Administration, June 2006

[37] S.Marinou, Project risk management. MSC Graduate, Greece, Volume2, Issue5

[38] C.Sevre, Réalisation d'une recette fonctionnelle outillée avec Quality Center et Quick Test Professional. HAL Id: dumas-00692443, Hardware Architecture, 2011

[39] R.Guillerm, Intégration de la Sûreté de Fonctionnement dans les Processus d'Ingénierie Système, L'Université Toulouse III, juin 2011

[40] S.Champenois, Acquisition et mise en place d'un logiciel de Gestion Electronique de Documents. HAL Id: dumas-00693935, May 2012

[41] M.Delmond, L'externalisation du développement d'applications, HEC PARIS, May 2014

[42] R.Guillerm, H.Demmou and N.Sadou, Safety evaluation and management of complex systems: A system engineering approach. Dec 2012, HAL Id: hal-00766112

[43] B.Changa, C.Kuoa, C.Wub and G.Tzeng, Using Fuzzy Analytic Network Process to assess the risks in enterprise resource planning system implementation, Elsevier 2014

[44] D.Gourc, Vers un modèle général du risque pour le pilotage et la conduite des activités de biens et de services : Propositions pour une conduite des projets et une gestion intégrée des risques. HAL Id: tel-00745260, Institut National Polytechnique de Toulouse - INPT, 2006

[45] P.Nassar, Security management in a dynamic services infrastructure: A risk management approach. HAL Id: tel-00828598, INSA de Lyon, May 2012

[46] G.Hardy and J. Heschl, "Aligning CobiT 4.1, ITILV3 and ISO/IEC 27002 for Business Benefit," IT Governance Institute, 2008

[47] M.Gehrmann, Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations, Navus Revista de Gesto e Tecnologia. Florianpolis: ISSN 2237-4558, August 2012

[48] I.Mukherjee, Cloud Security through COBIT, ISO 27001 ISMS Controls, Assurance and Compliance, ISACA, RSA Conference ASIA PACIFIC, Singapore, 2013.

[49] A.TORO, Securité opérationnelle : Conseils pratiques pour sécuriser le SI, ÉDITIONS EYROLLES, 2015

[50] Fraud Working Committee White Paper: Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, Biometrics in Banking and Payments, Javelin Strategy Research, www.javelinstrategy.com, April 2015

[51] Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices Version 1.1, Payment Card Industry (PCI), Point-to-Point Encryption, April 2012

[52] P.Dulany, H. Gong and K. Shah, "CA Technologies, Advanced Analytics and Data Science: 3D-Secure Authentication using Advanced Models," White paper, October 2014

[53] J.Conroy: 3D Secure: The Force for CNP Fraud Prevention Awakens, January, 2016

[54] Les 25 principes fondamentaux d'un contrôle bancaire efficace, comité de Bâle, bulletin de la commission bancaire n° 17, novembre 1997

[55] D.Labarthe, Bâle II et IAS 39: Les nouvelles exigences en fonds propres réglementaires, des banques et l'évaluation en juste valeur des instruments financiers

[56] F.Hache, Bâle 3 en 5 questions: des clefs pour comprendre la réforme, Augmenter le capital des banques pour renforcer le système financier, Mai 2012

[57] Institute of Operational Risk, Operational Risk Sound Practice Guidance, Risk Control Self-Assessment, March 2010

[58] Sobel and Paul, Auditor's Risk Management Guide, édition de 0002007, Chicago, Illinois, CCH, Inc., p.7.04-7.05. Ibid.

[59] Risk Management Information System, panorama publié par l'AMRAE, http://www.amrae.fr/docs/MR/panorama-sigr-2009-final-engversionfinale

[60] V.Svatá and M.Fleischmann, IS/IT RISK MANAGEMENT IN BANKING INDUSTRY, University of Economics, Prague, Faculty of Informatics and Statistics

[61] Managing the Business Risk of Fraud: A Practical Guide, The Institute of Internal Auditors, The American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners

[62] T.Bhatla, V.Prabhu and A.Dua, Understanding Credit Card Frauds, Tata Consultancy Services, Cards Business Review 1, June 2003

[63] Sullivan, How has the adoption of internet banking affected performance and risk in banks, Financial Industry Perspectives, 2000

[64] Mobile Payments: Risk, Security and Assurance Issues, IL 60008 USA An ISACA Emerging Technology White Paper, November, 2011

[65] D.Pyle, Bank Risk Management: Theory, University of California, Berkeley, July 1997

[66] S.Bratanovic: Analyzing Banking Risk, Framework for Assessing Corporate Governance and Risk Management, 3rd Edition Hennie, van Greuning, The International Bank for Reconstruction and Development, the World Bank, 2009

[67] A.Santomero, Commercial Bank Risk Management: an Analysis of the Process, the Wharton School, University of Pennsilvania, 1997

[68] O.Awojobi, R.Amel and S. Norouzi, Analysing Risk Management in Banks: Evidence of Bank Efficiency and Macroeconomic Impact, Eastern Mediterranean University, April 2011

[69] Analysis of credit risk management efficiency in Nigeria commercial banking sector, Onaolapo A. R. Department of Management and Accounting, Faculty of Management Science, Ladoke Akintola University of Technology, Ogbomoso, Nigeria, 2004-2009

[70] G.Ngurah, N.Mandalaa and C.Nawangpalupia, Assessing Credit Risk: an Application of Data Mining in a Rural Bank , Fransiscus, Rian Praktiktoa aIndustrial Engineering Department, Parahyangan Catholic University, Indonesia, 2012

[71] K.Matthews, Risk management and managerial efficiency in Chinese banks, A network DEA framework, Cardiff Business School Cardiff University Colum Drive, CF103EU, UK, 2012

[72] Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of Cybercrime II, June 2014

[73] Risk Assessment Process Information Security, Risk management, Principles and guidelines, AS/NZS ISO 3100, February 2014

[74] A.Grody, P.Hughes and S.Toms, Risk Accounting: A Next Generation Risk Management, System for Financial Institutions, Enterprise Risk Management Symposium Society of Actuaries, March 2011

[75] S.Claessens and L.Ratnovski, What Is Shadow Banking?, IMF Working Paper, Research Department, International Monetary Fund WP/14/25, february 2014

[76] D.Okehi, Modelling Risk Management in Banks: examining, why banks fail?, Walden University, 2014

[77] J.Kambhu and A.Rodrigues, Residual risk factors, portfolio composition and risk measurement, Federal Reserve Bank of New York

[78] Risk Management Framework, HITRUST, March 2013

[79] M.Ciorciari and Dr.Blattner, Enterprise Risk Management maturity-level assessment tool, 2008 ERM Symposium, Chicago, April 2008

[80] J.Creasey and S.Marvell, A complete Information Risk Management solution for ISF Members using IRAM and STREAM, ERM Symposium, Chicago, April 2008

[81] H.Peter, Y.Kim, T.Lee, C.Moon, Y.Jung and I. Kim, A Security Risk Analysis Model for Information Systems, Springer-Verlag Berlin Heidelberg, 2005

[82] J.Pagett, Improving residual risk management through the use of security metrics, Technical Report, March 2010

[83] C.Renoux, Tout ce qu'il faut savoir sur le RSCA, DUMG, 2015

[84] Risk Assessment Process Information Security, AS/NZS ISO 31000:2009, February 2014

[85] Méthodologie for privacy risk management, How to implement the Data Protection Act, É d i t i o n 2 0 1 2

[86] P.Kellogg, Evolving Operational Risk Management for Retail Payments, Emerging Payments Occasional Papers Series, Federal Reserve Bank Of Chicago, 2003

[87] Risk Assessment, The Critical First Step to Developing an Effective IT Audit Plan, Crowe Horwath LLP, March 2010

[88] N.Mathur, H.Mathur and T.Pandya, Risk Management in Information System of Organisation: A Conceptual Framework, International Journal of Novel Research in Computer Science and Software Engineering Vol. 2, Issue 1, pp: (82-88), January - April 2015

[89] M. F. Unuakhalu, D.Sigdel and M. Garikapati, Integrating Risk Management in System Development Life Cycle, Kentucky State University, U.S.A, International Journal of Software and Web Sciences (IJSWS), March-May 2014, pp. 01-09

[90] D.Simpson, Cybersecurity Risk Reduction, Public Safety & Homeland Security Bureau Federal Communications Commission, January 2017

[91] A.Szubin, National Money Laundering Risk Assessment, 2015

[92] M.Toburen, steps to a grc risk management framework-5: residual risk, August 2017

[93] C.AMANCEI, Practical Methods for Information Security Risk Management Academy of Economic Studies, Bucharest, Romania, Informatica Economică vol. 15, no. 1/2011

[94] Supervisory Guidance Paper on ML and TF Institutional/Business Risk Assessment Issued jointly by the Financial Intelligence, Analysis Unit and the Malta Financial Services Authority, February 2018

[95] Risk Assessment Process Information Security, All-of-Government Risk Assessment Process: Information Security, February 2014

[96] V.Dumbrav, T.Maiorescu and V.Iacob, Using Probability Impact Matrix in Analysis and Risk Assessment, Journal of Knowledge Management, Economics and Information Technology, Special Issue, December 2013

[97] G.Tolbert, Residual risk reduction, November 2005

[98] Humtom and William, Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, CIPL GDPR Interpretation and Implementation Project, December 2016

[99] Risk Assessment: Groups of young people visiting QPAC, RA0001 Groups of young people visiting QPAC.docx Page 3 of 3, Update version: 2, 15 Mars 2016

[100] Supplier Risk Management, Schulmynn Leung Manager, Supply Chain Strategy & Operations

[101] J.Confais et M.Le Guen, premiers pas en régression linéaire, SAS® et SAS/INSIGHT, SAS Institute Inc., Cary, NC, USA, Revue MODULAD, 2006

[102] J.Bickel, Transformer la variable dépendante, Statistique II -SPO8

[103] R.Bourbonnais, logiciel EVIEWS, Université de Paris–Dauphine, janvier 2012

[104] P.Micheaux, R.Drouilhet et B.Liquet, Le logiciel R : Maitriser le langage et Effectuer des analyses (bio) statistiques, Springer

[105] M.Ndaw, G.Mendy and S.Ouya, A quantification model of internal control impact on banking risks using FMECA, IEEE, 5th World Congress on Information and Communication Technologies (WICT), Marrakech, 2015

[106] M.Ndaw, G.Mendy and S.Ouya, Modeling the impact of controls on information system risks, 18th International Conference on Computer, Communication and Information Sciences, and Enginiering (ICCCISE), Londres, 2016

[107] M.Ndaw, G.Mendy and S.Ouya, Improving the quantification model of internal control impact on banking risks using FMECA, 18th International Conference on Finance, Banking and Insurance (ICFBI), Paris, 2016

[108] M.Ndaw, G.Mendy, S.Ouya and D.Seck: Quantify the Maturity of Internet Banking Security Measures in WAEMU Banks, 1st EAI International Conférence on Innovations and Interdisciplinary Solutions for Underserved Areas EAI, INTERSOL, DAKAR, APRIL 11–12, 2017

[109] M.Ndaw, G.Mendy and S.Ouya, Modeling the Effect of Security Measures on Electronic Payment Risks, 13th International Conférence on Information Assurance and Security (IAS), Marrakech, 2018

[110] Régression linéaire : Chapitre 4 : Université Paris Ouest Nanterre La Défense, UFR SPSE-Master 1, PMP STA 21 Méthodes statistiques pour l'analyse des données en psychologie

[111] F.Picard, Premières notions de statistique : Régression Linéaire, UMR CNRS-5558, Laboratoire de Biométrie et Biologie Evolutive,franck.picard@univ-lyon1.fr

[112] M.Aglietta, Macroéconomie financière, cinquième édition, collection manuels, grands reperes, mars 2008