INSTITUT DE FINANCEMENT DU DÉVELOPPEMENT DU MAGHREB ARABE

Institut de Financement du Développement du Maghreb Arabe

معهد تمويل التنمية المغرب العربي

Mémoire de fin d'Etudes

Thème :

Elaboration d'une cartographie des risques liés au processus monétique et au dispositif DAB/GAB et TPE

Présenté et soutenu par :

BELKACEM IMANE

Encadré par :

Mr AMAR ABSESSALEM

Etudiant(e) parrainé(e) par :

La Banque de Développement Local BDL

Dédicaces

Je dédie ce travail à

Mes chers parents ***Farida*** et ***Arezki*** pour leur amour inestimable, leur dévouement inconditionnel, leur confiance, leur compréhension et pour toutes les valeurs qu'ils ont su m'inculquer.

Mes chers frères ***Islam***, ***Ahmed*** et ***Adam***

Nana ***Adouda***

Aux âmes de mes chers grands parents ***Zehor*** et ***Akli***

Qui ont voulu me voir exceller dans mes études, qui m'ont toujours encouragé, soutenu et réconforté avec leurs douces paroles, qui m'ont imprégnée.

Ma grand-mère ***Dahbia***

Mes tantes et oncles maternels

La fraternité Algéro-Tunisienne

Ce travail est pour vous

Remerciements

Mes remerciements vont à l'endroit de ceux qui ont contribué à la réalisation de ce travail.

Je tiens à remercier mon encadrant Monsieur
« AMAR Abdessalem »
Son expérience, ses compétences, ses recommandations et son sens de coopération m'ont été une aide inestimable.

Mes sincères remerciements s'adressent également à mon tuteur professionnel Monsieur
« BAOUIA Djoubair »
Pour m'avoir accueillie dans son département, pour son écoute, sa patience, son aide, ses orientations et son encadrement.

Je remercie aussi les équipes du Département Risque Opérationnel, Direction Monétique et Banque Digitale et Direction des Moyens de Paiements au sein de la BDL pour leur aide.

Je tiens à remercier le Président et les membres de jury qui me font le grand honneur d'évaluer ce travail.

Je ne saurai terminer sans adresser tous mes remerciements, ma sincère gratitude et mon profond respect aux enseignants de l'Institut de Financement du Développement du Maghreb Arabe, à qui je dois mes réussites, et aussi à tous ceux qui ont contribué à ma formation dès mon plus jeune âge.

Sommaire

Liste des tableaux :

Liste des figures :

Liste des annexes :

Liste des abréviations :

- **Français :**

- **AME: Anep Messagerie Express**
- **ANADE : Agence Nationale d'Appui et de Développement de l'Entreprenariat**
- **ANGEM : Agence Nationale de gestion du Microcrédit**
- **ATCI : Algérie Télé-Compensation Interbancaire**
- **BADR : Banque de l'Agriculture et du Développement Rural**
- **BDL : Banque de Développement Local**
- **BEA: Banque Extérieure d'Algérie**
- **BNA : Banque Nationale d'Algérie**
- **CE : Commission Européenne**
- **CI : Contrôle Interne**
- **CIB : Carte interbancaire**
- **CMI : Centre Monétique Interbancaire**
- **CNAC : Caisse Nationale d'Assurance Chômage**
- **CNEP : Caisse Nationale d'Epargne et de Prévoyance**
- **CNMA : Caisse Nationale de Mutualité Agricole**
- **CPA : Crédit Populaire d'Algérie**
- **CPI : Centre de Pré-compensation Interbancaire**
- **CPPC : Clients Produits Pratiques Commerciales**
- **CSC : Chef de Service Caisse**
- **DMR: Dispositif de Maîtrise des Risques**
- **DA : Dinar Algérien**
- **DAB : Distributeur automatique de billets**
- **D-agc /DAG : Directeur d'Agence**
- **DGA RCC : Direction Générale Adjointe Risques Contrôle Conformité**
- **DAP : Dommages aux Actifs Physiques**
- **DG : Direction Générale**
- **DMBD : Direction de la Monétique et la Banque Digitale**
- **DRO : Département des Risques Opérationnels**
- **DSI : Direction des Systèmes d'Informations**
- **EFP: Exigences en Fonds Propres**
- **ELGP : Exécution, Livraison et Gestion des processus**

- **FE : Fraude Externe**
- **FI : Fraude Interne**
- **GAB : Guichet automatique de Banque**
- **GIE : Groupement d'Intérêt Economique**
- **IADS : Interruptions d'Activités et Dysfonctionnement de Systèmes**
- **IFACI : Institut Français de l'Audit et du Contrôle Internes**
- **LDC : Lettre De Change**
- **M-com: Manager Commercial**
- **PCA : Plan de Continuité d'Activité**
- **PESLT : Personnels, Emplois et Sécurité de Lieu de Travail**
- **PME : Petites et Moyennes Entreprises**
- **PNB: Produit Net Bancaire**
- **PSG : Prêt Sur Gage**
- **RMI : Réseau Monétique Interbancaire**
- **RO : Risque Opérationnel**
- **SATIM : Société d'Automatisation des Transactions Interbancaires et de Monétique**
- **SI : Système d'informations**
- **SPA : Société Par Actions**
- **TPE : Terminal de Paiement Electronique**
- **VA : Valeur ajoutée**

Anglais :

- **AMA: Advanced Measurement Approaches**
- **ATM: Automated Teller Machine**
- **ISO: International Organization for Standardization**
- **BIA: Basic Indicator Approach**
- **DDoS: Distributed Denial-of-Service**
- **IMA: Internal Measurement Approach**
- **KRI: Key Risk Indicators**
- **LDA: Loss Distribution Approach**

INTRODUCTION GÉNÉRALE

INTRODUCTION GENERALE

Le secteur des transactions financières électroniques a connu une croissance exponentielle au cours des dernières décennies, transformant radicalement la manière dont les individus et les entreprises effectuent des paiements. L'évolution constante des technologies monétiques, combinée à la prolifération des Distributeurs Automatiques de Billets (DAB), des Guichets Automatiques de Banque (GAB), et des Terminaux de Paiement Électronique (TPE), a créée un écosystème complexe.

Les systèmes monétiques, impliquant des processus complexes et une infrastructure technologique sophistiquée, sont inévitablement sujets à des risques multiples, allant des fraudes financières à la compromission des données sensibles. De même, les dispositifs DAB/GAB/TPE, omniprésents dans notre quotidien, sont exposés à des menaces telles que les attaques physiques, les manipulations électroniques et les cyberattaques. Les menaces sont nombreuses et en constante évolution.

Dans ce contexte et face à ces défis, il devient impératif pour les institutions financières, les organismes de régulation et les acteurs du secteur monétique de comprendre en profondeur les risques associés à leurs opérations. Il devient indispensable pour les banques de cartographier précisément ces risques afin de mieux s'en prémunir.

C'est dans cette optique que se place notre projet de fin d'études, qui porte sur l'élaboration d'une cartographie des risques liés au processus monétique et aux dispositifs DAB/GAB/TPE. Cette étude se positionne au carrefour des enjeux liés à la sécurité des transactions électroniques et à la fiabilité des services financiers, explorant les diverses facettes des menaces potentielles qui pèsent sur ces systèmes.

L'objectif est donc double :

- Identifier de la manière la plus exhaustive possible les différents risques associés à l'utilisation des cartes bancaires et des équipements monétiques, qu'ils soient d'ordre technique, humain ou organisationnel.
- Hiérarchiser ces risques en fonction de leur fréquence de survenance et de leur impact potentiel, afin de déterminer les zones à risque prioritaires sur lesquelles les banques doivent agir.

Dans ce travail, nous nous intéresserons à la question suivante : **Comment la cartographie des risques peut-elle être un outil efficace et pertinent pour la gestion des risques du dispositif de la monétique dans une banque ?**

Pour répondre à cette problématique, nous analyserons les questions suivantes :

Q1 : Quels sont les principaux risques associés au processus monétique et au dispositif DAB/GAB/TPE dans le secteur bancaire? Comment peuvent-ils être identifiés et évalués de manière exhaustive?

Q2 : Quelles sont les bonnes pratiques pour structurer et présenter une cartographie des risques efficace et pertinente dans le contexte bancaire ? Quels éléments essentiels doit-elle contenir?

Q3 : Comment intégrer l'analyse des risques opérationnels, de fraude et cyber-sécurité dans la cartographie pour avoir une vision globale des risques monétiques?

Nous formulons les hypothèses suivantes :

H1 : L'analyse des processus monétiques et le recensement des incidents historiques permettent d'identifier de manière exhaustive les principaux risques opérationnels, de fraude et cyber-sécurité.

H2 : La structuration de la cartographie par processus avec une évaluation des risques bruts et nets permet de présenter une cartographie efficace et pertinente.

H3 : L'identification des risques opérationnels, de fraude et cyber-sécurité par processus dans la cartographie permet une vision globale des risques monétiques.

Pour mener à bien ce travail, nous allons nous appuyer sur une méthodologie de trois étapes :

1. Recensement des risques à travers l'analyse de la documentation existante (rapports, études antérieures, statistiques sur la fraude) ainsi que des entretiens avec des experts du domaine bancaire.
2. Evaluation de la criticité des risques selon une grille de cotation prédéfinie, en croisant probabilité d'occurrence et gravité d'impact.
3. Positionnement de chaque risque sur une cartographie matricielle, permettant de visualiser les zones à risque majeur, intermédiaire et mineur.

L'étude sera consacrée à la réalisation de trois (03) chapitres : un premier chapitre qui évoquera la cartographie des risques opérationnels, un deuxième chapitre qui servira d'un aperçu sur la monétique et un troisième chapitre qui sera consacré pour le cas pratique intitulé : « L'élaboration d'une cartographie des risques liés au processus monétique et au dispositif DAB/GAB/TPE ».

L'élaboration d'une cartographie des risques revêt un intérêt certain, tant d'un point de vue académique que pratique.

D'un point de vue académique, la cartographie des risques est un exercice complexe nécessitant une méthodologie rigoureuse pour identifier, analyser et évaluer les risques auxquels une organisation est confrontée. La réalisation d'une cartographie demande de

solides connaissances en gestion des risques, audit et analyse de processus. Ce projet sera donc l'occasion de mettre en pratique et d'approfondir mes compétences dans ces domaines.

D'un point de vue pratique, la cartographie des risques est un outil stratégique essentiel pour les établissements financiers et bancaires dans le pilotage de leurs risques. Les livrables de ce projet, en particulier la cartographie des risques et les préconisations qui en découleront, présenteront une utilité directe pour ces organisations.

C'est donc un sujet présentant à la fois des enjeux méthodologiques stimulants et des applications opérationnelles concrètes qui a motivé notre choix pour ce projet de fin d'études.

L'élaboration d'une cartographie des risques liés au processus monétique et au dispositif DAB/GAB/TPE est un projet important qui permettra à l'entreprise de mieux gérer les risques auxquels elle est exposée.

CHAPITRE 01 :

LA CARTOGRAPHIE DES RISQUES OPÉRATIONNELS

CHAPITRE 01 : LA CARTOGRAPHIE DES RISQUES OPÉRATIONNELS

La gestion des risques est devenue un enjeu stratégique majeur pour les banques et institutions financières. Parmi les risques auxquels elles sont confrontées, le RO représente une part importante. Pour identifier et évaluer ce risque, les établissements financiers ont progressivement mis en place des cartographies des risques opérationnels.

Dans ce chapitre, nous nous intéresserons à l'utilisation de la cartographie des RO par les banques. Nous définirons tout d'abord ce qu'est le RO et quelles sont ses principales sources. Nous expliciterons ensuite le principe et les objectifs d'une cartographie des risques.

Nous détaillerons les différentes étapes de construction d'une cartographie des RO : identification des processus, recensement des risques, évaluation qualitative et quantitative de ces risques, représentation graphique. Nous aborderons également l'utilisation de la cartographie dans le cadre du contrôle et de la gestion des risques opérationnels.

Enfin, nous étudierons les limites et points d'amélioration de cet outil, devenu incontournable dans le secteur bancaire. La cartographie des RO permet une meilleure maîtrise des risques mais nécessite des mises à jour régulières pour refléter l'évolution de l'environnement bancaire.

SECTION 01 : LE CADRE GENERAL DU RISQUE OPÉRATIONNEL

Le risque opérationnel est devenu un sujet de préoccupation majeur pour les établissements bancaires et financiers ces dernières années. Cependant, sa définition et son périmètre restent parfois flous et sujets à interprétation.

Dans cette section introductive, nous poserons donc le cadre général du risque opérationnel. Nous commencerons par définir précisément ce qu'est le risque opérationnel, en le distinguant des autres risques bancaires que sont le risque de crédit et le risque de marché.

Nous présenterons ensuite les principales sources du risque opérationnel au sein d'une banque : risques liés aux processus, aux systèmes d'informations, aux ressources humaines, aux fraudes etc. Cette analyse des sources nous permettra de mieux cerner le périmètre du RO.

Enfin, nous aborderons les enjeux de la gestion du RO pour les banques en termes de coûts financiers, d'image et de réputation. Nous verrons également les principaux défis auxquels sont confrontés les établissements financiers dans la maîtrise de ce risque diffus.

Ce cadre général nous permettra de disposer des éléments de définition et de contexte nécessaires pour aborder par la suite l'identification, l'évaluation et la gestion spécifique du risque opérationnel.

1-1- La notion du risque :

1-1-1- Définition du risque :

Le moteur de recherche propose plusieurs synonymes de ‘‘risque’’ : Danger, menace, nuage, aléa, hasard, inconvénient, péril .

Par référence au dictionnaire « le robert » de la langue française, le mot ‘’ risque " désigne : [1]

1. Danger éventuel plus ou moins prévisible ;
2. Éventualité d’un événement qui peut causer un dommage.
3. Fait de s’exposer à un danger (dans l’espoir d’obtenir un avantage).

Selon ISO 31000 : «*le risque est l’effet (Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces) de l’incertitude sur l’atteinte des objectifs. Menace qu’un événement, une action, ou une inaction affecte la capacité de l’organisation à atteindre ses objectifs et compromettre la création de valeur.* »[2]

L’IFACI, quant à elle, donne la définition suivante au risque : « *un ensemble d’aléas susceptibles d’avoir des conséquences négatives sur une entité et dont le contrôle interne et l’audit ont notamment pour mission d’assurer autant que peut se faire la maîtrise* »[3]

Le risque donc peut être défini comme étant tout événement probable dont la survenance engendre des pertes.

1-1-2- Les types des risques bancaires :

La banque à travers son activité, est exposée à une multitude de risques. Ces derniers sont classés selon leur nature, des risques financiers et des risques non financiers.

A- Les risques financiers :

Un risque financier est tout risque lié aux variations de prix des actifs financiers. On distingue généralement quatre grandes familles de risques financiers :

1- Les risques de contrepartie

Le risque de contrepartie-ou de crédit ou encore de signature, est le risque de défaillance d’une contrepartie sur laquelle est détenue une créance ou un engagement de hors-bilan assimilable.

À titre principal, le risque de contrepartie est le risque de perte lié à la défaillance d’un débiteur sur lequel l’établissement de crédit détient un engagement, quelles que soient la nature du débiteur et la forme de cet engagement.

---

[1] **https://dictionnaire.lerobert.com/ consulté le 09/07/2023 à 20h45**
[2] **ISO 31000 DEUXIEME édition 2018-02**
[3] **Coopers-Lybrand, La Pratique du contrôle interne, IFACI (institut français de l’audit et du contrôle interne), ED. ORGANISATION, p19**

Il s'agira donc :

- De crédits octroyés, lesquels peuvent être assortis de différentes garanties ;
- De titres détenus (actions, obligations) dans le cadre des métiers de banque commerciale et/ou de banque de marché ;
- D'engagement de hors-bilan, engendrant un risque de contrepartie certain par exemple, si la banque accorde une garantie (caution) contre de crédits distribués par d'autres établissements de crédit ou potentiel tel que l'ouverture de crédit documentaire, laquelle représente un crédit potentiel qui deviendrait effectif en cas de tirage.

La défaillance du débiteur se traduit, en effet, par la survenance d'une perte correspondant au non-recouvrement partiel ou total des fonds prêtés ou à l'appel en garantie.

2- **Risque de liquidité :**

Le risque de liquidité (d'illiquidité) représente pour un établissement de crédit l'éventualité de ne pas pouvoir faire face, à un instant donné, à ses engagements ou à ses échéances même par la mobilisation de ses actifs. Le risque d'illiquidité dépend d'une part de sa situation propre, d'autre part de facteurs externes comme l'offre des marchés financiers.

La matérialisation du risque de liquidité peut en effet survenir à l'occasion :

- D'un retrait massif de l'épargne ou des dépôts de la clientèle. Ce risque peut aussi provenir de retard ou de non-recouvrement des créances sur sa clientèle, risque de défaillance de contrepartie ;
- D'une perte de confiance du marché envers l'institution en question.
- D'une crise de liquidité générale du marché (cause exogène à l'établissement).

- **Risque de solvabilité :** Ce risque représente l'insuffisance des fonds propres pour le but d'absorber les pertes éventuelles par la banque, néanmoins, il ne découle pas uniquement d'un manque de fonds propres, mais aussi des divers risques encourus par la banque tel que, le risque de crédit, le risque de marché, du taux d'intérêt et de change. Les banques sont conscientes que l'exposition à ce type de risque peut mettre en péril leur activité, c'est pourquoi les institutions financières essaient d'adapter leurs FP aux risques pour faire face à ce type de risque d'insolvabilité.

3- **Le risque de marché :** désigne le risque de pertes sur des positions de bilan et de hors bilan à la suite de variations et des fluctuations des prix du marché, il regroupe les risques relations aux instruments liés aux taux d'intérêt et titres de propriété du

portefeuille de négociation ; les deux risques de marché les plus importants sont : le risque de taux d'intérêt et le risque de change.

- **Risque du taux d'intérêt :** Le risque est encouru suite à une variation des taux d'intérêt du fait de l'ensemble des opérations de bilan et de hors bilan, à l'exception, le cas échéant des opérations soumises aux risque de marché.[1]
- **Risque de change :** Le risque de change, également connu sous le nom de risque de devises, est la possibilité qu'une fluctuation des taux de change affecte la valeur des investissements ou des transactions dans des devises étrangères.[2]

B- Risques non financiers :

1- **Le risque de réputation :** La réputation de l'entreprise est liée à son activité, elle ne peut risquer de l'entacher sous peine de subir une atteinte à son image, qui se manifeste par des conséquences qui peuvent affecter le volet économique, juridique et financier allant même jusqu'à menacer la pérennité de l'entité.

2- **Risque systémique** : Désigne toute éventualité pour une économie qu'apparaissent des états dans lesquels les réponses des agents aux risques qu'ils perçoivent les amènent à élever l'insécurité générale.[3]

3- **Risque stratégique** : lié au choix du management, la banque procède à une planification complexe qui nécessite un engagement colossal en ressources (ex : pénétration d'un nouveau marché) ; la banque prend un risque majeur en cas d'échec : les ressources engagées seraient perdus dans une optique d'acquérir un avantage stratégique.

4- **Risque de garantie** : Ce type de risque peut apparaître si la garantie attendue n'est pas valide ou si une chute des cours ne permet plus à la banque d'exercer sa garantie de nantissement sur titres.[4]

5- **Le cyber-risque : Un risque opérationnel** : Le cyber-risque et le cyber fraude, défini comme un risque unique et ponctuel, tel que la défaillance des systèmes, les erreurs et omissions, la fraude ou les dommages non assurés aux installations et aux équipements (Henrard, 2009). Il s'agirait donc d'un RO dans le cyber environnement. Ainsi, cette définition du cyber risque couvre : tous les risques émanant de l'emploi de

---

[1] **Règlement de la banque d'Algérie n°11-08**
[2] **Règlement de la banque d'Algérie n°11-08**
[3] **Http://www.iefpedia.com/malay/wp-content/uploads/2009/08/risques-bancaires-etenvironnement-international**
[4] **Inspiré du mémoire : Mr Benaceur Youcef, « le rôle de l'audit dans la gestion des risques opérationnels », ESB, 2011, p11.**

données électroniques et de leur transmission, les dégâts physiques pouvant être causés par des cyber attaques, les fraudes commises par abus des données, toute responsabilité découlant de l'emploi fautif des données, du stockage et du transfert de ceux-ci, la disponibilité, l'intégrité et la confidentialité des infos électroniques, qu'elles soient liées aux particuliers, aux Entreprise s ou aux gouvernements.

6- **Le risque de non-conformité** :C'est le risque de sanction judiciaire, administrative ou disciplinaire, risque de pertes financières significatives, il naît du non-respect des dispositions législatives ou réglementaires, des normes professionnelles ou les instructions de l'organe lui-même.

7- **Le risque opérationnel:** C'est le risque de pertes résultant de carences ou de défaillances attribuables à des procédures, au personnel, les systèmes internes ou à des événements extérieurs.[1] (nous allons détailler ce risque par la suite).

1-2- Notions sur le risque opérationnel :

1-2-1- Définitions du risque opérationnel :

La définition du risque opérationnel selon le comité de Bâle :[2]

« Le risque opérationnel se définit comme le risque de pertes résultant de carences ou de défaillances attribuables à des procédures, personnels et systèmes internes ou à des Evènements extérieurs. La définition inclut le risque juridique, mais exclut les risques stratégiques et d'atteinte à la réputation ».

La définition du risque opérationnel selon la Banque d'Algérie : [3]

« On entend par risque opérationnel, le risque de perte résultant de carences ou de défaillances inhérentes aux procédures, personnels et systèmes internes des banques et établissements financiers, ou à des événements extérieurs. Cette définition exclut les risques stratégiques et de réputation, mais inclut le risque juridique. »

1-2-2- Typologie du risque opérationnel :

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

1- **Fraude interne :** pertes résultant des actes qui visent à frauder, détourner des biens ou à tourner des règlements, la législation ou la politique de l'Entreprise et qui implique au moins une partie interne à l'entreprise.

---

[1] **Support de cours Mr chihebGhanmi, IFID, 2023.**

[2] **https://www.bis.org/bcbs/cp3fullfr.pdf consulté le 10/07/2023 à 13h40.**

[3] **Selon l'article 20 du REGLEMENT N°2014-01 DU 16 FEVRIER 2014 PORTANT COEFFICIENTS DE SOLVABILITE APPLICABLES AUX BANQUES ET ETABLISSEMENTS FINANCIERS**

2- **Fraude externe :** toute perte due à des actes visant à frauder, détourner des biens ou à tourner des règlements, la législation de la part d'une tierce personne. Notons que les fraudes internes et externes sont intentionnelles. Par ailleurs, dans ce qui suit l'erreur est non intentionnelle.

3- **Insuffisance des pratiques internes concernant les ressources humaines et la sécurité du lieu de travail :** Ce sont les pertes résultant d'actes non conformes à la législation ou aux conventions liées à l'emploi, la santé ou encore la sécurité, des demandes d'indemnisation au titre d'un dommage personnel ou d'atteintes à l'égalité ou actes de discrimination.

4- **Négligence des règles clients, produits et pratiques commerciales:** Il s'agit des pertes résultant d'un manquement, non intentionnel ou dû à la négligence, à une obligation professionnelle envers des clients particuliers ou de la nature ou conception d'un produit.

5- **Dommages aux actifs corporels :** Toute perte due à une destruction ou dommage résultant d'une catastrophe naturelle ou d'autres sinistres.

6- **Interruption d'activité et dysfonctionnement des systèmes :** Cette composante couvre les interruptions et dysfonctionnements des systèmes en ce qui concerne le matériel, le logiciel, la télécommunication et les perturbations d'un service.

7- **Dysfonctionnement des processus de traitement (exécution, passation, livraison, produits finis) :** Ce sont des pertes résultant d'un problème dans le traitement d'une transaction ou dans la gestion des processus ou des relations avec les contreparties externes.

A ces sept catégories d'événements viennent s'ajouter huit lignes (08) de métiers donnant une matrice de 56 cases représentatives de l'ensemble des activités bancaires et risques associés.

Tableau N°01: Présentation des 08 lignes de métiers telles que définies par Bâle II

Niveau 1	Niveau 2	Activités
Ingénierie financière	Financement des entreprises	F&A, engagements, privatisations, titrisations, recherche, titre de dette, actions, prêts consortiaux, intro en bourse, placement sur le marché secondaire.
	Financement des collectivités locales	
	Banque d'affaires	
	Service conseil	
Négociation de vente	Ventes	Valeurs à revenus fixes, actions, change, MP, crédit financement, titres sur position propre, prêts et pensions, courtage, titre sur dettes, courtage de premier rang.
	Tenue de marché	
	Positions pour compte propre	
	Trésorerie	
Banque de détail	Banque de détail	Prêts et dépôts, services bancaires, fiducie, gestion de patrimoine, conseil en placements, carters, commerçants/entreprises
	Banque privée	
	Cartes	
Banque de gros	Banque commerciale	Financement de projets , immobilier, exportations, commerce, crédit bail, prêts, garanties, LDC.
Paiements et règlements	Clientèle extérieure	Paiements et recouvrements, transferts de fonds, compensations et règlements
Fonction d'agent	Conservation	Dépôts, certificats, prêts de titres, opérations de société
	Prestations d'agents aux entreprises	
	Service fiducie aux entreprises	
Gestion d'actifs	Gestion de portefeuille discrétionnaire	Agents émetteurs et payeurs
	Gestion de portefeuille non discrétionnaire	
Courtage	Courtage de détail	Exécution et service complet

Source : Comité de Bâle sur le Contrôle Bancaire 2004

1-3- Cadre réglementaire et Calcul des Exigences en Fonds Propres pour la couverture des risques opérationnels :

1-3-1- Le cadre réglementaire des risques opérationnels :

a. La règlementation Bâloise :

Les accords de Bâle, élaborés par le Comité de Bâle, constituent la réglementation prudentielle internationale dans le secteur bancaire.

- **Bâle I (1988) :** introduit un ratio de fonds propres sur les risques de crédit à 8%.
- **Bâle II (2004) :**

❖ **Pilier 1 :** calcul des fonds propres pour le risque de crédit, de marché et opérationnel.

❖ **Pilier 2 :** procédures de surveillance prudentielle par les autorités.

❖ **Pilier 3 :** discipline de marché via la communication financière.

- **Bâle III (2010) :** renforcement des fonds propres, ratios de liquidité, ratio d'effet de levier.
- **Bâle IV (en cours) : révision** de Bâle III sur la comparabilité des actifs pondérés et les planchers de fonds propres.
- En Algérie, transposition de Bâle II via différents règlements de la Banque d'Algérie sur le contrôle interne, les coefficients de solvabilité, etc.

En résumé, les accords de Bâle successifs visent à renforcer la réglementation prudentielle bancaire, notamment sur les fonds propres et la prise en compte des risques.

b. La règlementation Algérienne :

- Le règlement n°11-08 du 28 novembre 2011 vise à aligner le système Algérien sur les procédures prudentielles du Comité de Bâle sur le Contrôle Bancaire.
- Il impose aux banques et établissements financiers de mettre en place des systèmes de mesure et de surveillance des risques (opérationnels, de crédit, de marché, etc.) et d'établir une cartographie des risques.
- Il exige aussi des plans de continuité d'activité et un dispositif de contrôle interne efficace.
- La loi sur la monnaie et le crédit de 2010 renforce la surveillance des risques et le contrôle interne dans le secteur bancaire.
- Le règlement n°14/01 du 16 février 2014, inspiré de Bâle II et III, impose un coefficient minimum de solvabilité de 9,5% et l'intégration des RO et d'un coussin de sécurité de 2,5% dans le calcul.
- Les banques doivent aussi constituer des provisions pour RO et intégrer un coussin de sécurité supplémentaire en fonds propres.

En résumé, ces réglementations visent à renforcer la solidité du secteur bancaire Algérien face aux risques.

1-3-2- Calcul des exigences en fonds propres :

Trois approches sont définies par Bâle II pour le calcul des exigences en fonds propres pour la couverture du RO:

1. **L'approche de l'indicateur de base (BIA)** [1]

- Méthode la plus simple, pas de critère d'éligibilité
- Applique un taux forfaitaire (alpha=15%) au PNB moyen sur 3 ans

[1] **Ariane Chapelle, Georges Hübner et Jean-Philippe Peters « Le risque opérationnel implication de l'accord de bâle pour le secteur financier », Edition : Larcier.2005,p61.**

2. **L'approche standard**

Distingue 8 catégories d'activités auxquelles sont associés des coefficients spécifiques (bêta)

EFP = Sommes des bêta x PNB de chaque activité

3. **L'approche avancée (AMA)**

La plus sophistiquée, repose sur des modèles internes développés par la banque 4 méthodes :

- IMA : mesure de la perte attendue pour chaque couple risque/ligne de métier
- LDA : analyse des distributions statistiques des fréquences et sévérités de pertes
- Scorecard : indicateurs quantitatifs et qualitatifs par catégorie de risque
- Scénarios : évaluation de la fréquence et sévérité d'événements générateurs de pertes

L'AMA permet un rapprochement entre les besoins en fonds propres et les risques réels de la banque.

- **Limites :** manque de comparabilité entre établissements du fait de modèles mathématiques différents.

En résumé, Bâle II définit 3 approches de complexité croissante pour le calcul des exigences de fonds propres pour couvrir le RO, la plus sophistiquée étant l'approche de mesures avancées basée sur des modèles internes.

1-4- Dispositif de maîtrise des risques opérationnels (DMRO)

- La gouvernance du dispositif de management du RO (DMRO) définit les rôles, les politiques et les procédures pour identifier, évaluer, gérer et surveiller les risques.
- Les principales étapes de la gestion du risque opérationnel sont :

1. Identification des risques via des outils comme la cartographie des processus.
2. Évaluation qualitative et quantitative des risques à travers des méthodes comme la cartographie des risques et l'analyse de scénarios.
3. Révision et mise à jour régulière des risques.
4. Traitement des risques par des mesures d'atténuation comme le contrôle interne, l'analyse bow-tie et les plans d'actions.

- Le contrôle interne permet de prévenir, détecter et corriger les risques via des contrôles à 3 niveaux. Son efficacité se mesure par des tests de contrôle.
- Le reporting du risque opérationnel implique la collecte de données, leur analyse, la production de rapports et la communication aux parties prenantes afin de prendre des décisions éclairées et démontrer la conformité.

En résumé, le DMRO définit la gouvernance et le processus pour identifier, évaluer, traiter et suivre les risques opérationnels, notamment via le contrôle interne et le reporting.

Au terme de cette section délimitant le périmètre du risque opérationnel, nous disposons désormais des éléments de définition et de contexte nécessaires. Le RO est un risque diffus, aux sources variées, qui peut impacter significativement les performances des banques s'il n'est pas correctement géré.

La maîtrise du risque opérationnel impose aux établissements financiers d'avoir une approche transverse, afin d'identifier l'ensemble des zones de risque au sein de leurs activités. Parmi les outils utilisés à cette fin, la cartographie des risques opérationnels tient une place centrale.

Dans la prochaine section, nous nous intéresserons ainsi plus spécifiquement à la cartographie comme méthode d'évaluation et de gestion des risques opérationnels. Nous détaillerons les objectifs, les modalités de construction et les limites de cet outil devenu incontournable dans le secteur bancaire.

La cartographie des risque opérationnel permet une vue d'ensemble des expositions d'une banque et hiérarchise les zones de risque prioritaires. Elle constitue un pré-requis essentiel pour mettre en place des actions ciblées de prévention et de mitigation de ces risques.

SECTION 02 : GÉNÉRALITÉS SUR LA CARTOGRAPHIE DES RISQUES

La cartographie des RO est devenue un outil incontournable pour les établissements bancaires et financiers dans le cadre de leur gestion des risques. Cependant, cet exercice complexe nécessite de bien comprendre les concepts, objectifs et méthodologies qui le sous-tendent.

Cette section a pour but de présenter les généralités relatives à la cartographie des risques opérationnels. Nous commencerons par définir précisément ce qu'est une cartographie des risques et quels sont ses apports pour l'identification et l'évaluation des risques.

Nous expliciterons ensuite les objectifs recherchés à travers la mise en place d'une cartographie des risques opérationnels au sein d'un établissement financier. Les enjeux en termes de gestion des risques seront présentés.

Enfin, nous aborderons les principales étapes méthodologiques pour la construction d'une cartographie des risques opérationnels : périmètre, identification des processus, recensement des risques, évaluation qualitative et quantitative.

Cette section permettra de disposer des bases conceptuelles et méthodologiques en vue d'appréhender par la suite la mise en œuvre opérationnelle de la cartographie au sein des banques.

2.1. Définition et objectifs de la cartographie :

2.1.1. Définition de la cartographie :

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

L'IFACI dans une étude menée en 2005 présente la cartographie des risques comme «***une représentation graphique de la probabilité et de l'impact d'un ou de plusieurs risques. Les risques sont représentés de manière à identifier les risques les plus significatifs (probabilité et / ou impact la ou le plus élevé(e)) et les moins significatifs (probabilité et / ou impact la ou le plus faible)***».

Suite à ces différentes définitions, nous pouvons conclure que la cartographie des risques est un outil d'aide à la décision :

- Permettant l'identification et la hiérarchisation des risques selon leur impact et leur degré de survenance.
- Qui se présente comme un outil dynamique permettant de recenser, évaluer et classifier les risques d'une organisation selon leur signification (en fonction de deux critères à savoir, la probabilité d'occurrence et l'impact d'un ou plusieurs risques) tout en décrivant le plus précisément possible les risques majeurs auxquels l'entreprise est confrontée.
- Permettant la mise en place d'un plan en vue de la maîtrise des risques et/ou la réduction de leurs impacts.[1]

2.1.2. Les objectifs de l'élaboration de la cartographie :

Les objectifs de la cartographie des risques sont :[2]

- Recenser de façon exhaustive les risques potentiels dans l'organisation ;
- Inventorier, évaluer et classer les risques par domaine, fonction ou processus de gestion ;[3]

---

[1] MVOM Yannick Rahmane, Elaboration d'une cartographie des risques opérationnels de trésorerie, 2009, p37.

[2] Altair Conseil, Maitrise des risques : Elaborer la cartographie des risques (démarches et méthodes), Paris, 2008, p2

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

- Hiérarchiser les risques selon leur impact et probabilité d'occurrence, en décrivant précisément les risques majeurs ;
- Elaborer graphiquement une représentation des risques pour mieux les visualiser et les maîtriser ;
- Renforcer le processus de gestion des risques ;
- Améliorer le contrôle interne et l'élaboration de plans d'audit ;
- Perfectionner la communication sur les risques entre les parties prenantes ;
- Informer les responsables pour adapter la gestion de leurs activités ;

L'objectif global est d'élaborer des plans d'actions pour ramener les niveaux d'incertitude à des niveaux acceptables.

2.2. Les types de cartographie :

a. La cartographie thématique :

La cartographie thématique est un outil de recensement et d'hiérarchisation des risques liés à un thème précis. Gilbert de Mareschal (2003) définit la cartographie thématique comme « ***un outil d'identification et de hiérarchisation des risques liés à un thème spécifique*** ».

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

b. La cartographie globale :

La cartographie globale des risques vise à recenser, quantifier et cartographier l'ensemble des risques de l'organisation, tous sujets confondus. Nous pouvons également la définir comme un ensemble de cartographies thématiques et donc une synthèse, car la consolidation des cartographies thématiques des différents risques pour chaque entité pourrait mener à une cartographie globale, sous l'hypothèse que tous les risques sont cartographiés et que toutes les entités sont prises en compte.

2.3. Caractéristiques de la cartographie [1]

La cartographie des risques peut s'avérer comme étant un outil de gestion des risques, un outil d'allocation optimale des ressources et de communication :

- **Outil de gestion des risques:** la cartographie guide l'entreprise pour améliorer le contrôle interne et mettre en place de nouveaux contrôles et plans d'action pour maîtriser les risques.

[1] ***DE MARESCHAL, Gilbert (2003), La cartographie des risques, Edition Afnor, Paris.26***

- **Outil d'allocation optimale des ressources:** elle permet d'éviter le gaspillage et de répartir les ressources en fonction des priorités et profils de risques. Elle affecte les ressources aux risques majeurs.
- **Outil de communication:** elle permet d'informer les responsables pour adapter la gestion de leurs activités. Elle aide la direction générale et les « **risk managers**» à élaborer une politique de risques.

Après conception, il faut diffuser la cartographie au sein de la banque pour une meilleure prise en charge des risques par les opérationnels et instaurer une culture de gestion des risques.

2.4. Les étapes d'élaboration d'une cartographie :

2.4.1 La phase de préparation :

- Cette phase comprend: la constitution d'une équipe qualifiée, la préparation des moyens nécessaires, la définition du périmètre de la cartographie, le choix d'une typologie des risques, le choix de la démarche de conception, et l'analyse du contexte[1] avec la fixation des objectifs.
- Elle nécessite une capacité d'apprentissage et de compréhension de l'entité à travers l'analyse de ses choix stratégiques, son organisation, ses systèmes d'informations et ses activités.
- Les objectifs sont de clarifier les rôles et responsabilités et de définir le périmètre d'élaboration de la cartographie.
- Il s'agit de définir: le thème étudié, le périmètre d'activité, le niveau de réponse, le seuil de pertinence, et la règle de mesure du risque.
- Cette phase permet aussi de mettre en place la cartographie des processus, préalable logique pour mener la démarche de gestion des risques.

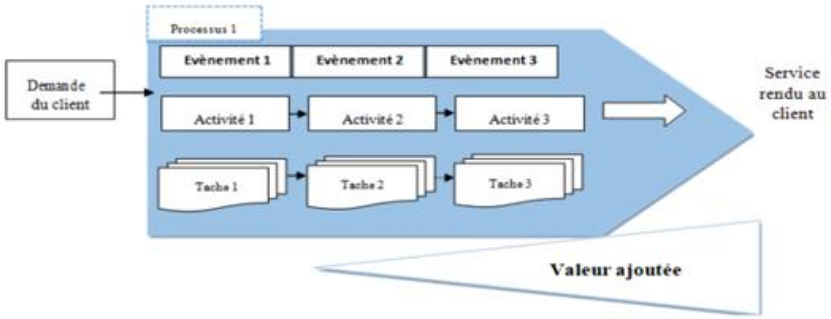
a- Définition d'un processus :

Un processus est généralement défini comme :

«***Un processus est un ensemble de ressources et d'activités liées qui transforment des éléments entrants en éléments sortants, autrement dit, c'est une boîte noire qui a une finalité (les données de sortie) et qui, pour atteindre cette finalité, utilise des éléments extérieurs***». [2]

[1] ***C.JIMENEZ &P.MERLIER,***
[2] **Y.mougin, « la cartographie des processus, édition d'organisation », paris 2004, P 37**

Figure N°01 : Représentation schématique d'un processus



Source : C. Jimenez &P. Merlier &D. Chelly, Risque opérationnel, revue banque, 2008, p57

b- Les différents types de processus :

Nous pouvons désormais distinguer trois types de processus à savoir :

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

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

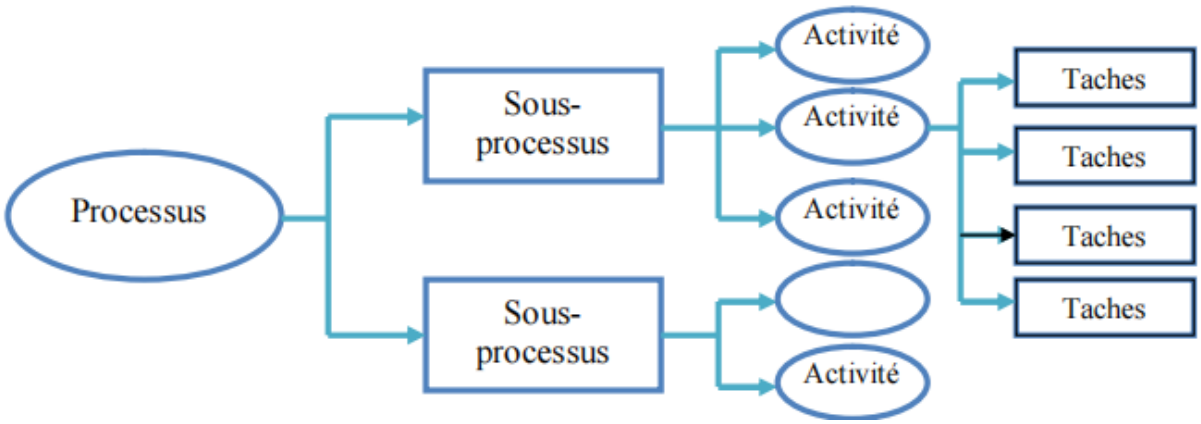
- **Les processus de pilotage (ou managériaux) :**

Ce sont les processus de management notamment les processus liés à la planification stratégique, à l'établissement des politiques, à la fixation des objectifs, à la mise en place de la communication, à la mise à disposition des ressources nécessaires et aux revues de direction et de prendre les mesures correctives nécessaires.

- **Les processus de support :**

Qui sont reliés à la bonne gestion : la GRH, la finance, la comptabilité, l'informatique et la logistique. Ils fournissent les ressources (humaines, matérielles, financières…) à tous les processus.

Figure N°02 : Décomposition d'un processus



Source : Y. Mougin La cartographie des processus, 2004, P37

c- Les caractéristiques d'un processus :

«***Il s'agit de définir le niveau de granularité de description. Un détail des processus trop léger amènera à une mauvaise interprétation de la nature et du niveau de risque***»[1].Ces caractéristiques sont communes à toutes les catégories de processus :

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

2.4.2. La phase de réalisation :

A. L'identification des risques

- Elle consiste à recenser tous les risques auxquels l'activité est exposée, en se basant sur les processus décrits.
- À chaque processus sont associés les incidents susceptibles de perturber son déroulement et d'entraver la réalisation des objectifs.[2]
- Il faut faire abstraction des contrôles existants et du dispositif de maîtrise des risques.
- L'association processus-événements à risque permet de distinguer entre des événements identiques mais situés sur des processus différents, avec des caractéristiques différentes en termes de fréquence et d'impact.

B. Evaluation des risques : L'évaluation des risques constitue une phase cruciale dans l'élaboration de la cartographie des risques. Elle se divise en deux catégories :

- ➢ **L'évaluation quantitative :** Son utilisation est étroitement liée à la disponibilité des données historiques sur les incidents, ce qui permet d'estimer la probabilité d'occurrence et l'impact d'un risque en se basant sur des évaluations par intervalles.
- ➢ **L'évaluation qualitative :** Moins précise que la méthode précédente, elle est employée lorsque la quantification des risques est impossible ou lorsque les données fiables sont insuffisantes. Cette évaluation se concentre sur l'appréciation de l'impact du risque, que ce soit sur le plan financier ou en termes d'image, ainsi que sur la fréquence des événements identifiés.

---

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

[22]« Comprendre et gérer les risques », Franck Moreau, Edition d'Organisation, 2002, p42.

Après leur identification, l'exposition aux risques inhérents est évaluée en se basant sur deux critères : la fréquence et l'impact. [1]

- « La fréquence se réfère à la probabilité qu'un événement se produise, c'est-à-dire combien de fois le risque pourrait survenir sur une période donnée. Cette mesure peut être évaluée qualitativement ou quantitativement :

- Qualitativement, la fréquence peut être catégorisée comme élevée, modérée, ou selon une échelle de 1 à 4, par exemple.
- Quantitativement, elle se base généralement sur une probabilité réelle pour une période donnée (entre 0 et 1), ou une fréquence par jour, par mois, par an, etc. Cela nécessite des infos à jour pour estimer la probabilité d'occurrence. »

- « L'impact se rapporte aux répercussions financières (perte), juridiques (non-conformité avec la réglementation en vigueur) ou les effets sur la réputation de l'établissement qui résultent de la matérialisation du risque. De la même manière que pour la fréquence, l'impact peut être évalué selon deux méthodes distinctes :

- En utilisant des critères qualitatifs : qualifiant l'impact comme étant faible, modéré ou élevé. Ces qualificatifs seront ensuite convertis en notes, par exemple, sur une échelle de 1 à 4.

- En utilisant des critères quantitatifs : basés sur des données financières ou opérationnelles liées aux pertes. »

Il peut être complexe d'évaluer de manière précise les conséquences financières en utilisant des méthodes qualitatives ce qui nécessite des ressources humaines et techniques considérables. De plus, certains impacts, tels que ceux sur le plan humain ou de la réputation, peuvent être difficiles à quantifier. Par conséquent, l'adoption d'une approche qualitative et le recours à des échelles de gravité peuvent simplifier cette évaluation.

Une fois que les données concernant la « fréquence » et l'"impact" sont acquises, le risque peut être évalué en appliquant la formule suivante :

Risque brut=Impact*Fréquence

C. Évaluation du (DMR) :

Conformément à la norme ISO 31000, le DMR représente une « *action qui maintient et/ou modifie un risque* »

[1] **Gilbert de Marshal, La Cartographie Des Risques, ED. AFNOR, 2003,p9**

C'est « *Un moyen de maîtrise du risque inclut, sans toutefois s'y limiter, n'importe quels processus, politique, dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient un risque* ».

L'évaluation du DMR repose sur l'analyse des structures organisationnelles et des mécanismes de contrôle interne. L'efficacité de ce système contribue à diminuer le risque initial. Les DMR peuvent être classés en trois catégories :

- Contrôles automatiques /Outils (appareils, machines…) ;
- Directives /Procédures ;
- Contrôles manuels / Visuels.

D. Identification et appréciation des contrôles internes existants

- Elle vise à mettre en lumière les mesures prises pour prévenir les conséquences négatives des risques, avant d'établir la cartographie.
- Il faut énumérer de manière détaillée les procédures en vigueur.
- Vérifier si elles sont adaptées à la nature des risques et si elles réduisent leurs conséquences négatives.

D'après IFACI (2006), l'évaluation de l'efficacité du dispositif de contrôle se fait pour chaque combinaison risque/processus, sur base de critères comme:

- **Pertinence:** utilité du contrôle par rapport à son coût.
- **Fiabilité:** capacité à fonctionner de manière continue.
- **Qualité de conception et mise en œuvre.**
- **Efficience:** optimisation des coûts, performance et délais.
- **Efficacité:** capacité à atteindre les objectifs.

E. Détermination des risques résiduels :

Le risque résiduel, ou risque net, représente l'importance du risque une fois que les mesures de contrôle ont été appliquées. Il mesure l'impact réel que l'organisation pourrait potentiellement subir en termes financiers et d'image, en tenant compte des systèmes de prévention et de détection en place.

L'évaluation du risque résiduel peut être réalisée de la manière suivante :[1]

Risque résiduel (risque Net)= (impact inhérent*probabilité inhérent)-DMR

Pour attribuer une cote aux risques résiduels, le processus est similaire à celui utilisé pour les risques inhérents (bruts). L'évaluation du risque net implique le calcul de la gravité

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

inhérente du risque après avoir pris en compte l'efficacité et la performance des mesures de contrôle.

F. La hiérarchisation des risques :

La hiérarchisation des risques vise à les classer selon leur niveau d'importance, facilitant ainsi leur gestion. Cette étape permet d'établir une liste précise de risques en fonction de leur degré de criticité. Le classement des risques se base sur les paramètres d'évaluation. Trois scénarii peuvent se présenter :

- **Cas 01 :** Si la fréquence et la gravité sont toutes deux élevées, le risque est considéré comme majeur, mettant ainsi en péril les objectifs de l'entreprise.
- **Cas 02 :** Si la fréquence et la gravité sont toutes deux faibles, le risque est qualifié de mineur, n'impactant pas les objectifs de l'entreprise.

- Lorsque les deux paramètres d'évaluation ne sont pas simultanément élevés ou simultanément faibles, le risque est qualifié d'intermédiaire. Il peut potentiellement compromettre la réalisation des objectifs.

Puisque l'organisation comporte divers risques, il n'est pas envisageable de contrôler les tous risques simultanément. Il est donc crucial de les classer du risque le plus élevé au risque le moins élevé. Cela permet de se focaliser sur les risques les plus critiques, d'améliorer le système de gestion, et de mettre en place des plans d'actions efficaces pour prioriser les mesures visant à maîtriser les risques et à les ramener à un niveau acceptable.

G. La matrice risque :

Il s'agit d'un diagramme à deux axes, généralement axé sur la probabilité et l'impact. Cette représentation graphique offre une perspective sur les risques majeurs et facilite l'identification des zones nécessitant une attention prioritaire. Les risques sont positionnés de manière à distinguer les plus significatifs des moins significatifs.

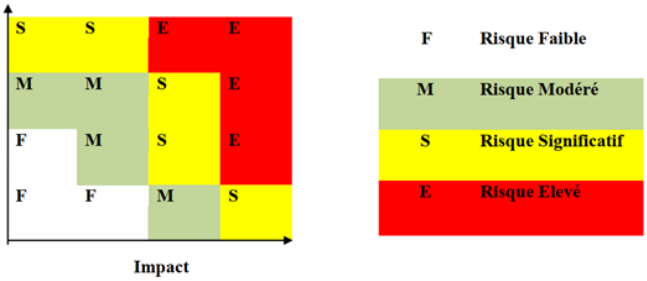
- ⇨ L'élaboration de cette matrice des risques constitue ainsi une phase cruciale lors de la mise en place de la cartographie des risques...

Il existe différentes méthodes pour visualiser une cartographie, entre autres:

- ❖ **Le graphique à « deux axes » :**

Dans ce schéma, les risques sont exprimés en fonction de leurs attributs de "fréquence" et "impact". « L'impact », ou «la gravité », est indiquée sur l'axe des ordonnées (Y), tandis que « la probabilité » est située sur celui des abscisses (X).

Figure N°03: Le diagramme à deux axes



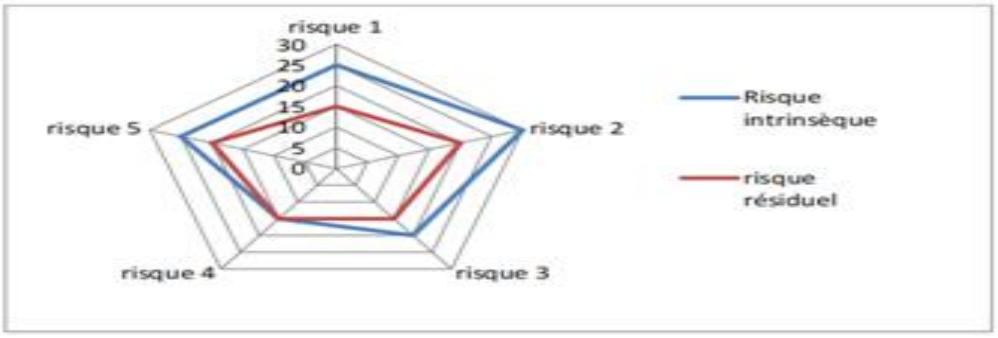
Source : « cartographie des risques », IFACI, op.cit, p 39

Ainsi, cette matrice des risques simplifiera le processus de prise de décisions et la formulation des stratégies nécessaires en vue de définir et mettre en place des plans d'actions qui visent à renforcer le « niveau de maîtrise des risques ».

❖ **La visualisation en mode RADAR ou toile d'araignée :**

Cette méthode vise à offrir une vision globale de l'exposition de l'organisation aux risques, en tenant compte de son appétence pour ces derniers. Dans ce contexte, l'échelle mesure la criticité d'un risque (c'est-à-dire un coefficient résultant de la multiplication de l'ampleur par la probabilité d'occurrence). Il s'agit d'un diagramme à multiples axes, où chaque axe représente une catégorie de risque spécifique.

Figure N°04: Diagramme Radar des risques d'une organisation



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

2.4.3. La phase d'action :

Une fois que les risques ont été identifiés, évalués et hiérarchisés en fonction de leur importance, il est judicieux pour l'organisation de déterminer les actions à entreprendre pour chaque risque. Cela commence par aborder en priorité ceux qui sont considérés comme majeurs et les plus critiques, comme déterminé dans la phase de hiérarchisation et dans l'élaboration de la matrice des risques. (MADERS & al, 2009).

a- Traitement des risques :

La gestion des risques s'effectue par le biais de différentes approches, déterminées par les particularités des risques auxquels l'entreprise est confrontée. On distingue :

- **Évitement :** Cette approche implique l'arrêt des activités à l'origine du risque ;
- **Acceptation :** Il s'agit de ne prendre aucune mesure pour altérer la « probabilité d'occurrence » et son « impact » ;
- **Réduction ou atténuation du risque :** Il s'agit d'appliquer des mesures préventives et de protection afin de réduire respectivement la probabilité de survenue du risque et son impact en cas de réalisation.
- **Partage :** Cette méthode consiste pour l'Entreprise à externaliser une partie du risque en concluant un contrat avec une société d'assurance. Cela permet de partager les charges liées aux risques, selon des conditions préalablement définies entre les parties ;

b- La mise en place d'un plan d'actions :

Dans la majorité des situations, l'instauration d'un plan d'actions implique l'introduction de contrôles additionnels ou différents de ceux déjà en place. En conséquence, il peut être nécessaire de réallouer de façon plus efficace les ressources humaines, financières et matérielles pour mettre en œuvre les décisions. Le succès du plan d'actions reposera sur l'aptitude et la proactivité des responsables désignés pour superviser les risques.

c- Plans de Continuité d'Activité :

- Un incident peut entraver l'exécution des engagements de la banque et causer d'importantes pertes financières, surtout en cas de dommages sur les infrastructures.
- Les banques doivent donc élaborer des programmes de reprise et de continuité d'exploitation pour différents scénarios plausibles.
- La gestion de la continuité d'activité identifie les menaces potentielles et leurs conséquences opérationnelles.
- Elle établit un cadre pour renforcer la résilience de l'organisation.

❖ **Les avantages du PCA :**

- ✓ Prendre en charge financièrement sa part de rétention
- ✓ Assurer la continuité des activités vitales et cruciales
- ✓ Améliorer l'image auprès des clients et partenaires
- ✓ Protéger l'entreprise contre une perte d'activité

2.4.4. La phase de reporting

Le reporting sur les risques vise à présenter de manière synthétique et claire, sous forme de tableau de bord, les éléments essentiels de la gestion des risques à toutes les parties

prenantes[1]. Les destinataires de ces tableaux de bord sont nombreux et ont des objectifs variés, parmi lesquels :

- Les responsables de processus, qui ont besoin d'un outil d'alerte et de prévention pour éviter les situations à risque ;
- Les responsables des RO, qui recherchent un indicateur du niveau de maîtrise atteint à un instant donné, ainsi que son évolution ;
- Les dirigeants, qui ont besoin d'un outil de communication facilitant la prise de décision basée sur une évaluation consensuelle des risques encourus et de leur évolution.[2]

Chaque destinataire doit recevoir des informations cohérentes, adaptées à ses besoins spécifiques, et ce, à différents niveaux de détail.[3]

La phase de reporting a pour objectif de fournir en temps réel un état d'avancement du plan d'actions d'une part, et une évaluation du niveau de maîtrise des risques d'autre part. La fiabilité de ces données doit être impeccable, car elles peuvent influencer les décisions visant à corriger le plan d'actions en cours d'exécution.

2.4.5. La phase de suivi

Cette étape englobe la supervision de la mise en œuvre concrète et de l'efficacité des plans d'actions, ainsi que leur évaluation. Son succès dépend des résultats et des décisions engendrés par le reporting. Elle implique de questionner l'efficacité des plans d'actions en se basant sur des indicateurs prédéfinis.

Les erreurs d'exécution sont identifiées et examinées, et les plans d'actions inappropriés sont remplacés par des stratégies plus efficaces. C'est durant cette phase qu'il est possible de vérifier l'adéquation entre « les risques » et les « dispositifs de contrôle mis en place ».[4]

2.4.6. Actualisation de la cartographie

La cartographie des risques est établie à un instant précis et offre une représentation du profil de risque à ce moment précis. C'est pourquoi il est impératif de la mettre à jour, de la réexaminer et de l'ajuster régulièrement. Habituellement, cela se fait de manière annuelle, mais il est évident qu'à chaque incident ou changement ayant un impact sur un événement à risque, une mise à jour de la cartographie est nécessaire.

Dans de tels cas, cela pourrait potentiellement se traduire par une augmentation de l'évaluation d'un risque. De plus, le lancement d'un nouveau produit ou la promulgation d'une

---

[1] ***KERBEL Pascal, « mise en œuvre d'un contrôle interne efficace », Edition AFNOR, 2007, p45.***
[2] ***J. Christian & al***
[3] ***MOREAU,***
[4] ***MOREAU, op.cit, p 97.***

nouvelle réglementation introduiront des risques associés qui devront être intégrés à la cartographie.

Il est vrai que la création de la cartographie des risques peut être considérée comme un exercice exigeant, compte tenu de la mobilisation de nombreuses personnes et du temps qui y est consacré. Cependant, sa mise à jour est une tâche beaucoup plus aisée en comparaison.

2.4.7. Utilisation de la cartographie des risques :

Le but de cette partie est de présenter trois axes fondamentaux qui représentent l'application principale de la cartographie des risques.

- La cartographie des risques permet d'adapter les contrôles, en offrant une vue synthétique des risques pour aider à la prise de décision et déterminer les missions de contrôle.
- Le contrôle interne vise à fournir une assurance raisonnable sur la réalisation des objectifs. Sa mise en place repose sur un référentiel cible et l'évaluation des dispositifs existants.
- L'auto-évaluation par les opérationnels permet d'identifier les risques initiaux, évaluer les dispositifs de contrôle, déduire l'exposition nette et élaborer des plans d'action.
- La cartographie est un outil pour l'audit interne dans la définition de son plan de missions,
- Elle permet de classifier les incidents, identifier les processus à risque élevé, évaluer les possibilités de transfert/financement des risques, et élaborer des stratégies d'action pour renforcer le contrôle permanent.
- Les plans d'action intègrent les dispositifs existants et sont suivis/ajustés après leur mise en œuvre.

Au terme de cette section, nous disposons désormais d'une vue d'ensemble des concepts clés et de la méthodologie relative à la cartographie des risques opérationnels.

Nous avons vu que cet outil permet d'identifier de manière structurée les principales zones de risque d'une banque. Sa construction repose sur l'analyse des processus, l'inventaire des risques et leur évaluation selon des critères qualitatifs et quantitatifs.

Cependant, la réalisation d'une cartographie représente un projet complexe. Sa mise en œuvre au sein d'un établissement financier nécessite la réunion de certains facteurs clefs de succès.

Dans la prochaine section, nous nous intéresserons précisément aux motivations, freins et bonnes pratiques dans le cadre d'une démarche de cartographie des risques opérationnels. L'adhésion des équipes et la qualité des données apparaissent notamment comme des éléments déterminants pour tirer tous les bénéfices de cet outil de pilotage des risques.

SECTION 03 : LES MOTIVATIONS, LES OBSTACLES ET LES FACTEURS DE RÉUSSITE D'UNE CARTOGRAPHIE DES RISQUES

La cartographie des risques opérationnels est un exercice stratégique dans le cadre de la gestion des risques bancaires. Cependant, sa mise en œuvre au sein d'un établissement financier représente un projet complexe, soumis à certaines conditions de réussite.

Cette section sera consacrée à l'analyse des motivations, des principaux obstacles et des facteurs clés de succès pour la réalisation d'une cartographie des risques opérationnels.

Nous présenterons tout d'abord les objectifs recherchés par les banques à travers cet exercice de cartographie, en termes de connaissance des risques, de conformité réglementaire et d'aide à la décision.

Nous identifierons ensuite les principales difficultés rencontrées lors de l'élaboration d'une cartographie des RO : adhésion des équipes, qualité des données, maintien dans le temps.

Enfin, nous détaillerons les bonnes pratiques et points de vigilance permettant de mener à bien un projet de cartographie au sein d'un établissement bancaire. Cette analyse permettra de comprendre les conditions nécessaires pour tirer tous les bénéfices de cet outil de pilotage des risques.

3.1. Les motivations de la mise en place d'une cartographie des risques

Plusieurs motivations peuvent inciter les dirigeants d'une banque à opter pour l'élaboration d'une cartographie des risques plutôt que de recourir à d'autres outils de gestion des risques :

- **Plan d'actions:** La cartographie simplifie la gestion en mettant en évidence les domaines d'actions prioritaires sur les risques.
- **Référentiel des risques:** Elle fournit un référentiel homogène sur les risques aux dirigeants et opérationnels, avec une définition commune et une méthode partagée d'évaluation et de contrôle.
- **Communication sur les risques:** C'est un outil de communication interne permettant aux dirigeants de suivre l'évolution des risques majeurs, et un outil de communication externe. (DE MARSCHAL, 2003).
- **Contraintes réglementaires bancaires:** Les banques doivent constituer des fonds propres pour couvrir leurs risques, d'où la nécessité d'outils d'identification et d'évaluation des risques. La cartographie est une étape préalable de gestion des risques.
- **Aide à l'allocation des ressources:** La cartographie permet d'allouer les ressources aux secteurs les plus exposés aux risques.

3.2. Les principaux facteurs de réussite d'une cartographie des risques

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

- Des objectifs clairs et soigneusement communiqués.
- Un soutien motivé de la DG.
- La constitution d'une équipe de travail de haute qualité.
- La désignation d'un responsable de projet compétent.
- Une définition précise et complète du périmètre des risques pertinents.
- L'assurance de la disponibilité des ressources nécessaires.
- La prise en considération de la culture d'entreprise, car la gestion des risques dans une organisation est étroitement liée à sa culture d'entreprise.
- L'approche opérationnelle et concrète du projet.

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

- Surcroît de travail et d'efforts pour les opérationnels déjà occupés par leurs tâches quotidiennes.
- Incompréhension de l'utilité de cet exercice qui peut révéler des faiblesses et lacunes.
- Complexité due à l'hétérogénéité et la diversité des risques opérationnels.
- Absence pendant longtemps d'un langage commun et de définitions claires sur les concepts de risque opérationnel.
- Difficulté à prendre en compte les spécificités régionales et des métiers dans les grands groupes.
- Risque de manque d'objectivité en cas d'auto-évaluation.
- Nature intrinsèque du lien entre les RO et l'organisation.
- Complexité de la quantification des pertes, surtout si l'impact est étalé dans le temps.
- Difficulté à maintenir une cartographie complète et validée par les métiers.

La cartographie des risques opérationnels est devenue un outil incontournable pour les banques et établissements financiers. Nous avons vu au cours de ce chapitre que la cartographie permet une identification structurée des principaux risques opérationnels et une évaluation de leur criticité.

La construction d'une cartographie suit une méthodologie rigoureuse, depuis l'analyse des processus jusqu'à l'évaluation qualitative et quantitative des risques. Cet exercice stratégique vise à améliorer la connaissance du profil de risque opérationnel de l'établissement.

[1] **FORTUGUE & al, « cartographie des risques : quelle valeur ajoutée ? Quel processus ? », 2001, P76**

Cependant, la réussite d'un projet de cartographie nécessite de surmonter certains défis : adhésion des équipes, qualité des données, maintien dynamique de l'outil. Une gouvernance adaptée et une démarche participative sont des facteurs clés de succès.

La cartographie des risques opérationnels permet in fine de hiérarchiser les priorités en matière de maîtrise des risques et d'allouer les ressources à la prévention et à la réduction des risques les plus critiques. Cet outil de pilotage s'impose désormais comme une composante essentielle des dispositifs de gestion des risques dans le secteur bancaire.

CHAPITRE 02 :

UN APERCU SUR LA MONÉTIQUE

CHAPITRE 02 : UN APERCU SUR LA MONÉTIQUE

La monétique, également appelée « transactions bancaires électroniques », occupe une place croissante dans les services bancaires et les moyens de paiement. Elle regroupe l'ensemble des techniques permettant d'effectuer des opérations bancaires à distance via des terminaux électroniques et des automates de banque.

Dans ce chapitre, nous proposerons un aperçu général sur la monétique, son évolution et ses enjeux pour les banques.

Nous commencerons par définir précisément ce qu'est la monétique et quelles sont les opérations qu'elle recouvre, comme le paiement par carte bancaire, les retraits d'espèces ou les virements électroniques.

Nous retracerons ensuite l'historique du développement de la monétique, des premiers distributeurs automatiques de billets jusqu'à la démocratisation récente du paiement sans contact et du paiement mobile.

Enfin, nous aborderons les perspectives d'avenir et les défis que représente la monétique pour les banques, entre innovation technologique, concurrence accrue et impératifs de sécurité.

Ce chapitre permettra ainsi de disposer d'une vue d'ensemble sur la place grandissante qu'occupe la monétique dans les services bancaires contemporains.

SECTION 01 : PRÉSENTATION GLOBALE DE LA MONÉTIQUE

La monétique, contraction de "monnaie" et "électronique", désigne l'ensemble des moyens de paiement scripturaux ne faisant pas appel à des espèces ou des chèques. Elle occupe une place centrale dans les services bancaires modernes.

Cette section a pour objectif de présenter une vue d'ensemble de la monétique bancaire, ou monétique de paiement.

Nous commencerons par définir précisément le concept de monétique et les opérations qu'il recouvre : paiement par carte, virement électronique, prélèvement... Nous présenterons les différents instruments monétiques utilisés aujourd'hui par les banques.

Nous détaillerons ensuite les acteurs qui interviennent dans le système monétique, depuis l'émetteur de la carte jusqu'aux réseaux d'acceptation. Leurs rôles respectifs seront explicités.

Enfin, nous aborderons les enjeux de la monétique en termes de gains de productivité, de rapidité et de sécurité des transactions, mais aussi de concurrence entre les prestataires de services de paiement.

Cette vue d'ensemble permettra de mieux appréhender le fonctionnement et les défis de la monétique bancaire.

1-1- Définition de la monétique :

La CE définit la monnaie électronique comme : *« une valeur monétaire stockée électroniquement sur un support électronique tel une carte à puce ou une mémoire d'ordinateur, émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise, acceptée comme moyen de paiement par des entreprises autres que l'institution émettrice, produite pour être mise à la disposition des utilisateurs comme substitut électronique des pièces et des billets de banque »* [1]

La monétique englobe toutes les technologies mises en place pour l'utilisation des cartes bancaires. Elle permet, en plus des échanges d'argent de manière dématérialisée, la gestion des risques des cartes bancaires, de la distribution automatique des billets ainsi que des systèmes électroniques de transfert d'infos ou de fonds.

En effet, la monétique permet de contourner l'utilisation d'argent liquide, d'automatiser les opérations de gestion, de renforcer la sécurité des installations, de rendre l'utilisation des services plus aisée et de fidéliser la clientèle.

1-2- Objectifs de la monétique

Lors de l'introduction de la monétique, plusieurs objectifs ont été définis :

1. Réduire l'utilisation d'argent liquide dans les transactions commerciales, ce qui conduira à une diminution de l'importance de l'économie informelle dans le pays.
2. Favoriser le développement de nouveaux services bancaires, contribuant ainsi à la généralisation des moyens de paiements modernes.
3. L'évolution de la monétique permettra aux titulaires de comptes bancaires de retirer de l'argent de manière ubiquitaire.

Ainsi, le lancement de la monétique vise à moderniser la population et, par conséquent, à accroître le taux de bancarisation de l'économie.

1-3- Les concepts de la monétique :

La monétique englobe trois concepts fondamentaux :[2]

1-3-1. Système de paiement électronique :

La monétique concerne le domaine des paiements électroniques, impliquant les éléments suivants :

- Les cartes à puce ou à piste magnétique.
- Les terminaux de paiement électronique TPE et/ou les DAB/GAB.

---

[1] Article de la recommandation des opérations KJ, Revue de la Commission Européenne, n°97/489/CE, juillet, 1997.

[22] ALPHONSE CHRISTIANE IVINZA LEPAPA, « Monétique et transaction électronique » édition Bookelis, 2018, P 16.

- Les institutions bancaires.

1-3-2. Sécurité des transactions :

Certains associent le terme "monétique" à un élément central : la sécurisation des transactions. Dans cette optique technologique, les applications telles que les cartes d'accès, d'identification ou les puces intégrées aux téléphones (comme les cartes SIM), entrent dans le champ de la monétique. D'un point de vue technologique, il y a peu de différences entre une puce bancaire et une puce téléphonique (SIM).

1-3-3. La dématérialisation de la monnaie :

La monétique repose sur la dématérialisation de la monnaie et l'usage de moyens de paiements électroniques. Elle vise à minimiser l'utilisation de supports matériels dans les échanges de valeurs ou de services. Cette transition vers le numérique remplace les intervenants traditionnels par des flux numériques, réduisant ainsi la nécessité de manipuler physiquement les valeurs et renforçant l'efficacité et la sécurité des transactions dématérialisées, aussi bien à l'échelle individuelle que collective.[1]

Ce virage vers la dématérialisation a également ouvert la voie à de nouveaux concurrents pour les formes traditionnelles de monnaie, qu'il s'agisse de monnaie fiduciaire ou scripturale. Cela a engendré l'émergence de la monnaie électronique, numérique et virtuelle.

A- La monnaie électronique

La monnaie électronique représente une forme spécifique et contemporaine de la monnaie dématérialisée. Elle se matérialise sous forme d'argent stocké sur une puce Proton ou conservé sur le disque dur d'un ordinateur. [2]Bien que relativement récente, elle constitue une évolution notable dans le domaine des transactions financières.

B- La monnaie virtuelle

La monnaie virtuelle peut être considérée comme une référence à un compte bancaire ou à un autre type de compte. Sa valeur n'est pas détenue physiquement par le titulaire, car elle n'a pas de forme matérielle concrète en termes de support, de représentation ou de mode de paiement. Elle est plutôt enregistrée dans des logiciels qui permettent d'effectuer des paiements sur des réseaux ouverts, notamment sur Internet.[3] De plus, la monnaie virtuelle peut prendre la forme d'un jeton virtuel émis par un émetteur de confiance, destiné à un usage unique et utilisé dans un circuit commercial spécifique et fermé.

---

[1] HASHEM SHERIF Moustafa et SERHROUCHNI Ahmed, "La monnaie électronique (Systèmes de paiement sécurisé)", Editions Romandes, 1999, p 52.

[2] EFEE CD 15 Cours de Gestion, Mons, 2006, Dossier de paiement ABB, page 4.

[3] Idem page 46.

C- La monnaie numérique

La monnaie numérique marque une avancée supplémentaire dans le processus de dématérialisation de la monnaie. En effet, chaque unité monétaire numérique est un signe monétaire avec une valeur d'échange effective, acceptée par les acteurs économiques de l'espace qui consentent à la recevoir en paiement. Chaque pièce de monnaie numérique est codée et possède un numéro de série unique, ce qui permet des échanges en temps réel via le réseau.

1-4- Les composants de la monétique :

Le système monétique repose sur l'emploi de deux catégories de composants :

- Les moyens de paiements électroniques réduisent les risques liés à la perte ou au vol en dématérialisant totalement ou partiellement la monnaie.
- La monnaie électronique convient aux paiements à distance et ne requiert pas d'échange physique contre des espèces, ni l'intervention de tiers dans le processus de paiement (comme c'est le cas pour les cartes prépayées ou les portefeuilles électroniques).
- Elle autorise le maintien de l'anonymat.
- Les nouvelles méthodes de paiement électroniques (cartes, portefeuilles électroniques) intègrent leurs propres dispositifs de sécurité, que ce soit pour les paiements en personne ou à distance.
- La monnaie électronique n'est pas restreinte par les frontières nationales et peut être employée dans l'ensemble de l'Union Européenne.

1-4-1. Le support

Le dispositif se manifeste sous la forme d'une carte en matière plastique, munie d'une bande magnétique, éventuellement agrémentée d'une puce électronique. Sa configuration peut varier selon son dessein spécifique.

1-4-2. Le système de traitement

Il s'agit d'équipements électroniques conçus pour extraire les données contenues dans les divers supports de la monétique. Ils sont habituellement reliés à un centre de contrôle des comptes des utilisateurs.

1-5- Les acteurs de la monétique

La monétique implique la participation de quatre (4) acteurs [1]:

[1] www.comprendrelespaiements.com/abc-de-la-monetique-les-acteurs-et-leurs-roles/

a- L’émetteur « la banque du client »

C'est l'institution financière qui fournit à ses clients un support (comme une carte interbancaire) et gère les opérations de débit/crédit sur le compte du titulaire ainsi que les éventuels litiges liés à l'utilisation de la carte.

b- Le porteur « le client »

Il s'agit du possesseur de la carte. Le titulaire du compte peut être une entité telle qu'une entreprise, un individu ou un commerçant. Le titulaire de la carte doit établir un contrat spécifique concernant l'usage de la carte bancaire, précisant les termes et conditions liés à sa délivrance, son utilisation, sa sécurité et son renouvellement, entre autres. Il est important de noter que le titulaire de la carte n'en devient pas le propriétaire. La carte reste la propriété de la banque, qui peut décider de la récupérer si nécessaire.

c- L’accepteur « le commerçant »

L'acceptant peut être soit le professionnel qui accepte l'usage d'une carte bancaire pour le règlement d'un produit ou d'un service, soit la banque qui met à disposition le DAB/GAB pour les retraits d'espèces. Le commerçant est équipé d'un TPE fourni par sa banque. La banque en charge des DAB/GAB s'équipe de manière à jouer simultanément le rôle de l'acceptant et de l'acquéreur pour les retraits et les transactions effectuées sur ces appareils.

En tant que commerçant, l'acceptant doit honorer ses engagements envers sa banque et veiller à la régularité des paiements par carte.

d- L’acquéreur : la BANQUE du commerçant

L'acquisition d'une transaction de paiement peut avoir lieu soit chez un commerçant lors du paiement par le titulaire de la carte, soit lorsque ce dernier effectue un retrait d'espèces à partir d'un distributeur automatique de billets ou d'un guichet automatique bancaire (DAB/GAB). Pour réaliser la transaction, le titulaire doit insérer la carte dans le terminal de paiement électronique (TPE) du commerçant ou dans le DAB/GAB de la banque. Dans le premier cas, l'acquéreur est la BANQUE du commerçant qui lui a fourni le TPE. Dans le second cas, il s'agit de la banque du DAB/GAB .

A- Les Cartes Bancaires :

De nos jours, la carte trouve une grande variété d'applications. Elle peut non seulement servir de moyen de reconnaissance visuelle du porteur, mais aussi de support d'infos codées

pour divers usages. [1]En pratique, on distingue principalement deux types de cartes bancaires : les cartes de paiement, les cartes de retrait et les porte-monnaie électroniques.

1- La carte de paiement :

La carte de paiement offre à son titulaire la possibilité d'effectuer des règlements, que ce soit en personne ou à distance, pour des achats ou des services auprès des commerçants autorisés par l'ensemble des réseaux interbancaires, et qui disposent d'un terminal de paiement électronique (TPE).[2]

- **Carte de débit immédiat** : Le montant retiré ou dépensé est déduit du compte du titulaire dès que la transaction est effectuée (parfois instantanément en temps réel).
- **Carte à débit différé** : Elle autorise son détenteur à effectuer des dépenses dans la limite d'un montant préalablement autorisé. Cependant, contrairement à une carte de crédit, la carte de débit différé ne propose aucune ligne de crédit, exigeant le règlement intégral du montant dû à la fin d'une période fixée (par exemple, mensuellement).
- **Carte de paiement national ou international** : Elle est utilisable aussi bien dans les pays de la zone Euro que dans le reste du monde.

2- Carte de retrait :

Sous le terme explicite de "carte de retrait", il est possible d'effectuer des retraits d'argent aux distributeurs automatiques et aux guichets bancaires. Cependant, elle ne donne pas la possibilité de réaliser des paiements chez les commerçants.[3]

3- Carte de crédit :

La carte de crédit est définie comme « Un accréditif qui permet à son porteur d'effectuer des achats de biens ou de services apurés d'établissements affiliés, par simple apposition désignateurs sur une facture standardisée ou sur bordereau, où son produite les mentions de la carte »[4]

La carte de crédit qui permet de payer généralement toutes formes de biens et de services, domine jusqu'à présent les transactions du commerce électronique.

B- Le porte-monnaie électronique (PME) :

L'évolution de la monnaie électronique au fil du temps a entraîné des avancées significatives dans les paiements électroniques, telles que l'intro du porte-monnaie

---

[1] Didier-Pierre MONOD, « Moyens et Technique de Paiement Internationaux –import-export » 4éme édition ESKA, Paris, 2007, P 25.

[2] Support de cours Techniques bancaires, Khaled Bettaieb, 2022, IFID

[3] https://billetdebanque.panorabanques.com/banque/carte-retrait.

[4] FREDERIC.G, « La saisie de la monnaie scripturale », Edition L'acier, Bruxelles 2006, p576

électronique. Cette innovation simplifie les procédures tant pour les institutions émettrices que pour les utilisateurs.

Définition de porte-monnaie électronique (PME) :

Le porte-monnaie électronique est une carte de paiement prépayée rechargeable, sur laquelle une somme d'argent préalablement définie est chargée, permettant d'effectuer des paiements électroniques pour des montants limités. Il s'agit d'un dispositif qui permet de stocker de la monnaie sans nécessiter de compte bancaire, autorisant ainsi des paiements directs sur des terminaux de paiement.

C- Les guichets automatiques de BANQUE (GAB) :

Les automates offrent aux détenteurs de carte bancaire la possibilité d'effectuer diverses opérations de leur propre initiative, 24 heures sur 24[1], sans avoir besoin de se rendre en personne à leur agence bancaire. Ces opérations comprennent notamment la consultation du solde, la demande de RIB, de chèque, les virements internes à la banque, le dépôt de chèque, les versements et les retraits d'espèces. De plus, ces automates peuvent également fonctionner comme des DAB pour tous les porteurs de carte acceptés par l'appareil.

D- Les (DAB)

Les DAB sont des dispositifs mis en place par les agences bancaires, les bureaux de poste ou les émetteurs de cartes, que ce soit dans leurs locaux ou dans des lieux publics tels que les grands magasins ou les supermarchés. Ils visent à réduire la circulation importante d'argent liquide.

Tout retrait effectué à un DAB requiert une autorisation préalable. Cette autorisation peut être accordée soit par le service d'autorisation de la banque émettrice, s'il est en place, soit par délégation de la société monétique du pays concerné.

E- Les terminaux de paiement électroniques (TPE)

Les terminaux de paiement sont déployés auprès des commerçants qui adhèrent au système de paiement. Ces derniers doivent se conformer à des obligations contractuelles, notamment en respectant un plafond de garantie convenu.

Ces automates en accès libre, en plus de permettre les retraits d'espèces, offrent la possibilité de déposer des chèques avec capture d'image, d'émettre des relevés d'identité bancaire (RIB), d'effectuer des virements, et en général, de réaliser toutes les opérations bancaires en libre-service.

[1] **https://financeland.fr/lexique/distributeur-automatique-de-billets--dab/, consulté le 24/07/2023 à 17h**

En conclusion, nous avons pu délimiter dans cette section le concept de monétique bancaire et en comprendre les principaux enjeux.

La monétique regroupe l'ensemble des moyens de paiement scripturaux comme la carte bancaire, le virement ou le prélèvement. Elle fait intervenir différents acteurs, de l'émetteur de la carte au commerçant.

Si la monétique présente des avantages en termes de rapidité et de traçabilité, elle implique également des défis technologiques et sécuritaires pour les banques. La concurrence dans ce domaine ne cesse de s'accroître.

Dans la section suivante, nous nous intéresserons plus spécifiquement au contexte de la monétique en Algérie. Nous analyserons l'évolution de la monétique dans le pays et les perspectives de développement pour les prochaines années. L'enjeu pour les banques Algériennes est d'étendre l'usage des moyens de paiement électroniques tout en maîtrisant les risques associés.

SECTION 02 : LA MONÉTIQUE EN ALGÉRIE

La monétique occupe une place croissante dans le paysage bancaire Algérien, mais son développement en est encore à un stade intermédiaire. Cette section sera consacrée à l'analyse du marché de la monétique en Algérie.

Nous commencerons par retracer l'historique de l'introduction de la monétique dans le secteur bancaire Algérien à partir des années 1990. Les principales étapes de déploiement des cartes bancaires, des DAB/GAB et des TPE seront présentées.

Nous dresserons ensuite un état des lieux quantitatif du parc de cartes, de terminaux et des volumes de transactions monétiques en Algérie. Ceci nous permettra de mesurer la progression de la monétique mais aussi le chemin restant à parcourir.

Enfin, nous étudierons les perspectives de développement de la monétique dans le pays pour les prochaines années. Nous analyserons les opportunités ainsi que les défis à relever par les banques Algériennes en matière de paiement digital.

Cette section donnera ainsi un aperçu détaillé de l'écosystème monétique Algérien et de son potentiel de croissance dans un futur proche.

2-1- L’évolution de la monétique dans l’environnement bancaire Algérien

Pour reconstituer l'évolution de la monétique en Algérie, nous avons dressé une chronologie des événements significatifs qui ont contribué à son développement. La plupart de ces événements sont liés aux modifications apportées au secteur bancaire depuis 1990. Le Tab ci-dessous présente cette chronologie :

Tableau N°02 : Chronologie d'évolution de la monétique en Algérie

Année	Événement
1990	**Adoption de la loi « *90-10 du 14 avril 1990* »[1] relative à la monnaie et au crédit :** Cette loi introduit la restructuration institutionnelle et redéfinit le rôle de tous les acteurs du secteur bancaire, à savoir : la banque centrale, le trésor public, les banques commerciales et les établissements financiers. Ainsi, cette réforme apporte les transformations majeures suivantes : - Le changement des statuts et la recapitalisation des banques publiques. - L'ouverture du secteur bancaire aux capitaux privés. - La modernisation des SI. - La mise en place d'une chambre de compensation. Le but de cette réforme est d'apporter du dynamisme et de la concurrence au secteur bancaire.
1993	**Algérie Télécom met en service le réseau national « DZPAC »[2] :** Ce réseau informatique à haut débit a pour but d'offrir des connexions sécurisées entre les branches distantes des différentes institutions et établissement nationaux tel que la Poste, les ministères, Sonelgaz, Naftal et les établissements bancaires et financiers. Nous allons voir plus loin dans le chapitre que le fonctionnement de la SATIM repose entièrement sur ce réseau.
1995	**Création de la « SATIM »[3] :** 8 banques publiques (BADR, BDL, BEA, BNA, CPA, CNEP, CNMA et ALBARAKA) créent la Société d'Automatisation des Transactions Interbancaires et de Monétique dont ils sont actionnaires majoritaires, d'autres banques commerciales adhéreront par la suite à cette association. Cette société est chargée de gérer les transactions interbancaires.
1997	**Première réforme concernant la chambre de compensation :** « Le règlement N°97-03 du 17 novembre 1997 relatif à la chambre de compensation fixe les conditions d'adhésion et d'exclusion des membres de la chambre et instaure des frais de fonctionnement que les adhérents doivent supporter.» **La SATIM lance le Réseau Monétique Interbancaire « RMI »[4] :** Ce réseau interconnecte les SI des banques adhérentes ainsi que leurs DAB. **Emissions des premières Cartes Interbancaires** Les premières cartes émises ne permettent que le retrait au niveau des DAB/GAB des banques membres de la SATIM.
1998	**Les banques à capitaux étrangers commencent à s'installer en Algérie.** Les premières banques à obtenir des agréments sont les banques d'investissement, suivies par la suite de celles à clientèle privée et particulier. La plupart des capitaux proviennent des groupes financiers français et des pays du Golf.
2002	**Accord entre Algérie Telecom et la Banque d'Algérie pour la mise en place d'un réseau spécial** « *La Banque d'Algérie signe une convention avec le Ministère de la Poste et des Technologies de l'Information et de la Communication (MPTIC) pour la réalisation au profit de la communauté bancaire un réseau d'abonnés fermés, à grand débit, fiable, efficace et sécurisé.*» [5] **La Banque d'Algérie lance un projet de modernisation de la chambre de compensation** « *Au cours de la même année ont été mis en place les groupes de travail ayant pour mission de définir la stratégie de modernisation des paiements dit paiements de masse. Il s'agit en particulier de statuer sur l'architecture de la chambre de compensation électronique, .., de faire un état de lieu des réseaux de transmission et des SI des participants, de voir les conditions nécessaires pour* *le développement des instruments de paiements, en particulier, des instruments électroniques.* »[6]
2004	**Création du Centre de Pré-compensation Interbancaire (CPI) :** « *La Banque d'Algérie créé la filiale CPI avec la participation des banques et d'Algérie Poste pour assurer la*

[1] Journal Officiel de la République : Loi n°90-10 du 14 Avril 1990 relative à la Monnaie et au Crédit.
[2] Algérie Télécom : (Site officiel) in www.algerietelecom.dz/siteweb.php?p=dzpac
[3] SATIM : Activité de SATIM, (Site officiel de la SATIM CIB) in http://www.satim-dz.com/
[4] Règlements de la Banque d'Algérie : Règlement N°97-03 du 17 Novembre 1997 in www.bank-of-algeria.dz
[5] SATIM : Activité de SATIM, (Site officiel de la SATIM CIB) in http://www.satim-dz.com/
[6] Idem. P.17

	réalisation du futur système de télé compensation. Le CPI a par la suite signé une convention régissant ses relations avec l'ensemble des participantes.»
2006	**Démarrage du nouveau système de télé compensation ATCI :** « Le 15 mai, l'opérateur du CPI démarre le nouveau système de télé compensation ATCI (Algérie Télé-Compensation Interbancaire) pour le traitement des chèques et des virements. En octobre, le RMI de la SATIM est connecté au CPI pour permettre la compensation des transactions par cartes interbancaires. »[1] **Premiers paiements par Cartes Interbancaires à Alger** La SATIM lance un projet pilote qui consiste à équiper des commerçants de TPE afin de promouvoir le paiement par carte bancaire.
2010	**« Visa et Mastercard s'installent en Algérie » :**[2] La SATIM se lance dans un projet prometteur en introduisant les cartes internationales Visa et Mastercard. La BDL, la BEA et le CPA sont les premières banques Algériennes à adhérer à Visa.
2014	**Création du Groupement d'Intérêt Economique-monétique juin 2014**
2016	**Le lancement d'e-paiement le 4 octobre 2016**

2-2-La situation de la monétique en Algérie

2-2-1- La situation actuelle en chiffres

1- Evolution des cartes CIB

Tableau N°03 : Evolution des cartes CIB

Année	2016	2017	2018	2019	2020	2021	2022	Mai 2023
Nbr de cartes	**804 674**	**877 708**	**1 140 741**	**8 926 229**	**9 620 000**	**11 609 624**	**14 256 145**	**15 371 853**

Source :[3]

- ⇨ Ce tableau présente l'évolution du nombre de cartes bancaires en circulation en Algérie sur la période 2016-mai 2023.
- ⇨ On constate une augmentation constante et rapide du nombre de cartes bancaires sur la période. En 7 ans, de 2016 à 2022, le nombre de cartes a été multiplié par plus de 17.
- ⇨ Cette augmentation reflète le développement des services bancaires et des moyens de paiement électronique en Algérie.
- ⇨ On note trois périodes d'accélération particulière de cette croissance : entre 2018 et 2019 où le nombre de cartes a quasiment été multiplié par 8 ; entre 2020 et 2021 où il a crû de plus de 20% ; et entre 2021 et 2022 où la hausse a été de près de 23%.
- ⇨ En mai 2023, le nombre de cartes bancaires dépasse les 15 millions, contre seulement 800 000 en 2016.
- ⇨ Cette croissance rapide peut s'expliquer par la généralisation de l'usage des cartes bancaires en Algérie, tirée par l'inclusion financière, la digitalisation et les innovations en matière de paiement.

[1] **Banque d'Algérie, Rapport annuel de 2006. P.109**
[2] **Idem. P.110-111.**
[33] **https://giemonetique.dz/ consulté le 25/07/2023 à 20h**

2- Evolution des TPE en Algérie:

Tableau N°04 : Evolution des TPE

Année	Nombre global de TPE
2016	5049
2017	11 985
2018	15 397
2019	23 762
2020	33 945
2021	37 561
2022	46 263
A Mai 2023	49 375

Source : [1]

- On constate une croissance continue et rapide du nombre de TPE sur la période de 2016 à 2022.
- En 2016, il y avait seulement 5049 TPE recensés en Algérie. Ce nombre a été multiplié par 9 en l'espace de 6 ans pour atteindre 46 263 TPE en 2022.
- La croissance la plus forte est observée entre 2019 et 2021, avec une augmentation de 13 799 TPE sur cette période, soit une hausse de 58%.
- Sur l'ensemble de la période 2016-2022, le taux de croissance annuel moyen du nombre de TPE est d'environ 39%, ce qui est très élevé.
- Cette forte croissance traduit un essor des initiatives entrepreneuriales et du secteur des TPE en Algérie sur cette période récente.
- Elle peut s'expliquer par une volonté des pouvoirs publics de promouvoir l'entrepreneuriat et les TPE, ainsi que par l'émergence d'une nouvelle génération d'entrepreneurs.
- La tendance se confirme sur les premiers mois de 2023, avec 49 375 TPE recensées à mai 2023, en hausse de 6,5% par rapport à fin 2022.

En conclusion, ces chiffres montrent le dynamisme des TPE en Algérie et leur poids croissant dans le tissu économique national depuis 2016. Leur développement semble s'inscrire dans une trajectoire de long

4- Evolution des DAB/GAB en Algérie

Tableau N°05 : Evolution des DAB/GAB

Année	Nombre global de DAB
2016	1370
2017	1443
2018	1441
2019	1621
2020	3030
2021	3053
2022	3640
A Mai 2023	3728

Source :[2]

- On observe une croissance régulière mais relativement faible du nombre de DAB entre 2016 et 2019, avec une augmentation d'environ 18% sur 4 ans.
- En 2020, il y a une très forte accélération avec le quasi-doublement du nombre de DAB qui passe de 1621 à 3030 en un an seulement.
- Cette augmentation exceptionnelle peut s'expliquer par les effets de la pandémie de Covid-19, qui a accéléré la transition vers le numérique et poussé les banques à déployer rapidement des DAB pour limiter les contacts.
- Après ce rattrapage, la croissance ralentit à nouveau entre 2021 et 2022 (+7%).
- Sur l'ensemble de la période 2016-2022, le nombre de DAB a été multiplié par 2,7. Le taux de croissance annuel moyen est de 14%.
- A mai 2023, la tendance se poursuit avec 3728 DAB, soit une augmentation limitée de 2,4% depuis début 2022.
- Ce ralentissement récent pourrait indiquer un début de saturation du marché des DAB après le boom de 2020-2021.

En résumé, on observe une forte croissance du parc de DAB sur la période, avec une accélération exceptionnelle en 2020 due à la pandémie, puis un retour à une progression plus modérée début 2023.

2-2-2- Les forces et faiblesses de la MONÉTIQUE en Algérie [3]

- Le cadre réglementaire présente des lacunes, avec un vide juridique et un manque de textes encadrant la monétique. Cependant, des normes internationales ont été adoptées.
- Sur le plan technique, les équipements restent insuffisants et le réseau de télécommunications pose des problèmes de disponibilité. Mais les banques ont la volonté d'investir dans ce domaine.
- Commercialement, il manque une stratégie proactive, une culture monétique et le marketing est quasi-inexistant. La méfiance des clients persiste.

[1] **https://giemonetique.dz/ consulté le 25/07/2023 à 21h**
[2] **https://giemonetique.dz/ consulté le 25/07/2023 à 23h**
[3] **Mr. LAZREG Mohamed, Développement de la Monétique en Algérie, Réalité et Perspectives, Thèse Présentée pour l'obtention d'un diplôme de doctorat en sciences de gestion. UNIVERSITE ABOU BAKR BELKAID TLEMCEN.2015.p71**

- Économiquement, la monétique permet une bancarisation accrue mais le faible revenu moyen des clients et le coût des services sont des freins. Le tourisme peu développé limite aussi les perspectives.

En conclusion, de nombreux défis restent à relever en Algérie pour développer la monétique, que ce soit en termes réglementaires, techniques, commerciaux ou économiques. Mais le potentiel existe, à condition de lever ces différents obstacles.

2.3 Présentations des organismes qui gèrent la monétique en Algérie :

2-3.1-Présentation de La Société d'Automatisation des Transactions Interbancaire s et de MONÉTIQUE (SATIM) [1]

- SATIM est un opérateur monétique Algérien créé en 1995 à l'initiative de 8 banques Algériennes.
- C'est une société par actions dont le capital s'élève à 1,145 milliard de dinars.
- SATIM est structuré autour d'un centre serveur front-office, d'un centre back-office, d'une station de personnalisation et d'un serveur de compensation.
- Les principales fonctions de SATIM sont : la gestion du front-office, la gestion du back-office, et la fonction info-centre.
- Les missions de SATIM sont : promouvoir les moyens de paiement électroniques, gérer la plateforme technique du réseau monétique, élaborer des règles pour la gestion des produits monétiques, personnaliser les cartes bancaires, et assurer le fonctionnement du système monétique.

En résumé, SATIM est l'acteur central du réseau monétique Algérien, avec pour rôle de gérer l'infrastructure technique et d'encadrer le développement des services de paiement électronique dans le pays.

2-3.2- Le Réseau Monétique Interbancaire Algérien (RMI)[2]

- Le RMI a été lancé en 1997 à l'initiative de SATIM pour mettre en place une solution monétique interbancaire.[2]
- Il permet à toutes les banques Algériennes d'offrir des services de retrait et de paiement électronique à leurs clients.
- Les acteurs du RMI sont les institutions financières et SATIM en tant que gestionnaire du réseau.

---

[1] Document interne SATIM Alger, 2006

[2] A.BENCHABLA, responsable de la monétique au niveau de la SATIM, PME Magazine, n°13, du 15 Mars 2002

- Le RMI comprend le serveur SATIM qui gère les transactions et les DAB qui distribuent les espèces.

- Les missions du RMI sont : faciliter l'interopérabilité, intégrer les DAB des banques, autoriser les retraits, gérer les transactions entre DAB et TPE, et pré-compenser les transactions.

En résumé, le RMI fournit l'infrastructure technique permettant l'interopérabilité des services monétiques entre les banques Algériennes et la gestion des transactions électroniques au niveau national.

2-3.3- Le Groupement d'Intérêt Economique (GIE-MONÉTIQUE) [1]

- Le GIE Monétique est une organisation communautaire créée en 2014 pour réguler le système monétique interbancaire Algérien.

- Il regroupe 19 membres dont 18 banques et Algérie Poste. La Banque d'Algérie y participe en tant que membre non-adhérent.

- Les objectifs du GIE sont : piloter la stratégie de développement de la monétique, superviser l'industrie monétique, garantir l'interopérabilité et la sécurité du système.

- Ses principales missions sont : surveiller les normes monétiques, développer les produits bancaires liés à la monétique, assurer la sécurité, clarifier les règles pour stimuler l'innovation.

En résumé, le GIE Monétique vise à encadrer et faire progresser l'écosystème monétique interbancaire en Algérie, en édictant des règles et normes communes pour plus d'efficacité et de sécurité.

Nous avons pu constater dans cette section que la monétique s'est progressivement développée dans le secteur bancaire Algérien, même si sa part reste encore limitée dans les transactions. Les cartes bancaires et les terminaux de paiement se sont largement diffusés depuis les années 1990.

Cependant, de nombreux défis restent à relever pour accélérer l'usage des moyens de paiement électronique en Algérie, notamment en termes d'infrastructures, d'éducation financière et de confiance des consommateurs.

Les banques Algériennes ont ainsi une carte à jouer dans les prochaines années pour promouvoir la monétique, saisir les opportunités du digital et fidéliser leur clientèle.

Mais le développement de la monétique s'accompagne également de nouveaux risques, qui feront l'objet de la section suivante. Nous analyserons les principaux risques liés à la monétique pour les banques, qu'ils soient opérationnels, technologiques ou liés à la fraude. La

[1] https://giemonetique.dz

maîtrise de ces risques constituera un enjeu clé pour assurer le déploiement sécurisé des services monétiques en Algérie.

SECTION 03 : LES RISQUES LIES À LA MONÉTIQUE

La monétique fait référence à l'ensemble des technologies et des systèmes utilisés pour les opérations de paiement électronique, tels que les cartes de crédit, les cartes de débit, les transactions en ligne et les paiements mobiles. Bien que la monétique offre de nombreux avantages, elle comporte également certains risques, notamment :

1. Fraude par carte de crédit ou de débit: Les transactions effectuées via des cartes de crédit ou de débit peuvent être sujettes à la fraude. Les pirates peuvent voler les infos de carte de crédit et les utiliser illégalement pour effectuer des achats en ligne ou dans des magasins physiques.

2. Vols d'identité: Lorsque les infos personnelles des clients sont stockées par les commerçants ou les fournisseurs de services de paiement, il existe un risque de vol d'identité si ces données sont compromises. Les infos telles que les numéros de sécurité sociale, les dates de naissance et les adresses peuvent être utilisées par des criminels pour commettre des fraudes ou des crimes financiers.

3. Phishing et ingénierie sociale: Les attaques de phishing et d'ingénierie sociale ciblant les utilisateurs de services monétiques peuvent conduire à la divulgation d'infos sensibles. Les fraudeurs envoient souvent des e-mails ou des messages trompeurs pour inciter les utilisateurs à divulguer leurs infos de compte.

4. Cyber attaques: Les systèmes de paiement électronique peuvent être la cible de cyber attaques, telles que les attaques par déni de service (DDoS) ou les intrusions dans les bases de données. Ces attaques peuvent entraîner des perturbations du service, des vols de données ou des défaillances du système.

5. Contrefaçon de cartes: Les cartes de crédit et de débit peuvent être contrefaites, ce qui permet à des individus malveillants d'utiliser de fausses cartes pour effectuer des achats ou retirer de l'argent aux guichets automatiques.

6. Problèmes de sécurité des terminaux: Les terminaux de paiement utilisés dans les magasins physiques peuvent être compromis, permettant aux fraudeurs de capturer les infos des cartes lorsqu'elles sont insérées ou balayées.

7. Vol ou perte de cartes: Si une carte est perdue ou volée, elle peut être utilisée frauduleusement par quelqu'un d'autre jusqu'à ce qu'elle soit signalée et bloquée.

8. Risques de conformité et de réglementation: Les Entreprise s traitant des paiements électroniques doivent se conformer à des réglementations strictes en matière de protection des données et de sécurité financière. Le non-respect de ces réglementations peut entraîner des amendes et des sanctions.

9. Dépendance technologique: Avec la monétique, les entreprises et les consommateurs deviennent de plus en plus dépendants des technologies de paiement électronique. Tout dysfonctionnement ou panne du système peut perturber les transactions et causer des inconvénients aux utilisateurs.

Pour atténuer ces risques, les Entreprise s et les fournisseurs de services de paiement mettent en œuvre diverses mesures de sécurité, telles que le chiffrement des données, l'authentification à deux facteurs, la surveillance des transactions suspectes et la sensibilisation à la sécurité pour les utilisateurs. Il est également essentiel que les utilisateurs soient conscients des pratiques de sécurité recommandées et qu'ils signalent immédiatement toute activité suspecte à leur banque ou à leur fournisseur de services de paiement.

3-1- Les risques liés à la carte bancaire :

Les cartes bancaires sont des outils pratiques et couramment utilisés pour effectuer des transactions financières. Cependant, elles peuvent présenter certains risques, notamment :

1. Fraude et piratage : Les cartes bancaires peuvent être piratées ou clonées, ce qui permet aux fraudeurs d'accéder aux infos sensibles du titulaire de la carte et d'effectuer des transactions non autorisées.

2. Vol ou perte : Si une carte bancaire est volée ou perdue, une personne mal intentionnée pourrait l'utiliser pour effectuer des achats frauduleux avant que le titulaire de la carte ne signale sa disparition.

3. Utilisation non sécurisée en ligne : Lorsque vous effectuez des achats en ligne, vous courez le risque que vos infos de carte bancaire soient compromises si le site n'est pas sécurisé ou si vous partagez vos détails avec des entités non fiables.

4. Frais et surcoûts : Certaines cartes bancaires peuvent entraîner des frais cachés ou des surcoûts importants, notamment lors des retraits d'espèces à l'étranger ou lors de l'utilisation dans des d'autres banques.

5. Limites de responsabilité : En cas de fraude ou d'utilisation non autorisée de la carte, les titulaires peuvent avoir une responsabilité limitée, mais cela peut varier selon le pays et l'émetteur de la carte.

6. Phishing et escroqueries : Les fraudeurs utilisent souvent des techniques de phishing pour obtenir des infos personnelles et bancaires des utilisateurs, en prétendant être une institution financière légitime.

7. Dépenses excessives : L'utilisation d'une carte bancaire peut faciliter les achats impulsifs et les dépenses excessives, entraînant des difficultés financières pour certaines personnes.

3-2- Les risques liés au /DAB/GAB/

Les DAB ou GAB sont des machines qui permettent aux clients des banques d'effectuer certaines transactions financières en libre-service, telles que le retrait d'argent, le dépôt d'argent, le transfert de fonds, le paiement de factures, etc. Bien qu'ils offrent une grande commodité aux clients, il existe certains risques liés à l'utilisation de ces appareils. Voici quelques-uns des risques les plus courants associés aux DAB/GAB :

1. Vol de carte : Les criminels peuvent essayer de voler votre carte bancaire pendant que vous effectuez une transaction au DAB/GAB . Ils peuvent utiliser des dispositifs d'espionnage (skimmers) pour copier les infos de votre carte ou utiliser des caméras pour enregistrer votre saisie de code PIN.

2. Utilisation frauduleuse des informations de carte : Si des criminels parviennent à obtenir les infos de votre carte, ils peuvent les utiliser pour effectuer des achats frauduleux en ligne ou dans des magasins physiques.

3. Dispositifs de piratage du clavier : Les criminels peuvent installer des dispositifs sur les claviers des DAB/GAB pour enregistrer les touches que vous appuyez et ainsi voler votre code PIN.

4. Attaques de force brute : Les attaquants peuvent essayer de deviner votre code PIN en effectuant des attaques de force brute, où ils essaient toutes les combinaisons possibles jusqu'à ce qu'ils trouvent la bonne.

5. Fraude par distraction : Les criminels peuvent utiliser des techniques de distraction, comme vous demander de l'aide ou vous parler pendant que vous utilisez le DAB/GAB , afin de vous distraire pendant qu'ils essaient de voler votre carte ou votre argent.

6. DAB/GAB/ compromis : Il est possible que des DAB/GAB soient compromis par des logiciels malveillants ou des pirates informatiques, leur permettant de voler des infos sensibles, y compris les données de carte bancaire.

7. Retraits incomplets ou erreurs de transaction : Les DAB/GAB peuvent parfois dysfonctionner, entraînant des erreurs dans les transactions, des retraits incomplets ou des débits non effectués correctement.

8. Problèmes de connexion et de réseau : Si le DAB/GAB n'est pas correctement connecté au réseau de la banque, vous pourriez rencontrer des problèmes lors de vos transactions.

3-3-Les risques liés au TPE :

Les TPE (Terminaux de Paiement Électronique), également connus sous le nom de "lecteurs de cartes" ou "terminaux de carte bancaire", sont des dispositifs utilisés pour traiter les paiements électroniques lors d'achats en magasin, restaurants, stations-service et autres commerces. Bien que les TPE offrent une méthode de paiement pratique et rapide, ils comportent également certains risques pour les consommateurs et les commerçants. Voici quelques risques liés aux TPE :

1. Vol de données de carte : Les TPE peuvent être compromis par des skimmers ou des dispositifs malveillants installés par des fraudeurs pour voler les infos de carte de crédit ou de débit des clients lors du paiement.

2. Transactions frauduleuses : Si un TPE est compromis, les infos volées peuvent être utilisées pour effectuer des transactions frauduleuses en utilisant les cartes des clients sans leur autorisation.

3. Vol de données du commerçant : Les TPE enregistrent souvent les données de paiement des clients, et si le terminal est compromis, les infos de paiement des clients et du commerçant peuvent être volées.

4. Attaques de logiciels malveillants : Les TPE connectés à Internet sont vulnérables aux attaques de logiciels malveillants qui pourraient permettre aux pirates d'accéder aux infos sensibles.

5. Transactions non autorisées : Des erreurs peuvent survenir lors du traitement des transactions sur le TPE, ce qui pourrait entraîner des débits incorrects ou des paiements en double.

6. Pannes techniques : Les TPE peuvent parfois connaître des pannes techniques, empêchant ainsi les transactions de se dérouler correctement.

7. Manipulation de l'appareil : Des employés malhonnêtes ou des individus malveillants peuvent manipuler le TPE pour effectuer des transactions frauduleuses ou détourner des fonds.

8. Dysfonctionnement matériel : Un dysfonctionnement matériel du TPE peut entraîner des erreurs de transaction, des remboursements incorrects ou des problèmes de paiement pour les clients.

Ce chapitre nous a permis de brosser un panorama général du domaine de la monétique bancaire, qui occupe une place centrale et croissante dans les services financiers modernes.

Nous avons pu délimiter le concept de monétique et comprendre son fonctionnement à travers les différents acteurs et instruments qui la composent. Le développement historique de la monétique a également été retracé, des premiers DAB jusqu'à la démocratisation récente du paiement mobile.

L'analyse du marché monétique Algérien a mis en lumière des progrès indéniables mais aussi des défis importants à relever pour accélérer la transition vers le tout électronique. Les banques Algériennes ont un rôle clé à jouer pour promouvoir et sécuriser les usages.

Enfin, ce chapitre a permis d'identifier les principaux risques induits par la monétique, qu'il s'agisse des risques opérationnels, de fraude ou cyber. La maîtrise de ces risques multifacettes constituera un enjeu primordial pour les banques dans les années à venir.

Ce premier aperçu sur la monétique bancaire pose donc les bases pour appréhender plus en détails dans les chapitres suivants les rouages de ce secteur complexe et stratégique, ainsi que les défis qu'il recèle en termes de gestion des risques.

CHAPITRE 03 : CAS PRATIQUE : ÉLABORATION D'UNE CARTOGRAPHIE DES RISQUES LIÉS AU PROCESSUS MONÉTIQUE ET AU DISPOSITIF DAB/GAB/TPE

CHAPITRE 03 : CAS PRATIQUE : ÉLABORATION D'UNE CARTOGRAPHIE DES RISQUES LIÉS AU PROCESSUS MONÉTIQUE ET AU DISPOSITIF DAB/GAB/TPE

Ce chapitre présente un cas pratique concret d'élaboration d'une cartographie des risques associés au processus monétique et aux dispositifs DAB/GAB/TPE. Nous allons détailler les différentes étapes nécessaires à la réalisation de cette analyse, de l'identification des risques jusqu'à l'évaluation de leur niveau de criticité.

SECTION 01 : PRÉSENTATION DE LA BANQUE DE DEVELOPPEMENT LOCAL

Cette section vise à présenter la Banque de Développement Local qui fait l'objet de notre analyse de risques. Nous décrirons son historique, ses activités principales ainsi que sa politique de tarification.

1.1.Historique la Banque de Développement Local BDL :

La Banque de Développement Local, par abréviation B.D.L, est la plus jeune banque publique en Algérie. Elle représente un organisme financier, public, économique qui a été créé par décret n°85/85 du 30 avril 1985.

La B.D.L, qui a été dotée d'un capital de 500 millions de dinars, a hérité au départ 39 agences, 1succursale, le siège social et un effectif de 700 agents, issus du Crédit Populaire d'Algérie, dans le cadre de la restructuration du secteur financier. Le démarrage de l'activité a eu lieu le 1er juillet 1985. Au mois d'août de la même année, la banque a repris les activités des Caisses de Crédit Municipal d'Alger, d'Oran et de Constantine, regroupées en un réseau de huit (08) agences dont cinq (05) agences spécialisées dans les opérations de prêts sur gages (PSG).

Le démarrage de cette banque a été difficile, même si en 1986, elle a bénéficié de cinq agences issues des ex-caisses de Crédit Municipal, elle a tenté de s'imposer sur un marché déjà conquis par d'autres banques d'envergure national (CPA, BNA, BEA) et qui ont accumulé beaucoup d'expérience.

La B.D.L ne disposait pas alors de l'outil informatique, tant au niveau central, qu'au niveau des agences. Les opérations étaient donc traitées manuellement. D'autre part, la création de cette banque a coïncidé avec la crise économique qui a secoué le pays, en 1986 en raison de la baisse brutale du prix du pétrole, qui a rendu aléatoire son développement.

Les ressources de la clientèle étaient alors de seulement deux milliards de dinars et avec cent mille (100.000) comptes clients.

Suite à sa transformation juridique en société par actions (SPA) et sur la base de la loi 88-04 portant sur l'autonomie des entreprises, elle est passée à l'autonomie le 20 février 1989. Enfin le siège social de la Banque de Développement Local (B.D.L) est situé au 5, rue Gaci Amar Staouéli-wilaya d'Alger.

Le capital social de la B.D.L est passé successivement de 500 millions de dinars lors de sa création, à 720 millions de DA en 1994, à 1 milliard 440 millions DA en 1995, à 13.390.000.000 DA en 2004, à15.800.000.000 DA en 2010, à 36.800.000.000 en 2017, à 73.000.000.000 DA, actuellement.

La B.D.L a dans son actif un réseau de 156 agences judicieusement implantées sur tout le territoire national, dont 02 antennes, 147 traitant les opérations bancaires attribuées aux banques et 06 dédiées aux Prêts sur Gage PSG, une activité dont la B.D.L a l'exclusivité.

1.2.Activité de la B.D.L :

Après avoir été la banque des entreprises publiques locales, la B.D.L se distingue aujourd'hui en étant la banque des PME/PMI, des professions libérales, des micros entreprises créées dans le cadre des différents dispositifs de soutien à l'emploi, des promoteurs immobiliers et des particuliers.

En outre, elle est la seule banque publique à prendre en charge l'activité de prêts sur gage héritée des ex-caisses du crédit municipal, et qu'elle continue de promouvoir au bénéfice des particuliers, des ménages qui trouvent dans ce crédit une réponse à leurs besoins de trésorerie en contrepartie de gage d'objets en or.

Sa stratégie est orientée vers la participation active au développement de l'économie nationale et particulièrement la relance de l'investissement à travers le financement des PME/PMI tous secteurs confondus, et la participation à tous les dispositifs mis en place parles pouvoirs publics (ANADE, CNAC, ANGEM).La B.D.L joue un rôle important dans le financement de l'habitat à travers différents produits notamment le crédit immobilier et la promotion immobilière.

Enfin, la BDL est adhérente à la monétique nationale (carte de retrait, de paiement visa et au système de télé compensation).

1.3.Stratégie et objectifs de la B.D.L :

L'objectif fondamental de la B.D.L est de conforter sa part de marché et d'améliorer sa marge d'intermédiation bancaire pour assurer une rentabilité soutenue et garantir sa pérennité et sa

prospérité. L'accroissement et la diversification de son portefeuille clientèle industrielle et commerciale constitue désormais une priorité pour son développement.

Pour cela, elle se soucie de fidéliser sa clientèle de petites et moyennes entreprises et chercher de nouvelles cibles pour développer sa part de marché. Il est primordial pour une banque installée dans un paysage concurrentiel de moderniser aussi son réseau commercial, améliorer ses services et bien prendre en charge sa clientèle devenue de plus en plus exigeante.

Selon Monsieur l'ex-Président Directeur Général de la B.D.L Mohamed KRIM :

Le plan stratégique de la B.D.L s'articule autour de six axes fondamentaux suivants :

- ✓ Gouvernance ;
- ✓ Orientation Client ;
- ✓ Amélioration de l'efficacité opérationnelle ;
- ✓ Maîtrise des risques
- ✓ Contrainte de liquidité et gestion bilancielle ;
- ✓ Capital humain

Et les principaux axes du plan de développement de la B.D.L :

-Implémentation et mise en place du nouveau système d'information ; Le projet « Moustakbal BDL », le projet moteur de la banque, a pour objectif de la mise en place d'un progiciel bancaire intégré fonctionnant en temps réel (Core Banking) ;

-Mise en application de la nouvelle organisation de la banque ; a pour objectif de l'adaptation de l'organisation de la B.D.L à son nouveau SI et ses objectifs stratégiques qui positionnent le client au centre de ses intérêts ;

-Développement des produits bancaires et améliorer ses prestations à savoir :

- ✓ Lancement de l'e-Banking ;
- ✓ Lancement du compte épargne « EL BADIL » ;
- ✓ Déploiement intensif des Terminaux de Paiement Electronique TPE ;
- ✓ Développement et densification du parc DAB et GAB ;
- ✓ Développement du paiement par internet et acquisition des web-marchands.

-L'approche Capital Humain, concerne l'aspect organisationnel et procédural consolidé par la mise en œuvre de politiques d'emploi, de formation, d'évaluation et de gestion de carrière ainsi que le volet social.

Depuis sa création, la BDL avait pour mission essentielle d'accompagner et de financer les entreprises publiques locales dans leur développement local et régional. Ces entreprises représentaient toujours une grande partie des emplois de la BDL. Et en février 1989, elle a été transformée en société par actions et a commencé à se transformer en une banque universelle.

Les emplois de la BDL sont maintenant constitués d'une clientèle très diversifiée formée de PME et PMI, des professions libérales et des particuliers et des ménages. La banque s'engage aussi dans le financement des projets et des micro-entreprises développés dans le cadre des dispositifs spécifiques d'aide à l'emploi mis en place par les pouvoirs publics. Ainsi on peut voir l'engagement et la participation de la banque au développement de l'économie nationale et la relance de l'investissement.

Initialement, elle a été créée sous la forme d'une société nationale de banque, ce n'est qu'à partir de 1989 qu'elle s'est transformée en société par action (SPA) avec l'Etat comme actionnaire unique, représenté par le ministère des finances.

En 1985, la création de la BDL avait pour vocation de contribuer au développement économique et social des collectivités locales à travers le financement des entreprises et établissements publics à caractère économique sous tutelle des wilayas et des communes ; des opérations d'investissements productifs planifiées initiées par les collectivités locales ; des opérations ayant trait aux prêts sur gage ; et des entreprises privées non agricoles et ce, au même titre que les autres banques commerciales.

Actuellement, la banque BDL s'est insérée davantage dans le financement des PME/PMI tous secteurs confondus, mais pas seulement, elle est devenu aussi une banque des professions libérales, des particuliers et des ménages. Ainsi, elle participe à l'ensemble des dispositifs spécifiques d'aide à l'emploi mis en place par les autorités publiques (Ansej, Cnac, Angem).

Simultanément à la célébration du 19 mars 1962, Aid Nasr, la BDL a installé le 19 mars 2017 un nouveau système d'information baptisé S.I NASR. Ce nouveau système vient pour aider la banque à améliorer la qualité de ses prestations de services, diversifier ses produits, et accentuer son rôle dans le financement de l'économie.

La banque BDL s'est inscrite dans l'accomplissement d'un plan de développement (2016-2020) qui vise à la mise en place d'une nouvelle organisation de la banque, à l'implémentation d'un nouveau système d'information, à l'adoption d'une nouvelle identité visuelle, et à la mise en place de nouveaux produits financiers (e-paiement, e-banking, compte épargne El Badil…).

L'organigramme de la B.D.L :

L'organigramme général de la banque de développement local (B.D.L) est composé d'ensemble de directions, départements, des pôles commerciaux et d'opérations et des agences rattachées au front office et au back office, qui entretiennent entre elles des relations

hiérarchiques et fonctionnelles, afin de répartir l'ensemble des tâches dévolues à la banque dans la cadre des missions qui lui sont attribuées.

Le D.G est assisté par quatre (04) directeurs généraux adjoints qui lui sont directement rattachées dont :

- La Division de l'Inspection et de l'Audit.
- La Direction du Capital Humain.
- La Direction du Management de la Qualité.
- La Cellule Management des Projets.

- **La Direction Générale Adjointe chargée du « commercial » ;** Elle regroupe sous son autorité huit (08) directions.
- **La Direction Générale Adjointe chargée du back-offices et opérations ;** Elle est composée de six (06) Directions et d'un Département ;
- **La Direction Générale Adjointe chargée du support et systèmes d'information ;** Elle regroupe en son sein huit (08) directions et deux (02) départements :
- **La Direction Générale Adjointe chargée des Risques, Contrôle et conformité** ; Elle regroupe sous son autorité cinq (05) directions, une (01) structure et trois (03) départements.

Le schéma général d'organisation de la B.D.L est présenté par le schéma en annexe :

I- Département Risques opérationnels DRO :

1. Missions et attributions principales :

Le Département Risques Opérationnels, rattaché à la Direction Générale Adjointe des Risques, Contrôle et Conformité, a pour missions principales de mettre en place et de piloter le dispositif de gestion des risques opérationnels. Ce dispositif consiste à identifier et à évaluer l'impact des risques opérationnels sur la bonne marche et sur la rentabilité de la Banque, puis à définir et à mettre en œuvre la stratégie de leur maîtrise en adaptant en permanence les méthodes utilisées afin de les mettre aux normes de la réglementation en vigueur.

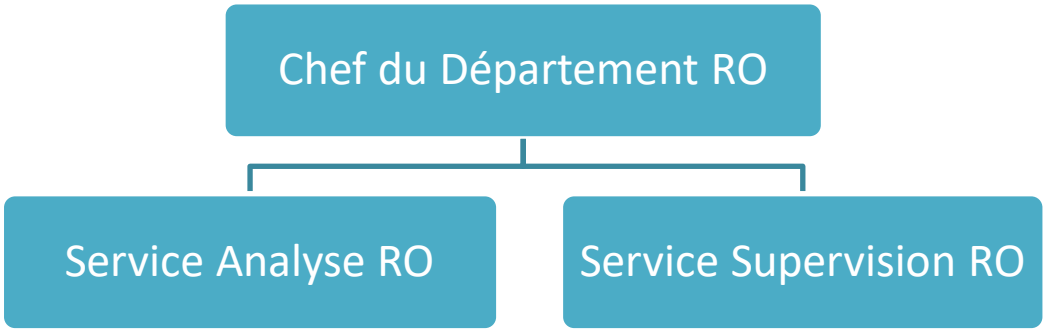
A ce titre, le Département est en charge des missions suivantes :

- Aligner le dispositif sur la politique de risques définie par la direction générale
- Mettre en place des systèmes de mesure, d'analyse et de surveillance des risques opérationnels conformément à la réglementation
- Vérifier régulièrement l'efficacité du dispositif et l'adapter aux évolutions
- Établir et mettre à jour la cartographie des risques
- Définir des plans d'actions pour atténuer/prévenir les risques

- Identifier, évaluer et suivre les indicateurs clés de risques (KRI)
- Contribuer à la mise en place des dispositifs de contrôle pour réduire les risques
- Concevoir les outils et formaliser les procédures de gestion des risques opérationnels
- Coordonner les actions avec les autres structures de gestion des risques et de contrôle
- Collecter et analyser les incidents opérationnels pour définir des plans d'actions correctifs
- Promouvoir une culture du risque au sein de la banque
- Veiller aux ressources et compétences du département
- Former et sensibiliser aux bonnes pratiques de gestion des risques opérationnels
- Rapporter régulièrement sur la mise en œuvre du dispositif
- Contribuer au rapport annuel sur le contrôle interne et la gestion des risques

2. Macro structure du DRO :

Figure N°05 : Organigramme du DRO



Source : Doumentation interne à la BDL

II- <u>Direction Monétique et Banque Digitale :</u>

1. Missions et attributions principales

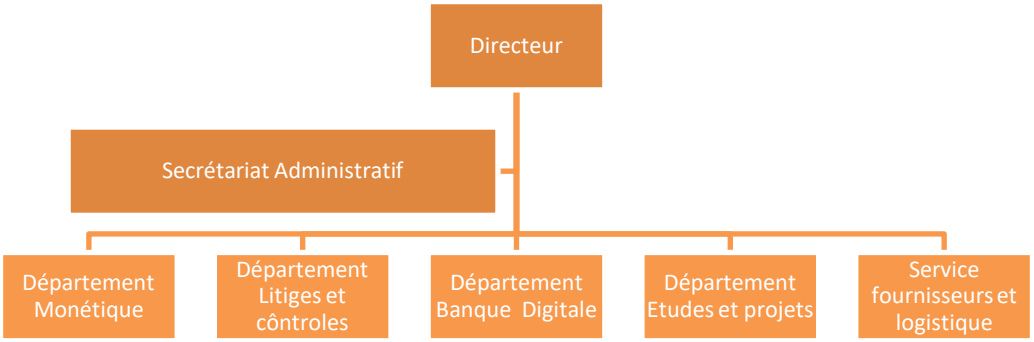
Les missions de la DMBD:

- Contribuer à la stratégie multi canal et nouvelles technologies
- Mettre en œuvre la stratégie de développement monétique/digital
- Suivre le plan d'actions monétique/digital
- Définir l'évolution des services, concevoir de nouveaux produits/services
- Assurer une veille technologique
- Gérer les relations avec les partenaires internes/externes
- Conduire les études et définir les spécifications de nouveaux produits
- Définir le plan marketing multi canal.
- Définir la politique tarifaire des services monétiques/digitaux
- Contrôler les factures monétiques
- Promouvoir et développer les services monétiques/digitaux
- Définir et suivre les indicateurs de pilotage et productivité
- Mettre en place les processus/procédures monétiques/digitaux

- Contribuer au dispositif de contrôle interne et gestion des risques
- Rapporter sur le développement monétique/digital
- Participer au rapport annuel sur le contrôle interne et la gestion des risques
- Rapporter sur la mise en œuvre des plans d'actions monétique/digital

2. Macro structure du DMBD :

Figure N°06 : Organigramme DBMD



Source : Source : Doumentation interne à la BDL

III- Tarification :[1]

Particuliers :

Cartes nationales :

Tableau N°06 : Tarification des cartes nationales CIB classique/ GOLD

Service	Tarif
Création+renouvellement CIB classique	Gratuit
Création+renouvellement CIB GOLD	Gratuit
Remplacement CIB classique	400 DZD/an
Remplacement CIB GOLD	800 DZD/an
Mise en opposition CIB classique	150 DZD
Mise en opposition CIB GOLD	200 DZD
Résiliation CIB classique	300 DZD
Résiliation CIB GOLD	600 DZD
Réédition code confidentiel CIB classique	200 DZD
Réédition code confidentiel CIB GOLD	300 DZD

Interprétation:

- Création et renouvellement gratuits :

Cela facilite grandement l'accès aux services bancaires pour tous. En supprimant ces frais, la BDL favorise l'inclusion financière dans le pays, conformément à sa mission.

- Remplacement payant :

Ces tarifs couvrent les coûts de fabrication, personnalisation et envoi d'une nouvelle carte. Le montant plus élevé pour la Gold s'explique par davantage de mesures de sécurité (puce, cryptogramme, etc) impliquant un coût supérieur.

[1] **Les tableaux des tarifs sont parvenus par la BDL**

- Mise en opposition bon marché :

Ce faible tarif pour le blocage de la carte en cas de perte/vol reflète la volonté de la BDL de protéger les clients. En facilitant cette démarche cruciale, elle limite les risques de fraude.

- Résiliation onéreuse :

Les frais élevés de clôture de compte ont un effet dissuasif, incitant à maintenir la relation bancaire. Ils visent à fidéliser les clients et assurer des revenus récurrents aux banques.

- Réédition du code payante :

Ces frais modérés évitent les demandes abusives de réédition du code confidentiel. Le tarif plus élevé pour la Gold compense le service prioritaire fourni à ces clients premium.

Cette tarification reflète un équilibre entre accessibilité bancaire, couverture des coûts, protection des clients et fidélisation. Elle tient compte du standing de la carte pour modulerer certains services.

Cartes internationales VISA :

Tableau N°07 : Tarification des cartes internationales Visa

Service	Tarif
Création+renouvellement+remplacement	2000 DZD/an
Création+renouvellement+remplacement	5000 DZD/an
Réédition code confidentiel	500 DZD
Mise en opposition	1000 DZD
Résiliation	1000 DZD

Interprétation :

- Frais de création élevés (2000 à 5000 DZD) :

Cela couvre les coûts de setup initial (personnalisation, fabrication), mais aussi la licence d'utilisation de la marque Visa. Ce sont des cartes à autorisation systématique, avec un plafond de retrait important.

- Renouvellement onéreux :

Outre la refabrication de la carte, cela inclut la prolongation de l'affiliation au réseau international Visa. Et potentiellement une revalorisation des assurances attachées à la carte (voyage, achats, etc).

- Remplacement très coûteux :

En plus des coûts de fabrication, cela compense les risques de fraude plus élevés sur ce type de carte. Des contrôles et une surveillance accrus sont nécessaires en cas de perte/vol.

- Réédition du code à 500 DZD :

Ce tarif élevé limite les demandes non fondées pour un produit premium. Il finance aussi les moyens renforcés de sécurisation de la procédure de réédition.

- Mise en opposition très chère (1000 DZD) :

Cela reflète les diligences internationales requises pour bloquer la carte sur le réseau Visa. Et la nécessité d'augmenter les contrôles ensuite pour éviter la fraude.

- Résiliation à 1000 DZD :

Ce prix fort décourage la clôture des comptes et incite à conserver ces cartes premium, sources de revenus récurrents.

Cartes internationales MASTERCARD :

Titanium :

Tableau N° 08: Tarification des cartes internationales MASTERCARD/Titanium

Création+renouvellement+remplacement	**8000 DZD/an**
Réédition code confidentiel	1000 DZD
Mise en opposition	2000 DZD
Résiliation	2000 DZD

- Les frais de création, renouvellement et remplacement sont très élevés (8000 DZD/an) car cette carte Titanium est la gamme la plus premium de Mastercard.

- La réédition du code confidentiel est facturée 1000 DZD, un tarif dissuasif pour éviter les demandes non fondées et financer la sécurisation renforcée de cette procédure.

- La mise en opposition coûte 2000 DZD. Ce montant important reflète les procédures spécifiques du réseau Mastercard en cas de perte/vol, encore plus complexes pour cette carte haut de gamme.

- Les frais de résiliation s'élèvent aussi à 2000 DZD. L'objectif est clairement de fidéliser sur le long terme les détenteurs de cette carte premium réservée à une élite.

- Globalement, cette tarification très onéreuse se justifie par le positionnement prestige de la gamme Titanium. Elle offre des services exclusifs à très forte valeur ajoutée (conciergerie, assurances top niveau, accès salons aéroport, etc).

- La banque rentabilise ainsi ce produit en ciblant une clientèle "private banking" prête à payer très cher pour ces services luxury. Le tarif élevé reflète bien ce statut premium.

Platinium :

Tableau N°09 : Tarification des cartes internationales MASTERCARD/Platinium

Service	**Tarif**
Création+renouvellement+remplacement	14 000 DZD/an
Réédition code confidentiel	1000 DZD
Mise en opposition	2500 DZD
Résiliation	2500 DZD

- Les frais de création, renouvellement et remplacement sont extrêmement élevés, à 14 000 DZD par an. Cela s'explique par le positionnement ultra-premium de cette carte, réservée à une clientèle Fortune.

- La réédition du code confidentiel est facturée 1000 DZD. Ce tarif très dissuasif reflète le haut niveau de sécurité requis sur cette carte et limite les demandes non fondées.
- La mise en opposition coûte 2500 DZD. Ce montant très important couvre les procédures spécifiques du réseau Mastercard pour cette carte, avec des contrôles renforcés en cas de perte/vol.
- Les frais de résiliation atteignent 2500 DZD. L'objectif est clairement de verrouiller sur le très long terme les détenteurs de cette carte, synonyme de statut social élevé.
- De manière générale, cette tarification extrême traduit le caractère prestigieux de la Mastercard Platinum, réservée à une clientèle ultra-aisée avec des exigences très pointues.
- Elle donne accès à des services et des avantages uniques au monde (conciergerie 24/7, assurances haut de gamme, invitations évènements exclusifs, etc). D'où les tarifs prohibitifs à chaque étape.

Professionnels :

Tableau N°10 : Tarification des cartes destinées aux professionnels

Service	Tarif
Création+renouvellement Corporate Silver	**Gratuit**
Création+renouvellement Corporate GOLD	**Gratuit**
Remplacement Corporate Silver	1500 DZD
Remplacement Corporate GOLD	1950 DZD
Mise en opposition Corporate Silver	200 DZD
Mise en opposition Corporate GOLD	400 DZD
Résiliation Corporate Silver	200 DZD
Résiliation Corporate GOLD	400 DZD
Réédition code confidentiel Corporate Silver	200 DZD
Réédition code confidentiel Corporate GOLD	200 DZD

- La création et le renouvellement gratuits facilitent l'équipement des professionnels indépendants et petites entreprises avec ces cartes.
- Le remplacement est facturé au prix coûtant pour la Silver, légèrement majoré pour la Gold qui requiert plus de frais fixes.
- La mise en opposition bon marché rend ce service critique accessible en cas de perte/vol.
- Les frais de résiliation modérés permettent une certaine flexibilité dans la relation commerciale.
- La réédition du code au même prix abordable pour les deux cartes traduit un niveau de service équivalent sur la sécurité.
- Globalement, cette tarification se veut attractive pour cibler les professionnels/PME, avec une différenciation limitée entre Silver et Gold.

- L'objectif est de promouvoir l'usage des cartes Mastercard auprès de cette clientèle, d'où des conditions avantageuses.

- On note que l'essentiel des services de base est gratuit ou peu onéreux. Les prix augmentent sur les services à valeur ajoutée.

Cette stratégie compétitive vise à acquérir des parts de marché chez les professionnels et petites entreprises.

Entreprises :

Tableau N° 11: Tarification des cartes destinées aux Entreprises

Cartes Corporate Silver

Service	Tarif
Création+renouvellement	Gratuit
Remplacement	1500 DZD
Mise en opposition	200 DZD
Résiliation	200 DZD
Réédition code confidentiel	200 DZD

Cartes Corporate GOLD :

Service	Tarif
Création+renouvellement	Gratuit
Remplacement	1950 DZD
Mise en opposition	400 DZD/an
Résiliation	400 DZD/an

Pour la Corporate Silver :

- Création et renouvellement gratuits pour faciliter l'équipement des collaborateurs
- Remplacement à prix coûtant (1500 DZD)
- Mise en opposition et résiliation peu chères (200 DZD) pour plus de flexibilité
- Réédition du code confidentiel également à un tarif abordable (200 DZD)

Pour la Corporate Gold :

- Création et renouvellement gratuits malgré une offre de services étendue
- Remplacement à 1950 DZD reflétant des coûts supérieurs (design, assurance, assistance, etc.)
- Mise en opposition plus chère (400 DZD) vu les risques accrus sur cette carte premium
- Résiliation également à 400 DZD pour fidéliser en partie les entreprises clientes

On note que cette tarification est alignée sur les cartes professionnelles et se veut donc attractive pour les entreprises, avec seulement une légère différenciation sur la gamme Gold plus haut de gamme.

L'objectif est de promouvoir l'usage des cartes Mastercard par les entreprises, d'où des conditions avantageuses, surtout sur les services de base.

SECTION 02 : MÉTHODOLOGIE D'ÉLABORATION DE LA CARTOGRAPHIE DES RISQUES DE LA BDL

L'élaboration de la cartographie des risques passe par deux majeures étapes : l'élaboration de la cartographie des processus puis la cartographie des risques :

I- Élaboration de la cartographie des processus

La première étape, et sans doute la plus importante, consiste à modéliser l'activité de la Banque tout en la décomposant afin d'établir une **cartographie des processus**. Cette phase consiste à analyser l'organisation de la BDL afin d'identifier l'ensemble des processus et leur sous processus gérés par ses structures.

Cette tâche incombe au DRO.

1. Périmètre de la cartographie des processus

La définition des processus répond en premier lieu à un découpage économique de l'activité de la banque (selon la nature de l'activité), et non un découpage organisationnel (par structure).

L'identification des processus part ainsi des différents produits, services et activités et identifie les acteurs (qui peuvent appartenir à des entités différentes au sein de la banque) et les tâches impliquées dans la fourniture de ces produits. La cartographie des processus doit couvrir l'ensemble des processus de la Banque, qu'ils soient des processus de ***Management***, ***Opérationnel*** ou de ***Support***.

- **Processus de Management et de Supervision**: ils retranscrivent la stratégie, les objectifs et permettent de piloter la démarche Qualité tout en assurant son amélioration continue.

  Ce sont par exemple les processus de planification des actions, de pilotage de l'amélioration ou de définition et suivi des objectifs.
- **Processus Opérationnels** : ce sont ceux qui contribuent directement à la réalisation d'un produit ou service, depuis la détection du besoin du client jusqu'à sa satisfaction. Ils représentent le cœur de métier de la banque.

  On peut citer par exemple les processus d'octroi de crédit, de réalisation d'opérations de commerce extérieur, d'ouverture de compte, de placements, etc.
- **Processus Support**: Ils fournissent les ressources matérielles et immatérielles nécessaires au bon déroulement des autres processus. Ces processus regroupent la maintenance, la mise à disposition de matériel ou de ressources humaines, la maîtrise de la documentation et de la communication, la métrologie, etc.

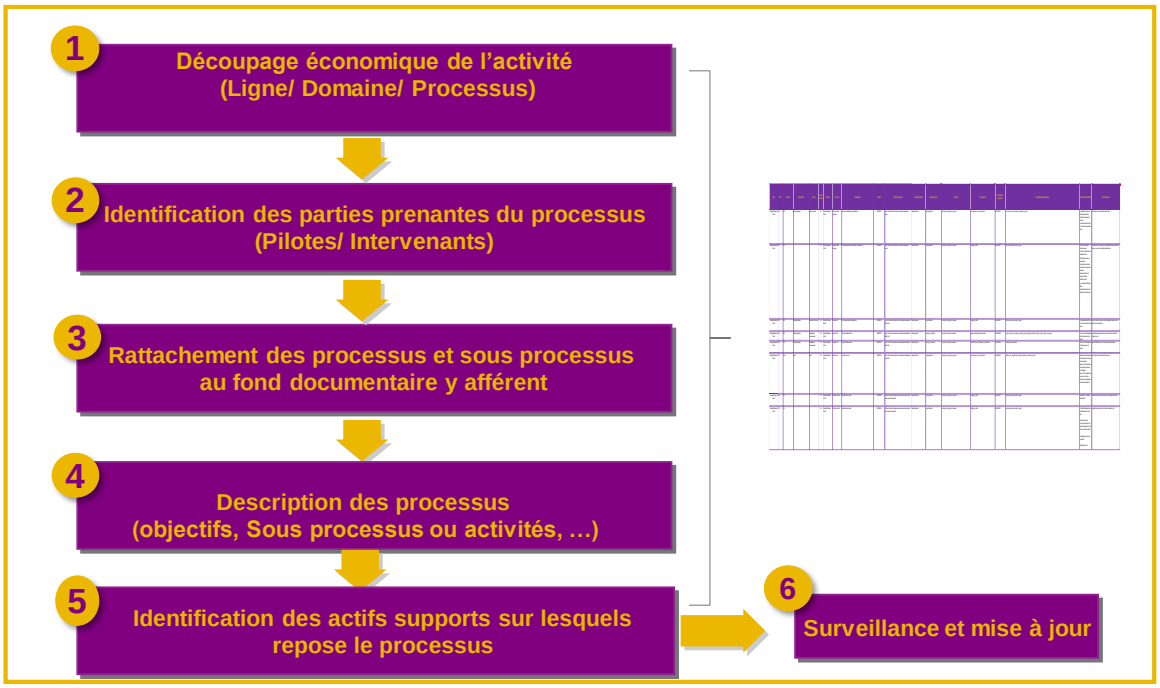
2. Démarche d'élaboration de la cartographie des processus :

Tenant compte de la couverture de l'ensemble des activités de la banque, l'approche adoptée pour le découpage des activités est l'approche « Top-down » (du haut vers le bas).
Le principe consiste de partir d'une cartographie macroscopique représentant l'organisation de la banque dans son ensemble pour ensuite s'acheminer progressivement vers les processus clés puis des niveaux de description plus détaillés.
La cartographie des processus doit comprendre à minima les informations suivantes:

- Lignes métiers ;
- Domaines d'activités;
- Processus ;
- Pilotes des processus ;
- Les intervenants du processus ;
- Objectifs des processus ;
- Sous processus ;
- Les actifs supports sur lesquels reposent les processus.

Le travail consiste alors en, ce qui suit :

Figure N°07 : Les étapes d'élaboration d'une cartographie des processus



Source : Doumentation interne à la BDL

- A travers l'organigramme de la banque, découper les activités par lignes métier puis par domaine d'activité.
- A travers les manuels de fonctions, identifier les activités attribuées à chaque fonction. Les processus attribués à deux ou plusieurs fonctions, chacune en ce qui la concerne, ne doivent pas être dupliqués ; ainsi chaque nouveau processus identifié doit être classé dans le domaine et la ligne d'activité le concernant.
- A travers cette même analyse, affecter à chaque processus les structures y intervenant (les duplications doivent apparaitre à ce niveau)
- Identification des pilotes de chaque processus. Cette attribution se fait par voie de décision de la Direction Générale.

- Décrire le processus: en précisant en quoi consiste le processus et quel est l'objectif attendu.
- A travers les entretiens avec les opérationnels, découper le processus en sous processus. Cette étape peut être complétée par l'exploitation des procédures opérationnelles.
- A travers le même entretien et/ou à partir de la cartographie des actifs, identifier les actifs supports sur lesquels repose le processus.

3. Règles de codification des processus

Afin de faciliter la gestion et le suivi des processus, une règle de codification a été arrêtée selon le principe suivant:

✓ **Type du processus:** En fonction que le processus soit de type Management, Opérationnel ou Support, les processus sont codifiés PM, PO ou PS respectivement ;

✓ **N° de la ligne:** 4 lignes métier ont été retenues pour la banque en plus des lignes de gestions numérotées de 01 à N ;

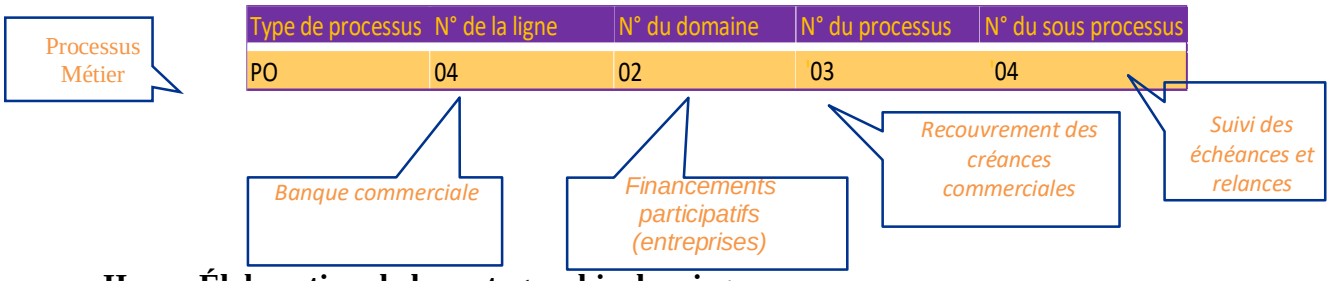
✓ **N° du domaine:** Chaque ligne contient un ou plusieurs domaines d'activités ;

✓ **N° du processus:** Chaque domaine contient un ou plusieurs processus numérotés de 01 à N ;

✓ **N° du sous processus:** Chaque processus se décompose en au moins deux ou plusieurs sous processus numérotés de 01 à Nn.

La liste exhaustive des lignes métiers et des domaines d'activités est reprise en annexe N°02 ;

Exemple: le suivi des échéances et relance codifié PO04020304



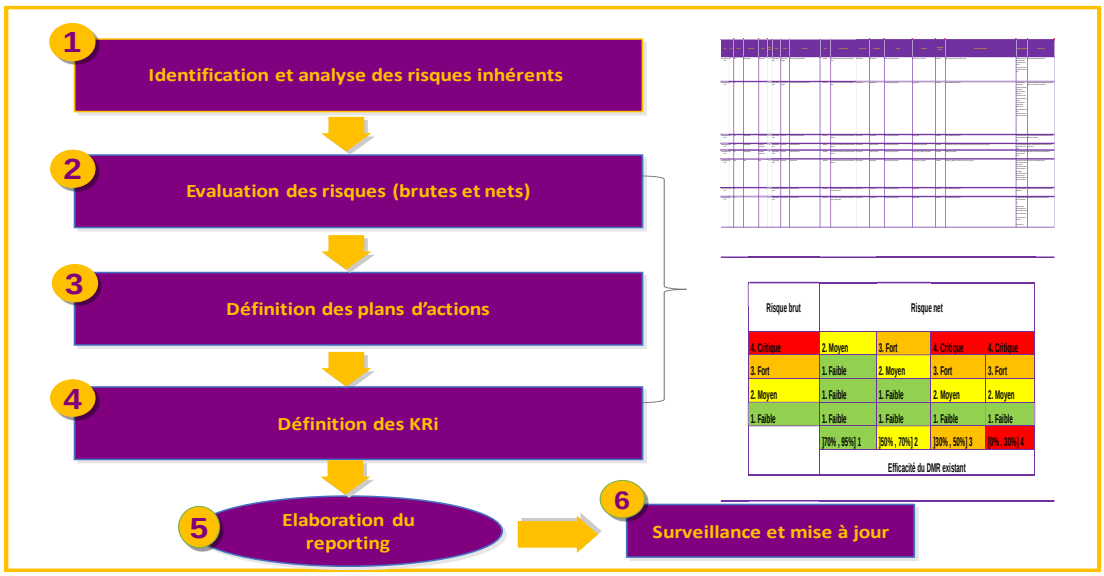
II- Élaboration de la cartographie des risques

La cartographie des risques se définit comme la démarche d'identification, d'évaluation, de hiérarchisation et de gestion des risques inhérents aux activités de la Banque.

Sa construction procède d'une description objective, structurée et documentée des risques existants. La description fait ressortir l'existence des risques et leur probabilité (occurrence), les éléments susceptibles de les accroître (facteurs aggravants), et les réponses apportées ou à apporter, dans le cadre d'un plan d'actions.

Dans ce contexte, l'élaboration d'une cartographie des risques efficace nécessite de respecter les étapes suivantes:

Figure N°08 : Elaboration de la cartographie des risques



Source : Doumentation interne à la BDL

1. Identification et analyse des risques inhérents

A ce stade, il convient de comprendre où sont les risques au sein de la banque et quelles activités les génèrent. Il s'agit dans cette phase d'identifier les risques potentiellement encourus par la banque.

Chaque processus/ Sous processus doit donc être rattaché aux risques associés. Ce rattachement prend en considération les éléments suivants:

- Type de risque ;
- Catégorie de risque ;
- Sous-catégorie de risque ;
- Evènement générique de risque ;
- Les vulnérabilités de la banque.

En se référant aux règles baloises et avec corrélation avec les définitions du règlement 11/08 de la Banque d'Algérie, une nomenclature de catégories et de sous catégories des risques ainsi que d'événements génériques a été adoptée.

Le principe d'identification des risques consiste à :

- Dérouler pour chaque processus/ Sous processus, la liste des événements génériques;
- A chaque fois que l'événement est susceptible d'affecter le processus ou le sous processus, il est reporté dans la colonne réservée à cet effet dans la cartographie des risques;
- Rattacher chaque événement à sa catégorie et sa sous-catégorie de risques ;
- Identifier les vulnérabilités internes ;
- Une fois les menaces « événement générique » et les vulnérabilités identifiées, il s'agira

de décrire le scénario du risque. Celui-ci consiste à décrire la scène ou la façon dont le risque se produit.

2. Evaluation des risques

Les risques ont la caractéristique d'être identifiables et mesurables. Leur valorisation peut se faire soit :

- sur la base d'études quantitatives par récupération de coûts précédemment identifiés (base de remonté d'incidents) ;
- à dire d'expert (retour d'expérience).

Le mode d'évaluation adopté par la BDL suit une approche qualitative et ce en absence d'une base de remonté des incidents.

Cette approche tend à évoluer vers une approche quantitative. Une base de remontée des incidents ainsi que la procédure de gestion des incidents est alors mise en place (Cf. Procédure de gestion des incidents).

Cette valorisation des coûts du risque permettra, d'une part, d'identifier les probabilités d'exposition aux risques et de leur gravité potentielles et d'autre part, de pouvoir apprécier le poids moyen du risque (Coût du risque moyen lorsque l'approche tendra vers des appréciations de plus en plus quantitatives).

Dans le cadre de la cartographie mise en place par la BDL, la cotation des risques repose sur un système de notation construit à partir de seuils d'appétence et de tolérance au risque, définis par le Comité de Contrôle Interne et approuvé par l'Organe délibérant.

L'objectif est de maintenir en permanence une situation solvable de la Banque avec prise en considération de l'ensemble des risques.

L'évaluation des risques passe par deux étapes, la première dite "évaluation du risque brut" et la seconde dite "Evaluation du risque net".

2.1. Evaluation des risques bruts

Cette première évaluation, dite brute, ne prend pas en considération les dispositifs de maitrise des risques existants. Elle permet d'avoir un aperçu sur le poids de la combinaison de l'ensemble des menaces et des vulnérabilités auxquels fait face la banque dans leur état brut.

Chaque évènement de risque identifié est ainsi soumis à une première évaluation fondée sur l'appréciation de :

- Sa fréquence (probabilité) d'occurrence ;
- Son impact (financier, continuité, Image, Juridique (conformité)).

La mission d'évaluation des risques est pilotée par le Département Risques Opérationnels,

sous la supervision de la DGA RCC.

Les grilles de cotation retenues par la BDL sont comme suit :

- **Grille de cotation de la fréquence**

Tableau N°12 : grille de cotation de la fréquence

Cotation	Valeur	Valeurs temps
4. Très fréquent	**4**	Plusieurs fois par mois X>12 :]12, +∞[
3. Assez Fréquent	**3**	Une fois par mois X=12
2. Assez rare	**2**	Moins d'une fois par mois 1<=X< 12 :[1, 12[
1. Très rare	**1**	Une fois tous les 5 ans en moyenne X<=1 :[0, 1[

- **Grille de cotation de l'impact**

L'impact global du risque est évalué sur la base d'une formule combinant 4 impacts potentiels (Impact : Financier, Continuité, Image, Juridique).

La valorisation de l'impact global du risque consiste à la prise en considération l'impact le plus élevé entre (Financier /Continuité/ Image /Juridique.

Les grilles de cotation de chacun des impacts sont les suivantes :

Tableau N°13 : Grille d'évaluation de l'impact

Financier :

Cotation	Valeur	Intervalles de pertes
4. Critique	**4**	X >= 500 MDZD
3. Fort	**3**	100<=X<500 MDZD
2. Moyen	**2**	50<=X<100 MDZD
1. Faible	**1**	X<50 MDZD

Image/réputation

Impact	Valeur	Appréciation
4. Critique	**4**	Perte de confiance suite à une médiatisation négative au niveau national et international.
3. Fort	**3**	Couverture médiatique négative au niveau national. L'image et la réputation sont affectées à court terme
2. Moyen	**2**	Information relayée sur Internet, réseaux sociaux … Impact potentiel sur l'image et la notoriété
1. Faible	**1**	Rumeurs au niveau interne uniquement. Impact non significatif sur la notoriété, l'image et la réputation.

Continuité

Impact	Valeur	Appréciation
4. Critique	**4**	Arrêt de l'activité
3. Fort	**3**	Perturbation importante pour la BDL
2. Moyen	**2**	Perturbation modérée pour la BDL
1. Faible	**1**	Faible perturbation sur l'activité

Juridique :

Impact	Valeur	Description
4. Critique	**4**	Retrait d'agrément, interdiction définitive d'exercer l'activité.

3. Fort	**3**	Retrait temporaire de licence, interdiction temporaire d'exercer l'activité.
2. Moyen	**2**	Amende
1. Faible	**1**	Avertissement

Source : Doumentation interne à la BDL

➢ **Grille de cotation de la criticité brute du risque**

Une fois la fréquence d'un évènement de risque et son impact global calculé, une cotation brute du risque inhérent est obtenue comme suit : Valeur du risque = Impact x Probabilité d'occurrence

Matrice de cotation des risques Bruts :

	Probabilité	**Très rare**	**Assez rare**	**Assez fréquent**	**Très fréquent**
Impact	Faible (1)	**1**	**2**	**3**	**4**
	Moyen (2)	**2**	**4**	**6**	**8**
	Fort (3)	**3**	**6**	**9**	**12**
	Critique (4)	**4**	**8**	**12**	**16**

De 1 à 3	**Risque Faible**
De 4 à 6	**Risque Moyen**
Entre 8 et 9	**Risque Fort**
Entre 12 et 16	**Risque Critique**

Source : Doumentation interne à la BDL

2.2. Stratégie de traitement des risques :

En fonction de l'évaluation des risques, le mode de traitement des risques doit être arrêté par le management exécutif de la banque sur proposition du DGARCC.

Les différents modes de traitement sont les suivants:

- **Acceptation :** Le couple Risque/rentabilité justifie la prise de risque, l'espérance de gain est largement supérieure aux risques encourus ;
- **Réduction :** qui peut être de deux natures **:**

✓ Prévention: Atténuer l'occurrence en renforçant le DMR – mettre en place contrôle niveau 1 ou 2

✓ Protection: Limiter l'impact en agissant sur les conséquences – Mise en place d'un PCA par exemple ou tout autre moyen de régularisation.

- **Transfert :** Transférer contractuellement une partie de l'activité et donc la maîtrise du risque à un tiers (externalisation, délégation de gestion).
- **Evitement :** Refus de l'intégralité du risque : abandon de l'activité.

La stratégie de traitement des risques peut intervenir après la phase d'évaluation des risques bruts comme après celle de l'évaluation des risques nets.

En effet, cette analyse permet à la phase d'évaluation brute d'identifier les surplus de DMR mis en place pour la couverture de risques acceptés dans le cadre de la politique de la Banque. Une

optimisation du dispositif de contrôle peut alors être opérée et réaliser en conséquent des économies. Lorsqu'elle est réalisée après la phase d'évaluation des risques nets, elle permet d'orienter les plans d'actions et de les optimiser.

2.3. Evaluation du risque net

L'évaluation du risque net consiste à apprécier le niveau du risque résiduel persistant après la mise en place des dispositifs de maitrise des risques. Il mesure le risque que la BDL pourrait effectivement subir et repose sur un principe de double cotation (Risque brut x Efficacité du DMR mis en place).

- **Grille de cotation des DMR :** exprimée en %, l'efficacité du DMR donne une appréciation sur le niveau de couverture du risque brut et donc du degré de son d'atténuation.

Efficacité du DMR existant:

Tableau N°14: Evaluation de l'efficacité du DMR

Degré d'atténuation	Valeur	Evaluation
4. [0%, 30%]	**4**	Aucun contrôle mis en place (Contrôle non existant)
3.] 30%, 50%]	**3**	Le contrôle mis en place couvre partiellement le risque - Contrôle mal conçu
2.] 50%, 70%]	**2**	Le contrôle mis en place couvre totalement le risque mais son application est non efficace - Contrôle bien conçu mais son application présente des défaillances
1.] 70%, 95%]	**1**	Le contrôle mis en place couvre totalement le risque et son application est efficace - Contrôle bien conçu et bien appliquer

Source : Doumentation interne à la BDL

- **Grille de cotation des risques nets :**

Le risque net mesure l'impact que la BDL pourrait effectivement subir, en intégrant les dispositifs de prévention et de détection existants. Il repose sur un principe de double cotation (Risque brut x Efficacité du DMR mis en place) selon l'échelle suivante:

Tableau N°15: Grille de cotation des risques nets

Risque brut	Risque net			
4. Critique	**2. Moyen**	**3. Fort**	**4. Critique**	**4. Critique**
3. Fort	**1. Faible**	**2. Moyen**	**3. Fort**	**3. Fort**
2. Moyen	**1. Faible**	**1. Faible**	**2. Moyen**	**2. Moyen**
1. Faible	**1. Faible**	**1. Faible**	**1. Faible**	**1. Faible**
	]70%, 95%] 1	**]50%, 70%] 2**	**]30%, 50%] 3**	**[0%, 30%] 4**
	Efficacité du DMR existant			

Source : Doumentation interne à la BDL

Interprétation :

- Lorsque le DMR est coté **4** ou **3**, cela implique qu'il est inefficace et non effectif : la cotation du risque brut demeure de ce fait **inchangée**.
- Lorsque le DMR est coté **2**, cela implique qu'il est plus-tôt efficace mais non effectif et reste de ce fait à parfaire : La cotation du risque brute est alors réduite **d'un niveau**.
- Lorsque le DMR est coté **1**, cela implique qu'il est efficace et permettrait de réduire le risque à un seuil acceptable : la cotation du risque brute est réduite systématiquement à un niveau de risque faible **« niveau 1 »**, à l'exception du risque brut critique qui ne peut être réduit que graduellement en passant par un « niveau 2 », puis à un niveau 1 lors des prochaines évaluations par mesure de prudence.

Cette évaluation nécessite une identification et une connaissance des dispositifs existant qui repose sur les critères d'appréciation suivants:

Tableau N°16: Classification des contrôles

Classification des contrôles			
Nature	**Typologie**	**Contrôle clé**	**Formalisation du DMR**
Automatique : **paramétré ne nécessitant aucune intervention humaine.**	**Préventif :** permet d'empêcher ou de prévenir l'incident. Il s'agit de moyens de contrôle déployé avant l'exécution de l'opération.	Oui : couvre l'ensemble ou la majorité des attributs de risques.	Oui : DMR décrit dans une procédure et sa réalisation est standardisée.
Semi-automatique : **paramétré, nécessitant l'intervention humaine partielle ou totale. Cette catégorie comprend aussi un mix entre contrôle automatique et contrôle manuel.**	**Détectif :** permet de détecter tout anomalie ou incident dès sa survenance. Il s'agit de moyens de maitrise déployés post-opération.	Non : ne couvre pas plusieurs attributs de risque.	Non : DMR non décrit dans une procédure et sa réalisation n'est pas standardisée.
Manuel : **réalisé en extra-système, 100% manuel.**	**Correctif :** permet de corriger toute anomalie, dysfonctionnement après sa survenance.	N/A	N/A

3. Plan d'Actions

Il s'agit dans cette phase de déterminer pour chaque évènement de risque des axes d'améliorations cibles permettant de pallier les insuffisances du dispositif de maîtrise de risques existant et de réduire au maximum l'exposition aux risques. En répondant aux bonnes pratiques, ce plan d'actions décrit les outils, activités de contrôle et procédures à mettre en place par la BDL, dans des délais déterminés.

La politique arrêtée consiste à définir un plan d'actions pour chaque risque coté "3" ou "4"

selon la grille de cotation des risques nets reprises plus haut et conformément au seuil de tolérance retenu.

La détermination des plans d'actions relève de la responsabilité des responsables métiers des processus sous la supervision des pilotes des processus désignés à cet effet.

Les plans d'actions sont communiqués au DRO, selon le calendrier fixé, qui procédera à son analyse sous la supervision du DGA-RCC. Cette dernière doit permettre d'apprécier le niveau d'adéquation des plans d'actions proposés par rapport aux spécificités du risque identifié, au niveau d'atténuation ainsi qu'aux délais de prise en charge.

Le plan d'actions global doit être validé par le Comité de Contrôle Interne de la BDL en fonction du niveau du risque encouru et la stratégie de traitement retenue.

SECTION 03:DÉTERMINATION DES RISQUES OPÉRATIONNELS DU PROCESSUS MONÉTIQUE

Dans cette présente section, nous allons évoquer le cœur du sujet qui est l'identification des processus, puis l'identification des risques et leur évaluation, l'élaboration des DMR, et la cartographie, puis la proposition des plans d'actions vers la fin.

III.1. Présentation des processus :

Nous allons aborder dans cette partie la présentation des processus de paiement carte bancaire notamment l'octroi et délivrance de la carte, sa gestion en matière de mise en opposition, modification de plafonds et la gestion des cartes capturées.

1. Processus d'octroi et délivrance des cartes :

L'octroi et la délivrance des cartes bancaires est un processus clé dans la relation entre une banque et ses clients. Il recouvre l'ensemble des étapes depuis la demande initiale du client jusqu'à la remise et l'activation de la carte bancaire.

Ce processus stratégique fait intervenir de nombreux acteurs au sein de la banque : les agences commerciales bien sûr, mais également les services centraux comme la fabrication des cartes, les systèmes d'information, la gestion des risques, etc. Il implique également des prestataires extérieurs pour la fabrication et la personnalisation des cartes notamment.

La fluidité et la rapidité de ce processus sont primordiales pour offrir une expérience client de qualité. Son optimisation permanente est donc un enjeu majeur pour la banque, afin de réduire les délais de mise à disposition des cartes tout en maîtrisant les risques de fraude.

Nous allons détailler ici les différentes étapes depuis la demande client jusqu'à l'activation de la carte en passant par la fabrication, la livraison aux agences et la remise au client.

- Processus : Octroi et délivrance de la carte P01

- Sous processus : Emission de la carte bancaire SP01
- Sous processus : Activation et remise de la carte SP02
- Sous processus : Non présentation du client SP03

Tableau N°17 : Processus Octroi et délivrance de la carte bancaire

Intervenants	Procédures	Tâche	T
Agence	Non couvert	Réceptionner la demande du Client.	T01
Agence		Faire signer au Client le contrat porteur.	T02
Agence		Saisir sur le Système d'Information la demande du client.	T03
Agence		Contrôler la conformité de la demande du client.	T04
DMBD		Réceptionner de la DSI le « Fichier Commandes » consolidé de toutes les Agences.	T05
DMBD		Introduire le « Fichier Commandes »dans la plateforme SATIM.	T06
DMBD		Réceptionner le mail de la SATIM une fois les cartes sont disponibles	T07
AME		Récupérer à des jours différents les cartes et les codes confidentiels	T08
AME		Processus de transmission des cartes	T09
Agence		Réceptionner les cartes et les codes confidentiels via le prestataire AME.	T10
Agence		Réception du pli des nouvelles cartes	T11
Agence		Réconcilier avec la commande passée	
Agence		Remettre le pli des cartes au M-com et les codes au D-agc	
Agence		Conserver, précieusement, les codes confidentiels.	T12
Agence		Stocker les cartes dans un coffre fermé à clé	T13
		Contacter le client pour l'informer de la disponibilité de sa carte CIB.	T01
		Client se présente? Si Oui	T02
Agence		Remettre la carte au Client	T03
		le diriger vers le D/A pour récupérer le code confidentiel.	T04
Agence		Recueillir auprès du Client l'accusé de réception sur le registre dédié à cet effet.	T05
Agence		Saisir sur le Système d'Information la remise de la carte	T06
DSI		Consolider en fin de journée les demandes d'activation parvenues de l'ensemble des Agences.	T07
DMBD		Transmettre un fichier d'activation global à la SATIM.	T08
		Client se présente? Si Non	T01
Agence		Relancer le Client après un délai de 30 jours, pour la récupération de sa carte	T02
		Le Client se présente ? Si oui	T03
Agence		Revenir à la tâche T02/SP02	T04
		Client se présente? Si Non	T05
Agence		Relancer le Client avec un nouveau délai de 15 jours.	T06
		Le Client se présente ? Si oui	T07
Agence		Revenir à la tâche T02/SP02	T08
		Le Client se présente ? Si Non	T09
Agence		après 03 mois carte non réclamée, opposition de la carte sur système	T10
Agence		Destruction de la carte	T11

Source : Elaboré par nos soins

Le processus d'octroi et de délivrance de la carte contient trois principaux sous-processus :

1. Emission de la carte (SP01) : l'agence reçoit la demande du client, fait signer le contrat, saisit la demande dans le SI, contrôle la conformité, transmet la commande à la DMBD. Celle-ci commande les cartes à la SATIM. L'AME récupère les cartes et codes et les transmet à l'agence.

2. Remise et activation de la carte (SP02) : l'agence contacte le client, lui remet la carte et le code. Le client signe l'accusé de réception. L'agence saisit l'activation dans le SI et la DMBD transmet le fichier global des activations à la SATIM.

3. Non présentation du client (SP03) : l'agence relance le client après 30 jours puis 15 jours. Si pas de présentation après 3 mois, l'agence fait opposition sur la carte et la détruit.

Les intervenants principaux sont : agence, DMBD, AME, SATIM, DSI, client.

Les procédures clés sont : commande et personnalisation des cartes, remise au client, relances en cas de non retrait, opposition et destruction si non réclamée après 3 mois.

2. Les processus de gestion des cartes :

2.1.Le processus de gestion des cartes capturées :

La gestion des cartes capturées est une procédure cruciale dans la gestion du risque lié à l'utilisation frauduleuse des cartes. Elle permet de bloquer l'usage d'une carte capturée ou perdue afin de protéger le porteur.

Cette procédure stratégique est déclenchée lorsqu'une carte est capturée par un automate ou signalée perdue/volée par un client. Elle implique une coordination étroite entre l'agence bancaire, les équipes centrales d'analyse des fraudes et la direction des moyens de paiement.

Le processus suit un enchaînement rigoureux d'étapes afin de tracer précisément le blocage de la carte : retrait de l'automate, remplissage des formulaires, transmission aux services centraux, analyse du dossier, décision finale sur l'opposition, et information du client.

La rapidité de traitement est essentielle pour limiter les risques de transactions frauduleuses. Nous détaillerons ici les procédures en place dans la banque pour garantir une mise en opposition efficace des cartes capturées ou signalées perdues/volées.

- Processus : Gestion des cartes bancaires P02
- Sous processus : cartes capturées SP02

Tableau N°18 : Processus de gestion des cartes capturées

Intervenants	Procédures	Tâche	T
	Non couvert	**Gestionnaire de DAB**	
Agence		Retirer la carte de DAB	T01
Agence		Renseigner le registre destiné à cette fin ainsi que le formulaire d'autorisation d'oblitération/restitution	T02
Agence		Transmettre le formulaire à la structure monétique de sa banque	T03
Agence		Renseigner le formulaire de contrôle de carte capturée	T04
Agence		Transmettre le formulaire au CMI	T05
		Structure monétique	
DMBD		Analyse les informations renseignées dans le formulaire	T06
DMBD		Transmet ses conclusions au gestionnaire de DAB en indiquant si le porteur est en droit ou pas de se faire restituer sa carte	T07
DMBD		Décision de restitution ou pas	T08

Source : Elaboré par nos soins

Lorsqu'une carte est capturée par un DAB, un processus précis se met en place. Dans un premier temps, l'agence bancaire retire la carte de l'automate et remplit les formulaires nécessaires : registre interne, formulaire d'autorisation d'oblitération et formulaire de contrôle de la carte capturée. Ces documents sont transmis à la structure monétique de la banque et au

Centre Monétique Interbancaire (CMI). La DMBD analyse alors le dossier et prend la décision finale de restituer ou non la carte au porteur. Cette décision est communiquée au gestionnaire de l'ATM. Ce processus de mise en opposition, impliquant l'agence, les services centraux et la DMBD, suit donc un cheminement précis pour traiter chaque carte capturée afin de limiter les risques de fraude.

2.2.Le processus de la mise en opposition des cartes :

La mise en opposition d'une carte bancaire est une procédure cruciale déclenchée à la demande d'un client victime de perte ou de vol de sa carte. Elle vise à bloquer immédiatement toute transaction frauduleuse sur cette carte compromise.

Cette procédure stratégique requiert une coordination efficace entre l'agence bancaire, qui réceptionne la demande du client, et les services centraux (DSI, DMBD), qui exécutent techniquement la mise en opposition.

Le processus suit un enchaînement rigoureux d'étapes : réception du client en agence, authentification, saisie dans le SI, contrôles, transmission aux équipes centrales, validation et introduction dans le système interbancaire pour le blocage effectif de la carte.

La rapidité de traitement est cruciale pour limiter le risque de fraude. La communication entre les équipes sur le terrain et les services centraux doit donc être fluide. Nous détaillerons ici les procédures en place pour assurer une mise en opposition réactive des cartes signalées perdues ou volées.

- Processus : Gestion des cartes P02
- Sous processus : Mise en opposition des cartes SP01

Tableau N° 19: Processus de gestion des mises en opposition des cartes

Intervenants	Procédures	Tâche	T
Agence		Réceptionner le Client et procéder à :	T01
Agence		Saisir la mise en opposition sur le Système d'Information.	T04
Agence		Editer le bordereau de saisie,	T05
Agence		Remettre au directeur d'agence la demande de mise en opposition.	T06
Agence		Procéder au contrôle de conformité et à la vérification de la saisie.	T07
		Contrôles concluants ? Si Non :	
Agence		Rejeter au M-COM en indiquant les anomalies constatées.	T08
		Contrôles concluants ? Si Oui :	
Agence		Numériser la demande de mise en opposition pour visualisation par le Département Monétique.	T09
		A la réception du fichier transmis par l'Agence :	
DSI		Procéder à la validation de la saisie sur le Système d'Information.	T10
DSI		Consolider les demandes parvenues de l'ensemble des Agences dans un fichier global.	T11
DMBD		Introduire le fichier dans la plateforme de la SATIM.	T12
DMBD		Procéder à la demande d'émission de nouvelles cartes au profit des Clients concernés.	T13
P01		Processus « Emission de la carte ».	T14

Source : Elaboré par nos soins

Lorsqu'un client se présente en agence pour procéder à une mise en opposition de sa carte bancaire (en cas de perte, vol, etc.), l'agence réceptionne le client, procède à son identification

et à l'authentification de sa signature avant de saisir la demande dans le système d'information. Un bordereau de saisie est édité et transmis au directeur d'agence pour contrôle de conformité. Si les contrôles sont validés, la demande est numérisée pour transmission au Département Monétique. La DSI valide alors la saisie dans le SI, consolide l'ensemble des demandes des agences dans un fichier transmis à la DMBD. Celle-ci introduit le fichier dans le système de la SATIM pour procéder à la mise en opposition effective de la carte. En parallèle, la DMBD déclenche l'émission d'une nouvelle carte pour le client concerné via le processus standard d'émission des cartes bancaires. L'enchaînement rigoureux de ces tâches entre l'agence, la DSI et la DMBD permet une mise en opposition rapide et sécurisée des cartes signalées par les clients

2.3.Modification des informations de la carte :

La gestion du cycle de vie des cartes bancaires requiert de pouvoir modifier certaines informations associées à une carte, notamment les plafonds d'utilisation. Ce processus de modification des données de la carte est crucial pour répondre aux évolutions des besoins des clients.

Cette procédure stratégique nécessite une coordination efficace entre l'agence bancaire, qui recueille la demande du client, et les services centraux qui exécutent techniquement la modification dans le système d'information de la banque.

Le processus implique plusieurs étapes de contrôle et de validation entre les différents services, afin de sécuriser toute modification des données sensibles liées à une carte. La conformité de la demande et des justificatifs est vérifiée à chaque étape avant modification effective dans le SI.

Nous détaillerons ici les procédures rigoureuses déployées par la banque pour permettre aux clients de modifier les informations de leurs cartes bancaires tout en garantissant la sécurité et la fiabilité des données.

- Processus : Gestion des cartes bancaires P02
- Sous processus : Modifications des informations de la carte SP03

Tableau N°20 : Processus de modifications des informations de la carte

Intervenants	Procédures	Tâches	T
Client	Non couvert	Se présenter en Agence pour demander la modification des informations	T01
Agence		A la réception de la demande et des pièces justificatives :	T02
Agence		Identifier le Client	
Agence		Authentifier la signature,	
Agence		Procéder à la saisie de la modification sur le Système d'Information et éditer le bordereau de modification,	
Agence		Remettre le bordereau au D-agc	
Agence		Etudier la conformité de la demande de modification ainsi que les pièces justificatives et le bordereau de saisie.	T03
Agence		Comparer la saisie avec les documents.	
Agence		Contrôles concluants ?	T04
Agence		Si Non : Rejeter la demande en indiquant les motifs du rejet.	T04.1
DMBD		Si Oui : Numériser la demande ainsi que les pièces justificatives pour visualisation par le DMBD	T04.2
DMBD		A la réception des documents numérisés :	T05
DMBD		Procéder au contrôle de conformité de la demande ainsi que des pièces justificatives.	
DMBD		Contrôles concluants ?	T06
DMBD		Si Non : Rejeter la demande en indiquant les motifs du rejet.	T06.1
DMBD		Si Oui : Procéder à la validation de la modification initiée par l'Agence concernée.	T06.2

Source : Elaboré par nos soins

Lorsqu'un client se présente en agence pour demander une modification des informations de sa carte bancaire (plafonds, etc.), l'agence réceptionne la demande et les justificatifs. Elle identifie le client, authentifie sa signature et saisit la modification dans le Système d'Information, avant d'éditer un bordereau transmis au service concerné .Ce service étudie la conformité de la demande et des justificatifs et compare avec la saisie. S'il valide la demande, il la numérise pour transmission au service central DMBD. Ce dernier contrôle à nouveau la conformité et, si validation, procède à la modification effective des informations de la carte dans le SI. En cas de non-conformité à chaque étape, la demande est rejetée en indiquant les motifs. L'enchaînement des contrôles et validations entre l'agence et les services centraux vise à sécuriser toute modification des données sensibles liées à une carte bancaire.

3. Gestion des DAB :

3.1.Arrêté d'un DAB :

Les DAB doivent régulièrement faire l'objet d'opérations de maintenance et d'arrêt afin de réapprovisionner les automates en liquide. Ces arrêts de DAB suivent un processus rigoureux visant à sécuriser la manipulation et le décompte des fonds.

Cette procédure stratégique requiert l'intervention concertée du directeur d'agence et du CSC. Elle implique plusieurs étapes sensibles : inventaire et déchargement sécurisé des casettes, décompte minutieux des billets, comptabilisation précise des montants retirés.

Le respect des procédures en place est essentiel pour éviter toute perte ou vol lors de ces opérations. Nous détaillerons ici les mesures déployées par la banque pour encadrer les arrêts de DAB et garantir la traçabilité des fonds manipulés à chaque étape du processus.

- Processus : Gestion des DAB P03
- Sous processus : Arrêté DAB SP01

Tableau N°21 : Processus d'arrêté d'un DAB

Intervenants	Procédures	Tâche	T
CSC		Débiter la caisse principale sur SI	T03
CSC		Créditer la caisse DAB sur SI	T04
DAG+CSC		Compter l'argent à alimenter	T05
CSC		Ouverture du DAB en combinaison	T06
DAG+CSC		Arrêter les casettes après les avoir inventoriées	T07
DAG+CSC		Procéder au déchargement des casettes	T08
CSC		Retrait de la casette de rejet et compter les billets rejets	T09
CSC		Retrait de chaque casette d'alimentation et compter les billets restant et les noter dans un PV de caisse	T10
CSC		Vider les casettes d'alimentation + la casette rejet	T11
CSC		Comptabiliser le montant restant dans les casettes sur SI	T12
CSC		Comptabiliser l'excédent/déficit (s'il existe) sur un module dédié pour ça sur SI	T13

Source : Elaboré par nos soins

Lors d'un arrêt de DAB, le directeur d'agence et le CSC mettent d'abord le DAB en maintenance. Ils procèdent ensuite à l'arrêt physique de l'automate et à l'inventaire des casettes. Les casettes sont alors déchargées une à une par les deux intervenants : la casette de rejet est retirée et les billets rejetés sont comptés, puis chaque casette d'alimentation est retirée, les billets restants sont comptés et notés dans un PV. Les casettes sont ensuite vidées. Le CSC comptabilise sur le SI le montant restant dans chaque casette. Enfin, il comptabilise l'éventuel excédent ou déficit constaté lors de l'opération. Le processus d'arrêt de DAB suit donc une procédure précise visant à sécuriser et tracer le retrait et le décompte des fonds.

3.2.Alimentation DAB :

Le réapprovisionnement régulier des DAB en espèces constitue une opération cruciale pour assurer la disponibilité du service pour les clients. Ce processus d'alimentation suit un enchaînement rigoureux d'étapes afin de sécuriser la manipulation des fonds.

Cette procédure stratégique requiert une collaboration étroite entre le directeur d'agence et le CSC. Elle implique le transfert sécurisé des espèces, leur chargement physique dans l'automate, la saisie des données de réapprovisionnement, et des vérifications minutieuses avant remise en service.

Le respect des règles en vigueur à chaque étape est indispensable pour prévenir les risques de vol ou de détournement lors de la manipulation des fonds. Nous détaillerons ici les mesures mises en place par la banque pour encadrer le processus sensible d'alimentation des DAB.

- Processus : Gestion DAB P03
- Sous processus : Alimentation DAB

Tableau N°22 : Processus d'alimentation DAB

Intervenants	Procédures	Tâches	T
DAG+CSC	Non couvert	Détermination du montant à alimenter le DAB	T01
DAG+CSC		Alimenter les casettes après leurs arrêts (Procéder au chargement des casettes et saisie des données)	T02
CSC		Remettre la casette rejet vide à sa place après son verrouillage	T03
CSC		Remettre les autres casettes vides à leurs places	T04
DAG+CSC		Procéder à la fermeture de coffre avec la combinaison	T05
DAG+CSC		Vérification de la nouvelle alimentation	T06
DAG+CSC		Vérification de réapprovisionnement	T07
DAG+CSC		Vérification de la partie supérieure du DAB	T08
CSC		Remise en service du DAB	T09
CSC		Mise à disposition	T10

Source : Elaboré par nos soins

Lors de l'alimentation d'un DAB, le directeur d'agence et le CSC déterminent d'abord le montant à charger dans l'automate. Ils procèdent ensuite au chargement physique des casettes et à la saisie des données correspondantes. Le CSC remet ensuite en place la casette de rejet vide après l'avoir verrouillée, ainsi que les autres casettes réapprovisionnées. Les deux intervenants ferment le coffre du DAB avec la combinaison avant de vérifier la bonne alimentation, le réapprovisionnement et la partie supérieure de l'automate. Le CSC finalise en remettant en service le DAB et en le mettant à disposition des clients. Le processus d'alimentation suit donc une série d'étapes sensibles visant à sécuriser le transfert et le chargement des fonds dans le DAB.

3.3.Acquisition DAB :

L'installation de DAB constitue un projet stratégique pour la BDL, afin d'étendre son réseau et offrir plus de services à ses clients. Ce processus suit plusieurs étapes clés, de l'évaluation des besoins à la mise en service opérationnelle du DAB.

Cette procédure implique de nombreux services au sein de la banque : la direction commerciale, les équipes techniques, la sécurité, la logistique, etc. Elle nécessite également de collaborer avec des partenaires externes comme les fournisseurs de DAB.

Chaque aspect doit être mené avec rigueur : appel d'offres fournisseur, paramétrage technique, approvisionnement, formation du personnel, tests. Le respect des différentes étapes est crucial pour garantir la fiabilité et la sécurité du DAB pour les clients. Nous détaillerons ici les procédures déployées par la banque pour mener à bien ce projet d'installation.

- Processus : Gestion DAB P03
- Sous processus : Acquisition DAB

Tableau N°23 : Processus d'acquisition DAB

Intervenants	Procédures	Les tâches	T
DMBD	Non couvert	Evaluation du besoin : La banque doit d'abord évaluer ses besoins en matière de DAB, en termes de nombre de machines nécessaires, d'emplacement, de fonctionnalités requises, etc.	T01
BDL		Faire une étude de marché pour déterminer l'emplacement optimal pour installer le DAB. Il faut prendre en compte la densité de population, la proximité des commerces, la sécurité du lieu, etc.	T02
BDL		Sélectionner le fournisseur du DAB en lançant un appel d'offres. Comparer les différentes offres en termes de coûts, fonctionnalités, maintenance, etc.	T03
BDL+ Fournisseur		Signer un contrat avec le fournisseur retenu pour l'achat ou la location du DAB. Le contrat doit couvrir la livraison, l'installation, la maintenance, les mises à jour logicielles, etc.	T04
Fournisseur		Préparer le lieu d'installation du DAB. S'assurer que l'alimentation électrique et la connexion réseau sont disponibles. Renforcer la sécurité si nécessaire (caméras, alarmes, etc.)	T05
BDL		Réceptionner la livraison du DAB et vérifier son bon fonctionnement lors de l'installation par le fournisseur.	T06
Fournisseur		Paramétrer le DAB en le connectant aux systèmes informatiques de la banque. Configurer les aspects financiers, de sécurité, les écrans, etc.	T07
Agence		Approvisionner le DAB en espèces. Établir des procédures pour les réapprovisionnements réguliers.	T08
BDL		Former le personnel qui sera en charge des opérations et de la maintenance du DAB.	T09
Agence		Faire des tests finaux avant la mise en service. Vérifier tous les aspects : distribution des billets, communications, sécurité, etc.	T10
BDL		Annoncer l'installation du nouveau DAB aux clients par des affiches sur place, le site web, les réseaux sociaux, etc.	T11
Agence		Surveiller régulièrement le fonctionnement du DAB et procéder à sa maintenance selon les recommandations du fournisseur.	T12

Source : Elaboré par nos soins

Tout d'abord, la banque évalue ses besoins en matière de DAB et réalise une étude pour déterminer l'emplacement optimal. Elle lance ensuite un appel d'offres pour sélectionner le fournisseur et signe un contrat d'achat ou de location avec le fournisseur retenu. La banque prépare le lieu d'installation et réceptionne la livraison du DAB en vérifiant son bon fonctionnement. Les équipes techniques paramètrent et connectent le DAB aux systèmes informatiques de la banque puis l'approvisionnent en espèces. Le personnel est formé aux opérations et à la maintenance du DAB. Des tests finaux sont effectués avant la mise en service et l'annonce aux clients de cette nouvelle installation. Enfin, la banque assure une surveillance régulière du fonctionnement du DAB et effectue sa maintenance selon les recommandations du fournisseur.

3.4.Maintenance DAB :

La maintenance régulière des DAB est un enjeu majeur pour les banques afin de garantir un service optimal pour les clients. Ce processus stratégique requiert une coordination étroite entre les techniciens bancaires et les équipes techniques des fournisseurs de DAB.

Chaque étape, du diagnostic de la panne à la réparation sur site, suit une procédure rigoureuse visant à rétablir rapidement le fonctionnement des automates défectueux. La rapidité

d'intervention et la qualité de la maintenance sont essentielles pour minimiser les temps d'indisponibilité des DAB.

Nous détaillerons ici l'organisation et le déroulement des opérations de maintenance préventive et corrective des DAB. Ces processus mobilisent différents acteurs internes et externes à la banque pour assurer la continuité de ce service critique pour les clients.

- Processus : Gestion DAB P03
- Sous processus : Maintenance DAB SP04

Tableau N°24 : Processus de maintenance DAB

Source : Elaboré par nos soins

Intervenants	Procédures	Tâches	T
DMBD	Non couvert	Vérification initiale sur site par le technicien bancaire des problèmes et dysfonctionnements du DAB.	T01
DMBD		Si le problème n'est pas résolu sur place, ouverture d'un ticket d'incident auprès du support technique du fournisseur du DAB.	T02
Fournisseur		Le support technique fait des vérifications à distance et un diagnostic approfondi grâce aux logs et informations transmises par le DAB.	T03
Fournisseur		Si le problème ne peut pas être résolu à distance, planification d'une intervention sur site par un technicien du prestataire.	T04
Fournisseur		Le technicien se rend sur site avec les pièces de rechange nécessaires identifiées lors du diagnostic.	T05
Fournisseur		Le technicien effectue les réparations requises : remplacement de composants défectueux, nettoyage, ajustements mécaniques, etc.	T06
Fournisseur		Une fois la panne résolue, le technicien effectue des tests complets de validation du bon fonctionnement du DAB.	T07
Fournisseur		Le technicien remplit un rapport détaillé d'intervention mentionnant les diagnostics, les réparations effectuées, les pièces remplacées, etc.	T08
BDL		La banque valide la bonne résolution du problème et la reprise du fonctionnement normal du DAB.	T09
BDL		La banque récupère les pièces défectueuses remplacées pour analyse ou destruction selon les procédures.	T10
BDL		La banque règle la facture de l'intervention auprès du fournisseur selon le contrat de maintenance.	T11
BDL		Mise à jour des registres de maintenance du DAB par la banque.	T12

Le processus de maintenance des DAB débute par une vérification sur site des dysfonctionnements par le technicien bancaire. Si le problème persiste, un ticket d'incident est ouvert auprès du support technique du fournisseur pour un diagnostic approfondi à distance. Si la panne ne peut être résolue à distance, le fournisseur planifie une intervention sur site avec les pièces adéquates. Le technicien effectue alors les réparations nécessaires, des tests de validation et rédige un rapport détaillé. La banque valide la résolution du problème, récupère les pièces remplacées et règle la facture selon le contrat. Enfin, elle met à jour les registres de maintenance du DAB. Ce processus coordonné entre techniciens bancaires et fournisseur vise à rétablir rapidement le fonctionnement des DAB défectueux.

3.5.Retrait DAB :

Le retrait d'argent liquide via les DAB est l'une des fonctionnalités essentielles des cartes bancaires pour les clients. Ce processus stratégique suit une séquence étroitement régulée entre l'utilisateur, l'automate et les systèmes bancaires.

Chaque étape, de l'authentification du client à la délivrance des billets, répond à des procédures strictes visant à garantir la sécurité et la fluidité de la transaction. La coordination entre les différents acteurs permet un contrôle rigoureux avant autorisation du retrait.

Nous détaillerons ici le déroulement du processus pas à pas, des vérifications interbancaires d'usage à la distribution effective d'espèces du DAB. Comprendre cet enchaînement technique est essentiel pour mesurer l'importance d'une disponibilité optimale des DAB pour les banques.

- Processus : Gestion DAB P03
- Sous processus : Retrait DAB SP05

Tableau N°25 : Processus de retrait DAB

Intervenants	Procédures	Tâche	T
Client	Non couvert	Introduction de la carte bancaire dans le lecteur.	T01
Client		Saisie du code PIN.	T02
Client		Choix du service « Retrait »	T03
Client		Saisie du montant de retrait	T04
Client		Valider l'opération	T05
DAB		La demande d'autorisation est transmise à la SATIM.	T06
SATIM		La SATIM transmet la demande d'autorisation à la BDL.	T07
BDL		La BDL vérifie l'identité du titulaire de la carte et le solde disponible et la validité de la carte.	T08
BDL		La BDL autorise ou refuse le retrait.	T09
BDL		Si le retrait est autorisé, la BDL transmet une confirmation à la SATIM.	T10
BDL		À ce stade, le montant du retrait est réservé sur le compte, ce qui signifie qu'il est mis de côté et ne peut pas être utilisé pour d'autres transactions.	T11
SATIM		La SATIM transmet la confirmation au distributeur automatique	T12
DAB		Le distributeur automatique délivre l'argent /Retrait de l'argent.	T13
DAB+BDL		Simultanément, le DAB transmet l'information du retrait à la BDL pour débiter le montant.	T14
Client		Récupération de la carte bancaire.	T15
DAB		Le DAB imprime un ticket confirmant la transaction pour le client	T16

Source : Elaboré par nos soins

Le processus débute par l'insertion de la carte bancaire et la saisie du code PIN par le client. Celui-ci choisit le service de retrait d'espèces, saisit le montant souhaité et valide l'opération. La demande d'autorisation est transmise à la SATIM puis à la BDL. Cette dernière vérifie l'identité du porteur, le solde disponible et la validité de la carte avant d'accorder ou refuser le retrait. Si autorisé, la BDL réserve le montant, confirme à la SATIM qui transmet au DAB. Le DAB délivre alors les billets demandés et transmet l'information à la BDL pour débit. Enfin, la carte est restituée et un ticket imprimé avant d'être récupéré par le client. Ce processus

coordonné entre le client, le DAB et les acteurs bancaires vise à sécuriser et fluidifier les retraits.

4. Gestion TPE

4.1.Paiement TPE :

Le paiement par carte bancaire via un terminal de paiement électronique (TPE) est un moyen de paiement dématérialisé très répandu, qui permet d'effectuer rapidement et en toute sécurité des transactions entre un commerçant et un client. Lors d'un paiement par TPE, plusieurs acteurs interviennent et différentes étapes techniques se enchaînent afin d'autoriser et de valider la transaction. Ce processus fait intervenir le commerçant, le client payeur, le TPE, le réseau interbancaire sécurisé, et la banque du commerçant et du client. Dans ce document, nous allons détailler précisément les différentes tâches effectuées par chaque intervenant lors d'un paiement par carte bancaire via TPE, depuis la saisie du montant par le commerçant jusqu'au débit du compte client et au crédit du compte commerçant.

- Processus : Gestion TPE P04
- Sous processus : Paiement TPE SP01

Tableau N°26 : Processus de paiement TPE

Intervenants	Procédures	Tâche	T
Commerçant	Non couvert	Le commerçant saisit le montant de la transaction sur le TPE.	T01
Client		client présente sa carte bancaire avec puce et code confidentiel ou celle sans contact au commerçant	T02
Commerçant		commerçant insère la carte dans le lecteur de puce du TPE ou approche la carte sans contact du lecteur	T03
TPE		le TPE récupère les données de la carte (numéro de carte, date d'expiration, cryptogramme visuel)	T04
Client		client saisit son code confidentiel sur le clavier du TPE	T05
SATIM		TPE chiffre ces données et les transmet au serveur d'autorisation de la BDL via le réseau interbancaire sécurisé SATIM.	T06
BDL		La réponse d'autorisation ou de refus est renvoyée au TPE sous la forme d'un code d'autorisation en quelques secondes. Si toutes les vérifications sont positives, la BDL génère un numéro d'autorisation unique et le renvoie crypté au TPE.	T07
TPE		En cas d'autorisation, la transaction est validée, le TPE stocke les informations de la transaction dans sa mémoire interne	T08
TPE		TPE déchiffre la réponse et affiche l'autorisation ou le refus sur l'écran	T09
TPE		ticket de paiement est imprimé	T10
Client		Le client retire sa carte	T11
Client		commerçant récupère une copie du ticket.	T12
TPE		Le client récupère l'original comme justificatif	T13
		À la fin de la journée, le TPE transmet les informations des transactions stockées à la banque acquéreur (BDL dans ce cas là).	T14
BDL		Le paiement est débité du compte bancaire du client dans les jours suivants et crédité sur le compte du commerçant.	T15
		Le relevé bancaire du client et l'état récapitulatif du commerçant feront apparaître la transaction.	T16

Source : Elaboré par nos soins

Le commerçant saisit le montant sur le TPE et le client présente sa carte bancaire. Le commerçant insère la carte dans le lecteur de puce du TPE ou approche la carte du lecteur

sans contact. Le TPE récupère les données de la carte, le client saisit son code confidentiel. Le TPE chiffre les données et les transmet à la banque (BDL) via le réseau SATIM.

La BDL vérifie le solde du compte et accorde ou refuse l'autorisation, qu'elle renvoie cryptée au TPE. En cas d'autorisation, la transaction est validée et stockée dans le TPE, qui imprime un ticket.

Le client retire sa carte, le commerçant récupère une copie du ticket. À la fin de la journée, le TPE transmet les transactions à la banque acquéreur (BDL). Le paiement est débité du compte du client et crédité sur celui du commerçant dans les jours suivants.

4.2.Acquisition TPE :

Le paiement par carte bancaire via un terminal de paiement électronique (TPE) est un moyen de paiement dématérialisé très répandu, qui permet d'effectuer rapidement et en toute sécurité des transactions entre un commerçant et un client. Lors d'un paiement par TPE, plusieurs acteurs interviennent et différentes étapes techniques se enchaînent afin d'autoriser et de valider la transaction. Ce processus fait intervenir le commerçant, le client payeur, le TPE, le réseau interbancaire sécurisé, et la banque du commerçant et du client. Dans ce document, nous allons détailler précisément les différentes tâches effectuées par chaque intervenant lors d'un paiement par carte bancaire via TPE, depuis la saisie du montant par le commerçant jusqu'au débit du compte client et au crédit du compte commerçant.

- Processus : Gestion TPE P04
- Sous processus : Acquisition TPE SP02

Tableau N°27 : Processus acquisition TPE

Intervenants	Procédures	Tâches	T
DMP	Non couvert	Étude des besoins et du parc de TPE existant pour déterminer le nombre de terminaux à acquérir.	T01
BDL		Rédaction d'un cahier des charges avec les fonctionnalités requises: type de lecteur de carte, options de connectivité, imprimante, écran tactile, etc.	T02
BDL		Consultation des fournisseurs et comparaison des offres sur la base du cahier des charges.	T03
BDL		Négociation des conditions commerciales: prix unitaire, maintenance, SAV, durée du contrat, etc.	T04
BDL		Choix du fournisseur en fonction des critères technico-commerciaux.	T05
BDL+Frs		Signature du contrat avec le fournisseur retenu.	T06
Fournisseur		Paramétrage des TPE par la banque avant livraison: logo, identifiant banque, clés de sécurité, etc.	T07
Fournisseur		Livraison des TPE dans les agences bancaires.	T08
Fournisseur		Installation des TPE par les techniciens de la banque ou du prestataire.	T09
BDL		Formation du personnel bancaire à l'utilisation et à la maintenance de base des TPE.	T10
BDL		Tests de transactions et de communications avec le système d'information bancaire.	T11
BDL		Déploiement auprès des commerçants partenaires de la banque.	T12

Source : Elaboré par nos soins

Le processus d'acquisition des TPE (code P04/SP02) comprend plusieurs sous-processus, procédures et tâches. Il débute par une étude des besoins et du parc de TPE existant

afin de déterminer le nombre de terminaux à acquérir. Un cahier des charges est ensuite rédigé en précisant les fonctionnalités requises. Une consultation des fournisseurs est menée et leurs offres sont comparées sur la base du cahier des charges. Les conditions commerciales sont négociées (prix, maintenance, etc.) et le fournisseur est choisi. Le contrat est signé puis les TPE sont paramétrés par la banque avant leur livraison dans les agences. Les techniciens installent et forment le personnel à l'utilisation des TPE. Des tests de transactions sont effectués avant le déploiement auprès des commerçants partenaires.

4.3.Maintenance TPE :

La maintenance des TP est un élément clé pour assurer la continuité de service auprès des commerçants clients de la banque. Elle nécessite une organisation rigoureuse ainsi qu'une coordination efficace entre la banque et les prestataires externes. Le sous-processus de maintenance, référencé SP03, permet de prendre en charge rapidement les dysfonctionnements et pannes signalés, depuis le diagnostic à distance jusqu'à la réparation physique des équipements en passant par leur récupération sur le terrain. La réactivité et la qualité de ce sous-processus sont primordiales pour limiter l'indisponibilité des TPE et les pertes d'activité pour les commerçants. Sa bonne exécution repose sur le respect des procédures par chaque intervenant ainsi que sur la fluidité des échanges d'informations entre les acteurs.

- Processus : Gestion TPE P04
- Sous processus : Maintenance TPE SP03

Tableau N°28 : Processus maintenance TPE

Intervenants	Procédures	Tâche	T
BDL	Non couvert	Surveillance quotidienne des transactions et détection des éventuels dysfonctionnements par la banque.	T01
BDL		Signalement des pannes et demandes d'intervention par la banque au centre de support client du prestataire.	T02
Fournisseur		Diagnostic à distance par le support client et tentatives de résolution logicielle de la panne.	T03
Fournisseur		Si échec du dépannage à distance, ouverture d'un ticket d'intervention avec codification du problème.	T04
DMP		Récupération du TPE auprès du commerçant	T05
DMP		Transmettre le TPE au fournisseur pour réparation	T06
Fournisseur		Remplacement des pièces défectueuses et réparation du TPE par le technicien.	T07
Fournisseur		Réalisation de tests de fonctionnement et impulsion de transactions factices.	T08
commerçant		Clôture de l'intervention et signature du rapport d'intervention par le commerçant.	T09
DMP		Récupération des TPE réparés et réinstallation chez les commerçants.	T10
DMP		Clôture du ticket d'intervention après validation du bon fonctionnement par la banque.	T11
BDL		Paiement de la prestation de maintenance selon les termes du contrat.	T12

Source : Elaboré par nos soins

Le sous-processus de maintenance des TPE (code SP03) implique différents intervenants et procédures. La banque surveille quotidiennement les transactions et détecte les

dysfonctionnements. Elle signale alors les pannes au support client du prestataire qui tente un dépannage à distance. Si cela échoue, un ticket d'intervention est ouvert avec codification du problème. Le TPE est récupéré chez le commerçant puis transmis au fournisseur pour réparation. Le technicien remplace les pièces défectueuses et effectue des tests. Le commerçant signe le rapport d'intervention. Les TPE réparés sont réinstallés et la banque valide leur bon fonctionnement avant de clôturer le ticket. Elle paie enfin la prestation de maintenance selon le contrat.

III.2. Identification et évaluation des risques :

1. Octroi et délivrance de la carte :

T	risque	FR	Vulnérabilités	img	cont	fin	jur	IB	FRQ	CB	DMR	Cot°	RN
T01	fraude à l'identité si les justificatifs fournis sont falsifiés/usurpation d'identité	FE	Documents falsifiés de qualité, complicité interne, contrôles d'identité défaillants	3	2	2	3	3	1	3	- Vérification systématique des pièces d'identité - Rapprochement avec des bases de données externes- Demande de pièces complémentaires en cas de doute	2	1. FA
T02	non conformité si le contrat n'est pas correctement renseigné et signé	CPPC	Défaut de vérification, négligence, pression commerciale	2	1	1	2	2	2	4	- Contrôle systématique par un agent différent de celui ayant fait signer le contrat- Checklist de contrôle- Validation par le responsable avant mise en production du contrat	2	1. FA
T03	erreur de saisie	ELGP	Inattention, surcharge de travail, formation insuffisante, erreur de transcription	1	2	1	1	2	3	6	- Contrôle automatisé des données saisies- Validation par le client des informations le concernant- Double saisie par deux opérateurs différents avec rapprochement	1	1. FA
T04	erreur ou omission dans le contrôle entraînant une non-conformité/validation d'une demande non conforme	ELGP	Supervision défaillante, contrôles aléatoires insuffisants, pression hiérarchique	2	2	1	2	2	2	4	- Checklist de contrôle- Séparation des tâches de préparation et validation- Validation hiérarchique	2	1. FA
T05	Risque de non prise en compte d'une commande/ réception d'un fichier de commandes erroné/	ELGP	Erreur dans fichier transmis, contrôles défaillants émetteur/récepteur	2	3	2	1	3	2	6	- Accusé de réception systématique- Rapprochement commande/facture- Contrôle de cohérence	2	1. FA
T06	erreur technique empêchant le traitement	ELGP	Défaillance système, bug logiciel, maintenance insuffisante, défaut de tests	2	2	1	1	2	1	2	- Doubles contrôles- Monitoring des systèmes- Procédures de secours	2	1. FA
T07	non réception de l'email/non réception de l'avis de disponibilité des cartes	ELGP	Problème technique, erreur d'adressage, non suivi des non réceptions	1	2	1	1	2	2	4	- Accusé de réception- Relance client- Mise en place d'alertes	2	1. FA
T08	perte, vol carte/code	ELGP	Procédures de sécurité défaillantes, négligence, complicité interne	3	3	4	2	4	2	8	- Ligne téléphonique dédiée- Opposition immédiate- Renouvellement rapide	1	1. FA
T09	perte, vol ou erreur de transmission	ELGP	Suivi des envois insuffisant, adressage erroné, interception frauduleuse	3	2	4	1	4	3	12	- Validation adresse par le client- Double contrôle interne	2	3. FO
T10	non réception des cartes et des	ELGP	Contrôles défaillants à	2	3	2	1	3	2	6	- Accusé de réception- Relance client- Mise en	2	1. FA

	codes		réception, complicité interne								place d'alertes		
T11	erreur de réconciliation avec la commande	ELGP	Contrôles défaillants, inattention	1	2	1	1	2	3	6	- Rapprochement des bons de commande et livraison- Comptage à réception	2	1. FA
T12	perte, vol ou divulgation non autorisée des codes confidentiels	FE	Négligence, complicité interne, contrôles d'accès insuffisants	4	4	4	3	4	4	16	- Rappel procédures- Sensibilisation des employés- Accès restreints	3	4.C
T13	perte, vol ou divulgation non autorisée des cartes	DAP	Négligence, complicité interne, contrôles d'accès insuffisants	4	4	4	3	4	4	16	- Ligne téléphonique dédiée- Opposition immédiate- Renouvellement rapide	1	2. M
T01	le client ne puisse être joint ou ne se présente pas/non information du client	CPPC	Coordonnées erronées, relance insuffisante	1	2	1	1	2	3	6	- Procédure de relances- Coordination interne	3	2. M
T03	remise à un tiers non autorisé en l'absence de vérification d'identité	CPPC	Contrôle d'identité défaillant, usurpation, négligence	3	3	4	2	4	3	12	- Contrôle d'identité systématique- Limitation des mandats	2	3.FO
T04	divulgation non autorisée si le code est récupéré par un tiers	CPPC	Confidentialité non respectée, complicité interne	3	3	3	2	3	1	3	- Rappel procédures- Sensibilisation des employés- Accès restreints	3	1.FA
T05	non traçabilité en cas d'absence de signature du registre par le client	ELGP	Négligence, précipitation	1	1	1	1	1	3	3	- Signature électronique- Numérisation des registres	2	1.FA
T06	erreur ou oubli de saisie	ELGP	Surcharge, stress, formation insuffisante	1	2	1	1	2	3	6	- Contrôle par un second opérateur- Validation du client	2	1.FA
T07	activation non sécurisée/activation frauduleuse de la carte	FI	Failles système, complicité interne	4	4	4	3	4	1	4	- Sécurisation procédures d'activation- Traçabilité- Contrôle a posteriori	2	1.FA
T08	non activation et blocage du client	ELGP	Défaut relance et suivi du client	1	2	1	1	2	2	4	- Procédure de déblocage- Assistance téléphonique- Communication au client	3	2. .M
T02	non activation si relance non effectuée ou non traçable	ELGP	Défaut relance et suivi du client	1	2	1	1	2	2	4	- Procédure de relances- Coordination interne	3	2. M
T10	opposition non effectuée en temps voulu sur le SI	ELGP	Délais non respectés, négligence	2	2	3	2	3	4	12	- Sensibilisation interne- Procédure accélérée d'opposition- Contrôle a posteriori	2	3. FO
T11	non destruction effective de la carte.	ELGP	Procédures défaillantes, complicité interne	2	2	3	2	3	3	9	- Traçabilité des destructions- Inventaires- Contrôles	2	2. M

Source : Elaboré par nos soins

2. Gestion des cartes capturées :

T	Risque	FR	Vulnérabilités	img	cont	fin	jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Risque de dommage à la carte due à une manipulation incorrecte/ perte ou de vol de la carte lors du retrait du DAB	DAP	- Mauvaise surveillance des distributeurs- Manque de formation des utilisateurs sur la manipulation sécurisée- Absence de caméras de surveillance	2	3	3	1	3	2	6	Surveillance par caméras, formation des utilisateurs, limitation du montant des retraits	2	2.M
T02	Risque d'erreur humaine lors de la saisie des informations/ erreurs dans le remplissage des formulaires	ELGP	- Complexité des formulaires- Mauvaise ergonomie- Manque de contrôle et de vérification	1	2	1	1	2	3	6	Formulaire simplifié, ergonomie améliorée, contrôle systématique	1	1.FA
T03	Risque de non transmission ou de transmission erronée des formulaires	ELGP	Mauvaise gestion documentaire- Problèmes techniques- Manquement de procédures	1	2	1	1	2	2	4	Procédure de transmission, accusés de réception, traçabilité	2	2.M
T04	Risque d'omission d'informations importantes.	ELGP	- Complexité des formulaires- Manque de vérification- Négligence	2	3	2	2	3	2	6	Formulaire simplifié, vérification systématique, check-list	1	1.FA
	Risque d'erreur dans le contrôle, ce qui pourrait influencer la décision finale.	ELGP	- Manque de compétences- Surcharge de travail- Manque de vérifications indépendantes	2	3	2	2	3	2	6	Vérification par un tiers, rotation des contrôleurs, supervision	2	2.M
T05	Risque de transmission non sécurisée lors de l'envoi au CMI.	IADS	Faiblesse du chiffrement- Accès non contrôlés- Absence de mesureses de sécurité	3	4	3	3	4	1	4	Chiffrement renforcé, politique d'accès stricte, canal sécurisé	1	1.FA
	Risque de perte ou de manipulation frauduleuse du formulaire pendant le transfert.	FE	- Procédures de transfert non définies- Traçabilité insuffisante	2	2	2	2	2	2	4	Traçabilité renforcée, procédure formalisée et sécurisée	2	2.M
T06	Risque d'analyse erronée des informations du formulaire	ELGP	Manque de compétences- Complexité du traitement- Absence de contrôle qualité	2	3	2	2	3	2	6	Compétences renforcées, supervision	2	2.M
	Risque de négliger des éléments importants dans l'analyse.	ELGP	- Surcharge de travail- Manque de méthodologie- Absence de vérification	2	3	2	2	3	2	6	Méthodologie, vérification systématique, répartition de la charge	1	1.FA
T07	Risque d'erreur dans la communication des conclusions	ELGP	- Mauvaise compréhension des conclusions- Manque de précision- Absence de validation	2	3	2	2	3	2	6	séparation des tâches	2	2.M
T08	Risque de non transmission ou transmission erronée/ incorrectes des conclusions au gestionnaire sur le droit à restitution	ELGP	- Mauvaise gestion documentaire- Absence de procédures- Manque de contrôle	1	2	1	1	2	2	4	Procédure de transmission, accusés de réception, traçabilité	2	2.M

Source : Elaboré par nos soins

3. Gestion des mises en opposition :

T	Risque	FR	Vulnérabilités	Img	Cont	Fin	Jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Usurpation d'identité du client	FE	Procédures d'identification insuffisantes, documents falsifiés	2	2	2	3	3	2	6	Renforcement des contrôles d'identité, vérification documents officiels, biométrie	1	1.FA
T02	erreur d'identification du client	ELGP	Inattention, fatigue, négligence	1	2	1	1	2	3	6	Check-list identification client, double contrôle, rotation des équipes	1	1.FA
T03	mauvaise authentification de la signature	ELGP	Procédures non respectées, documents falsifiés	2	2	2	3	3	2	6	Vérification par 2ème agent, numérisation des signatures	1	1.FA
T04	Erreur humaine dans la saisie	ELGP	Inattention, distraction, fatigue, manque de formation	1	2	1	1	2	4	8	Double saisie, validation croisée, contrôles automatisés	2	2.M
T05	Perte/vol du bordereau	FE	Procédures de gestion documentaire défaillantes	1	2	1	1	2	2	4	Traçabilité des documents, coffre-fort, dématérialisation	1	1.FA
T06	Transmission à mauvais destinataire	ELGP	Erreur d'aiguillage, procédures peu claires	2	2	2	3	3	1	3	Procédure de vérification des destinataires, chiffrement des données	1	1.FA
T07	Non détection d'erreurs ou anomalies	ELGP	Contrôles insuffisants, fatigue, routine	1	2	2	2	2	3	6	Contrôles aléatoires renforcés, rotation des équipes de contrôle	1	1.FA
	Validation d'opposition erronée	ELGP	Inattention, négligence	2	3	2	3	3	2	6	Vérification systématique, double validation manuelle	1	1.FA
T09	Perte/corruption du fichier numérisé	IADS	Matériel défectueux, mauvais paramétrages	1	2	1	1	2	1	2	Doubles sauvegardes, contrôles d'intégrité des données	1	1.FA
T10	Erreur de validation	ELGP	Contrôles défaillants, négligence	2	2	2	2	2	2	4	Check-list, rotation des équipes, contrôle aléatoire	1	1.FA
T11	Erreur dans la collecte ou le traitement des données provenant des différentes agences,	ELGP	Interfaces défaillantes, problèmes de paramétrage	2	2	2	2	2	1	2	Monitoring des interfaces, logs d'erreurs, traçabilité	1	1.FA
	Problème technique empêchant la récupération ou la consolidation des données des agences	IADS	Architecture IT défaillante, back-up insuffisant	2	3	2	1	3	3	9	Redondance des systèmes, sauvegardes externes, PRA	2	2.M
	Fichier global corrompu ou illisible suite à un problème technique lors de la consolidation	IADS	Contrôle d'intégrité défaillant	2	2	1	1	2	2	4	Contrôle d'intégrité, rejeu des données	1	1.FA
	Perte de confidentialité des données	IADS	Sécurité défaillante,	3	2	2	4	4	1	4	Chiffrement, contrôle des accès,	1	1.FA

	lors de la transmission depuis les agences ou lors de la consolidation		absence de chiffrement								cybersécurité		
T12	Erreur de transmission du fichier	IADS	Contrôle défaillant, problème technique	1	2	1	1	2	2	4	Accusés de réception, logs de transferts	1	1.FA
T14	Retard dans l'émission des nouvelles cartes	ELGP	Capacité de production insuffisante, problème d'approvisionnement	1	1	1	1	1	2	2	Suivi des délais fournisseurs, stocks de sécurité	2	1.FA

Source : Elaboré par nos soins

4. Gestion de modification des informations (plafonds) :

T	Risque	FR	Vulnérabilités	img	cont	fin	jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Usurpation d'identité du client	FI	- Faible contrôle d'identité lors de l'ouverture de compte- Accès non sécurisé aux données personnelles	3	2	2	3	3	2	6	- Vérification des pièces d'identité avec documents originaux- Consultation des bases de données officielles d'identité- Authentification forte du client	2	2.M
T01	Falsification des documents justificatifs	FI	- Contrôles insuffisants sur les documents reçus- Manque de vérification des documents auprès des autorités émettrices	2	1	2	3	3	2	6	- Vérification des documents auprès des autorités émettrices- Analyse des documents par des experts en fraude documentaire- Comparaison avec documents authentiques	2	2.M
T02	Erreur de saisie des informations	ELGP	- Mauvaise conception des interfaces de saisie- Manque de contrôle et revue des informations saisies	1	1	1	1	1	3	3	- Double saisie et vérification- Validations et contrôles automatisés- Revue par un superviseur	2	1.FA
T02	Non authentification de la signature	ELGP	- Absence de signature électronique sécurisée- Pas de vérification de la signature manuscrite	2	1	2	3	3	2	6	- Signature électronique sécurisée- Vérification de la signature manuscrite	1	1.FA
T03	Non détection d'anomalies ou falsifications	ELGP	- Contrôles insuffisants sur les données et documents- Manque d'outils de détection de fraude	3	2	3	4	4	3	12	- Outils de détection de fraude et d'anomalies- Analyse des données par un expert en fraude	3	3.FO
T06.2	Validation erronée de la demande	ELGP	- Procédures peu claires ou non respectées- Manque de revue et contrôle des validations	2	1	2	3	3	3	9	- Check-lists et procédures claires- Double validation par des personnes différentes- Piste d'audit	2	2.M

Source : Elaboré par nos soins

5. Arrêté DAB :

T	Risque	FR	Vulnérabilité	Img	Cont	Fin	Jur	IB	FRQ	CB	DMR	Cot°	RN
T01	panne ou indisponibilité du DAB pendant la maintenance	IADS	Défaut matériel, erreur de maintenance	2	3	2	1	3	2	6	Maintenance préventive, procédures de tests	2	2.M
T02	Risque d'erreur humaine lors de l'arrêt qui pourrait causer un dysfonctionnement	ELGP	Inattention, négligence	1	2	1	1	2	3	6	Formation, checklist, vérification par un second	1	1.FA
T03	Risque d'erreur de saisie comptable	ELGP	Inattention, complexité des opérations	1	1	2	1	2	2	4	Vérification par un second, rapprochement automatisé	1	1.FA
T04													
T05	Risque de vol d'argent lors du transport et de la manipulation	FE	Manque de surveillance, accès non sécurisé à l'argent	3	2	3	3	3	1	3	Agents assermentés, coffres sécurisés, traçabilité	1	1.FA
T06	Risque d'erreur de combinaison qui empêcherait l'ouverture du DAB	ELGP	Oubli, mauvaise note de la combinaison	1	2	1	1	2	2	4	Note confidentielle, changement régulier des codes	1	1.FA
T07	d'écart entre le décompte physique et le solde théorique des billets dans les cassettes	ELGP	Inattention, appareil de comptage défectueux	2	1	2	2	2	2	4	Vérification croisée, appareils calibrés	2	2.M
T08	Risque d'écart entre le décompte physique et le solde théorique des billets dans les cassettes	ELGP											
T09	Risque de vol ou de malversation lors du déchargement et du décompte des billets et cassettes	FI	Supervision insuffisante, cupidité	3	2	3	4	4	1	4	Supervision caméras, rotation équipes, traçabilité	1	1.FA
T10													
T11													
T12	Risque d'erreur de saisie comptable du montant restant	ELGP	Inattention, complexité	1	1	2	1	2	2	4	Vérification par un second, rapprochement comptes	2	2.M
T13	Risque de non détection d'éventuels écarts de caisse.	ELGP	Contrôles insuffisants, outils de détection inadéquats	2	1	4	2	3	3	12	Rapprochements automatisés, audits réguliers	2	3.FO

Source : Elaboré par nos soins

6. Alimentation DAB :

T	Risque	FR	Vulnérabilité	Img	Cont	Fin	Jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Risque d'erreur dans le calcul du montant à alimenter	ELGP	Erreur de calcul	1	2	2	1	2	2	4	Double contrôle du calcul	1	1.FA
T02	Risque d'erreur dans le chargement des billets dans les cassettes ou dans	ELGP	Erreur de chargement/saisie	2	3	2	1	3	3	9	Contrôle par weighing + double saisie	1	1.FA

	la saisie des données												
T03	Risque de mauvais positionnement des cassettes	ELGP	Mauvais positionnement	1	2	1	1	2	2	4	Check visuel + alarme	2	2.M
T05	Risque d'erreur de combinaison qui empêcherait la fermeture du coffre	ELGP	Erreur de combinaison	1	3	1	1	3	1	3	Limitation essais + procédure réinitialisation	2	1.FA
T06	Risque que la nouvelle alimentation ne soit pas correctement prise en compte.	ELGP	Non prise en compte alimentation	2	3	2	1	3	2	6	Message d'alerte discordance	1	1.FA
T07	Risque de non détection d'un problème de réapprovisionnement des billets	ELGP	Non détection problème réapprovisionnement	2	3	2	1	3	3	9	Capteurs de niveau + test après réapprovisionnement	2	2.M
T08	Risque de ne pas détecter un problème dans la partie supérieure du DAB (lecteur de carte, écran, etc).	ELGP	Non détection problème partie supérieure	2	4	3	2	4	2	8	Tests automatiques réguliers	2	2.M
T09	Risque de panne ou de dysfonctionnement à la remise en service	IADS	Panne/dysfonctionnement remise en service	3	4	3	2	4	2	8	Procédures strictes redémarrage et tests	1	1.FA
T10	Risque de procéder à la mise à disposition alors que le DAB n'est pas pleinement opérationnel	ELGP	Disponibilité non opérationnel	4	4	3	3	4	1	4	Interverrouillage logiciel	2	2.M

Source : Elaboré par nos soins

7. Acquisition DAB :

	Risques	**FR**	**Vulnérabilités**	**img**	**cont**	**fin**	**jur**	**IB**	**FRQ**	**CB**	**DMR**	**Cot°**	**RN**
T01	Mauvaise estimation des besoins réels en nombre de DAB et emplacements	ELGP	- Manque de données sur les clients et leurs besoins - Projections de croissance erronées	2	2	2	1	2	2	4	Étude approfondie des données clients et prospectives, consultation des agences, benchmarking	2	2.M
T02	Choix d'un mauvais emplacement	ELGP	- Méconnaissance du territoire - Données démographiques obsolètes	2	1	2	1	2	2	4	Étude de marché détaillée, consultation des agences locales	2	2.M
T02	Données de marché erronées	ELGP	- Méconnaissance du territoire - Données démographiques obsolètes	1	1	1	1	1	1	1	Vérification des sources, recoupement des données	2	1.FA
T03	Offre technique inadéquate	ELGP	- Appel d'offres mal défini - Critères de sélection inadéquats - Clauses contractuelles insuffisantes	2	2	3	1	3	2	6	Cahier des charges précis, grille d'évaluation détaillée	1	1.FA

T03	Surcoût	ELGP	- Appel d'offres mal défini - Critères de sélection inadéquats - Clauses contractuelles insuffisantes	1	1	3	1	3	3	9	Négociation des prix, marge dans le budget	2	2.M
T03	Retards de livraison	ELGP	- Appel d'offres mal défini - Critères de sélection inadéquats - Clauses contractuelles insuffisantes	2	2	2	1	2	3	6	Planning détaillé, pénalités de retard	2	2.M
T04	Mauvaise définition des responsabilités	ELGP	- Imprécisions juridiques - Absence de clauses d'adaptation	1	2	2	3	3	2	6	Revue juridique du contrat	1	1.FA
T04	Manque de flexibilité	ELGP	- Imprécisions juridiques - Absence de clauses d'adaptation	1	2	2	2	2	2	4	Clauses d'adaptation dans le contrat	1	1.FA
T05	Problèmes d'alimentation électrique ou réseau	IADS	- Installations vétustes - Sous-estimation des besoins en sécurité	3	4	2	1	4	1	4	Audit des installations, onduleurs	2	2.M
T05	sécurité insuffisante	PESLT	- Installations vétustes - Sous-estimation des besoins en sécurité	4	4	3	2	4	2	8	Etude de sûreté, systèmes de sécurité renforcés	1	1.FA
T06	Dysfonctionnements à la livraison	ELGP	- Procédures de réception inadéquates - Installateurs non qualifiés	3	4	2	1	4	2	8	Procédures de réception et tests	2	2.M
T07	Problèmes de connexion aux systèmes bancaires Mauvais paramétrage fonctionnel ou sécurité	IADS	Incompatibilités systèmes - Personnel insuffisamment formé	2	4	1	1	4	2	8	Tests d'intégration, équipe projet dédiée	2	2.M
T08	Ruptures de stock en espèces	ELGP	- Mauvaise estimation des besoins - Procédures mal définies	3	4	1	1	4	3	12	Niveaux de stocks minimaux, procédure d'approvisionnement	2	3.FO
T09	Compétences insuffisantes	PESLT	Recrutement inadéquat Formations incomplètes	2	3	2	1	3	2	6	Formation du personnel, supports d'aide	2	2.M
T10	Défaillances critiques non détectées avant mise en service	ELGP	- Périmètre de test limité - Tests non exhaustifs	2	3	1	1	3	3	9	Formalisation des procédures, audits	1	1.FA
T11	Mauvaise diffusion de l'information auprès des clients	CPPC	- Supports de communication inadéquats - Ciblage clients erroné	1	1	1	1	1	1	1	Plan de communication multic anal	1	1.FA
T12	Vieillissement prématuré	DAP	Maintenance préventive insuffisante - Pièces détachées non disponibles	2	2	3	1	3	3	9	Maintenance préventive, contrat de service avec fournisseur	1	1.FA

Source : Elaboré par nos soins

8. Maintenance DAB :

T	Risques	FR	Vulnérabilité	img	con	fin	jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Mauvais diagnostic de la panne	ELGP	- Compétences techniques insuffisantes - Outils de diagnostic inadaptés - Informations erronées du client	2	3	2	1	3	2	6	Formation du personnel, outils de diagnostics, double contrôle	2	2.M
T02	Mauvaise description du problème	ELGP	- Expression imprécise du problème - Incompréhension des termes techniques	1	2	1	1	2	3	6	Formulaire de déclaration standardisé	1	1.FA
T03	Analyse incorrecte de la panne	ELGP	- Raisonnement défaillant - Expérience insuffisante - Pressions extérieures	2	3	2	2	3	2	6	Méthode d'analyse formalisée, revue par les pairs	2	2.M
T04	Délais importants pour intervention sur site	ELGP	- Retard dans la prise de rendez-vous - Éloignement géographique - Indisponibilité des techniciens	2	3	1	1	3	3	9	Planification des interventions, astreintes techniciens	2	2.M
T05	Oubli de pièces détachées nécessaires	ELGP	- Préparation incomplète - Stocks insuffisants - Processus d'approvisionnement défaillant	2	3	2	1	3	3	9	Check-list, gestion des stocks, procédure d'approvisionnement	1	1.FA
T06	Mauvaises réparations	ELGP	- Compétences techniques lacunaires - Pressions temporelles - Outillage inadapté	3	4	3	2	4	2	8	Supervision, contrôle qualité, évaluation des compétences	2	2.M
T06	Détériorations supplémentaires	DAP	- Maladresse - Méconnaissance de l'équipement - Précipitation	3	4	3	2	4	2	8	Sensibilisation aux risques, équipements de protection	2	2.M
T07	Tests insuffisants, panne non totalement résolue	ELGP	- Critères de test mal définis - Négligence - Equipements de test indisponibles	2	3	2	1	3	2	6	Protocoles de tests détaillés, contrôle aléatoire	2	2.M
T08	Informations manquantes	ELGP	- Reporting déficient - Perte d'informations - Transmission défaillante entre équipes	1	2	1	1	2	3	6	Compte-rendu d'intervention standardisé, réunions de debriefing	1	1.FA
T08	Traçabilité insuffisante	ELGP	- Outils de suivi des interventions défaillants - Manque de rigueur - Procédures non respectées	1	2	1	1	2	3	6	Système de suivi des interventions, audits	1	1.FA
T09	Résolution non validée à tort	ELGP	- Critères de validation ambigus - Précipitation - Pression client	2	3	2	2	3	2	6	Procédure de validation en 2 étapes	1	1.FA
T10	Perte ou vol des pièces défectueuses	FE	- Traçabilité défaillante - Procédures de sécurité non respectées - Surveillance insuffisante	1	2	2	1	2	1	2	Traçabilité renforcée, gardiennage	1	1.FA

T11	Facturation erronée	ELGP	- Mauvaise saisie des interventions - Processus de facturation complexe - Vérifications absentes	1	1	2	1	2	2	4	Double contrôle facturation, rapprochement interventions	1	1.FA
T11	Litiges	CPPC	- Engagements contractuels mal définis - Désaccord sur les responsabilités - Preuves insuffisantes	2	2	2	3	3	1	3	Contrats clairs, archivage des preuves	1	1.FA
T12	Registres non mis à jour	ELGP	- Transmission des infos aux services support défaillante - Manque de rigueur - Outils inadaptés	1	2	1	1	2	3	6	Automatisation des mises à jour, sauvegardes	2	2.M
T12	Données historiques perdues	IADS	- Sauvegarde des données défaillante - Suppression accidentelle - Cyberattaque	1	3	2	1	3	1	3	Politique de sauvegarde, traçabilité papier	1	1.FA

Source : Elaboré par nos soins

9. Retrait DAB :

T	Risque	FR	**Vulnérabilité**	**img**	**cont**	**fin**	**jur**	IB	**FRQ**	CB	**DMR**	**Cot°**	RN
T01	copie de carte bancaire par un dispositif frauduleux sur le DAB/substitution de la vraie carte par une fausse	FE	Dispositif frauduleux sur le DAB	3	1	2	1	3	2	6	Détecteurs de fraude sur les DAB, contrôle régulier des DAB, carte à puce avec cryptage	2	2.M
T02	Risque d'espionnage du code PIN par une caméra cachée	FE	Caméra cachée	3	1	2	1	3	1	3	Protections physiques sur le clavier, détecteur de caméras	2	1.FA
	Risque de divulgation du code PIN par un tiers malintentionné	FE	Tiers malintentionné	2	1	3	2	3	2	6	Sensibilisation des clients, code PIN aléatoire	2	2.M
	Risque de divulgation du PIN si saisi sur un faux clavier	FE	Faux clavier	2	1	3	2	3	2	6	Sensibilisation des clients, code PIN aléatoire	2	2.M
	Attaque par phishing: un fraudeur pourrait envoyer un e-mail ou un SMS frauduleux à un client, lui demandant de saisir son code PIN	FE	E-mail ou SMS frauduleux demandant le code PIN	3	1	3	2	3	3	9	Filtration des emails et SMS, authentification forte	2	2.M
T04	Risque mineur d'erreur de saisie du montant.	ELGP	Interface de saisie	1	1	1	1	1	3	3	Confirmation du montant sur l'écran, possibilité d'annulation	1	1.FA
T06	Risque d'interception des	FE	Communication non	3	2	3	2	3	1	3	Cryptage des communications,	1	1.FA

	données bancaires		sécurisée								protocoles sécurisés		
T07	Risque d'interception des données bancaires	FE	Communication non sécurisée	3	2	3	2	3	1	3	Cryptage des communications, protocoles sécurisés	1	1.FA
T08	Erreur de vérification	ELGP	Dysfonctionnement système	2	2	2	1	2	2	4	Contrôles automatisés, supervision humaine	2	2.M
T09	erreur entraînant autorisation d'un retrait frauduleux	ELGP	Dysfonctionnement système	3	1	3	3	3	1	3	Système de détection des fraudes, vérifications	2	1.FA
T10	Risque d'interception des données bancaires	FE	Communication non sécurisée	3	2	3	2	3	1	3	Cryptage des communications, protocoles sécurisés	1	1.FA
T11	surcharge de la réserve ou erreurs de comptabilisation.	ELGP	Dysfonctionnement système	2	1	2	1	2	2	4	Rapprochements bancaires, contrôles	1	1.FA
T13	Risque de dysfonctionnement entraînant non-distribution de l'argent malgré débit	IADS	Dysfonctionnement distribution	2	2	1	1	2	2	4	Capteurs de billets, maintenance préventive	2	2.M
	Risque de délivrance incorrecte de billets ou de dysfonctionnement du DAB	IADS	Mécanique ou électronique	2	3	1	1	3	2	6	Monitoring en temps réel, maintenance préventive	2	2.M
T14	Risque de débit multiple pour un même retrait	ELGP	Dysfonctionnement système	2	1	3	2	3	1	3	Journalisation des transactions, rapprochements	1	1.FA
	Risque de débit supérieur au montant retiré	ELGP	Dysfonctionnement système	2	1	3	2	3	1	3	Journalisation et rapprochements	1	1.FA
T15	Risque de non restitution de la carte après le retrait	ELGP	Mécanique	1	1	1	1	1	2	2	Capteur de rétention, procédure de restitution	2	1.FA
	Risque de vol de la carte oubliée dans le DAB	FE	Négligence de l'utilisateur	1	1	2	1	2	4	8	Messages de rappel, désactivation automatique	1	1.FA
T16	Risque d'absence de preuve du retrait en cas de dysfonctionnement l'imprimante du DAB	IADS	Dysfonctionnement imprimante	2	1	2	2	2	2	4	Journalisation électronique, caméras	1	1.FA

Source : Elaboré par nos soins

10. Acquisition TPE :

T	**Risques**	**FR**	**Vulnérabilité**	**img**	**cont**	**fin**	**jur**	**IB**	**FRQ**	**CB**	**DMR**	**Cot°**	**RN**
T01	Mauvaise estimation du parc nécessaire	ELGP	- Données de marché erronées - Projections de croissance trop	2	2	3	1	3	3	9	Etude quantitative du marché, benchmark,	2	2.M

			optimistes										
T02	Exigences techniques trop faibles ou irréalistes	ELGP	- Méconnaissance des besoins métiers - Manque d'expertise technique interne	1	2	2	1	2	2	4	Consultation des métiers, prototypage, proof of concept	2	2.M
T03	Offres non conformes au cahier des charges	ELGP	- Rédaction ambigüe ou lacunaire - Critères d'évaluation mal définis	2	1	1	1	2	2	4	Grille d'analyse détaillée, critères d'évaluation objectifs	1	1.FA
T04	Mauvaise négociation des conditions commerciales	ELGP	- Compétences insuffisantes en négociation - Analyse financière erronée	1	1	3	1	3	2	6	Assistance juridique et financière, simulation de scénarios	2	2.M
T05	Fournisseur techniquement ou financièrement risqué	ELGP	- Due diligence incomplète - Critères de sélection des fournisseurs inadéquats	2	3	3	2	3	2	6	Audit approfondi, certification, références	1	1.FA
T06	Non respect des exigences par le fournisseur	ELGP	- Supervision insuffisante - Pénalités contractuelles absentes ou légères	2	2	2	2	2	2	4	Reporting régulier, test de conformité, pénalités	2	2.M
T07	Erreurs de configuration	ELGP	- Paramétrage complexe - Formations utilisateurs insuffisantes	1	2	1	1	2	3	6	Tests utilisateurs, formation du personnel IT	2	2.M
T07	Sécurité compromise	PESLT	- Tests de pénétration absents - Clés cryptographiques mal gérées	4	4	2	3	4	1	4	Tests d'intrusion, politique de sécurité stricte	1	1.FA
T08	Retards de livraison	ELGP	- Planning irréaliste - Suivi des livraisons défaillant	2	2	1	1	2	3	6	Planning détaillé, clause de pénalités	2	2.M
T08	Perte ou vol	FE	- Sécurité physique des locaux insuffisante - Traçabilité des actifs lacunaire	1	3	3	1	3	1	3	Traçabilité renforcée, sécurité physique	1	1.FA
T09	Mauvaise installation	ELGP	- Compétences techniques des installateurs - Procédures d'installation floues	2	3	2	1	3	2	6	Supervision du fournisseur, procédures strictes	2	2.M
T09	Dysfonctionnements	IADS	- Tests de charge insuffisants - Processus de support et maintenance léger	3	4	2	1	4	2	8	Tests de charge poussés, monitoring des incidents	2	2.M
T10	Personnel non qualifié pour utiliser les TPE	PESLT	- Formation utilisateurs insuffisante - Change management déficient	2	3	1	1	3	3	9	Formation utilisateurs obligatoire, supports d'aide	2	2.M
T11	Anomalies non détectées avant déploiement	ELGP	- Tests d'intégration limités - Recette fonctionnelle partielle	2	3	2	1	3	2	6	Batterie de tests complète, recette approfondie	1	1.FA
T12	Retards de déploiement chez les commerçants	ELGP	- Planning de déploiement irréaliste - Moyens logistiques sous-dimensionnés	2	2	1	1	2	3	6	Planning réaliste, équipes dédiées	2	2.M

Source : Elaboré par nos soins

11. Maintenance TPE :

T	Risque	FR	Vulnérabilité	img	cont	fin	jur	IB	FRQ	CB	DMR	Cot°	RN
T01	Dysfonctionnements non détectés	ELGP	- Monitoring défaillant - Tests fonctionnels insuffisants - Processus d'escalade des anomalies déficient	2	3	2	1	3	2	6	Monitoring automatisé, procédure d'escalade, tableaux de bord	2	2.M
T02	Mauvaise description du problème	ELGP	- Expression du client peu claire - Incompréhension du vocabulaire technique - Mauvaise retranscription	1	1	1	1	1	3	3	Formulaire de déclaration standardisé, guides utilisateurs	2	1.FA
T03	Diagnostic erroné de la panne	ELGP	- Compétences techniques limitées - Outils de diagnostic inadaptés - Informations erronées du client	2	3	2	1	3	2	6	Arbre de décision, outils de diagnostics, expertise terrain	2	2.M
T04	Codification incorrecte du problème	ELGP	- Mauvaise interprétation des symptômes - Référentiel de codification complexe - Formation insuffisante	1	2	1	1	2	2	4	Référentiel de codification clair, formation du personnel	1	1.FA
T05	Perte ou vol lors du transport	FE	- Sécurisation défaillante - Traçabilité des biens insuffisante - Véhicules ou locaux vulnérables	1	2	2	1	2	1	2	Traçabilité des biens, sécurisation des véhicules	1	1.FA
T06	Détérioration pendant le transport	DAP	- Conditionnement inadapté - Manipulation sans précaution - Véhicules inadaptés	2	3	2	1	3	2	6	Conditionnement renforcé, manipulation avec précaution	2	2.M
T07	Mauvaise réparation, panne non résolue	ELGP	- Compétences techniques limitées - Documentation constructeur manquante - Outils inadaptés	3	4	3	2	4	2	8	Supervision, documentation constructeur, outillage adapté	1	1.FA
T08	Tests insuffisants, dysfonctionnements résiduels	ELGP	- Protocoles de tests incomplets - Equipements de test insuffisants - Vérifications superficielles	2	3	2	1	3	2	6	Protocoles de tests détaillés, contrôle qualité	1	1.FA
T09	Informations manquantes ou erronées	ELGP	Compte-rendu d'intervention lacunaire - Communication défaillante entre techniciens - Traçabilité des opérations insuffisante	1	2	1	1	2	3	6	Compte-rendu d'intervention standardisé, réunions de debriefing	2	2.M
T10	Perte ou vol lors du transport	FE	Sécurisation - Traçabilité des biens- Véhicules ou locaux vulnérables	1	2	2	1	2	1	2	Traçabilité des biens, sécurisation des véhicules	2	1.FA
T11	Clôture prématurée avant validation	ELGP	- Procédure de clôture non respectée - Pressions pour accélérer le traitement - Critères de validation flous	2	3	1	2	3	2	6	Validation métier en 2 étapes, critères de validation clairs	1	1.FA
T12	Facturation erronée des interventions	ELGP	- Saisie incorrecte des opérations - Comptabilisation défaillante du temps passé - Vérification insuffisante	1	1	2	1	2	2	4	Circuit de validation de la facture, rapprochement interventions	1	1.FA

12. Paiement TPE :

T	Risque	FR	Vulnérabilités	Img	Cont	Fin	Jur	IB	FRQ	CB	DMR	Cot°	RN
T01	fraude sur le montant (saisie montant supérieur au montant réel)	FI	- Erreur de saisie du commerçant	2	2	3	2	3	2	6	TPE avec contrôle automatique- Formation du commerçant- Validation par le client	2	2.M
T01	saisie incorrecte du montant (montant erroné)	ELGP	- Erreur de saisie du commerçant	1	1	2	1	2	3	6	TPE avec contrôle automatique- Formation du commerçant- Validation par le client	2	2.M
T02	fraude par vol/contrefaçon de la carte	FI	- Carte volée/contrefaite	3	2	4	3	4	2	8	Vérification puce et code confidentiel- Lecture bande magnétique avec cryptogramme	1	1.FA
T02	fraude par non utilisation du lecteur de puce	FI	Non utilisation de la puce- Défectuosité du lecteur	2	2	3	2	3	2	6	- Obligation d'utiliser la puce- Contrôle technique régulier	2	2.M
T02	insertion de la carte dans TPE trafiqué	FI	Non utilisation de la puce- Défectuosité du lecteur	3	2	4	3	4	1	4	- Contrôle visuel du TPE- Fixation solide du TPE	2	2.M
T02	défectuosité du lecteur pouvant entraîner une mauvaise lecture de la carte	IADS	Non utilisation de la puce- Défectuosité du lecteur	1	2	2	1	2	3	6	- Contrôle et maintenance réguliers- TPE de secours	2	2.M
T04	skimming (les données de la carte sont interceptées par un tiers malveillant)	FI	Interception des données	3	2	4	3	4	3	12	lecteur de puce intégré et détrompeur- Surveillance du site	1	2.M
T05	interception du code confidentiel	FI	- Interception du code	3	2	4	3	4	2	8	Protection du clavier- Recommandation de cacher la saisie	2	2.M
T06	interception des données chiffrées	FI	- Interception des données chiffrées	2	2	3	2	3	2	6	TLS robuste- Rotation fréquente des certificats	1	1.FA
T07	erreur de la banque (en matière de vérification et autorisation)	ELGP	- Erreur de la banque	1	1	2	1	2	2	4	- Double contrôle du solde- Limite du montant autorisé	1	1.FA
T08	interception de l'autorisation (entre les différentes autorisations)	FI	Interception de l'autorisation- Défaillance réseau	2	2	3	2	3	2	6	- Transmission sécurisée de l'autorisation	1	1.FA
T08	défaillance du réseau lors de la transmission	IADS	Interception de l'autorisation- Défaillance réseau	1	2	2	1	2	3	6	Authentification mutuelle/- Redondance réseau- Mode dégradé	1	1.FA
T09	modification des informations de la transaction par un tiers	FI	Perte/vol du TPE- Panne du TPE	2	2	3	2	3	2	6	- Signature électronique- Journalisation sécurisée	2	2.M

	malveillant												
T09	perte/vol du TPE	FI	Perte/vol du TPE- Panne du TPE	1	2	2	1	2	2	4	- Sauvegarde externalisée des transactions- Déclaration et blocage du TPE	1	1.FA
T09	non enregistrement de la transaction par le TPE	IADS	Perte/vol du TPE- Panne du TPE	1	2	2	1	2	2	4	- TPE redondant- Procédure de secours papier	2	2.M
T10	fraude si l'écran du TPE est intercepté par un tiers malveillant	FI	Perte/vol du TPE- Panne du TPE	2	2	3	2	3	2	6	- TLS sur l'écran client- Floutage des données sensibles	2	2.M
T10	panne du TPE pouvant entraîner une mauvaise communication des résultats de l'autorisation.	IADS	- Panne du TPE	1	2	3	1	3	4	12	- Notification également sur l'écran client- Ticket de secours	2	3.FO
T11	non impression ou impression multiple de tickets	IADS	- Défaut d'impression	1	1	1	1	1	3	3	- Contrôle du fonctionnement- Détection des impressions multiples	2	1.FA
T12	oubli de la carte par le client.	ELGP	- Oubli par le client	1	1	1	1	1	4	4	- Rappel par le commerçant	2	2.M
T13	transmission erronée des transactions vers la banque	IADS	- Transmission erronée	1	2	2	1	2	2	4	contrôle de cohérence- Accusés de réception	3	2.M
T14	non débit/crédit	ELGP	Erreur de comptabilisation- Perte de données	2	2	3	2	3	1	3	- Journalisation sécurisée- Archivage à long terme	2	1.FA
T15	erreur ou de fraude non détectée sans rapprochement comptable	ELGP	Absence de rapprochement/	2	2	3	2	3	3	9	- Rapprochement obligatoire- Outils de détection de fraudes	2	2.M
T16	contestation abusive par le client ou le commerçant.	CPPC	- Contestations abusives	2	1	2	2	2	3	6	- Réconciliation des données- Gestion des réclamations	1	1.FA
T16	erreur de comptabilisation pouvant conduire à des divergences dans les relevés	ELGP	Erreurs de comptabilisation	1	1	2	1	2	2	4	- Traçabilité des transactions- Clause contractuelle	1	1.FA

Source : Elaboré par nos soins

SECTION 04 : MAÎTRISE DES RISQUES OPÉRATIONNELS ET RECOMMENDATIONS À SUIVRE

IV.1. Elaboration de la cartographie des risques :

1. Octroi et délivrance de la carte

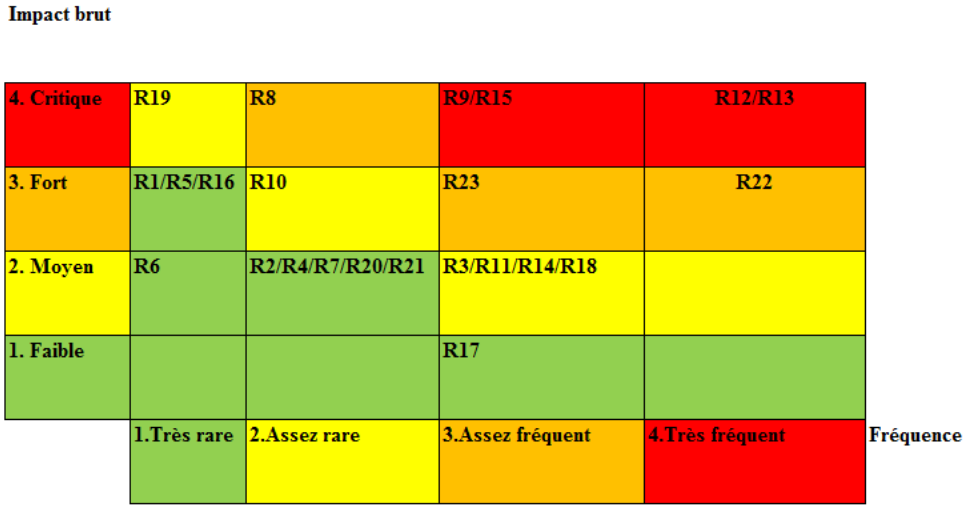
Tableau N°29 : Listing des risques liés au processus d'octroi et délivrance de la carte

risque	Attrib
fraude à l'identité si les justificatifs fournis sont falsifiés/usurpation d'identité	R1
non conformité si le contrat n'est pas correctement renseigné et signé	R2
erreur de saisie	R3
erreur ou omission dans le contrôle entraînant une non-conformité/validation d'une demande non conforme	R4
Risque de non prise en compte d'une commande/ réception d'un fichier de commandes erroné/	R5
erreur technique empêchant le traitement	R6
non réception de l'email/non réception de l'avis de disponibilité des cartes	R7
perte, vol carte/code	R8
perte, vol ou erreur de transmission	R9
non réception des cartes et des codes	R10
erreur de réconciliation avec la commande	R11
perte, vol ou divulgation non autorisée des codes confidentiels	R12
perte, vol ou divulgation non autorisée des cartes	R13
le client ne puisse être joint ou ne se présente pas/non information du client	R14
remise à un tiers non autorisé en l'absence de vérification d'identité	R15
divulgation non autorisée si le code est récupéré par un tiers	R16
non traçabilité en cas d'absence de signature du registre par le client	R17
erreur ou oubli de saisie	R18
activation non sécurisée/activation frauduleuse de la carte	R19
non activation et blocage du client	R20
non activation si relance non effectuée ou non traçable	R21
opposition non effectuée en temps voulu sur le SI	R22
non destruction effective de la carte.	R23

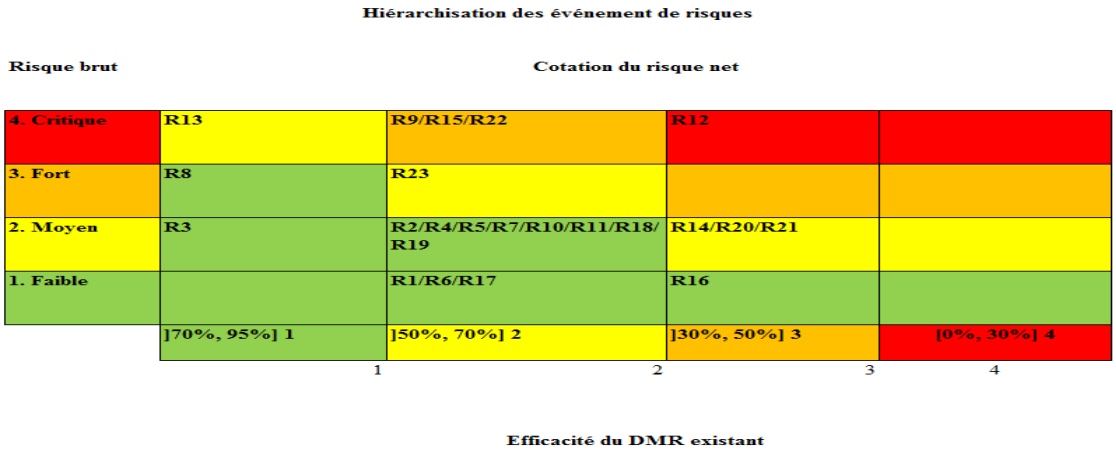
Source : Elaboré par nos soins

Figure N10° : Cartographie matricielle des risques liés au processus octroi et délivrance de la carte

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

<u>Interprétation des deux matrices de risque :</u>

La matrice brute évalue les risques bruts en fonction de deux critères :

- L'impact du risque sur une échelle de 1 (faible) à 4 (critique)
- La fréquence d'occurrence du risque sur une échelle de 1 (très rare) à 4 (très fréquent)

Nous pouvons voir que les risques ayant le plus fort impact brut sont situés en haut à droite de la matrice (R19, R8, R15, R12, R13).

La matrice nette hiérarchise les risques en tenant compte de l'efficacité des dispositifs de maîtrise des risques (DMR) existants. L'efficacité du DMR est notée de 1 (très efficace, réduction du risque brut de 70-100%) à 4 (peu efficace, réduction du risque brut de 0-30%).

Nous constatons que malgré les DMR en place, certains risques restent critique (R13) ou forts (R9, R15, R22). Les risques R12 et R8 passent de critique à moyen grâce à l'efficacité du DMR.

Ces matrices permettent donc d'identifier les risques prioritaires sur lesquels agir pour renforcer les dispositifs de maîtrise des risques. Les risques critiques et forts dans la matrice nette nécessitent une attention particulière.

2. Cartes capturées :

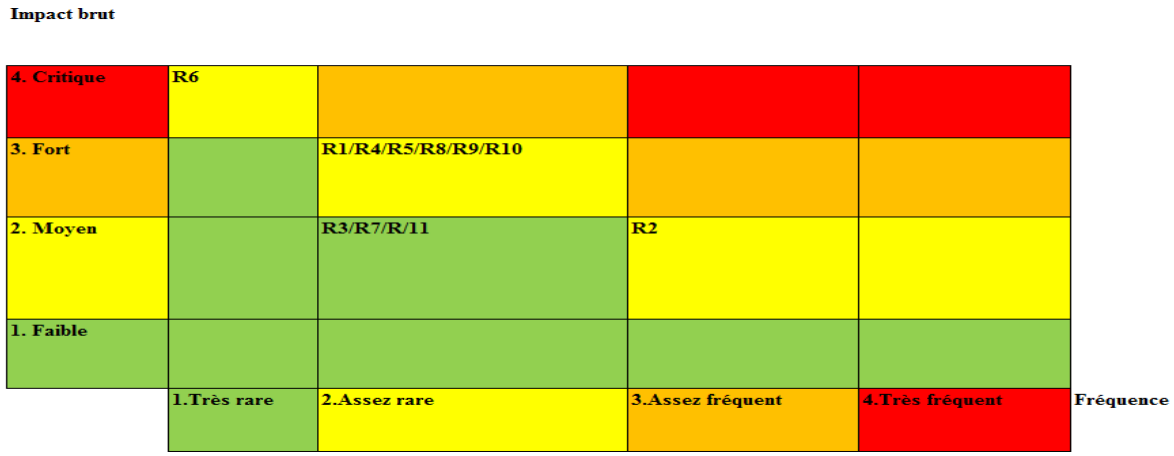
Tableau N° 30: Listing des risques liés au processus de gestion des cartes capturées

Risque	Attrib
Risque de dommage à la carte due à une manipulation incorrecte/ perte ou de vol de la carte lors du retrait de l'ATM	R1
Risque d'erreur humaine lors de la saisie des informations/ erreurs dans le remplissage des formulaires	R2
Risque de non transmission ou de transmission erronée des formulaires	R3
Risque d'omission d'informations importantes.	R4
Risque d'erreur dans le contrôle, ce qui pourrait influencer la décision finale.	R5
Risque de transmission non sécurisée lors de l'envoi au CMI.	R6
Risque de perte ou de manipulation frauduleuse du formulaire pendant le transfert.	R7
Risque d'analyse erronée des informations du formulaire	R8
Risque de négliger des éléments importants dans l'analyse.	R9
erreur dans la communication des conclusions	R10
Risque de non transmission ou transmission erronée/ incorrectes des conclusions au gestionnaire sur le droit à restitution	R11

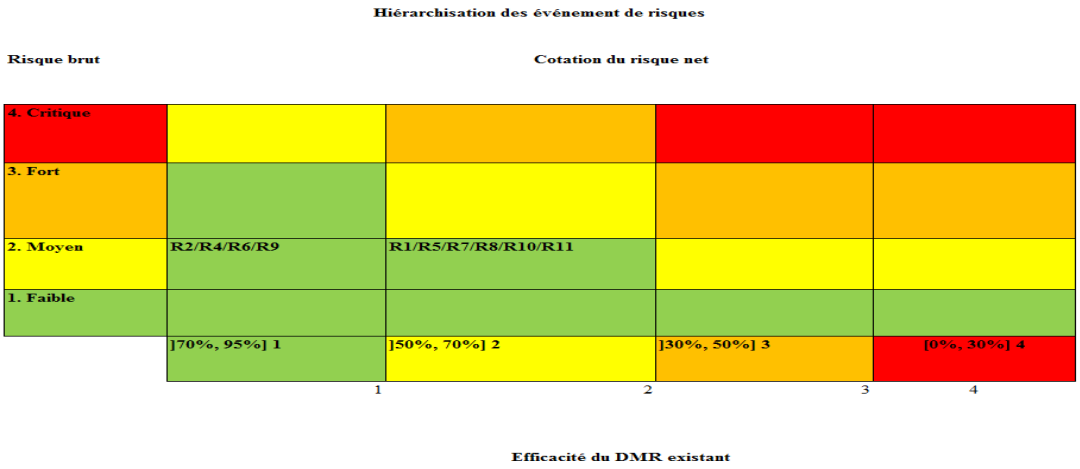
Source : Elaboré par nos soins

Figure N°11 : Cartographie matricielle des risques liés au processus de gestion des cartes capturées

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

Interprétation pour ces deux matrices :

Dans la matrice brute, les risques ayant le plus fort impact sont R6 (critique) et R1, R4, R5, R8, R9, R10 (fort). En termes de fréquence, la plupart des risques sont assez fréquents ou assez rares.

Dans la matrice nette, nous constatons que l'efficacité des DMR permet de faire passer tous les risques critiques et forts en risques moyens.

Les risques R2, R4, R6 et R9 restent toutefois des risques moyens malgré les DMR en place. Ces risques nécessitent donc une vigilance particulière et potentiellement un renforcement des DMR.

De manière générale, cette matrice nette est plus rassurante que la précédente, avec aucun risque classé critique ou fort après prise en compte des DMR. L'efficacité globale des DMR semble bonne pour ramener les risques bruts identifiés à un niveau moyen ou faible en net.

En conclusion, ces matrices permettent d'identifier les zones de risques prioritaires et l'impact des mesures mises en place. Elles constituent un outil d'aide à la décision pour orienter les plans d'actions visant à réduire les risques les plus importants.

3. Mise en opposition :

Tableau N°31 : Listing des risques liés au processus de gestion des mises en opposition

Risque	Attrib
Usurpation d'identité du client	R1
erreur d'identification du client	R2
mauvaise authentification de la signature	R3
Erreur humaine dans la saisie	R4
Perte/vol du bordereau	R5
Transmission à mauvais destinataire	R6
Non détection d'erreurs ou anomalies	R7
Validation d'opposition erronée	R8
Perte/corruption du fichier numérisé	R9
Erreur de validation	R10
Erreur dans la collecte ou le traitement des données provenant des différentes agences,	R11
Problème technique empêchant la récupération ou la consolidation des données des agences	R12
Fichier global corrompu ou illisible suite à un problème technique lors de la consolidation	R13
Perte de confidentialité des données lors de la transmission depuis les agences ou lors de la consolidation	R14
Erreur de transmission du fichier	R15
Retard dans l'émission des nouvelles cartes	R16

Source : Elaboré par nos soins

Figure N°12 : Cartographie matricielle des risques liés au processus de gestion des mises en opposition

Matrice brute :

Impact brut

4. Critique	R14				
3. Fort	R6/	R1/R8	R12		
2. Moyen	R9/R11	R5/R10/R13/R15	R2/R3/R7	R4	
1. Faible		R16			
	1.Très rare	2.Assez rare	3.Assez fréquent	4.Très fréquent	Fréquence

Matrice nette :

Hiérarchisation des événement de risques

Risque brut	Cotation du risque net			
4. Critique				
3. Fort		R4/R12		
2. Moyen	R1/R3/R8/R13/R14/15	R2/R5/R7/R10		
1. Faible	R6/R9/R11	R16		
	]70%, 95%] 1	]50%, 70%] 2	]30%, 50%] 3	[0%, 30%] 4
	1	2	3	4

Efficacité du DMR existant

Source : Elaboré par nos soins

<u>Interprétation pour ces matrices :</u>

Dans la matrice brute, le risque R14 est le seul classé critique. Les risques forts sont R6, R1, R8 et R12.

La fréquence de la plupart des risques est assez fréquente ou assez rare. Seul R16 semble très rare.

Dans la matrice nette, nous constatons que :

- R4 et R12 restent des risques forts malgré les DMR en place. Ils nécessitent des actions prioritaires.
- R1, R3, R8, R13, R14, R15 sont des risques moyens. Les DMR ont permis de réduire leur criticité mais ils méritent une vigilance soutenue.
- R6, R9, R11 et R16 sont désormais considérés comme faibles grâce à l'efficacité des DMR.

En conclusion, cette matrice nette montre que des efforts restent à faire pour maîtriser les risques R4 et R12 qui demeurent forts. Les autres risques semblent correctement couverts par

les DMR existants. L'analyse régulière de ces matrices permet d'orienter les plans d'actions sur les zones de risque prioritaires.

4. Modification des informations :

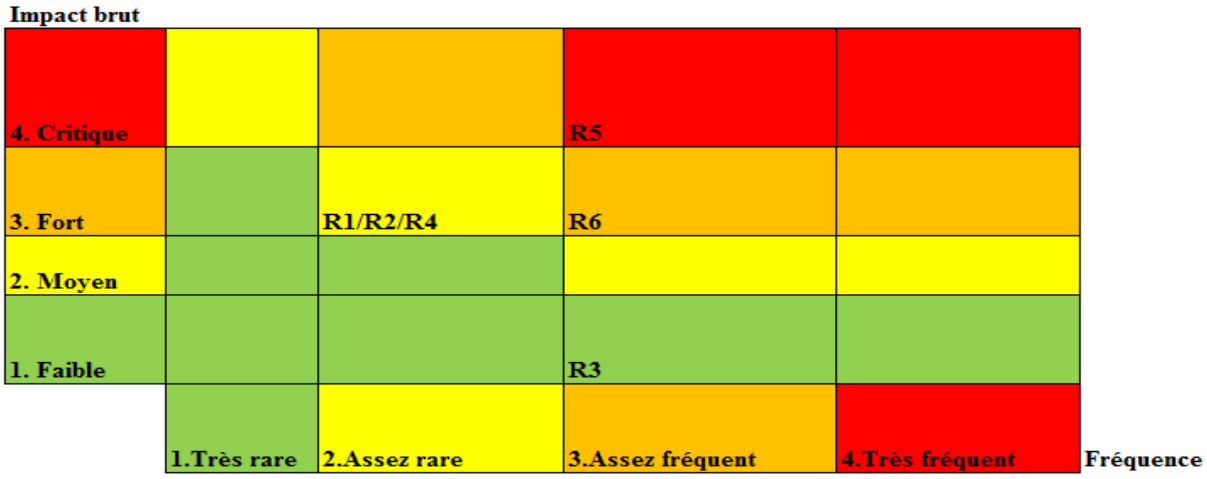
Tableau N°32 : Listing des risques liés au processus de modifications des plafonds

Risque	Attrib
Usurpation d'identité du client	R1
Falsification des documents justificatifs	R2
Erreur de saisie des informations	R3
Non authentification de la signature	R4
Non détection d'anomalies ou falsifications	R5
Validation erronée de la demande	R6

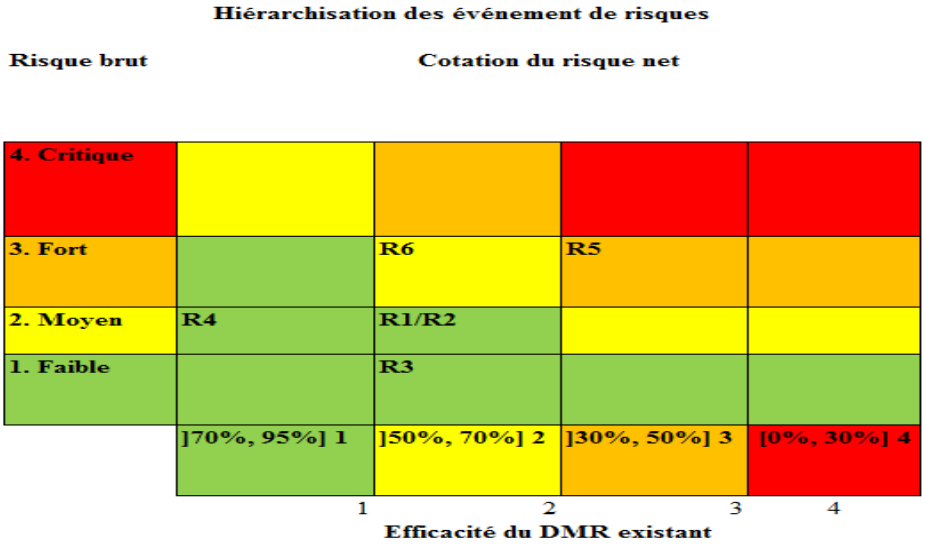
Source : Elaboré par nos soins

Figure N°13 : Cartographie matricielle des risques liés au processus de modifications des plafonds

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

Analyse des deux matrices :

Dans la matrice brute, le seul risque critique est le R5. Les risques forts sont R1, R2, R4 et R6.

La fréquence est majoritairement assez fréquente.

Dans la matrice nette, nous constatons que :

- Les risques R5 et R6 restent forts, les DMR sont insuffisants et doivent être renforcés.
- Le risque R4 passe de fort à moyen grâce au DMR mais nécessite une surveillance régulière.
- Les risques R1 et R2 passent de fort à moyen également grâce aux DMR.
- Le risque R3 passe de faible à très faible grâce à une DMR efficace.

En conclusion, cette matrice met en évidence des DMR globalement satisfaisantes mais des efforts sont nécessaires pour les risques R5 et R6 qui demeurent à un niveau fort. Le traitement de ces risques devra être prioritaire dans les plans d'actions.

5. Arrêté DAB :

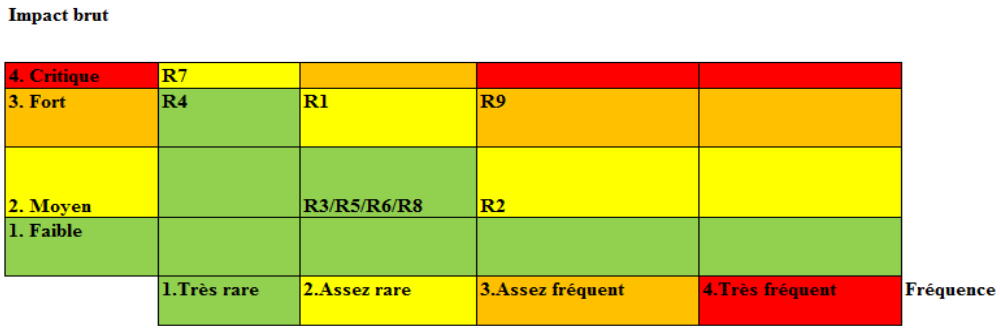
Tableau N°33 : Listing des risques liés au processus de l'arrêté de DAB

Risque	Attrib
panne ou indisponibilité du DAB pendant la maintenance	R1
Risque d'erreur humaine lors de l'arrêt qui pourrait causer un dysfonctionnement	R2
Risque d'erreur de saisie comptable	R3
Risque de vol d'argent lors du transport et de la manipulation	R4
Risque d'erreur de combinaison qui empêcherait l'ouverture du DAB	R5
écart entre le décompte physique et le solde théorique des billets dans les cassettes	R6
Risque de vol ou de malversation lors du déchargement et du décompte des billets et cassettes	R7
Risque d'erreur de saisie comptable du montant restant	R8
Risque de non détection d'éventuels écarts de caisse.	R9

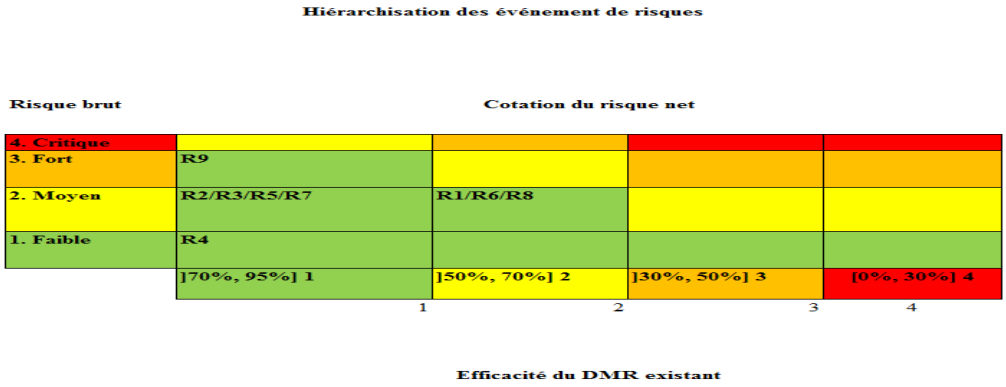
Source : Elaboré par nos soins

Figure N°14 : Cartographie matricielle des risques liés au processus d'arrêté DAB

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

Analyse pour ces matrices :

Dans la matrice brute, le risque R7 est le seul classé critique. Les risques forts sont R4, R1 et R9.

La fréquence est majoritairement assez fréquente ou assez rare.

Dans la matrice nette, on voit que :

- Le risque R9 reste fort malgré les mesures en place. Des actions prioritaires sont nécessaires pour ce risque.
- Les risques R2, R3, R5 et R7 passent de critique/fort à moyen grâce aux DMR. Une surveillance régulière reste nécessaire.
- R1, R6 et R8 sont désormais considérés comme faibles. Les DMR semblent efficaces sur ces risques.
- R4 passe même de fort à faible grâce à une DMR très efficace (réduction de 70-100% du risque brut).

En conclusion, cette matrice met en évidence l'efficacité globale des DMR à l'exception du risque R9 qui nécessite un traitement prioritaire pour le ramener à un niveau acceptable. L'analyse régulière de ces matrices permet d'orienter la gestion des risques.

6. Alimentation DAB :

Tableau N°34 : Listing des risques liés au processus d'alimentation DAB

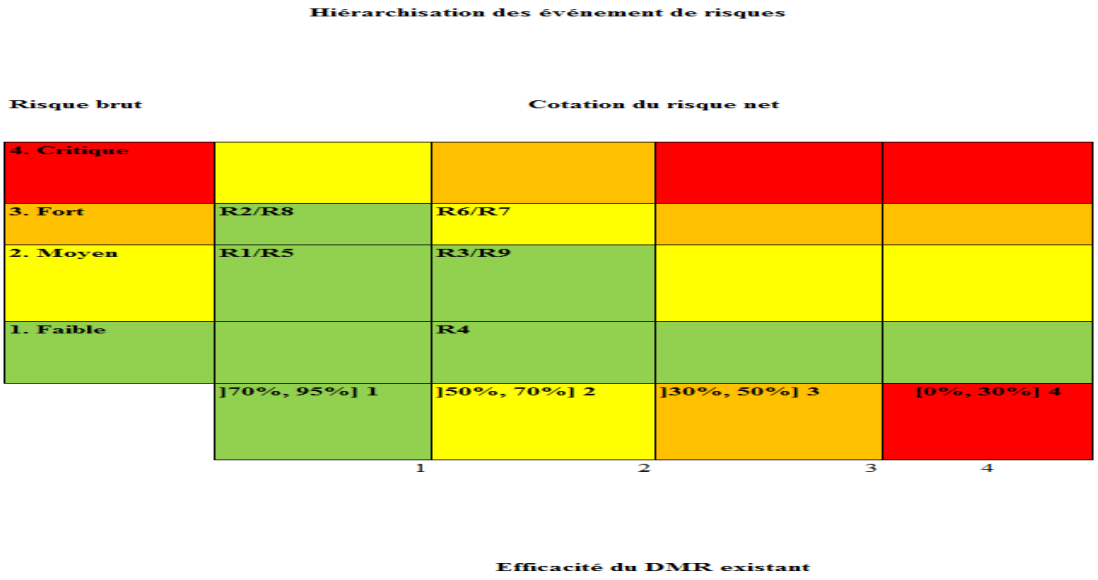
Risque	Attrib
Risque d'erreur dans le calcul du montant à alimenter	R1
Risque d'erreur dans le chargement des billets dans les cassettes ou dans la saisie des données	R2
Risque de mauvais positionnement des cassettes	R3
Risque d'erreur de combinaison qui empêcherait la fermeture du coffre	R4
Risque que la nouvelle alimentation ne soit pas correctement prise en compte.	R5
Risque de non détection d'un problème de réapprovisionnement des billets	R6
Risque de ne pas détecter un problème dans la partie supérieure du DAB (lecteur de carte, écran, etc).	R7
Risque de panne ou de dysfonctionnement à la remise en service	R8
Risque de procéder à la mise à disposition alors que le DAB n'est pas pleinement opérationnel	R9

Source : Elaboré par nos soins

Figure N°15 : Cartographie matricielle des risques liés au processus d'alimentation DAB

Matrice brute :

Matrice nette :



Source : Elaboré par nos soins

Analyse des matrices :

Dans la matrice brute, les risques critiques sont R9, R7 et R8. Les risques forts sont R4, R5 et R2/R6.

La fréquence est majoritairement assez fréquente pour la plupart des risques.

Dans la matrice nette, nous constatons que :

- R2, R8 et R7 restent des risques forts malgré les DMR en place. Ils nécessitent des actions prioritaires.
- R6 passe de fort à moyen grâce aux DMR. Une surveillance est nécessaire.
- R1, R3, R5 et R9 passent de critique/fort à moyen également grâce aux DMR.
- R4 passe de fort à faible grâce à une DMR très efficace.

En conclusion, cette matrice met en évidence que les risques R2, R7 et R8 demeurent préoccupants malgré les DMR. Des actions ciblées sont nécessaires pour renforcer leur maîtrise. Les autres risques semblent correctement gérés. L'analyse régulière de ces matrices guidera les plans d'actions de réduction des risques.

7. Acquisition DAB :

Tableau N°35 : Listing des risques liés au processus de l'acquisition DAB

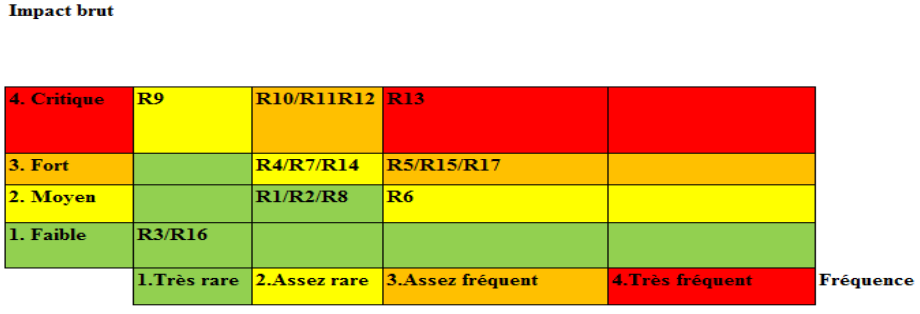
Risques	Attrib
Mauvaise estimation des besoins réels en nombre de DAB et emplacements	R1
Choix d'un mauvais emplacement	R2
Données de marché erronées	R3
Offre technique inadéquate	R4
Surcoût	R5
Retards de livraison	R6
Mauvaise définition des responsabilités	R7
Manque de flexibilité	R8
Problèmes d'alimentation électrique ou réseau	R9
sécurité insuffisante	R10
Dysfonctionnements à la livraison	R11
Problèmes de connexion aux systèmes bancaires Mauvais paramétrage fonctionnel ou sécurité	R12
Ruptures de stock en espèces	R13
Compétences insuffisantes	R14
Défaillances critiques non détectées avant mise en service	R15
Mauvaise diffusion de l'information auprès des clients	R16
Vieillissement prématuré	R17

Source : Elaboré par nos soins

Figure N°16 : Cartographie matricielle des risques liés au processus d'acquisition DAB

Matrice brute :

Matrice nette :



Hiérarchisation des événement de risques

Risque brut	Cotation du risque net			
4. Critique		R13		
3. Fort	R15/R17/R10	R5/R11/R12		
2. Moyen	R4/R7/R8	R1/R2/R6/R9/R14		
1. Faible	R16	R3		
	]70%, 95%] 1	]50%, 70%] 2	]30%, 50%] 3	[0%, 30%] 4
	1	2	3	4

Efficacité du DMR existant

Source : Elaboré par nos soins

<u>Analyse des deux matrices :</u>

Dans la matrice brute, les risques critiques sont R9 à R13. Les risques forts sont R4, R5, R7, R14, R15 et R17.

La fréquence est majoritairement assez fréquente ou fréquente.

Dans la matrice nette, on voit que :

- R13 reste critique malgré les DMR. Action prioritaire à mener.
- R10, R11, R12, R15 et R17 restent forts. Le DMR est insuffisant et doit être renforcé.
- R1, R2, R4, R6 à R9 et R14 passent de critique/fort à moyen grâce au DMR. Surveillance régulière.
- R3 et R16 passent à faible. DMR efficace.

En conclusion, cette matrice met en évidence des DMR globalement efficaces à l'exception des risques R10 à R13, R15 et R17 qui demeurent préoccupants. Le traitement de ces risques devra être prioritaire dans les plans d'actions afin de les ramener à un niveau acceptable. L'analyse régulière est importante pour ajuster les DMR.

8. Maintenance DAB :

Tableau N°36 : Listing des risques liés au processus de maintenance DAB

Risques	Attrib
Mauvais diagnostic de la panne	R1
Mauvaise description du problème	R2
Analyse incorrecte de la panne	R3
Délais importants pour intervention sur site	R4
Oubli de pièces détachées nécessaires	R5
Mauvaises réparations	R6
Détériorations supplémentaires	R7
Tests insuffisants, panne non totalement résolue	R8
Informations manquantes	R9
Traçabilité insuffisante	R10
Résolution non validée à tort	R11
Perte ou vol des pièces défectueuses	R12
Facturation erronée	R13
Litiges	R14
Registres non mis à jour	R15
Données historiques perdues	R16

Source : Elaboré par nos soins

Figure N°17 : Cartographie matricielle des risques liés au processus maintenance DAB :

Matrice brute

Impact brut

4. Critique		**R6/R7**			
3. Fort	**R14/R16**	**R1/R3/R8/R11**	**R4/R5**		
2. Moyen	**R12**	**R13**	**R2/R9/R10/R15**		
1. Faible					
	1.Très rare	**2.Assez rare**	**3.Assez fréquent**	**4.Très fréquent**	**Fréquence**

Matrice nette

Hiérarchisation des événement de risques

Risque brut **Cotation du risque net**

4. Critique				
3. Fort	**R5**	**R4/R6/R7**		
2. Moyen	**R2/R9/R10/R11/R13**	**R1/R3/R8/R15**		
1. Faible	**R12/R14/R16**			
	]70%, 95%] 1	**]50%, 70%] 2**	**]30%, 50%] 3**	**[0%, 30%] 4**

1 2 3 4

Efficacité du DMR existant

Source : Elaboré par nos soins

Analyse des deux matrices :

Dans la matrice brute, les risques critiques sont R6 et R7. Les risques forts sont R1, R3, R4, R5, R8, R11, R14 et R16.

La fréquence est majoritairement assez fréquente pour la plupart des risques.

Dans la matrice nette, nous constatons que:

- Le risque R5 reste fort, les mesures sont insuffisantes et doivent être renforcées.
- Les risques R4, R6 et R7 passent de critique/fort à moyen grâce aux DMR. Une surveillance régulière est nécessaire.
- Les risques R1, R3, R8, R15 passent de fort à moyen également grâce aux DMR.
- Les risques R2, R9, R10, R11 et R13 passent de moyen à faible grâce à une DMR efficace.
- Les risques R12, R14 et R16 passent directement de fort à faible.

En conclusion, cette matrice met en évidence l'efficacité globale des DMR, à l'exception du risque R5 qui doit être traité de manière prioritaire. L'analyse régulière permettra d'ajuster les plans d'actions sur les zones de risques nécessitant un meilleur traitement.

9. Retrait DAB :

Tableau N°37 : Listing des risques liés au processus de retrait DAB

Risque	Attrib
copie de carte bancaire par un dispositif frauduleux sur le DAB/substitution de la vraie carte par une fausse	R1
Risque d'espionnage du code PIN par une caméra cachée	R2
Risque de divulgation du code PIN par un tiers malintentionné	R3
Risque de divulgation du PIN si saisi sur un faux clavier	R4
Attaque par phishing: un fraudeur pourrait envoyer un e-mail ou un SMS frauduleux à un client, lui demandant de saisir son code PIN	R5
Risque mineur d'erreur de saisie du montant.	R6
Risque d'interception des données bancaires	R7
Risque d'interception des données bancaires	R8
Erreur de vérification	R9
erreur entraînant autorisation d'un retrait frauduleux	R10
Risque d'interception des données bancaires	R11
surcharge de la réserve ou erreurs de comptabilisation.	R12
Risque de dysfonctionnement entraînant non-distribution de l'argent malgré débit	R13
Risque de délivrance incorrecte de billets ou de dysfonctionnement du DAB	R14
Risque de débit multiple pour un même retrait	R15
Risque de débit supérieur au montant retiré	R16
Risque de non restitution de la carte après le retrait	R17
Risque de vol de la carte oubliée dans le DAB	R18
Risque d'absence de preuve du retrait en cas de dysfonctionnement l'imprimante du DAB	R19

Source : Elaboré par nos soins

Figure N°18: Cartographie matricielle des risques liés au processus Retrait DAB

Matrice brute :

Impact brut

4. Critique				
3. Fort	R1/R7/R8/R10/R11/R15/R16	R1/R3/R4/R14	R5	
2. Moyen		R9/R12/R13/R19		R18
1. Faible		R17	R6	
	1.Très rare	2.Assez rare	3.Assez fréquent	4.Très fréquent

Fréquence

Matrice nette :

Hiérarchisation des événement de risques

Risque brut	Cotation du risque net			
4. Critique				
3. Fort	R18	R5		
2. Moyen	R12/R19	R1/R3/R4/R9/R13/R14		
1. Faible	R6/R7/R8/R11/R15/R16	R2/R10/R17/R18		
	]70%, 95%] 1	]50%, 70%] 2	]30%, 50%] 3	[0%, 30%] 4
	1	2	3	4

Efficacité du DMR existant

Source : Elaboré par nos soins

Analyse des deux matrices :

Dans la matrice brute, les risques forts sont R1, R3, R4, R5, R7, R8, R10, R11, R14 à R16.

La fréquence est majoritairement assez fréquente ou assez rare.

Dans la matrice nette, nous constatons que :

- Le risque R18 reste fort, le DMR est insuffisant et doit être renforcé.
- Le risque R5 passe de fort à moyen grâce au DMR mais nécessite une surveillance.
- Les risques R1, R3, R4, R9, R12, R13, R14 passent de fort à moyen grâce aux DMR.
- Les risques R6, R7, R8, R10, R11, R15, R16 passent de fort à faible grâce à une DMR efficace.
- Les risques R2, R17 et R18 passent de moyen à faible également grâce aux DMR.

En conclusion, cette matrice met en évidence une DMR globalement efficace, à l'exception du risque R18 qui doit être traité de manière prioritaire pour le ramener à un niveau acceptable. L'analyse régulière permettra d'ajuster les plans d'actions.

10. Acquisition TPE:

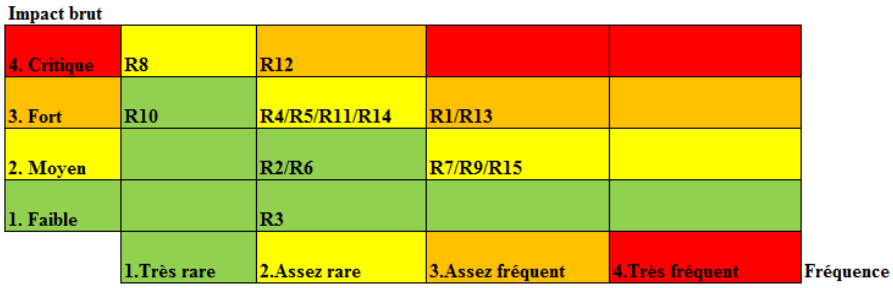
Tableau N°38 : Listing des risques liés au processus de l'acquisition TPE

Risques	attrib
Mauvaise estimation du parc nécessaire	R1
Exigences techniques trop faibles ou irréalistes	R2
Offres non conformes au cahier des charges	R3
Mauvaise négociation des conditions commerciales	R4
Fournisseur techniquement ou financièrement risqué	R5
Non respect des exigences par le fournisseur	R6
Erreurs de configuration	R7
Sécurité compromise	R8
Retards de livraison	R9
Perte ou vol	R10
Mauvaise installation	R11
Dysfonctionnements	R12
Personnel non qualifié pour utiliser les TPE	R13
Anomalies non détectées avant déploiement	R14
Retards de déploiement chez les commerçants	R15

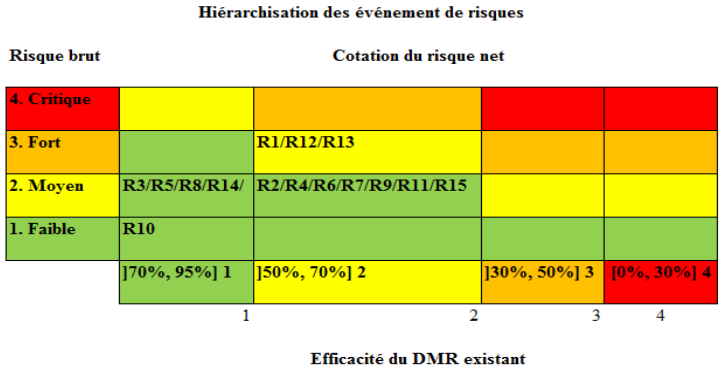
Source : Elaboré par nos soins

Figure N°19 : Cartographie matricielle des risques liés au processus d'acquisition TPE

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

<u>Analyse des deux matrices :</u>

Dans la matrice brute, les risques critiques sont R8 et R12. Les risques forts sont R1, R4, R5, R10, R11, R13 et R14.

La fréquence est majoritairement assez fréquente ou assez rare.

Dans la matrice nette, on voit que :

- Les risques R1, R12 et R13 restent forts, les DMR sont insuffisants et doivent être renforcés.
- Les risques R3, R5, R8 et R14 passent de critique/fort à moyen grâce aux DMR. Une surveillance régulière est nécessaire.
- Les risques R2, R4, R6, R7, R9, R11 et R15 passent de moyen/fort à faible grâce à une DMR efficace.
- Le risque R10 passe de fort à faible également grâce à une DMR très performante.

En conclusion, cette matrice met en évidence des DMR globalement satisfaisantes mais des efforts sont encore nécessaires pour les risques R1, R12 et R13 qui demeurent à un niveau fort. Le traitement de ces risques devra être prioritaire dans les plans d'actions.

11. Maintenance TPE :

Tableau N°39 : Listing des risques liés au processus de maintenance TPE

Risque	Attrib
Dysfonctionnements non détectés	R1
Mauvaise description du problème	R2
Diagnostic erroné de la panne	R3
Codification incorrecte du problème	R4
Perte ou vol lors du transport	R5
Détérioration pendant le transport	R6
Mauvaise réparation, panne non résolue	R7
Tests insuffisants, dysfonctionnements résiduels	R8
Informations manquantes ou erronées	R9
Perte ou vol lors du transport	R10
Clôture prématurée avant validation	R11
Facturation erronée des interventions	R12

Source : Elaboré par nos soins

Figure N° : Cartographie matricielle des risques liés au processus maintenance TPE

Matrice brute :

Impact brut				
4. Critique		R8		
3. Fort		R1/R3/R6/R11		
2. Moyen	R5/R10	R4/R12	R9	
1. Faible			R2	
	1.Très rare	2.Assez rare	3.Assez fréquent	4.Très fréquent

Fréquence

Matrice nette :

Hiérarchisation des événement de risques

Risque brut	Cotation du risque net			
4. Critique				
3. Fort	R1			
2. Moyen	R4/R8/R11/R12	R1/R3/R6/R9		
1. Faible	R5	R2/R10		
	]70%, 95%] 1	]50%, 70%] 2	]30%, 50%] 3	[0%, 30%] 4
		1	2	3 4

Efficacité du DMR existant

Source : Elaboré par nos soins

Analyse des deux matrices :

Dans la matrice brute, le seul risque critique est le R8. Les risques forts sont R1, R3, R6 et R11.

La fréquence est majoritairement assez fréquente ou assez rare.

Dans la matrice nette, nous constatons que :

- Le risque R1 reste fort, le DMR est insuffisant et doit être renforcé.
- Les risques R4, R8, R11 et R12 passent de critique/fort à moyen grâce aux DMR. Une surveillance régulière est nécessaire.
- Les risques R1, R3, R6 et R9 passent de fort à moyen également grâce aux DMR.
- Les risques R2, R5 et R10 passent de moyen à faible grâce à une DMR efficace.

En conclusion, cette matrice met en évidence une DMR globalement satisfaisante mais des efforts sont nécessaires pour le risque R1 qui doit être traité de manière prioritaire. L'analyse régulière permettra d'ajuster les plans d'actions sur les zones à risque.

12. Paiement TPE :

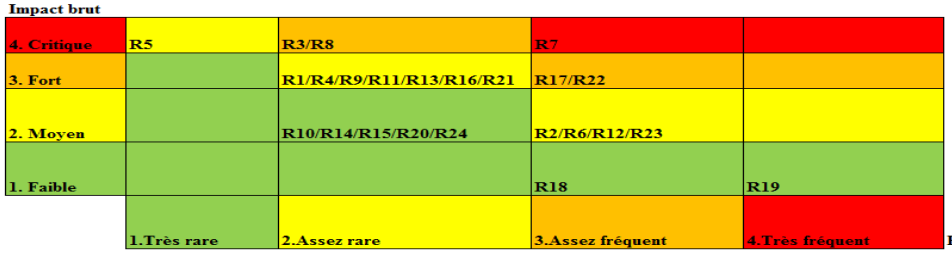
Tableau N°40 : Listing des risques liés au processus de paiement TPE

Risque	Attrib
fraude sur le montant (saisie montant supérieur au montant réel)	R1
saisie incorrecte du montant (montant érroné)	R2
fraude par vol/contrefaçon de la carte	R3
fraude par non utilisation du lecteur de puce	R4
insertion de la carte dans TPE trafiqué	R5
défectuosité du lecteur pouvant entraîner une mauvaise lecture de la carte	R6
skimming (les données de la carte sont interceptées par un tiers malveillant)	R7
interception du code confidentiel	R8
interception des données chiffrées	R9
erreur de la banque (en matière de vérification et autorisation)	R10
interception de l'autorisation (entre les différentes autorisations)	R11
défaillance du réseau lors de la transmission	R12
modification des informations de la transaction par un tiers malveillant	R13
perte/vol du TPE	R14
non enregistrement de la transaction par le TPE	R15
fraude si l'écran du TPE est intercepté par un tiers malveillant	R16
panne du TPE pouvant entraîner une mauvaise communication des résultats de l'autorisation.	R17
non impression ou impression multiple de tickets	R18
oubli de la carte par le client.	R19
transmission erronée des transactions vers la banque	R20
non débit/crédit	R21
erreur ou de fraude non détectée sans rapprochement comptable	R22
contestation abusive par le client ou le commerçant.	R23
erreur de comptabilisation pouvant conduire à des divergences dans les relevés	R24

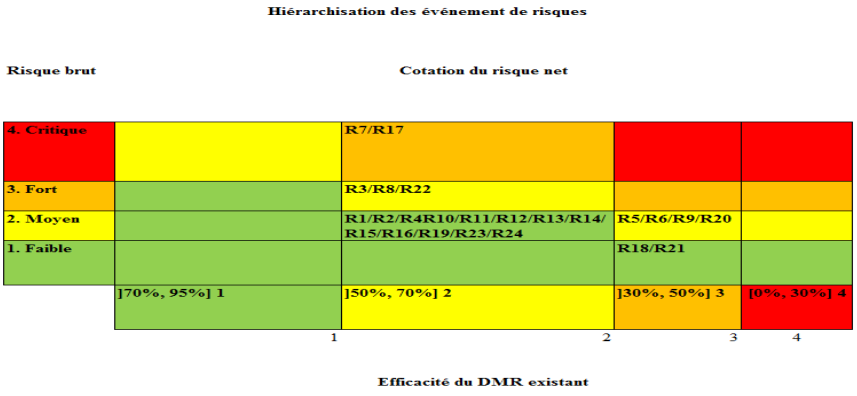
Source : Elaboré par nos soins

Figure N° 20: Cartographie matricielle des risques liés au processus paiement TPE

Matrice brute



Matrice nette :



Source : Elaboré par nos soins

Analyse des deux matrices :

Dans la matrice brute, les risques critiques sont R3, R5, R7 et R8. Les risques forts sont R1, R4, R9, R11, R13, R16, R17, R21 et R22.

La fréquence est majoritairement assez fréquente ou assez rare.

Dans la matrice nette, nous constatons que :

- Les risques R7 et R17 restent critiques, les DMR sont insuffisants et doivent être renforcés en priorité.
- Les risques R3, R8, R22 et R23 restent forts, les DMR doivent également être améliorés.
- Les risques R1, R2, R4 à R6, R9 à R16, R19 et R20 passent à un niveau moyen grâce aux DMR. Une surveillance régulière est nécessaire.
- Les risques R18 et R21 passent à un niveau faible grâce à une DMR efficace.

En conclusion, cette matrice met en évidence des DMR insuffisantes pour maîtriser les risques critiques R7 et R17, ainsi que les risques forts R3, R8, R22 et R23. Le traitement de ces risques devra être une priorité dans les plans d'actions.

i. Analyse des risques par familles de risques :

Ce tableau présente une analyse des risques opérationnels par famille de risques, réalisée sur un échantillon de 181 événements. Pour chaque famille de risques, identifiée par une abréviation, sont indiqués : le nombre d'occurrence dans l'échantillon, le pourcentage d'occurrence, les moyennes de criticité brute, de fréquence, d'impact brut, de cotation DMR (dispositif de maîtrise des risques), de criticité nette et de risque net.

Cette analyse permet d'identifier les principales familles de risques opérationnels auxquelles l'entreprise est exposée. Nous constatons notamment que la famille ELGP représente près de 60% des occurrences avec 108 événements. Les moyennes de criticité et de risque net sont également plus élevées pour ELGP.

Ce tableau donnera lieu à une analyse détaillée des risques par famille, afin de mettre en place des plans d'action pour réduire l'exposition aux risques opérationnels les plus critiques. Les résultats statistiques fournissent un état des lieux précis des risques et permettent de prioriser les actions.

Tableau N°41 : Analyse des risques par familles de risques

Abrév° famille	nbr d'occurrence	%	Moyenne Impact Brut	FRQ	Moyenne Criticité brute	Moyenne Risque brut	Moyenne cotation DMR	Moyenne criticité nette	Risque Net
CPPC	7	3.867%	2.42	2	5	1.857	1.857	3.571	1.428
DAP	5	2.762%	3.4	2.60	9	2.8	1.6	4.2	1.8
ELGP	108	59.669%	2.490	2.287	5.611	2.083	1.639	3.444	1.490
FE	28	15.470%	2.928	1.821	5.428	1.928	1.555	3.107	1.5
FI	8	4.420%	3.5	1.500	5	2	1.571	3.25	1.5
IADS	21	11.602%	2.761	2.047	5.380	2.142	1.6	3.571	1.571
PESLT	4	2.210%	3.5	2	6.75	2.5	1.591	3.75	1.5
	181	1							
MAX	108	59.67%	3.5	2.6	9	2.8	1.857	4.2	1.8

Source : Elaboré par nos soins

<u>Analyse par famille de risque :</u>

- La famille la plus représentée est de loin "Exécution, livraison et gestion des processus" (ELGP) avec 59,7% des occurrences. Cela s'explique par le caractère transverse et critique de l'exécution et la gestion des processus dans une organisation. Elle a une criticité brute moyenne de 2,08 traduisant des risques modérés mais son occurrence élevée en fait le premier contributeur au risque global (risque brut de 1,64). Les DMR permettent de réduire sa criticité à 1,49. Des efforts supplémentaires sur les contrôles et la surveillance des processus pourraient permettre d'abaisser davantage le niveau de risque.
- La deuxième famille est "Fraude externe" (FE) concentre des risques importants avec 15,5% des cas et une criticité de 1,93, impactée par une fréquence élevée. C'est la 3ème contributrice au risque brut. Les DMR minorent la criticité à 1,5 mais des efforts complémentaires semblent nécessaires. Les mesures de sécurité physiques, contrôles d'accès et surveillance sont à renforcer pour mieux maîtriser ces risques. Même après DMR, la criticité nette reste à 1,5, soulignant la difficulté à éliminer totalement les fraudes externes.
- "Interruptions d'activité et dysfonctionnements système" (IADS) représente 11,6% des cas avec une criticité de 2,14 liée à un impact et une fréquence importants. Des efforts sont nécessaires sur la résilience des systèmes, la reprise d'activité et la gestion de crise. Les DMR font baisser la criticité à 1,57 mais des tests réguliers des plans de continuité sont souhaitables.
- "Fraude interne" (4,4% des cas) et "Dommages aux actifs" (2,8%) ont des criticités brutes proches de 2,5. Pour DAP, l'impact est très élevé (9 en moyenne) compensé par une faible

fréquence. Sur FI, fréquence et impact sont plus équilibrés. Les DMR permettent de diviser par 2 la criticité sur ces 2 familles, démontrant leur efficacité. Les DMR réduisent efficacement les criticités.

- "Pratiques emploi et sécurité" (PESLT) et "Clients, produits..." (CPPC) sont peu fréquentes mais avec des criticités brutes élevées, nécessitant des actions préventives.

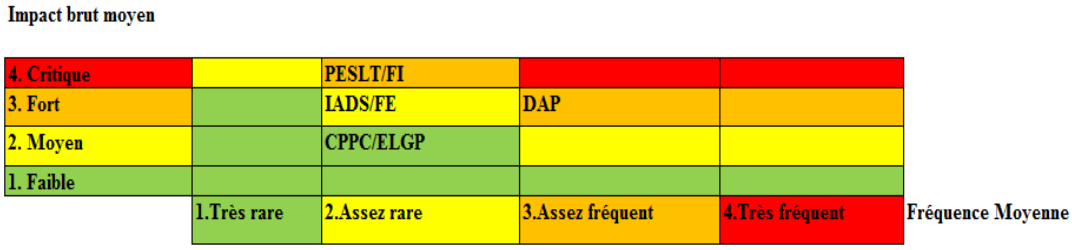
- Les familles FI et FE restent les plus sensibles malgré les DMR, nécessitant une vigilance soutenue.

- Après application des dispositifs de maîtrise des risques (DMR), la criticité nette baisse pour toutes les familles, montrant leur efficacité. Les DMR réduisent en moyenne la criticité de 37%.

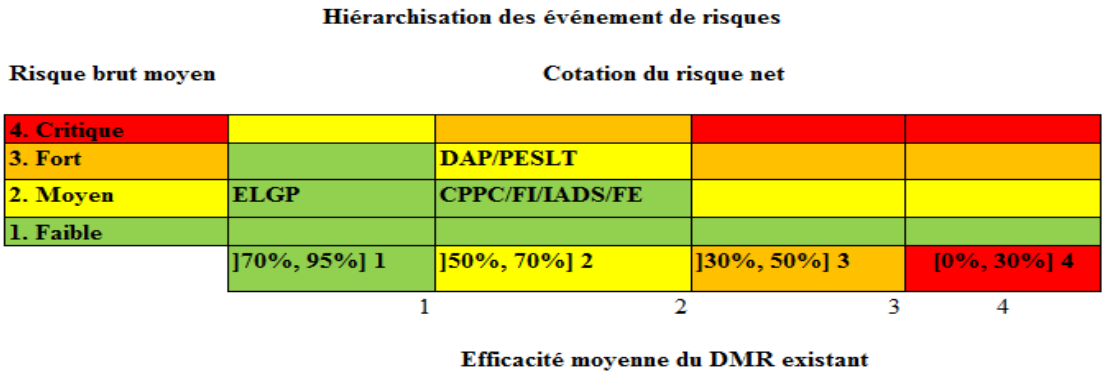
En conclusion, cette analyse montre l'importance du suivi fin des familles de risques pour adapter les plans d'action, même sur des familles peu fréquentes mais à criticité brute élevée.

Figure N°21 : Cartographie matricielle lié à la Distribution des familles des familles de risques :

Matrice brute :



Matrice nette :



Source : Elaboré par nos soins

<u>Interprétation des deux matrices :</u>

Sur la matrice brute, nous constatons que :

- Les risques les plus critiques (impact critique, fréquence assez fréquente) sont dans les familles PESLT et FI. Ces risques nécessitent une attention urgente.
- Les familles IADS, FE et DAP présentent des risques forts (impact fort, fréquence assez rare à assez fréquente). Des actions sont requises pour les maîtriser.
- Les familles CPPC et ELGP ont des criticités moyennes (impact moyen, fréquences assez rares). Une surveillance régulière est nécessaire.

Sur la matrice nette :

- Les familles DAP et PESLT restent parmi les plus critiques malgré les DMR, indiquant un besoin de renforcer ces derniers.
- Les familles ELGP, CPPC, FI, IADS et FE ont une criticité nette moyenne. Les DMR ont eu un effet positif sur ces risques.
- L'efficacité moyenne des DMR existants se situe entre 50 et 70%. Des marges de progression existent pour améliorer la maîtrise des risques.

En conclusion, cette analyse croisée des matrices brute et nette permet d'évaluer l'efficacité des DMR en place et d'identifier les familles nécessitant un renforcement prioritaire des actions de traitement des risques.

ii. <u>Analyse des risques par sous processus :</u>

Ce tableau détaille l'analyse des risques opérationnels par sous-processus pour le processus de gestion des cartes et des moyens de paiement. Pour chaque sous-processus sont indiqués : le code, les moyennes d'impact brut, de fréquence, de criticité brute, de risque brut, la cotation du dispositif de maîtrise des risques (DMR), la criticité nette et le risque net.

Cette analyse granulaire par sous-processus permet d'identifier les points de risques majeurs au sein du processus global. Nous constatons par exemple que le sous-processus "non présentation du client" a les moyennes de criticité et de risque bruts les plus élevées.

L'objectif de ce tableau est donc de prioriser les actions à mener par sous-processus, en ciblant en premier lieu ceux ayant les niveaux de risque résiduel les plus importants, malgré la cotation du DMR. Cette démarche vise à réduire les risques opérationnels de manière optimale sur l'ensemble de la chaîne de processus.

Tableau N° 42: Analyse des risques par sous processus

Les sous processus	Code sous processus	Moyenne Impact brut	Moyenne FRQ	Moyenne criticité Brute	Moyenne Risque Brut	Cotation DMR	criticité Nette	Risque Net	Réf SP
Emission de la carte	P01-SP01	2.846	2.385	7.154	2.385	1.846	4.385	1.500	R.SP1
Remise et activation de la carte	P01-SP02	2.571	2.286	5.429	2.000	2.429	4.714	1.571	R.SP2
Non présentation du client	P01-SP03	2.667	3.000	8.333	3.000	2.333	6.667	2.333	R.SP3
Cartes capturées	P02-SP01	2.375	2.063	4.750	1.875	1.438	2.813	1.375	R.SP4
Mise en opposition des cartes	P02-SP02	2.727	2.000	5.273	2.000	1.636	3.273	1.636	R.SP5
Modification des plafonds	P02-SP03	2.833	2.500	7.000	2.167	2.000	4.500	1.833	R.SP6
Arrêté DAB	P03-SP01	2.692	1.846	4.615	2.000	1.308	2.615	1.308	R.SP7
Alimentation DAB	P03-SP02	3.111	2.000	6.111	2.333	1.556	3.556	1.444	R.SP8
Acquisition DAB	P03-SP03	2.824	2.118	6.176	2.353	1.588	3.765	1.588	R.SP9
Maintenance DAB	P03-SP04	2.750	2.188	5.875	2.063	1.438	3.125	1.438	R.SP10
Retrait DAB	P03-SP05	2.526	1.842	4.368	1.632	1.526	2.579	1.368	R.SP11
Paiement TPE	P04-SP01	2.625	2.375	5.958	2.208	1.667	3.625	1.625	R.SP12
Acquisition TPE	P04-SP02	2.733	2.200	5.800	2.133	1.667	3.667	1.667	R.SP13
Maintenance TPE	P04-SP03	2.500	2.000	4.917	1.833	1.500	2.667	1.333	R.SP14
MAX		3.111	3.000	8.333	3.000	2.429	6.667	2.333	

Source : Elaboré par nos soins

Analyse des données par sous-processus :

- Le sous-processus avec la criticité brute moyenne la plus élevée est P03-SP02 (alimentation DAB) avec 3,11. Il présente également la fréquence et l'impact bruts les plus importants (6,11 et 2). Les procédures strictes d'alimentation sont essentielles pour éviter les pertes ou vols. Une rotation du personnel pourrait renforcer la sécurité.

- Viennent ensuite P03-SP03 (acquisition DAB) avec une criticité de 2,82 et P01-SP03 (Non présentation client) à 2,67.

- P01-SP03 (non présentation client) a également une criticité brute importante de 2,67. L'impact est majeur (3) en cas de fraude sur une carte non récupérée. Les relances clients sont un DMR essentiel mais pas toujours suffisant. Des blocages préventifs des cartes non retirées pourraient être envisagés.

- Les sous-processus P02-SP02 (Mise en opposition de carte), P03-SP04 (Maintenance DAB) et P04-SP01 (Paiement par TPE) ont des criticités brutes moyennes entre 2,5 et 2,7.

- La majorité des sous-processus (8) ont une criticité brute entre 2 et 2,5, traduisant des risques modérés.

- P02-SP02 (opposition de carte) a une criticité de 2,73 du fait des impacts en cas d'opposition frauduleuse ou erronée. La vérification systématique des demandes et la traçabilité constituent des DMR importants.

- Seul P03-SP01 (Arrêt DAB) présente une criticité inférieure à 2 (1,92), synonyme de risques faibles.

- L'application des DMR permet de réduire la criticité de 1,2 point en moyenne. P03-SP02 et P01-SP03 restent néanmoins les sous-processus les plus critiques après traitement.

- Le risque net le plus élevé est également constaté pour P03-SP02 et P01-SP03, du fait de leur criticité nette et de leur occurrence plus élevées.

- Les sous-processus P04-SP01, P03-SP04 et P02-SP03 ont des profils de risques relativement proches en termes d'impact et de fréquence. Des efforts similaires de maîtrise des risques sont à prévoir.

- P03-SP01 (arrêt DAB) présente les risques les plus faibles grâce aux procédures strictes d'arrêt et de contrôle des automates. Néanmoins, la vigilance reste de mise lors des manipulations de fonds.

En conclusion, cette analyse détaillée par sous-processus permet d'identifier les points de vigilance et de cibler les plans d'action pour renforcer la maîtrise des risques.

Figure N° 22: Cartographie matricielle des risques à chaque sous processus
Matrice brute

Impact brut moyen					
4. Critique					
3. Fort		R.SP1/R.SP2/R.SP5/R.SP7/R.SP8/R.SP9/R.SP10/R.SP11/R.SP12/R.SP13/R.SP	R.SP3/R.SP6		
2. Moyen		R.SP4			
1. Faible					
	1.Très rare	2.Assez rare	3.Assez fréquent	4.Très fréquent	Fréquence Moyenne

Matrice nette :

Hiérarchisation des événement de risques

Risque brut moyen	Cotation du risque net			
4. Critique				
3. Fort		R.SP3		
2. Moyen	R.SP4/R.SP7/R.SP10	R.SP1/R.SP2/R.SP5/R.SP6/R.SP8/R.SP9/R.SP11/R.SP12/R.SP13/14		
1. Faible				
	]70%, 95%] 1	]50%, 70%] 2	]30%, 50%] 3	[0%, 30%] 4

1 2 3 4

Efficacité moyenne du DMR existant

Source : Elaboré par nos soins

Interprétation des deux matrices :

Sur la matrice brute :

- Les sous-processus SP1, SP2, SP5, SP7, SP8, SP9, SP10, SP11, SP12, SP13 et SP14 (retrait DAB, acquisition DAB, paiement TPE, etc.) ont une criticité forte.

- Les sous-processus SP3 et SP6 (alimentation DAB, mise en opposition des cartes) ont une criticité moyenne.

- Le sous-processus SP4 (arrêt DAB) a une criticité plus faible.

Sur la matrice nette :

- Le sous-processus SP3 (alimentation DAB) conserve une criticité résiduelle forte, nécessitant un renforcement des contrôles lors de la manipulation des espèces.

- Les sous-processus SP4 (arrêt DAB), SP7 (acquisition DAB) et SP10 (paiement TPE) passent à une criticité moyenne grâce aux DMR. La vigilance doit être maintenue.

- Les autres sous-processus voient leur criticité réduite à un niveau faible après application des DMR, montrant leur efficacité.

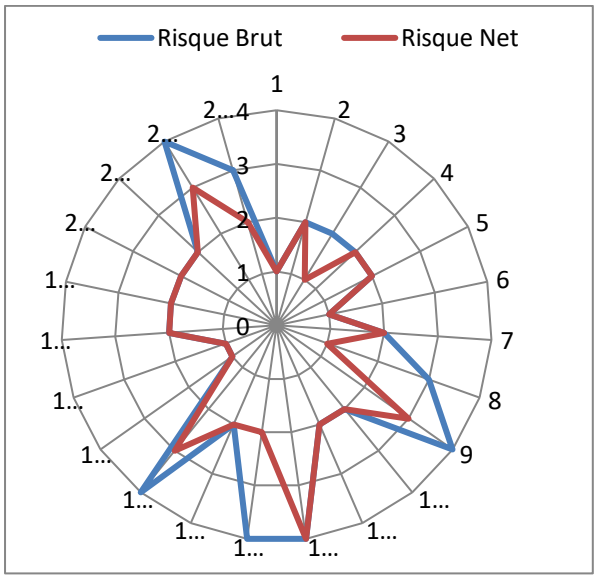
- L'efficacité moyenne des DMR est de 50-70%. Des améliorations peuvent être apportées.

En conclusion, croiser les matrices avant/après DMR avec les sous-processus permet d'identifier les points précis à traiter en priorité pour renforcer la maîtrise des risques.

iii. Analyse par risque brut et risque net : Vérification de l'efficacité du DMR :

1. Octroi et délivrance de la carte :

Figure N°23 : Représentation Radar des risques liés au processus Octroi et délivrance de la carte



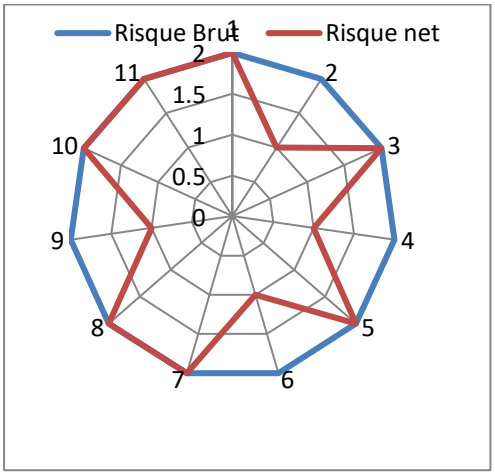
Source : Elaboré par nos soins

- On retrouve sur les axes du graphique 23 risques évalués selon leur criticité brute et leur criticité nette (après prise en compte des contrôles).
- Les risques sont hiérarchisés par criticité décroissante dans le sens des aiguilles d'une montre.
- Les risques R12, R15, R21 et R22 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R1, R16 et R17 apparaissent comme les moins critiques avec les scores les plus faibles.

- Certains risques voient leur criticité nette fortement réduite grâce aux contrôles en place : c'est le cas par exemple du R9.
- À l'inverse, d'autres risques conservent une criticité nette élevée malgré les contrôles comme le R12, le R21 et le R22. Il faut renforcer la maîtrise de ces risques.
-Globalement la plupart des risques se situent dans la zone de criticité modérée. Il faudra surveiller leur évolution.
- Ce graphique permet d'avoir une vue d'ensemble et comparée de la criticité des risques pour définir les priorités d'actions.

2. cartes capturées :

Figure N° 24: Représentation Radar des risques liés au processus gestion des cartes capturées

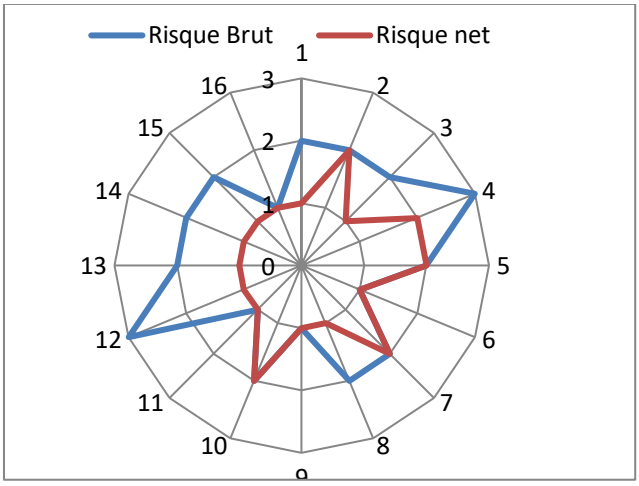


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et la criticité nette de 11 risques représentés sur les axes.
- Les risques sont hiérarchisés par criticité décroissante dans le sens des aiguilles d'une montre.
- Nous constatons que la majorité des risques (R1 à R8) voient leur criticité nette diminuer par rapport à la criticité brute, grâce à l'efficacité des contrôles.
- Seuls les risques R9, R10 et R11 conservent la même criticité nette. Les contrôles en place sur ces risques sont peu efficaces ou inexistants.
- Les risques R1, R6, R7 et R8 sont considérés comme prioritaires en criticité brute, mais ils passent en criticité modérée après prise en compte des contrôles.
- Les risques R9, R10 et R11 ressortent comme les plus critiques en net : ce sont les risques sur lesquels il faut agir en priorité pour renforcer les dispositifs de maîtrise.
-Globalement, cette cartographie montre que les contrôles permettent de réduire efficacement la criticité de la majorité des risques. Seuls quelques risques nécessitent le déploiement de plans d'actions pour les maîtriser davantage.

3. Mise en opposition

Figure N°25: Représentation Radar des risques liés au processus gestion des mises en oppositions

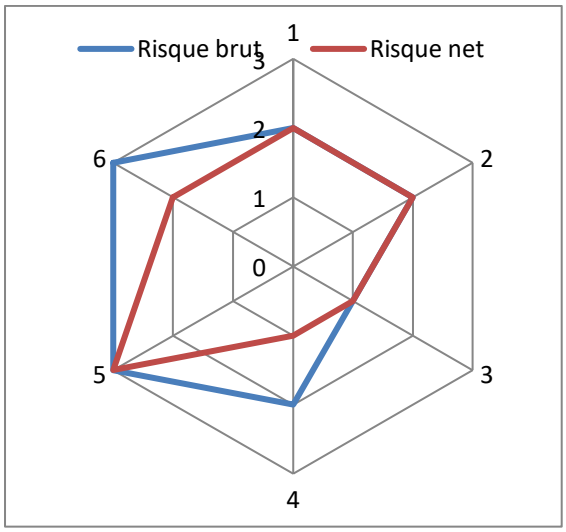


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 16 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- Nous constatons que la plupart des risques voient leur criticité diminuer après prise en compte des contrôles en place.
- Seuls les risques R2, R7 et R10 conservent une criticité nette identique à la criticité brute. Les dispositifs de maîtrise sont inefficaces pour ces risques.
- Les risques R4 et R12 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R15 et R16 apparaissent comme les moins critiques avec les scores les plus faibles.
- Certains risques ont une forte réduction de leur criticité grâce aux contrôles, comme R3, R11 et R13.
- Globalement, cette cartographie met en évidence l'efficacité des contrôles sur la majorité des risques. Quelques risques doivent faire l'objet de plans d'actions pour renforcer leur maîtrise.

4. Modification des informations :

Figure N°26 : Représentation Radar des risques liés au processus modification des informations

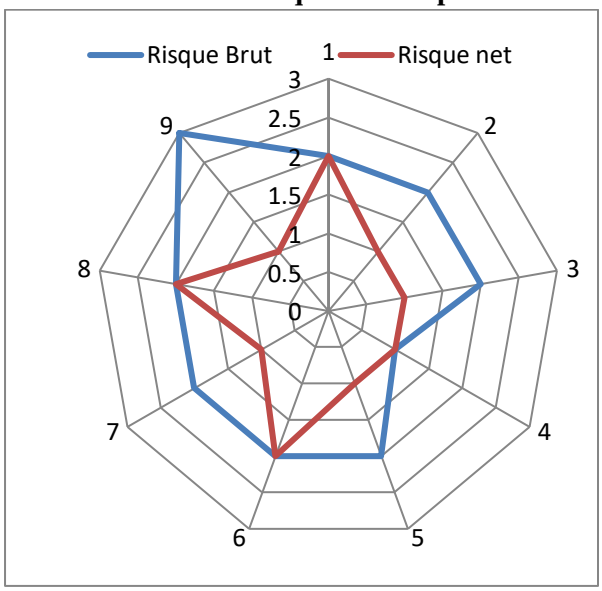


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 6 risques représentés sur les axes.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- Les risques R1 et R2 conservent la même criticité brute et nette. Les contrôles en place sur ces risques sont inefficaces.
- Le risque R3 voit sa criticité nette diminuer grâce à l'efficacité des contrôles.
- Les risques R4 et R5 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- On note toutefois une légère réduction de la criticité nette du R5 par rapport au brut, les contrôles sont donc partiellement efficaces.
- Le risque R6 apparaît comme le moins critique avec les scores les plus faibles.
- Globalement, cette cartographie met en évidence que les contrôles permettent de réduire la criticité de certains risques, mais qu'ils restent perfectibles pour les risques R1, R2 et R5 qui demeurent les plus critiques.

5. Arrêté DAB :

Figure N°27 : Représentation Radar des risques liés au processus arrêté DAB

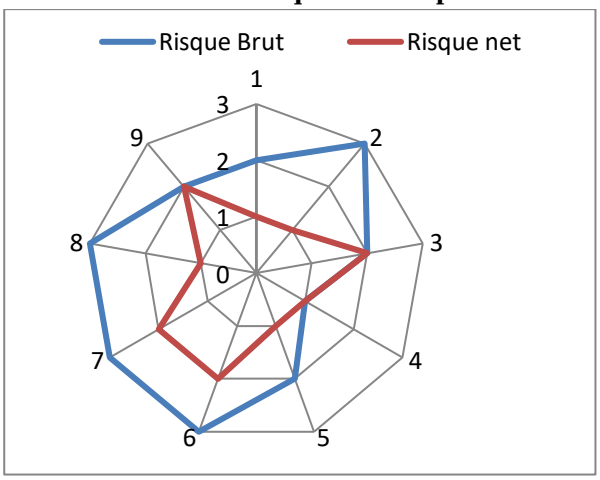


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 9 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer après prise en compte des contrôles, à l'exception de R5 et R8.
- Les risques R5 et R8 conservent une criticité nette identique à la criticité brute, reflétant une efficacité insuffisante des contrôles.
- Les risques R1 et R2 ressortent comme les plus critiques en brut, mais leur criticité nette est ramenée à un niveau modéré grâce aux contrôles.
- Le risque R9 apparaît comme le moins critique avec les scores les plus faibles.
- Certains risques ont une forte réduction de criticité grâce aux contrôles, comme R3, R6 et R7.
- Globalement, cette cartographie met en évidence l'efficacité des contrôles sur la plupart des risques à l'exception de R5 et R8, qui doivent faire l'objet de plans d'actions prioritaires pour renforcer leur maîtrise.

Alimentation DAB :

Figure N°28 : Représentation Radar des risques liés au processus alimentation DAB

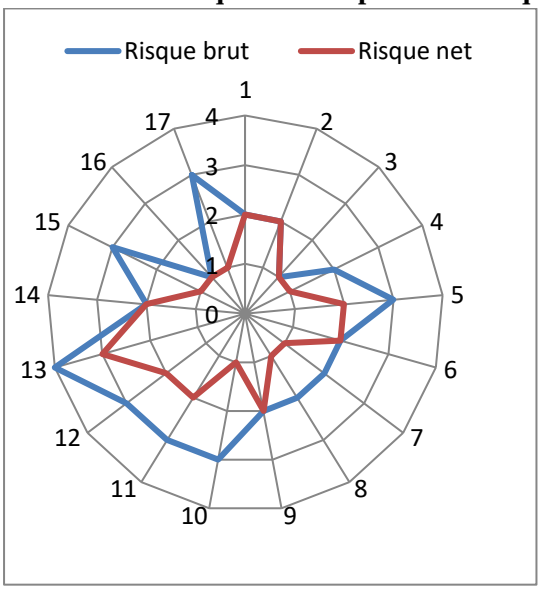


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 9 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer après prise en compte des contrôles, sauf R3 et R9.
- Les risques R3 et R9 conservent la même criticité nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R2 et R6 ressortent comme les plus critiques en brut, mais leur criticité nette est ramenée à un niveau modéré grâce aux contrôles.
- Le risque R4 apparaît comme le moins critique avec les scores les plus faibles.
- Certains risques comme R1, R5, R7 et R8 ont une nette réduction de criticité grâce aux contrôles efficaces.
- Globalement, cette cartographie met en évidence l'efficacité des contrôles sur la plupart des risques, à l'exception de R3 et R9 qui doivent faire l'objet de plans d'actions prioritaires pour améliorer leur maîtrise.

6. Acquisition DAB :

Figure N°29 : Représentation Radar des risques liés au processus acquisition DAB

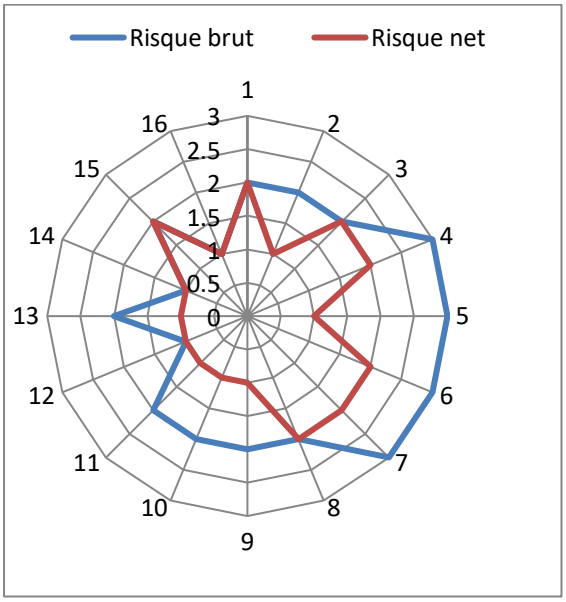


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 17 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer grâce aux contrôles, à l'exception de R1, R2, R6, R9, R12 et R14.
- Les risques R1, R2, R6, R9, R12 et R14 conservent la même criticité brute et nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R12 et R4 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R15 et R16 apparaissent comme les moins critiques avec les scores les plus faibles.
- Certains risques comme R5, R10, R11 et R13 ont une forte réduction de criticité grâce à des contrôles efficaces.
- Globalement, cette cartographie met en évidence des contrôles perfectibles pour 6 risques qui conservent une criticité élevée. Les actions prioritaires doivent porter sur le renforcement de la maîtrise de ces risques.

7. Maintenance DAB :

Figure N°30 : Représentation Radar des risques liés au processus maintenance DAB



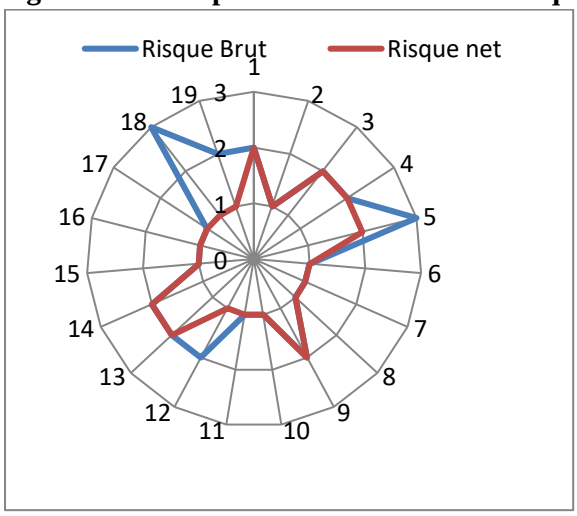
Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 16 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer grâce aux contrôles, à l'exception de R3, R6, R7 et R14.
- Les risques R3, R6, R7 et R14 conservent la même criticité brute et nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R4 et R6 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R15 et R16 apparaissent comme les moins critiques avec les scores les plus faibles.
- Certains risques comme R1, R5, R8, R9 et R10 ont une forte réduction de criticité grâce aux contrôles efficaces.

- Globalement, cette cartographie met en évidence des contrôles perfectibles pour 4 risques qui conservent une criticité élevée. Les actions prioritaires doivent porter sur le renforcement de la maîtrise de ces risques.

8. Retrait DAB :

Figure N°31 : Représentation Radar des risques liés au processus Retrait DAB

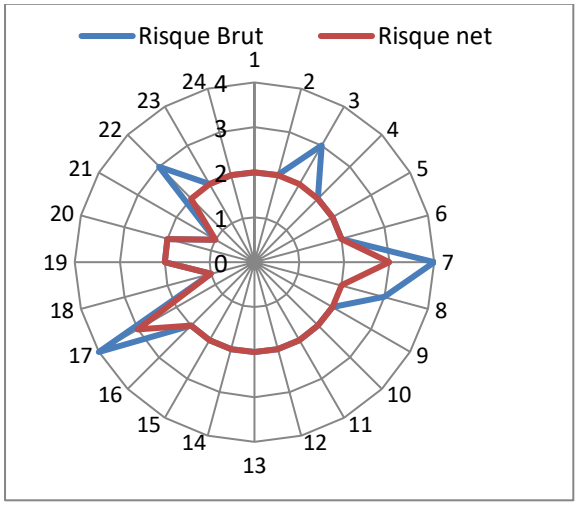


- Ce graphique radar compare la criticité brute et nette de 19 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer grâce aux contrôles, à l'exception de R3, R4, R12 et R13.
- Les risques R3, R4, R12 et R13 conservent la même criticité brute et nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R4 et R12 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R5 à R11 et R14 à R19 apparaissent comme les moins critiques avec les scores les plus faibles.
- Certains risques comme R1, R2, R11, R17 et R18 ont une forte réduction de criticité grâce aux contrôles efficaces.
- Globalement, cette cartographie met en évidence des contrôles perfectibles pour 4 risques qui conservent une criticité élevée. Les actions prioritaires doivent porter sur le renforcement de la maîtrise de ces risques.

Source : Elaboré par nos soins

9. Paiement TPE :

Figure N°32 : Représentation Radar des risques liés au processus paiement TPE



- Ce graphique radar compare la criticité brute et nette de 24 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques conservent la même criticité brute et nette, à l'exception de R3, R6, R7, R16 et R21.
- Les risques R3, R6, R7, R16 et R21 voient leur criticité diminuer grâce à des contrôles efficaces.
- Les risques R6 et R16 ressortent comme les plus critiques en brut, mais leur criticité nette est ramenée à un niveau modéré.
- Les risques R17, R18, R20 et R21 apparaissent comme les moins critiques avec les scores les plus faibles.
- La plupart des risques se situent dans une criticité modérée aussi bien en brut qu'en net.
- Globalement, cette cartographie met en évidence une efficacité limitée des contrôles, seuls 5 risques sur 24 voyant leur criticité réduite. Des actions sont nécessaires pour renforcer la maîtrise de l'ensemble des risques.

Source : Elaboré par nos soins

Analyse Comparative des deux processus : Retrait DAB et Paiement TPE :

Similarités :

- Les deux graphiques classent les risques par criticité décroissante dans le sens des aiguilles d'une montre.
- Quelques risques voient leur criticité diminuer grâce aux contrôles en place (5 risques pour le TPE, 4 risques pour le DAB).
- Certains risques ressortent comme très critiques aussi bien en brut qu'en net (R4 et R12 pour le DAB, R6 et R16 pour le TPE).

Différences :

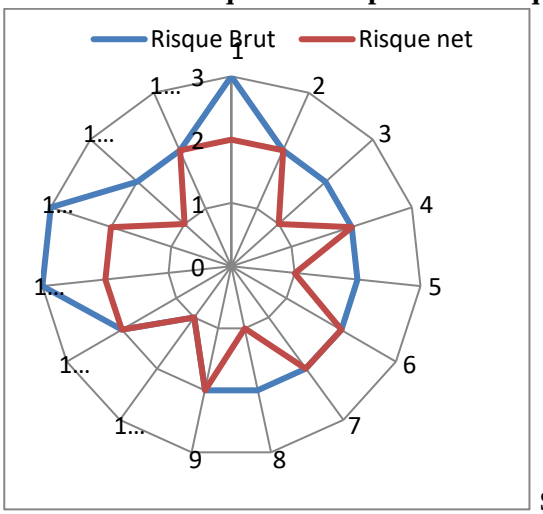
- 19 risques analysés pour le DAB, 24 pour le TPE.

- La majorité des risques DAB voient leur criticité baisser grâce aux contrôles vs seule une minorité pour le TPE.
- 4 risques DAB conservent la même criticité brute et nette vs la majorité pour le TPE.
- Les risques les moins critiques ont des scores plus faibles pour le DAB que le TPE.
- Les contrôles semblent globalement plus efficaces pour le processus DAB que TPE.

En conclusion, l'efficacité des contrôles est plus importante pour le retrait DAB, permettant de faire baisser la criticité de davantage de risques. Les actions prioritaires pour le TPE sont de renforcer les contrôles sur l'ensemble des risques afin d'améliorer leur maîtrise.

10. Acquisition TPE

Figure N° 33: Représentation Radar des risques liés au processus acquisition TPE

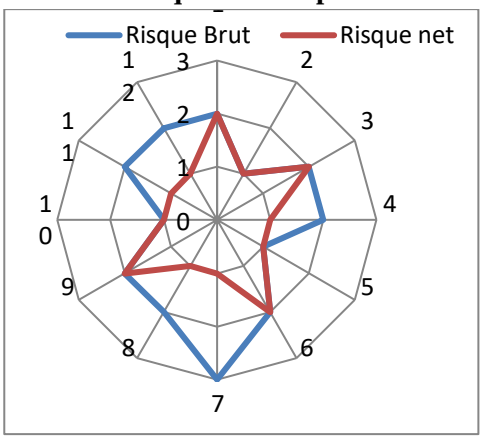


Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 15 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer après prise en compte des contrôles, à l'exception de R4, R6, R7, R10 et R11.
- Les risques R4, R6, R7, R10 et R11 conservent la même criticité brute et nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R1 et R12 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Le risque R9 apparaît comme le moins critique avec les scores les plus faibles.
- Certains risques comme R2, R3, R5, R13 et R14 ont une réduction significative de criticité grâce aux contrôles.
- Globalement, cette cartographie met en évidence des contrôles perfectibles pour 5 risques qui conservent une criticité élevée. Les actions prioritaires doivent cibler le renforcement de la maîtrise de ces risques.

11. Maintenance TPE :

Figure N°34 : Représentation Radar des risques liés au processus Maintenance TPE



Source : Elaboré par nos soins

- Ce graphique radar compare la criticité brute et nette de 12 risques.
- Les risques sont classés par criticité décroissante dans le sens des aiguilles d'une montre.
- La majorité des risques voient leur criticité diminuer grâce aux contrôles, à l'exception de R1, R3, R6 et R9.
- Les risques R1, R3, R6 et R9 conservent la même criticité brute et nette, reflétant une efficacité insuffisante des contrôles.
- Les risques R5 et R6 ressortent comme les plus critiques aussi bien en brut qu'en net. Ce sont les risques prioritaires à traiter.
- Les risques R4 et R10 apparaissent comme les moins critiques avec les scores les plus faibles.
- Certains risques comme R2, R7, R8, R11 et R12 ont une réduction significative de criticité grâce aux contrôles efficaces.
- Globalement, cette cartographie met en évidence des contrôles perfectibles pour 4 risques qui conservent une criticité élevée. Les actions prioritaires doivent porter sur le renforcement de la maîtrise de ces risques.

IV.2.Plans d'actions :

Nous allons dans cette présente partie proposer des plans d'actions pour les évènements qualifiés : Forts et Critiques après DMR pour tous les processus. Nous avons notamment proposé des plans d'actions et des plans de continuité d'activité pour tous les processus en **annexes 01.**

1. Octroi et délivrance de la carte :

❖ T09 Perte/vol transmission codes :

- Sécuriser les procédures d'envoi avec signature électronique des accusés de réception à chaque étape
- Former les équipes à la gestion sécurisée des envois
- Mettre en place un suivi en temps réel des envois sensibles
- Mettre en place un suivi des envois pour garantir que les informations personnelles sont correctement transmises.
- Valider l'adresse du destinataire avec le client avant d'effectuer l'envoi.
- Mettre en place un double contrôle interne pour vérifier que les informations personnelles ont été transmises correctement.
- Mise en place d'un plan de secours pour la transmission des informations personnelles en cas de défaillance du système de transmission principal.

- Basculer sur envoi des codes par SMS automatique en cas d'indisponibilité de la plateforme d'envoi sécurisé.

❖ **T12 Divulgation codes confidentiels :**

- Renforcer la sécurité physique et logique des locaux et systèmes
- Auditer les habilitations et révoquer les accès non nécessaires
- Imposer la double authentification pour l'accès aux données sensibles
- Rappeler les procédures de sécurité aux employés
- Sensibiliser les employés aux risques de perte ou de divulgation des codes confidentiels.
- Restreindre l'accès aux codes confidentiels aux personnes autorisées.
- Activer cellule de crise. Suspendre temporairement les accès et basculer sur autorisations directes par responsables habilités.
- Mise en place d'un plan de secours pour la protection des codes confidentiels en cas d'attaque informatique ou d'événement similaire.

❖ **T03 Remise à tiers non autorisé :**

- Former les équipes aux procédures de contrôle d'identité
- Vérifier l'identité par des moyens multiples (pièce d'identité + code reçu par le client)
- Limiter les possibilités de mandat à des cas exceptionnels dûment justifiés
- Mise en place d'un contrôle d'identité systématique pour tous les tiers qui ont accès aux informations personnelles.
- Limitation des mandats des tiers pour ne leur permettre d'accéder qu'aux informations personnelles dont ils ont besoin.
- Renforcer temporairement les contrôles d'identité par appel systématique au client avant remise. Recourir à du personnel supplémentaire formé pour absorber le surplus d'activité.

❖ **T10 Opposition non effectuée :**

- Réviser la procédure d'opposition pour raccourcir les délais
- Mettre en place des alertes automatiques en cas de non traitement dans les délais
- Renforcer le contrôle et le suivi des oppositions en attente
- Sensibilisation des employés à l'importance d'effectuer les oppositions en temps voulu.
- Mise en place d'une procédure accélérée d'opposition pour permettre aux employés d'effectuer les oppositions rapidement.
- Mise en place d'un contrôle a posteriori pour s'assurer que les oppositions ont été effectuées en temps voulu.
- Cellule dédiée pour traiter en urgence les oppositions en retard. Renforts par des équipes d'autres services formées au préalable. Extension des horaires d'ouverture.

2. Modification des plafonds :

- Identifier et mettre en place des outils spécialisés pour la détection de fraudes et d'anomalies dans les données et documents.
- Recruter ou former un expert en fraude chargé de surveiller les données et documents à la recherche de signaux d'anomalies ou de falsifications.
- Mettre en place des revues et audits réguliers pour identifier les incohérences ou les anomalies dans les données et documents.
- Mettre à jour et renforcer les procédures de contrôle pour inclure des vérifications spécifiques visant à détecter les falsifications.

- Fournir une formation régulière au personnel sur les méthodes de détection de fraudes et d'anomalies.
- Sensibiliser le personnel à l'importance de la sécurité et de la détection de la fraude dans leurs activités quotidiennes.
- Investir dans des technologies avancées de détection de fraudes, telles que l'intelligence artificielle et l'apprentissage automatique.
- Organiser des exercices de simulation de fraude pour évaluer la réactivité de l'organisation et identifier les améliorations nécessaires.

3. Acquisition DAB :

1. Mise en place de Niveaux de Stocks Minimaux

- Identifier les niveaux minimaux de stock nécessaires pour éviter les ruptures.
- Basé sur l'analyse des besoins passés et des tendances de la demande

2. Optimisation des Procédures d'Approvisionnement

- Revue et amélioration des procédures d'approvisionnement en espèces.
- Intégrer des mécanismes de prévision plus précis et des indicateurs de gestion.

3. Mise en Place d'un Système de Surveillance en Temps Réel

- Mettre en place un système de surveillance permettant de suivre en temps réel les niveaux de stock et les mouvements d'espèces.

4. Audit et Revue des Procédures Actuelles

- Engager une revue approfondie des procédures actuelles pour identifier les lacunes et les opportunités d'amélioration.

5. Amélioration de la Communication Interne

- Mettre en place des canaux de communication efficaces pour partager les informations sur les niveaux de stock et les besoins prévus.

4. Paiement TPE :

- Identifier un processus de remplacement rapide en cas de panne du TPE, tel que le recours à un TPE de secours ou un autre moyen de paiement électronique de secours.
- Mettre en place une procédure pour contacter le support technique du fournisseur du TPE en cas de panne, afin d'obtenir une assistance immédiate.
- Mettre en place un système de notification sur l'écran client en cas d'échec de l'autorisation pour informer le client de la situation.
- Envisager la mise en place d'une notification par SMS ou par e-mail en cas de panne du TPE.
- Mettre en place un système de surveillance pour suivre les incidents liés aux pannes du TPE et générer des rapports pour évaluer l'efficacité des mesures prises.

Nous avons décrit le processus monétique et les dispositifs DAB/GAB/TPE. Puis nous avons identifié et cartographié les risques inhérents selon plusieurs axes d'analyse. Ensuite, nous avons évalué et hiérarchisé ces risques selon leur criticité. Cette cartographie constitue une base solide pour la mise en place de plans d'actions visant à maîtriser ces risques. Les concepts présentés sont applicables pour performer des analyses de risques efficaces sur d'autres processus.

CONCLUSION GÉNÉRALE

CONCLUSION GÉNÉRALE

Ce travail avait pour objectif d'élaborer une cartographie exhaustive des risques associés aux opérations monétiques et aux équipements DAB/GAB/TPE utilisés par les banques. Un travail qui a constitué une exploration approfondie et méthodique des risques inhérents. Grâce à une méthodologie rigoureuse combinant recherche documentaire, entretiens avec des experts et analyse quantitative des risques, ce travail a permis d'identifier les principales menaces pesant sur le système monétique bancaire.

Les risques technologiques liés au piratage des cartes et des distributeurs ont notamment été mis en évidence. Mais des vulnérabilités organisationnelles et humaines ont également été révélées, comme la faille dans les processus de vérification d'identité ou le manque de sensibilisation des clients aux fraudes.

L'évaluation de la criticité de chaque risque a ensuite donné lieu à une hiérarchisation détaillée, faisant ressortir les zones de risque majeur sur lesquelles les banques doivent concentrer leurs efforts. La cartographie produite est à la fois un outil de pilotage stratégique et un guide opérationnel pour orienter les mesures de sécurisation prioritaires.

Bien que des difficultés aient été rencontrées, comme la confidentialité de certaines données bancaires, ce projet nous a permis de mettre en pratique et d'approfondir mes compétences en gestion des risques, analyse de processus et sécurité des systèmes d'information.

Les livrables fournis, validés par des professionnels du secteur, apportent une réelle valeur ajoutée aux établissements bancaires et financiers. Ils contribueront, nous l'espérons, à mieux sécuriser les services monétiques au bénéfice des banques comme des utilisateurs.

Après la réalisation de ce travail dédié à l'élaboration d'une cartographie des risques liés au processus monétique et au dispositif DAB/GAB/TPE, il apparaît clairement que la sécurisation des transactions électroniques est un défi complexe et évolutif qui requiert une attention constante et des solutions innovantes.

Synthèse des Résultats :

L'analyse approfondie des processus monétiques, des DAB, des GAB, et des TPE a permis d'identifier une gamme étendue de risques, allant des menaces traditionnelles telles que la fraude financière à celles plus modernes et sophistiquées liées aux cyberattaques. La création d'une cartographie des risques a fourni une vision structurée et holistique de ces défis, permettant aux parties prenantes de mieux comprendre les vulnérabilités inhérentes à ces systèmes critiques.

Contributions et Recommandations :

Ce travail de recherche apporte une contribution significative à la compréhension et à la gestion des risques dans le domaine monétique. En élaborant une méthodologie rigoureuse pour l'identification, l'évaluation, et la hiérarchisation des risques, cette étude offre aux acteurs du secteur des outils concrets pour renforcer la sécurité de leurs opérations.

Les recommandations formulées au fil de ce PFE mettent en évidence l'importance de la collaboration entre les institutions financières, les organismes de régulation, et les experts en sécurité informatique. Le partage d'informations et l'adoption de bonnes pratiques de sécurité sont essentiels pour atténuer les risques et renforcer la résilience des systèmes monétiques.

Perspectives Futures :

Alors que nous clôturons cette étude, il est crucial de souligner que le paysage des transactions financières électroniques continuera d'évoluer, présentant de nouveaux défis et opportunités. Les travaux futurs pourraient se concentrer sur l'intégration de technologies émergentes telles que l'intelligence artificielle et la blockchain pour renforcer encore davantage la sécurité des transactions.

De plus, la sensibilisation continue, la formation du personnel, et la mise en place de mécanismes de réponse aux incidents seront des éléments clés pour assurer la robustesse des systèmes monétiques dans un contexte en constante mutation.

Conclusion Finale :

En conclusion, l'élaboration d'une cartographie des risques liés au processus monétique et au dispositif DAB/GAB/TPE se révèle être un processus stratégique et nécessaire dans la gestion globale des risques. En comprenant et en anticipant les menaces potentielles, les institutions financières peuvent non seulement protéger leurs activités, mais également renforcer la confiance des utilisateurs dans les transactions électroniques.

Ce travail de recherche aspire à être un catalyseur de réflexion et d'action dans le domaine de la monétique. Il est notre espoir que les résultats présentés ici puissent inspirer des initiatives concrètes visant à créer un environnement monétaire plus sûr, plus résilient, et plus adapté aux défis technologiques du XXIe siècle.

Bibliographie

Bibliographie :

Ouvrages :

- Alphonse Christiane Ivinza Lepapa, « Monétique et transaction électronique » édition Bookelis, 2018.
- Antoine Sardi, « Management des risques bancaires », Edition AFGES, Paris 2001.
- Antoine Sardi, « Audit et contrôle interne bancaire », Edition AFGES, Paris 2002
- Ariane Chapelle, Georges Hübner et Jean-Philippe Peters « Le risque opérationnel implication de l'accord de bâle pour le secteur financier », Edition : Larcier, 2005
- Coopers-Lybrand, La Pratique du contrôle interne, IFACI (institut français de l'audit et du contrôle interne), ED. ORGANISATION.
- DE Mareschal (2003), la cartographie des risques, édition Afnor, 2003, paris.
- Didier-Pierre Monod, « Moyens et Technique de Paiement Internationaux –import-export » 4éme édition ESKA, Paris, 2007.
- FREDERIC.G, « La saisie de la monnaie scripturale », Edition L'acier, Bruxelles 2006.
- Henri-Pierre MADERS, Jean-Luc Masselin, « Contrôle interne des risques », Eyrolles, Paris, 2009.
- Franck Moreau, « Comprendre et gérer les risques », Edition d'Organisation, 2002.
- Yvon Mougin, « la cartographie des processus», édition d'Organisation, paris, 2004.
- HASHEM SHERIF Moustafa et SERHROUCHNI Ahmed, "La monnaie électronique (Systèmes de paiement sécurisé)", Editions Romandes, 1999.
- Jimenez Christian, Merlier Patrick, Prévention et Gestion des risques opérationnels, Ed Revue Banque, 2004.
- Pascal Kerbel, « mise en œuvre d'un contrôle interne efficace », Edition AFNOR, 2007.

Œuvres universitaires :

- Benaceur Youcef, « le rôle de l'audit dans la gestion des risques opérationnels », ESB, 2011
- Mohamed Lazreg, Développement de la Monétique en Algérie, Réalité et Perspectives, Thèse Présentée pour l'obtention d'un diplôme de doctorat en sciences de gestion. UNIVERSITE ABOU BAKR BELKAID TLEMCEN.2015.
- Mvom Yannick Rahmane, Elaboration d'une cartographie des risques opérationnels de trésorerie, 2009

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

Revues et publications bancaires :

- A.BENCHABLA, responsable de la monétique au niveau de la SATIM, PME Magazine, n°13, du 15 Mars 2002
- Altair Conseil, Maitrise des risques : Elaborer la cartographie des risques (démarches et méthodes), Paris, 2008.
- Comité de Bâle sur le Contrôle Bancaire 2004
- C.JIMENEZ, Risque Opérationnel, de la mise en place du dispositif à son audit, édition Revue Banque, Paris, 2008,
- Dominique Vincenti , Dresser une cartographie des risques, in Revue Audit .
- IFACI « Cahiers de la recherche, la cartographie des risques », 2013 ;
- FORTUGUE & al, « cartographie des risques : quelle valeur ajoutée ? Quel processus ? », 2001
- IFACI, « guide d'audit cartographie des risques », Edition Les Cahiers de la Recherche, 2006.
- IFACI(2006), Le management des risques de l'entreprise, Organisation, Paris.
- ISO 31000 DEUXIEME édition 2018-02
- Jimenez Christian, Merlier Patrick et Chelly Dan (2008), Risques opérationnels: de la mise en place du dispositive à son audit, Revue Banque Edition.
- Philippe Deniau et Etienne Renoux, « la cartographie du risque opérationnel : outil réglementaire ou outil de pilotage ? » revue d'économie financière, NO 84 ; Le opérationnel ; juin 2006
- Revue de la Commission Européenne, la recommandation des opérations KJ n°97/489/CE, juillet, 1997.

Textes législatifs et règlementaires :

- Décision réglementaire d'approbation N° 60/09 du 06 /05 /2009 ;
- Décision réglementaire DR N° 05/2014 du : 22 janvier 2014 ;
- Selon le règlement n°14-01 du 16 février 2014 portant coefficients de solvabilité applicables aux banques et établissements financiers, Article 21 ;
- Règlement de banque d'Algérie n°11-08

- Journal Officiel de la République : Loi n°90-10 du 14 Avril 1990 relative à la Monnaie et au Crédit.
- Règlements de la Banque d'Algérie : Règlement N°97-03 du 17 Novembre 1997 in www.bank-of-algeria.dz

Sites internet :

- **Http://www.iefpedia.com/**
- **https://www.bis.org/**
- **www.comprendrelespaiements.com/**
- **https://financeland.fr/**
- **https://billetdebanque.panorabanques.com/**
- **https://giemonetique.dz/**
- **http://www.satim-dz.com/**
- **www.algerietelecom.dz**
- **https://dictionnaire.lerobert.com/**

Autres :

- EFEE CD 15 Cours de Gestion, Mons, 2006, Dossier de paiement ABB
- LE NOUVEAU ROBERT « DICTIONNAIRE DE LA LANGUE FRANÇAISE », VERSION 2003 ;
- Support de cours risque opérationnel, Mr Chiheb Ghanmi, IFID, 2023.
- Support de cours Techniques bancaires, Khaled Bettaieb, IFID, 2022.

LES ANNEXES

Annexe 01 : Plans d'action et plans de continuité d'activité :

1. Octroi et délivrance de la carte :

Risque	Plan d'action	Plan de continuité d'activité
Fraude à l'identité	Renforcer le contrôle des justificatifs (originaux, vérification des tampons, hologrammes, etc.)	Procédure d'escalade pour contrôle renforcé des justificatifs par l'équipe Risk
Non conformité du contrat	Check-list de contrôle systématique du contrat avant signature	Archivage électronique systématique des contrats pour recherche rapide
Erreur de saisie	Double saisie par 2 agents différents avec validation croisée	Saisie possible depuis un site de backup en cas d'indisponibilité du SI principal
Erreur de contrôle	Sensibilisation et formation du personnel à l'importance des contrôles	Recours possible à une équipe de contrôle dédiée en centre de services partagés
Erreur sur commande	Audit régulier du processus de commandes, piste d'audit sur les fichiers	Fichiers de commandes sauvegardés pour ressaisie en mode dégradé
Non réception de l'avis	Message d'alerte automatique en cas de non réception dans les délais	Relances téléphoniques systématiques en cas de défaillance des mails
Perte/vol carte/code	Renforcer la sécurité physique du stockage (coffre, accès restreint, etc.)	Stock tampon de cartes/codes en coffre externe
Perte/vol transmission	Traçabilité et signature à chaque transfert de documents/matériels	Transport sécurisé par transporteur spécialisé avec traçabilité renforcée
Non réception	Vérification systématique réception/commande et relance fournisseur	Commande automatiquement dupliquée vers site de production secondaire
Erreur de réconciliation	Check-list de rapprochement commande/réception	Outillage Excel de rapprochement de secours
Divulgation des codes	Stockage sécurisé des codes et accès limité au coffre	Génération automatique de nouveaux codes en cas de compromission
Divulgation des cartes	Idem + inventaire périodique du stock de cartes	Renouvellement accéléré des cartes concernées
Client non joint	Coordonnées clients à jour, relances multiples par différents canaux	Relances par agence physique de proximité si défection des moyens habituels
Remise à tiers non autorisé	Contrôle systématique PI avec vérification biométrique	Recours à vidéo-identification du client à distance
Divulgation du code	Remise du code sous pli cacheté au client	Procédure d'envoi postal sécurisé en mode dégradé
Absence de signature	Alerte automatique si case non cochée dans le registre	Clôture manuelle du registre pour éviter blocage
Erreur de saisie activation	Double contrôle activation saisie/effective	Hotline dédiée pour activation d'urgence
Activation frauduleuse	Cloisonnement des tâches et traçabilité des accès/actions	Blocage et réémission carte automatique par la fraude
Non activation	Rappel automatique des non activations après échéance	Génération d'une nouvelle carte si délai dépassé
Opposition non effectuée	Supervision en temps réel des comptes en attente d'opposition	Cellule dédiée pour traitement manuel d'urgence
Non destruction de la carte	Archivage sécurisé et traçabilité de la destruction	Archivage externe et contrôles renforcés des cartes physiques

Source : Elaboré par nos soins

2. Gestion des cartes capturées :

Risque	Plan d'action	Plan de continuité d'activité
Dommage à la carte lors du retrait	Formation du personnel à la manipulation sécurisée des cartes, contrôles réguliers de l'ATM	Kit de nettoyage et réparation de cartes disponible en agence
Erreur humaine de saisie	Double saisie et validation croisée, vérifications automatisées	Saisie possible depuis un site de backup
Erreurs dans les formulaires	Check-list de contrôle du remplissage des formulaires	Formulaires pré-remplis numérisés utilisables en mode dégradé
Non transmission des formulaires	Accusé de réception automatique à l'émission et la réception	Archivage pdf systématique pour retransmission
Omission d'informations	Formulaire avec champs obligatoires, vérifications de complétude	Cellule centrale d'assistance pour complétude en mode dégradé
Erreur dans le contrôle	Sensibilisation des contrôleurs, fiche de points clés à vérifier	Contrôle renforcé par équipe dédiée au siège
Transmission non sécurisée	Chiffrement et signature électronique des formulaires	Recours à un transporteur privé sécurisé
Perte/manipulation frauduleuse	Traçabilité et signature à chaque transfert de documents	Traçabilité et contrôles aléatoires renforcés
Analyse erronée	Procédure formalisée d'analyse, revue par un contrôleur	Analyse d'un 2e analyste en cas de doute
Eléments négligés dans l'analyse	Check-list des points obligatoires à investiguer et vérifier	Check-list d'analyse de secours
Erreur dans la communication	Validation des conclusions par le responsable avant envoi	Validation par contrôleur avant envoi en mode dégradé
Transmission erronée des conclusions	Double envoi, par mail et courrier, avec AR demandé	Appel systématique au destinataire pour confirmation réception

Source : Elaboré par nos soins

3. Gestion de mise en opposition :

Risque	Plan d'action	Plan de continuité d'activité
Usurpation d'identité	Contrôle renforcé des justificatifs, vérification biométrique	Recours à vidéo-identification à distance
Erreur d'identification	Check-list identification client obligatoire	Service d'assistance en back-office pour correction
Mauvaise authentification	Double contrôle de la signature	Archivage électronique des signatures pour vérification
Erreur de saisie	Double saisie avec validation croisée	Saisie possible sur site de secours
Perte/vol bordereau	Traçabilité des documents avec signature à chaque transfert	Bordereaux pré-imprimés utilisables en repli
Transmission au mauvais destinataire	Contrôle automatique du destinataire	Redirection automatique vers le bon destinataire
Non détection d'erreurs	Supervision et échantillonnage des validations	Equipe de contrôle dédiée au siège
Validation d'opposition erronée	Sensibilisation des validateurs + droit de veto	Droit de veto hiérarchique
Perte/corruption fichier	Archivage sécurisé + envoi d'un accusé de réception	Archivage sur double site
Erreur de validation	Cloisonnement des tâches de saisie et validation	Validation manuelle d'urgence par le responsable
Erreur de collecte/traitement	Audit régulier du processus de collecte et traitement	Collecte via sites agences en direct
Problème technique	Plan de secours avec moyens alternatifs de collecte	Outils de collecte redondants
Fichier corrompu	Contrôles d'intégrité renforcés	Clés de contrôle pour détection
Perte de confidentialité	Chiffrement des données	Recours à un réseau privé sécurisé
Erreur de transmission	Accusé de réception systématique	Envois redondants + vérif téléphonique
Retard d'émission	Supervision en temps réel et relance fournisseur	Site de production secondaire

Source : Elaboré par nos soins

4. Gestion des modifications des informations :

Risque	Plan d'action	Plan de continuité d'activité
Usurpation d'identité du client	- Vérifier l'identité du client via pièce d'identité. - Vérifier que les infos clients correspondent aux documents.	- Processus d'escalade et alerte de la fraude. - Annulation de la demande. - Enquête et signalement aux autorités.
Falsification des documents justificatifs	- Former le personnel à détecter les falsifications. - Utiliser des outils de détection de falsification.	- Annulation de la demande. - Processus renforcé de vérification des documents. - Formation du personnel à la détection des falsifications.
Erreur de saisie des informations	- Double saisie par 2 agents différents. - Contrôle automatisé de cohérence.	- Correction des informations erronées. - Nouvelle saisie et vérification. - Formation du personnel à la vigilance.
Non authentification de la signature	- Vérifier la conformité de la signature. - Demander un justificatif d'identité signé.	- Demande de nouvelle signature authentifiée. - Suspension du traitement de la demande. - Sensibilisation du client à l'authentification.
Non détection d'anomalies ou falsifications	- Audit régulier des dossiers par sondage. - Monitoring automatisé des anomalies.	- Audit approfondi des dossiers récents. - Révision des contrôles et du monitoring. - Formation du personnel au contrôle vigilant.
Validation erronée de la demande	- Double validation par 2 agents différents. - Check-list de contrôle avant validation.	- Annulation de la validation. - Nouveau contrôle et validation du dossier. - Renforcement du double contrôle.

Source : Elaboré par nos soins

5. Arrêté DAB :

Risque	Plans d'action	Plans de continuité d'activité
Panne ou indisponibilité du DAB pendant la maintenance	Procédure stricte de maintenance et tests. Formation du personnel de maintenance. Contrats de maintenance et SLA avec fournisseurs.	Communication aux clients. Redirection vers autres DAB. Appoint manuel si nécessaire.
Erreur humaine lors de l'arrêt qui pourrait causer un dysfonctionnement	Checklist et procédure détaillée d'arrêt. Double contrôle. Traçabilité des opérations.	Diagnostic approfondi. Intervention rapide sur site si besoin. Escalade aux équipes compétentes.
Erreur de saisie comptable	Double saisie et validation croisée. Outils de détection d'erreurs. Formation du personnel.	Correction des écritures erronées. Contrôles comptables renforcés.
Vol d'argent lors du transport et de la manipulation	Procédures sécurisées de manipulation et transport. Traçabilité. Caméras de surveillance.	Enquête interne. Signalement aux autorités. Audit des flux et des accès.
Erreur de combinaison qui empêcherait l'ouverture du DAB	Checklist d'ouverture. Double contrôle des combinaisons. Test des combinaisons.	Intervention d'un technicien sur site. Changement des combinaisons si nécessaire.
Écart entre décompte physique et solde théorique	Inventaire et rapprochement réguliers. Outils de suivi des écarts. Formations du personnel.	Enquête approfondie. Ajustements comptables. Renforcement des contrôles.
Vol ou malversation lors des manipulations	Procédures sécurisées. Traçabilité totale. Surveillance vidéo.	Enquête interne. Signalement aux autorités. Sanctions disciplinaires.
Erreur de saisie comptable du montant restant	Double saisie avec validation. Outils de détection d'erreurs. Formations.	Corrections comptables. Contrôles renforcés avant validation.
Non détection d'éventuels écarts de caisse	Inventaires et rapprochements réguliers et inopinés. Outils d'analyse des écarts.	Enquête approfondie. Ajustements comptables. Renforcement des contrôles.

Source : Elaboré par nos soins

6. Alimentation DAB :

Risque	Plans d'action	Plans de continuité d'activité
Erreur dans le calcul du montant à alimenter	Double contrôle du calcul. Outils de calcul automatisé.	Nouveau calcul et réajustement du montant.
Erreur dans le chargement ou la saisie	Checklist détaillée. Double contrôle. Traçabilité des opérations.	Réouverture et réorganisation des cassettes. Mise à jour des données.
Mauvais positionnement des cassettes	Checklist et procédure stricte de positionnement. Contrôle systématique.	Réorganisation des cassettes dans le bon ordre.
Erreur de combinaison pour la fermeture	Checklist d'opérations. Double contrôle des combinaisons.	Intervention d'un technicien sur site. Changement des combinaisons.
Nouvelle alimentation mal prise en compte	Vérifications systématiques après alimentation. Traçabilité des opérations.	Diagnostic approfondi. Mise à jour des données si erreur.
Non détection d'un problème d'alimentation	Checklist rigoureuse après alimentation. Surveillance des niveaux de cash.	Intervention rapide sur site. Réapprovisionnement d'urgence si besoin.
Non détection d'un problème dans la partie supérieure	Contrôles systématiques. Monitoring à distance.	Intervention rapide d'un technicien sur site.
Panne ou dysfonctionnement à la remise en service	Tests complets avant remise en service. Checklist détaillée des opérations.	Diagnostic approfondi. Intervention d'un technicien. Prolongation de l'indisponibilité si besoin.
Mise à dispo alors que le DAB n'est pas opérationnel	Vérifications rigoureuses et tests complets avant mise à dispo. Traçabilité.	Blocage et remise hors service du DAB. Intervention urgente d'un technicien.

Source : Elaboré par nos soins

7. Acquisition DAB :

Risques	Plans d'action	Plans de continuité d'activité
Mauvaise estimation des besoins	Études approfondies. Simulation de scénarios. Benchmarks.	Réévaluation régulière. Ajustements progressifs.
Mauvais emplacement	Études détaillées. Critères exigeants de sélection.	Changement d'emplacement si nécessaire.
Données de marché erronées	Collecte de données variées. Recoupement des sources.	Actualisation fréquente des études.
Offre technique inadéquate	Cahier des charges précis. Appel d'offres exigeant.	Renégociation du contrat. Changement de prestataire.
Surcoût	Budget provisionné. Négociation des prix.	Rééchelonnement. Réduction des fonctionnalités.
Retards de livraison	Planning réaliste. Pénalités de retard. Suivi rapproché.	Planning adapté. Solutions provisoires.
Mauvaise définition des responsabilités	Organisation claire. Fiches de poste détaillées.	Réunion de crise. Réattribution des tâches.
Manque de flexibilité	Architecture évolutive. Clause de révision des contrats.	Renegociation des conditions. Changements organisationnels.
Problèmes d'alimentation	Cahier des charges exigeant. Doublement des arrivées.	Installation d'un groupe électrogène.
Sécurité insuffisante	Exigences sécurité renforcées. Audits réguliers.	Renforcement rapide de la sécurité.
Dysfonctionnements à la livraison	Tests de réception exigeants. Procédure rigoureuse.	Interventions correctives. Prolongation des tests.
Problèmes de connexion	Cahier des charges exigeant. Doublement des liens réseaux.	Basculement vers liens back-up. Interventions correctives.
Mauvais paramétrage	Vérifications et tests complets. Procédures stricte.	Reconfiguration. Intervention maintenance.
Ruptures de stock	Prévision des besoins. Stocks de sécurité.	Réapprovisionnement en urgence. Transport exceptionnel.
Compétences insuffisantes	Formation approfondie. Supports experts.	Renforts temporaires. Externalisation.
Défaillances critiques	Tests complets. Détection précoce des anomalies.	Prolongation des vérifications. Mise en service retardée.
Mauvaise information client	Plan de communication. Supports promotionnels.	Communication adaptée. Gestes commerciaux.
Vieillissement prématuré	Choix de matériels robustes. Maintenance préventive.	Remplacement anticipé. Renégociation contrats de maintenance.

Source : Elaboré par nos soins

8. Maintenance DAB :

Risques	Plans d'action	Plans de continuité d'activité
Mauvais diagnostic de la panne	Procédures rigoureuses de diagnostic. Recours à l'assistance technique.	Nouvelle intervention sur site. Diagnostic approfondi.
Mauvaise description du problème	Formation du personnel. Modèles de description. Validation systématique.	Prise de contact avec le client. Nouvelle description explicite.
Analyse incorrecte de la panne	Méthodologie d'analyse validée. Recours à l'expertise technique.	Réanalyse approfondie du problème. Tests complémentaires.
Délais importants pour intervention	Optimisation des plannings. Sous-traitance si besoin.	Intervention accélérée en heures supplémentaires.
Oubli de pièces détachées	Checklist des pièces. Vérification systématique des stocks.	Envoi en urgence de la pièce manquante.
Mauvaises réparations	Contrôles qualité. Traçabilité des opérations.	Nouvelle intervention corrective.
Détériorations supplémentaires	Procédures strictes d'intervention. Formation du personnel.	Réparations des dégâts. Mesures préventives.
Tests insuffisants après réparation	Protocoles de tests complets. Validation des résultats.	Nouveaux tests approfondis avant remise en service.
Informations manquantes	Procédure rigoureuse de collecte d'infos. Checklist.	Relance du client pour compléments d'infos.
Traçabilité insuffisante	Outils de suivi des interventions. Archivage systématique.	Recherche des données manquantes. Renforcement des procédures.
Résolution non validée à tort	Double validation systématique. Contrôle qualité.	Intervention corrective urgente sur site.
Perte/vol des pièces défectueuses	Suivi des pièces défectueuses. Archivage sécurisé.	Enquête interne. Mesures de sécurité renforcées.
Facturation erronée	Double contrôle. Validation par le client.	Correction et nouvelle facturation.
Litiges	Documentation précise des interventions. Archivage long.	Gestion amiable des litiges. Procédure contentieuse si nécessaire.
Registres non mis à jour	Procédure stricte de mise à jour. Contrôles réguliers.	Correction et mise à jour rétroactive des registres.
Données historiques perdues	Sauvegardes régulières. Archivage longue durée.	Recherche des données sur supports. Saisie manuelle si nécessaire.

Source : Elaboré par nos soins

9. Retrait DAB :

Risque	Plans d'action	Plans de continuité d'activité
Copie de carte bancaire	Lecteurs EMV avec puce. Contrôles réguliers d'altération.	Blocage de la carte. Remboursement du client.
Espionnage visuel du PIN	Protection physique du clavier. Floutage de l'écran.	Changement des codes PIN compromis. Surveillance accrue.
Divulgation du PIN	Sensibilisation des clients.	Changement du code PIN. Surveillance des transactions.
Saisie du PIN sur faux clavier	Contrôles physiques réguliers.	Inspection approfondie. Changement des serrures si nécessaire.
Phishing du code PIN	Sensibilisation clients aux e-mails frauduleux.	Blocage préventif des cartes piratées. Alerte clients.
Erreur de saisie du montant	Validation du montant avant retrait.	Correction après appel du client. Remboursement si débit erroné.
Interception des données bancaires	Transmission chiffrée. Protocoles sécurisés.	Blocage des cartes et comptes compromis. Surveillance renforcée.
Erreur de vérification	Contrôles automatisés. Traçabilité.	Enquête interne. Remboursement du client si nécessaire.
Autorisation frauduleuse	Vérifications renforcées. Monitoring des anomalies.	Blocage compte et carte. Enquête approfondie.
Surcharge de la réserve	Suivi précis des niveaux de cash.	Réapprovisionnement urgent en liquidités.
Non distribution de l'argent	Diagnostic approfondi. Tests réguliers.	-
Délivrance incorrecte de billets	Maintenance préventive. Capteurs de bourrage.	Remboursement du client. Réparation/remplacement.
Débit multiple	Journalisation des transactions. Rapprochement comptable.	Correction des écritures. Remboursement du client.
Débit supérieur au retrait	Journalisation et rapprochement des opérations.	Correction comptable. Remboursement de l'écart au client.
Non restitution de la carte	Capteurs de rétention. Maintenance préventive.	Désactivation de la carte. Récupération par le client.
Vol de la carte oubliée	Messages de rappel de la carte. Capteurs anti-oubli.	Blocage de la carte. Remplacement.
Absence de preuve (ticket)	Redondance imprimantes. Stock de tickets.	Enregistrements internes des transactions.

Source : Elaboré par nos soins

10. Acquisition TPE :

Risques	Plans d'action	Plans de continuité d'activité
Mauvaise estimation du parc	Études approfondies. Projections détaillées.	Réévaluation régulière. Adaptation progressive.
Exigences techniques trop faibles	Cahier des charges précis. Exigences élevées.	Renégociation du contrat. Changement de prestataire.
Offres non conformes	Critères d'évaluation stricts. Négociation exigeante.	Nouvel appel d'offres. allotissement des prestations.
Mauvaise négociation commerciale	Négociation encadrée. Analyse fine des offres.	Rénégociation si possible. Sinon changement de prestataire.
Fournisseur à risque	Critères de sélection exigeants. Notation financière.	Mise en demeure. Résiliation si pas d'amélioration.
Non respect des exigences	Pénalités contractuelles. Contrôles réguliers.	Rejet des livraisons non conformes. Tests complémentaires.
Erreurs de configuration	Procédures détaillées. Tests complets avant déploiement.	Reconfiguration sur site ou remotye.
Sécurité compromise	Exigences sécurité renforcées. Audits réguliers.	Blocage des transactions. Corrections urgentes.
Retards de livraison	Planning réaliste. Pénalités de retard. Suivi rapproché.	Action en justice si retard excessif. Commandes concurrentes.
Perte/vol	Sécurisation des transports et stocks.	Commande de remplacement en urgence.
Mauvaise installation	Check-lists. Procédures détaillées. Contrôles.	Réinstallation sur site. Formation renforcée.
Dysfonctionnements	Tests complets avant déploiement. Procédures d'escalade.	Diagnostic approfondi. Intervention SAV.
Personnel non qualifié	Formation et support utilisateurs. Guides pratiques.	Assistance téléphonique. Intervention sur site.
Anomalies non détectées	Batterie complète de tests. Recette exigeante.	Suspension du déploiement. Corrections urgentes.
Retards de déploiement	Planning concerté. Accompagnement des commerçants.	Pénalités contractuelles. Report de la mise en service.

Source : Elaboré par nos soins

11. Maintenance TPE :

Risque	Plans d'action	Plans de continuité d'activité
Dysfonctionnements non détectés	Tests complets avant déploiement. Procédures d'escalade.	Suspension des mises en service. Corrections urgentes.
Mauvaise description du problème	Formation du personnel. Modèles de description. Validation systématique.	Prise de contact avec le commerçant. Nouvelle description explicite.
Diagnostic erroné de la panne	Méthodologie validée. Recours à l'expertise technique.	Réanalyse approfondie. Tests complémentaires.
Codification incorrecte	Nomenclature claire. Formation des techniciens.	Correction rétroactive de la codification.
Perte/vol pendant transport	Sécurisation des transports. Traçabilité.	Enquête interne. Commande de remplacement urgent.
Détérioration pendant transport	Conditionnement renforcé. Sensibilisation transporteurs.	Réparation ou remplacement anticipé.
Mauvaise réparation	Procédures d'intervention. Contrôle qualité. Traçabilité.	Nouvelle intervention corrective.
Tests insuffisants après réparation	Protocoles de tests complets. Validation des résultats.	Nouveaux tests approfondis avant remise en service.
Informations manquantes ou erronées	Procédure rigoureuse de collecte d'infos. Checklist.	Relance du commerçant pour compléments d'infos.
Perte/vol pendant transport	Sécurisation des transports. Traçabilité.	Enquête interne. Commande de remplacement urgent.
Clôture prématurée	Double validation obligatoire. Contrôle qualité.	Réouverture pour intervention corrective.
Facturation erronée	Double contrôle. Validation par le commerçant.	Correction et nouvelle facturation.

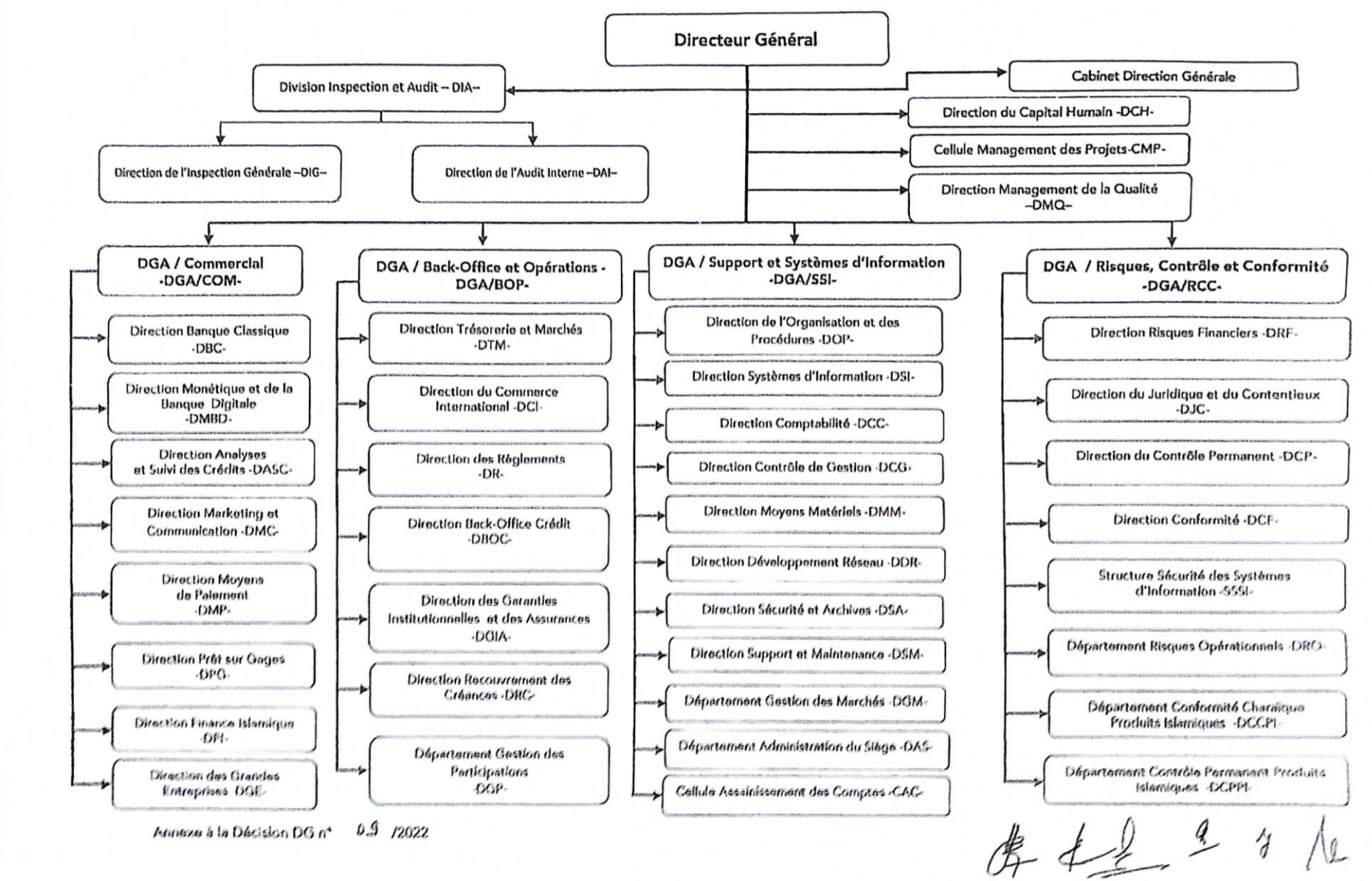
Source : Elaboré par nos soins

12. Paiement TPE :

Risque	Plans d'action	Plans de continuité d'activité
Fraude sur le montant	Sensibilisation commerçants. Lecteur de puce.	Remboursement client. Enquête interne.
Saisie incorrecte du montant	Validation du montant. Formation utilisateurs.	Correction après appel client. Remboursement si besoin.
Fraude par vol/contrefaçon carte	Lecteur de puce EMV. Contrôles physiques réguliers.	Blocage de la carte. Surveillance accrue.
Insertion dans TPE trafiqué	Inspection physique des TPE. Scellement inviolable.	Expertise, dépôt de plainte. Mesures préventives.
Défectuosité du lecteur	Maintenance préventive. Contrôles réguliers.	Réparation/remplacement urgent.
Skimming	Lecteur de puce EMV. Contrôles physiques.	Blocage des cartes compromises. Surveillance renforcée.
Interception du code	Protection physique du clavier. Sensibilisation client.	Changement des codes compromis. Surveillance accrue.
Interception des données	Transmission chiffrée. Protocoles sécurisés.	Blocage des cartes et comptes concernés.
Erreur de vérification/autorisation	Contrôles automatisés. Traçabilité.	Enquête interne. Remboursement client si nécessaire.
Interception de l'autorisation	Canaux de transmission sécurisés.	Blocage des transactions suspectes. Vérifications renforcées.
Défaillance du réseau	Redondance des liens réseau.	Basculement vers liens back-up. Intervention corrective.
Modification frauduleuse transaction	Signature électronique. Journalisation.	Annulation transaction. Enquête approfondie.
Perte/vol du TPE	Chiffrement des données. Déclaration de perte.	Blocage du TPE. Enquête interne.
Non enregistrement transaction	Journalisation interne. Traçabilité.	Enquête interne. Remboursement client.
Interception de l'écran	Protection physique de l'écran.	Vérification approfondie. Mesures préventives.
Panne du TPE	Maintenance préventive. Procédure d'escalade.	Diagnostic approfondi. Réparation/Remplacement.
Problème d'impression	Redondance imprimantes. Stocks tickets.	Enregistrements internes transactions.
Oubli de la carte	Messages de rappel. Procédure de rendu.	Neutralisation de la carte. Récupération par le client.
Transmission des transactions erronée	Contrôles avant transmission. Rapprochement comptable.	Régularisation et nouvelle transmission.
Erreur de comptabilisation	Rapprochement bancaire systématique.	Correction comptable. Régularisation relevés clients.
Contestation abusive	Archivage des justificatifs. Traçabilité.	Procédure de gestion des litiges. Recours juridique si nécessaire.

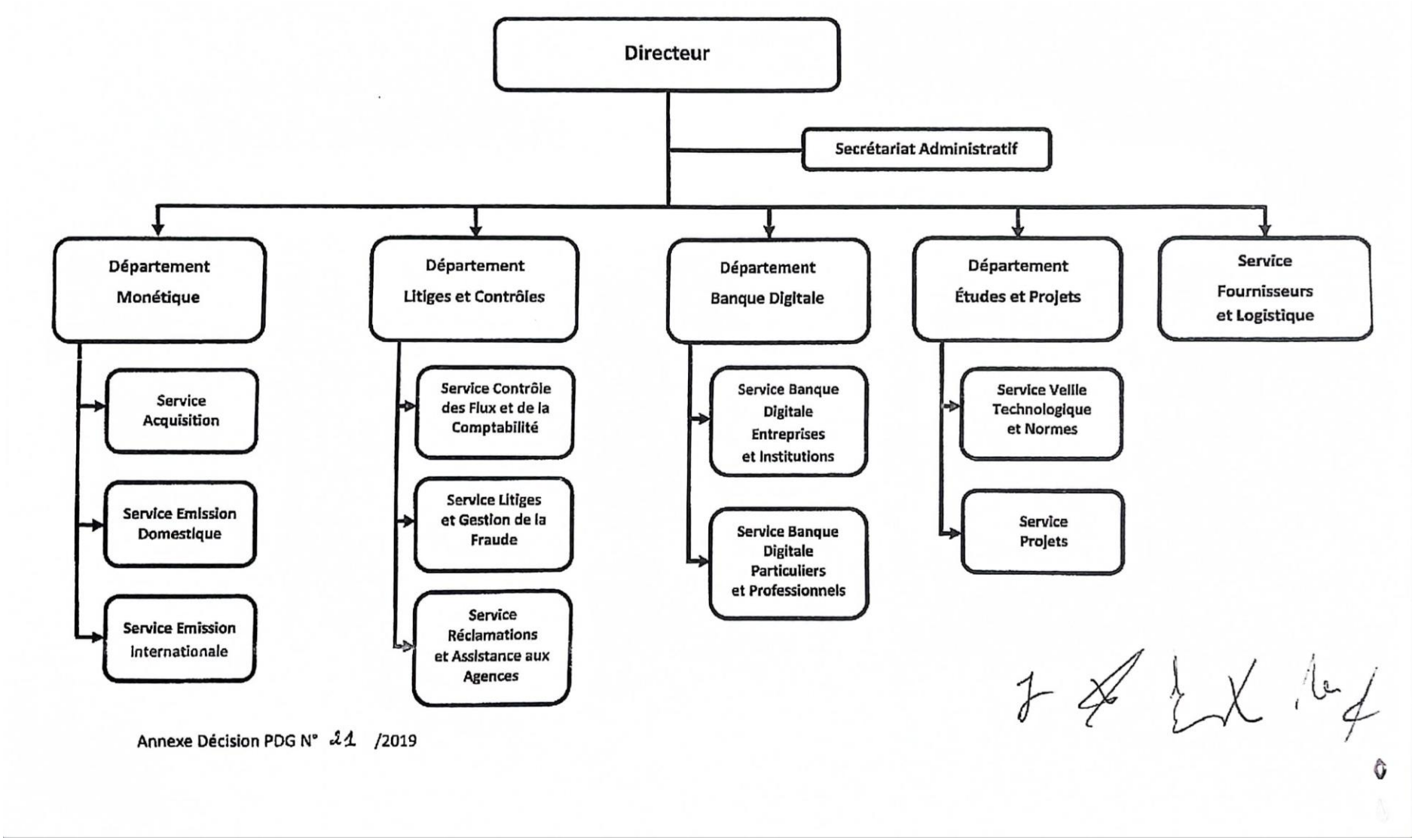
Source : Elaboré par nos soins

Annexe 02 : Organigramme de la Banque de Développement Local –BDL-

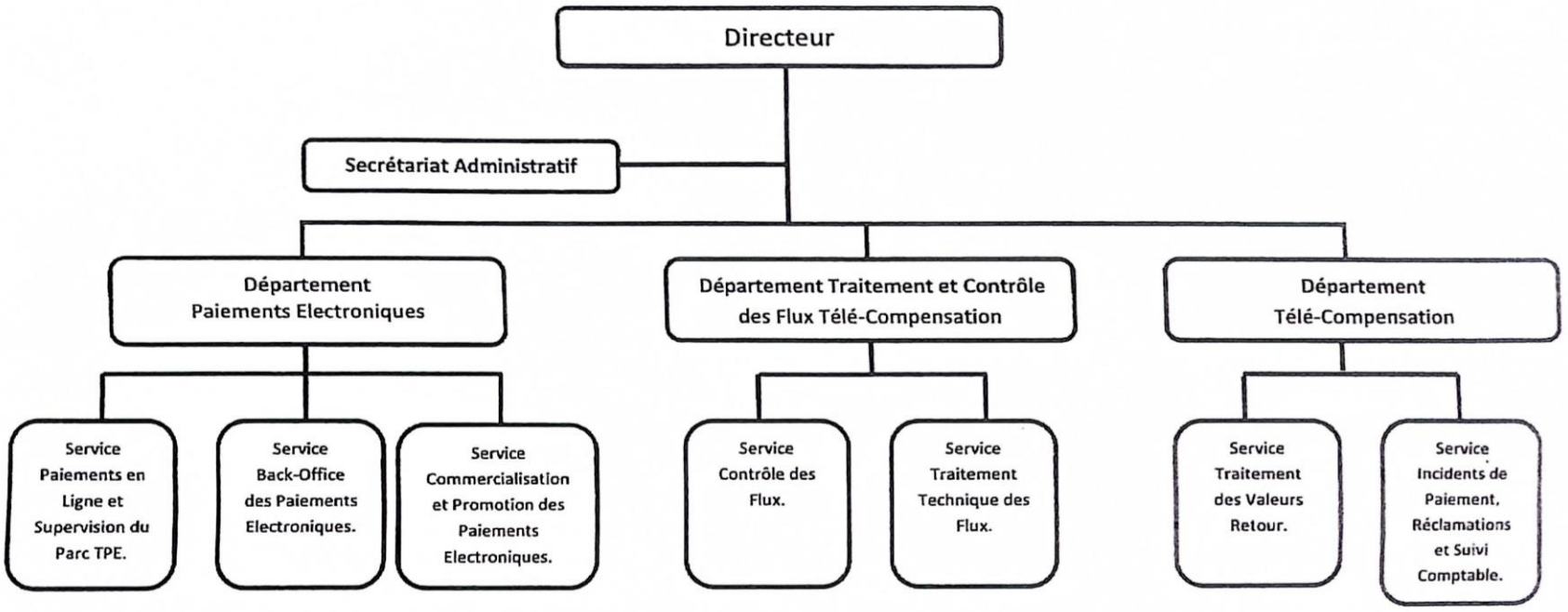


Annexe à la Décision DG n° 09 /2022

Annexe 03 : Organigramme de la Direction Monétique et Banque Digitale DMBD



Annexe 04 : Organigramme de la Direction des Moyens de Paiement DMP



Annexe à la Decision DG n° 59 /2022.

Annexe 05: Questionnaire pour la Cartographie des Risques liés aux Cartes Domestiques/Internationales

Je vous prie de bien vouloir répondre à ce questionnaire afin de m'aider à bien concevoir la cartographie.

1. **Nombre de Cartes Émises :**
   - Combien de cartes domestiques qui sont émises par la BDL en 2023 ? ……...
   - Combien de cartes domestiques qui sont émises par la BDL ? …… (en global)

2. **Taux d'utilisation des Cartes :**

- Quel pourcentage des clients qui utilisent régulièrement leur carte bancaire ? ……%

3. **Fréquence d'utilisation :**

- Combien de transactions par carte sont effectuées en moyenne par mois ? ……

4. **Type de Transactions Courantes :**

- Retraits aux distributeurs automatiques (DAB)

☐Oui

☐Non

- Paiements sur TPE

☐Oui

☐Non

- Transactions en ligne (e-commerce)

☐Oui

☐Non

5. **Historique des Incidents :**

- Avez-vous connaissance d'incidents antérieurs liés aux cartes bancaires (fraudes, utilisations non autorisées) ?

☐Oui

☐Non

- Si oui, veuillez fournir une brève description :

  ……
  ……

6. **Mesures de Sécurité Mises en Place :**

- Authentification forte (ex : code PIN, mots de passe à usage unique)

☐Oui

☐Non

- Vérification systématique des transactions suspectes

☐Oui

☐Non

- Autres mesures (préciser) : ……

7. Sécurité des Transactions en Ligne :

- Utilisez-vous des protocoles de sécurité spécifiques pour les transactions en ligne?

☐Oui

☐Non

Si oui, veuillez fournir une brève description :

……

……

- Avez-vous mis en place des systèmes de détection de fraudes en temps réel pour les transactions en ligne ?

☐Oui

☐Non

8. Formation et Sensibilisation :

- Le personnel et les clients sont-ils sensibilisés aux bonnes pratiques de sécurité liées aux cartes bancaires ?

☐Oui

☐Non

Si oui, comment sont-ils informés et à quelle fréquence ?

……

……

9. En tant qu'employé dans ce service, quels sont les risques auxquels vous êtes confrontés :

……

……

……

……

……

10. Selon votre expérience, quelle serait la cause des risques mentionnés en dessus :

☐ Mode de travail (processus)

☐ Facteurs humains

☐ Moyens nécessaires

☐ Facteurs externes

☐ Système d'informations

11. Évaluation globale des risques (échelle de 1 à 4, 1 étant le risque le plus faible, 4 le plus élevé) :

- Risque lié aux fraudes : ……
- Risque lié à la sécurité des transactions en ligne : ……..
- Risque global des cartes domestiques : …….

12. Survenance des risques (échelle de 1 à 4, 1 étant le moins fréquent, 4 le plus fréquent)

- Risque lié aux fraudes : ……
- Risque lié à la sécurité des transactions en ligne : ……..

Merci de prendre le temps de remplir ce questionnaire. Vos réponses seront précieuses pour évaluer et gérer les risques associés aux cartes domestiques /Internationales.

Annexe 06 : Questionnaire pour la Cartographie des Risques liés aux DAB

1. **Identification du DAB :**

- Combien de DAB que la BDL a-t-elle installé en 2023 ? .....
- Le parc DAB de la BDL est composé de combien de DAB ?.....
- Combien de DAB que la BDL a-t-elle installé et qui acceptent la Mastercard ? .....

2. **Fréquentation et Affluence :**

- Combien de transactions sont effectuées en moyenne par jour ? ……
- Les transactions sont-elles concentrées à certaines heures de la journée ? (Si oui, précisez)

  ……

  ……

3. **Accessibilité et Proximité :**

- Le DAB est-il situé dans une zone à risque particulier (ex : quartier sensible) ?

☐Oui

☐Non

- Y a-t-il des caméras de surveillance à proximité des DAB ?

☐Oui

☐Non

4. **Historique des Incidents :**

- Avez-vous connaissance d'incidents antérieurs (vols, tentatives de fraude, vandalisme) liés à ces DAB ?

☐Oui

☐Non

- Si oui, veuillez fournir une brève description :

  ……

  ……

  ……

5. **Maintenance et Surveillance :**

- À quelle fréquence le DAB est-il inspecté pour s'assurer de son bon fonctionnement et de son intégrité ?

……
……..

- Le DAB est-il surveillé par un agent de sécurité ou par des caméras de surveillance en temps réel ?

☐Oui

☐Non

6. Mesures de Sécurité Mises en Place :

- Quelles mesures de sécurité spécifiques sont mises en place pour protéger ces DAB (ex : alarmes, dispositifs de verrouillage, etc.) ?

……
……..

7. Formation et Sensibilisation :

- Les utilisateurs sont-ils informés des bonnes pratiques de sécurité lorsqu'ils utilisent ces DAB ?

☐Oui

☐Non

- Si oui, comment sont-ils informés ?

……
……

8. En tant qu'employé dans ce service, quels sont les risques auxquels vous êtes confrontés :

……
……
……
……
……

9. Selon votre expérience, quelle serait la cause des risques mentionnés en dessus :

☐ Mode de travail (processus)

☐ Facteurs humains

☐ Moyens nécessaires

☐ Facteurs externes

☐ Système d'informations

10. **Évaluation Globale du Risque (échelle de 1 à 4, 1 étant le risque le plus faible, 4 le plus élevé) :**

- Risque lié à la sécurité physique : ……
- Risque lié à la sécurité des transactions : ……
- Risque lié à l'environnement immédiat : ……
- Risque global lié au DAB: ……

11. **Survenance du Risque (échelle de 1 à 4, 1 étant le risque le moins fréquent, 4 le plus fréquent) :**

- Risque lié à la sécurité physique : ……
- Risque lié à la sécurité des transactions : ……
- Risque lié à l'environnement immédiat : ……

Merci de prendre le temps de remplir ce questionnaire. Vos réponses seront précieuses pour évaluer et gérer les risques associés au DAB.

Annexe 07 : Questionnaire pour la Cartographie des Risques liés aux TPE

Je vous prie de bien vouloir répondre à ce questionnaire afin de m'aider à bien concevoir la cartographie.

1. Identification du TPE :

- Combien de TPE que la BDL a-t-elle installé en 2023 ? .....
- Combien de TPE que la BDL a-t-elle installé ? ..... (en global)

2. Fréquentation et Utilisation :

- Combien de transactions sont effectuées en moyenne par jour sur ce TPE ?.....
- Le TPE est-il principalement utilisé par des clients ou par des employés ?

☐Clients

☐Employés

3. Historique des Incidents :

- Avez-vous connaissance d'incidents antérieurs liés à ce TPE (fraudes, dysfonctionnements, tentatives d'intrusion) ?

☐Oui

☐Non

- Si oui, veuillez fournir une brève description :

  ……
  ……..

4. Accessibilité et Sécurité Physique :

- Le TPE est-il situé dans un endroit sécurisé (ex : salle verrouillée) ?

☐Oui

☐Non

- Y a-t-il des caméras de surveillance à proximité du TPE ?

☐Oui

☐ Non

- Le TPE est-il protégé contre les accès non autorisés (ex : badge, code d'accès) ?

☐Oui

☐Non

5. Maintenance et Mises à Jour :

- À quelle fréquence le TPE est-il inspecté et mis à jour pour garantir son bon fonctionnement et sa sécurité ?

……
……..

- Qui est en charge de la maintenance du TPE ?

……

6. Protection des Transactions :

- Quelles mesures de sécurité sont en place pour protéger les transactions (ex : chiffrement, certificats SSL) ?

-

……
……..

-

……
……..

7. Sécurité des Données :

- Comment sont stockées et sécurisées les données sensibles (ex : numéros de cartes bancaires) ?

……
……..

8. Formation et Sensibilisation :

- Les utilisateurs et le personnel sont-ils formés sur les bonnes pratiques de sécurité en lien avec ce TPE ?

☐Oui

☐Non

- Si oui, comment sont-ils formés et à quelle fréquence ?

……
……

9. En tant qu'employé dans ce service, quels sont les risques auxquels vous êtes confrontés :

……

……

……

……

……

10. **Selon votre expérience, quelle serait la cause des risques mentionnés en dessus :**
    - ☐ Mode de travail (processus)
    - ☐ Facteurs humains
    - ☐ Moyens nécessaires
    - ☐ Facteurs externes
    - ☐ Système d'informations
11. **Évaluation Globale du Risque (échelle de 1 à 4, 1 étant le risque le plus faible, 4 le plus élevé) :**

- Risque lié à la sécurité physique : …….
- Risque lié à la sécurité des transactions : …….
- Risque lié à la protection des données :.....
- Risque global : ……..

12. **Survenance du Risque (échelle de 1 à 4, 1 étant le risque le moins fréquent, 4 le plus fréquent) :**

- Risque lié à la sécurité physique : ……
- Risque lié à la sécurité des transactions : ……
- Risque lié à l'environnement immédiat : ……

Merci de prendre le temps de remplir ce questionnaire. Vos réponses seront précieuses pour évaluer et gérer les risques associés aux Terminaux de Paiement Électronique (TPE).

Annexe 08 : Contrat Carte Interbancaire de Paiement CI

بنك التنمية المحلية

BANQUE DE DEVELOPPEMENT LOCAL

CONTRAT
CARTE INTERBANCAIRE DE PAIEMENT

SUCCURSALE : _____ **AGENCE :** _____ **CODE :** _____

N° du contrat _____ **Date** _____

Type de carte : Retrait paiement classique ☐ **Retrait paiement Gold** ☐

Titulaire du compte

Je soussigné(e) Mr, Mme, Melle (1) : Nom _____ et prénoms _____
Raison sociale : _____
Adresse du domicile : _____
Commune _____
Daira _____
Wilaya _____
Code postal : _____ Ville _____ Tél _____

Compte n° |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

Nature du compte : Particulier ☐ Société ☐

Date d'ouverture : _____
Date d'expiration : _____
Salaire mensuel ou chiffre d'affaires: _____
Sollicite de la banque la délivrance d'une carte interbancaire de paiement et reconnais avoir pris connaissance des conditions générales de fonctionnement de la carte de paiement et y adhère sans réserve

à mon nom ☐ au nom du porteur ci-après désigné ☐

Titulaire de la carte

Mr, Mme, Melle (1) : Nom _____ et prénoms _____
Date et lieu de naissance : _____ à _____ Wilaya _____
Profession : _____ tel _____
Adresse : _____ Code postal : _____
Commune : _____ Daira : _____ wilaya : _____
Plafond hebdomadaire de retrait : _____ DA)
Plafond hebdomadaire de paiement : _____ DA) à la date de signature du contrat
Montant limite des paiements sur TPE en off line : _____ DA
Limite de toutes les transactions : _____ DA

N° de la carte : |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|

(1) Rayer la mention inutile

Annexe 09 : Contrat de souscription Cartes VISA & MASTERCARD

بنك التنمية المحلية
BANQUE DE DEVELOPPEMENT LOCAL

CONTRAT DE SOUSCRIPTION CARTES
VISA & MASTERCARD

Informations Obligatoires Sur Le Titulaire du Compte N° de Contrat :

Date de souscription : ___/___/_____ Agence : _____ Code : _____

Pôle Commercial : _____ Code Pôle : _____

Nom (Mr / Mme) : _____ Prénom : _____

Adresse : _____ Commune : _____

Daïra : _____ Wilaya : _____ Code Postal : _____

N° de Téléphone Mobile : _____ Adresse Mail : _____

N° Identifiant : _____

N° de Compte Devise : _____ N° Compte Dinars : _____

Nature de client : Domicilier : ◯ Passager : ◯ Société : ◯

Informations Obligatoires sur le Titulaire de La Carte et les Clients de Passage

Nom du Porteur : _____ Prénom du porteur : _____

N° Pièce d'identité : CNI/PC : _____ Date de création : _____

Lieu de délivrance : _____ Date et lieu de naissance : _____

N° de Téléphone mobile porteur : _____ Adresse Mail : _____

Informations sur le type de carte souhaité

Electron classique : ◯ VISA Gold : ◯ Plafonds : _____€	Prépayée : ◯ Titanium : ◯ Platinium : ◯ mastercard. Plafonds : _____€

Information Obligatoires sur la Sécurité de votre carte

La saisie du numéro de Téléphone Mobile est obligatoire afin de bénéficier du paiement en ligne et le service SMS associés pour renforcer la sécurité de vos achats sur les sites internet affichant le logo « Verified by Visa » (3D-Secure).

☐ Je m'engage à utilisez ma carte seulement sur les réseaux internet sécurisés (https), si je l'utilise sur les sites dont l'adresse n'est pas sécurisée (http) La Banque du Développement Local décline toute responsabilité sur les débits frauduleuse sur ma carte.

☐ Je soussigné le présent contrat à l'adhésion du service VISA & MasterCard de la Banque du Développement Local sous les conditions générales et particuliers indiquées dans les pages qui suivent ci-après, dont je reconnais avoir pris connaissance.

Annexe 10 : Engagement d'utilisation de TPE

ENGAGEMENT

Je soussigne Mr ....., titulaire du numéro de compte ....., domicilié au sein de l'Agence..... « Code :..... », ayant signé un contrat de souscription pour bénéficier d'un Terminal de Paiement Electronique « TPE » en date du.....

Je m'engage à :

- Utiliser le Terminal de Paiement Electronique « TPE » qui sera installé par la Banque de Développement Local au niveau de mon local ;
- Maintenir l'appareil en service pendant les horaires de l'exercice de mon activité;
- Accepter le TPE pour le règlement des transactions de paiement par Carte Interbancaire « CIB » et/ou la Carte « Eddahabiya » avec une moyenne minimale de 20 transactions par mois.
- Veiller au bon entretien du TPE.
- Maintenir le TPE visible et indiqué.

Et **J'autorise** la Banque **à récupérer** le TPE mis à ma disposition en cas de non-utilisation de ce dernier dans **un délai de trois « 03 »mois** à compter de la date de son installation à mon niveau et ce conformément aux articles 06 et 07 du contrat d'adhésion au système de paiement par Carte Interbancaire et « Eddahabiya », signé avec la Banque lors de l'introduction de la commande du TPE.

Signatures et cachets :

Le commerçant : **La Banque**

(Écrire la mention manuscrite « Lu et approuvé »)

Résumé :

Ce mémoire s'articule autour de l'élaboration d'une cartographie des risques associés au processus monétique et aux dispositifs DAB/GAB/TPE, en mettant en lumière plusieurs aspects cruciaux et en se focalisant sur trois axes majeurs.

Le premier axe explore le cadre général des Risques Opérationnels (RO), offrant une compréhension approfondie de leurs bases conceptuelles et des normes qui les encadrent. Une attention particulière est portée aux principes fondamentaux de la cartographie des RO, mettant en lumière ses méthodologies et outils essentiels, ainsi que les motivations, obstacles, et facteurs clés de succès liés à cette démarche.

Le deuxième axe se concentre sur la monétique, offrant un aperçu spécifique de la situation en Algérie. Cette section analyse les développements clés de la monétique dans le pays, identifiant les acteurs principaux et mettant en évidence les risques spécifiques associés à ce secteur en constante évolution.

Enfin, le troisième axe présente un cas pratique axé sur l'élaboration d'une cartographie des risques au sein de la Banque de Développement Local (BDL). Il détaille la méthodologie utilisée, pour la détermination des risques opérationnels du processus monétique à la proposition de mesures de maîtrise des risques, offrant ainsi des recommandations concrètes pour renforcer la résilience du processus monétique et des dispositifs DAB/GAB/TPE.

Ce mémoire offre ainsi une approche holistique, combinant la théorie sur les RO et la monétique avec une étude de cas pratique au sein de la BDL. L'objectif est de fournir des recommandations tangibles et applicables pour la gestion efficace des risques dans le domaine complexe de la monétique.

Mots clés :

Cartographie, risque, opérationnel, monétique, impact, fréquence, cartes, DAB, TPE.

Abstract:

This thesis centers on the creation of a comprehensive risk map associated with the electronic payment process and ATM/EPT devices. Recognizing the dynamic landscape of electronic transactions, the study unfolds in several key dimensions.

The initial section navigates through the foundational aspects of operational risks, delineating a thorough understanding of their conceptual framework and the governing standards. Emphasis is placed on elucidating the core principles of risk mapping, outlining methodologies, crucial tools, and exploring the motivating factors, obstacles, and key success elements integral to this strategic approach.

The subsequent focus turns to the domain of electronic payments, spotlighting its critical role in the contemporary financial landscape. Special attention is devoted to scrutinizing the nuances of electronic payment processes, unveiling pivotal developments, and spotlighting potential risks that emerge in this rapidly evolving sphere.

The culmination of the thesis presents a practical application of the developed risk mapping within a specific context, perhaps a financial institution or an organization actively engaged in electronic transactions. This practical case study details the methodology employed, encompassing the identification of operational risks within the electronic payment process and the proposal of risk mitigation strategies. The intent is to furnish tangible recommendations aimed at fortifying the resilience of both the electronic payment process and the associated ATM/EPT devices.

In essence, this thesis endeavors to provide a holistic framework that seamlessly blends theoretical insights into operational risks and electronic payments with a pragmatic application. The ultimate objective is to deliver actionable recommendations for adept risk management in the intricate realm of electronic payments and associated technologies.

Keys words:

Risk mapping, risk, operational, electronic banking, impact, frequency, card, ATM, EPT.

Table des matières :