



2022

## Manuel de Procédure Interne LAB-FT



## I. Objet

Le présent **manuel de Procédure (ou le Livre Blanc)** décrit l'ensemble des principes, règles, normes, procédures et bonnes pratiques relatives à la lutte contre le Blanchiment d'Argent, Financement du Terrorisme et prolifération des Armes de Destruction massive.

Il a pour but de guider, accompagner l'ensemble des collaborateurs de la BH Bank, afin d'appréhender les risques et les enjeux de ce phénomène et adopter les mesures adéquates pour le combattre ou du moins l'atténuer. Il rassemble les Notes Organiques, Notes de Service, Directives de la CTAF, Codes, Chartes ainsi que, toutes dispositions normatives en rapport avec le sujet.

Il est rédigé conformément à la décision 2017-02 du 2 Mars 2017 de la CTAF, engageant les institutions financières à élaborer un **manuel de procédures interne**.

## II. Cadre réglementaire

Le cadre juridique national de lutte contre le blanchiment des capitaux comprend des dispositions figurant dans plusieurs lois, notamment dans le code pénal, le code de procédure pénale, ainsi que la **loi n° 2015-26 du 7 août 2015** relative à la lutte contre le terrorisme et à la répression du blanchiment d'argent.

### 1. Lois

- **Loi organique n°2015-26 du 7 août 2015**, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent.
- **La loi bancaire n°2016-48 du 11 juillet 2016** relative aux banques et aux établissements financiers.
- **La loi n°2018-52 du 29 octobre 2018** relative au registre national des entreprises.
- **Loi organique n° 2019-9 du 23 janvier 2019**, modifiant et complétant la **loi organique n° 2015-26 du 7 août 2015**, relative à la lutte contre le terrorisme et la répression du blanchiment d'argent).
- 

### 2. Décrets

- **Décret n°2014-3833 du 3 octobre 2014** portant fixation de la liste des paradis fiscaux concernés par les dispositions de l'article 44 de la loi n°2013-54 du 30 décembre 2013, portant loi de finances pour l'année 2014.
- **Décret Gouvernemental n°2018-1 du 4 janvier 2018** portant sur les procédures de mise en œuvre des résolutions prises par les instances onusiennes compétentes liées à la répression du blanchiment d'argent.
- **Décret gouvernemental n°2019-54 du 21 janvier 2019**, fixant les critères et les modalités d'identification du bénéficiaire effectif.
- **Décret gouvernemental n°2019-419 du 17 mai 2019**, relatif aux procédures de mise en œuvre des résolutions prises par les instances onusiennes compétentes liées à la répression du financement du terrorisme et de la prolifération des armes de destruction massive, tel que modifié par le **décret gouvernemental n°2019-457 du 31 mai 2019**.

### 3. Arrêtés

- **Arrêté de la ministre des finances du 19 janvier 2017**, portant visa du règlement du conseil du marché financier relatif aux mesures pratiques pour la répression du blanchiment d'argent, la lutte contre le financement du terrorisme et la prolifération des armes, tel que modifié par l'**arrêté du ministre des finances du 6 mars 2018**.
- **Arrêté du ministre des finances du 24 Juillet 2019** modifiant l'**arrêté du 1er Mars 2016** portant fixation des montants prévus aux articles 100, 107, 108, 114 et 140 de la

loi n°26-2015 du 07 août 2015 relative à la lutte contre le terrorisme et la répression du blanchiment d'argent.

#### 4. Circulaires

- **La Circulaire N°2017-08** relative à la mise en place des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme. Cette circulaire a commencé par la consécration de l'approche basée sur les risques comme moyen d'allocation optimale des ressources pour la gestion des risques de blanchiment d'argent et de financement du terrorisme
- **La circulaire BCT N° 2018-09** relative à la mise en place des règles de contrôle interne pour la gestion du risque de blanchiment d'argent et de financement du terrorisme.
- **La Circulaire BCT N°2021-05** relative au cadre de gouvernance des banques et des établissements financiers.

#### 5. Décisions

- **Décision de la CTAF n°2017-01 du 2 mars 2017** portant principes directeurs relatifs à la déclaration des opérations et transactions suspectes.
- **Décision de la CTAF n°2017-02 du 2 mars 2017** portant principes directeurs relatifs à la déclaration des opérations et transactions suspectes.
- **Décision de la CTAF n°2018-10 du 8 juin 2018** qui modifie et complète la décision n°2017-03 du 2 mars 2017 relative aux bénéficiaires effectifs.
- **Décision de la CTAF n°2018-12 du 30 mai 2018** portant principes directeurs des organismes à but non lucratif.

#### 6. Notes internes

- **Note Organique n°06-2021** relative à l'organisation, missions et attributions de la Direction Centrale de la Conformité, du Contrôle Permanent et de la Sécurité financière.
- **Note de Procédure n°630010** relative à la prévention du Blanchiment d'Argent et du Financement du Terrorisme.
- **Note de Procédure n°100020** relative à l'entrée en Relation et création d'un client dans la BDC.
- **Note de Procédure n°100040** relative à l'ouverture de Compte et Conservation du dossier juridique du client.
- **Note de Procédure n°133010** relative au paiement des ordres de transferts reçus des partenaires de transferts électroniques de fonds (MSB).
- **Note de Procédure n°630020** relative à l'identification et déclaration des données FATCA.
- **Note de Service N°08-2018** relative à la mise en Place de la Solution SIRON KYC-FATCA.
- **Note de Service n°21-2018** relative à l'entrée en relation avec les correspondants étrangers et les organismes internationaux de transfert d'Argent.
- **Note de Service n°93-2018** relative à l'identification des Bénéficiaires Effectifs.
- **Note de Service n°17-2019** relative au traitement des décisions onusiennes et nationales de gel des avoir des clients.
- **Note de Service n°52-2020** rappelant des vérifications requises lors de l'exécution des opérations effectuées sur les comptes de la clientèle.
- **Note de Service n°59-2020** relative à la détection et déclaration des opérations suspectes.
- **Note de Service n°15-2022** relative à la connaissance des prestataires de biens ou services sous l'angle LAB/FT « KYP ».

### III. Définitions des concepts

- **Blanchiment d'argent :** Selon les dispositions de l'**Article 92 de la Loi 2015-26** : Est considéré blanchiment d'argent, tout acte intentionnel qui vise par tout moyen à la justification mensongère de l'origine illicite des biens meubles ou immeubles ou des revenus résultant directement ou indirectement de tout crime ou délit passible d'une peine d'emprisonnement de trois années ou plus ainsi que tout délit sanctionné en vertu du code des douanes.  
Constitue également un blanchiment de biens, tout acte intentionnel ayant pour but le placement, dépôt, dissimulation, administration, intégration ou conservation du produit résultant directement ou indirectement d'un délit ou crime répondant aux critères ci-dessus mentionnés.  
Est, aussi, considéré comme blanchiment d'argent toute tentative, participation, incitation, facilitation, aide ou concours à la réalisation de ces opérations.
- **Financement de terrorisme :** est considéré comme financement du terrorisme toute forme de soutien et de financement aux personnes, organisations ou activités en rapport avec des infractions terroristes et autres activités illicites qu'ils leur soient octroyés de manière directe ou indirecte.
- **Actionnaire ou associé important :** l'actionnaire ou l'associé qui détient *10% ou plus du capital* du client personne morale. (**L'article 2 de la circulaire N°2017-08 du 19 septembre 2017, telle que modifiée par la circulaire n°2018-09 du 18 octobre 2018**).
- **Bénéficiaire effectif :** Selon l'**alinéa 2 de l'article 2 de la circulaire N°2018-09** : la ou les personnes physiques qui détient(nent), *directement ou indirectement, plus de 20 % du capital ou des droits de vote* de la personne morale ou de la construction juridique et d'une manière générale toute personne physique qui en dernier lieu possède ou exerce un contrôle effectif sur le client ou pour le compte de laquelle l'opération est effectuée.
- **PPE :** Selon l'**Alinéa 3 de l'article 2 (nouveau) de la circulaire N°2018-09** : « Personnes Politiquement Exposées » : les personnes tunisiennes ou étrangères qui exercent ou qui ont exercé, des hautes fonctions publiques ou des missions représentatives ou politiques en Tunisie ou à l'étranger et les personnes qui exercent ou qui ont exercé d'importantes fonctions au sein de /ou pour le compte d'une organisation internationale et notamment :
  - ✓ Chef d'État, Chef du gouvernement ou membre d'un gouvernement,
  - ✓ Gouverneurs,
  - ✓ Membre d'un parlement, les élus nationaux et régionaux,
  - ✓ Membre d'une cour constitutionnelle ou d'une haute juridiction,
  - ✓ Membre d'une instance constitutionnelle,
  - ✓ Officier militaire supérieur,
  - ✓ Ambassadeur, chargé d'affaires ou consul,
  - ✓ Membre de collèges ou de conseils d'administration des autorités de contrôle et de régulation ainsi que les premiers responsables de ces autorités,
  - ✓ Membre d'un organe d'administration, de direction ou de contrôle d'une entreprise publique,

- ✓ Membre des organes de direction ou du conseil d'une institution internationale créée par traité ou le premier responsable de sa représentation,
- ✓ Haut responsable d'un parti politique,
- ✓ Membre des organes de direction d'une organisation syndicale ou patronale.

Sont également considérés comme des PPE :

- ✓ Les membres directs de leur famille, les descendants et les descendants, au premier degré ainsi que leurs conjoints.
- ✓ Les personnes ayant des rapports étroits avec eux, qu'elles soient de nationalité tunisienne ou étrangère : toute personne physique connue comme entretenant avec les PPE des liens d'affaires étroits.
- **KYC (Know Your Customer)** : ou connaissance du client, est le nom donné au processus permettant de vérifier l'identité des clients. Le processus Know Your Customer est utilisé afin de s'assurer de la conformité des clients face aux législations anti-corruption ainsi que pour vérifier leur probité et intégrité. Cela a également pour but de prévenir l'usurpation d'identité, la fraude fiscale, le blanchiment d'argent et le financement du terrorisme. Ce processus se fait typiquement par collecte et analyse de données, vérification de la présence sur les listes de sanctions, l'analyse du comportement et des transactions, etc...
- **KYP (Know Your Provider)** : ou connaître son partenaire ou fournisseur est le nom donné au processus de l'identification du partenaire ou fournisseur personne physique et personne morale auprès de laquelle la banque réalise des achats de biens et services pour son activité.
- **KYE (Know Your Employee)** ou connaître son employé est le nom donné au processus d'identification des employés de la banque notamment au moment de recrutement.
- **Sources fiables et indépendantes** : Autorités officielles centrale ou locales ou établissements financiers établis dans un pays appliquant de manière suffisante les normes internationales de répression du blanchiment d'argent et de lutte contre le financement du terrorisme.
- **Relation d'affaires**: Est nouée lorsque la Banque et son client concluent un contrat en exécution duquel plusieurs opérations successives seront réalisées entre eux pendant une durée déterminée ou indéterminée, ou qui crée des obligations continues et peut faire l'objet d'une convention d'ouverture de compte. En l'absence d'une telle convention, une relation d'affaires est également nouée lorsqu'un client sollicite de manière régulière et répétée l'intervention de la Banque pour la réalisation d'opérations financières. En effet, un client occasionnel est considéré comme une relation d'affaires lorsqu'il effectue trois opérations occasionnelles au moins pendant une trimestre (Dix opérations au moins par an) ou dont le montant total par trimestre effectué en une opération ou en plusieurs opérations, est supérieur ou égal à 25 000 dinars (opération supérieure ou égale à 100 000 dinars par an réalisée d'une manière unitaire ou cumulée).
- **Client passager ou occasionnel** : est défini comme étant toute personne physique ou morale qui réalise une opération sans avoir de relation contractuelle ou habituelle avec la banque. Il s'agit de personnes physiques ou morales ne disposant pas de comptes ouverts dans les livres de la banque et qui, plus généralement, n'ont pas recourt de manière régulière aux produits et services offerts par la banque mais ils peuvent réaliser des opérations ponctuelles ne dépassant pas trois fois par trimestre

et dont le montant total, unitaire ou cumulé sur l'année est plafonné à 100 000 dinars et également limitée à dix (10) opérations par an.

- **Banque Intermédiaire** : toute banque qui, dans une série ou dans une chaîne de paiement de couverture, reçoit et transmet un virement électronique pour le compte de l'établissement du donneur d'ordre et de l'établissement du bénéficiaire ou une autre banque intermédiaire.
- **Virement électronique de fonds** : toute opération effectuée par voie électronique pour le compte d'un donneur d'ordre via une institution financière nationale ou étrangère, y compris les prestataires de transfert de fonds, en vue de mettre des fonds à la disposition d'un bénéficiaire par l'intermédiaire d'une autre institution financière. Le donneur d'ordre et le bénéficiaire peuvent être ou non la même personne.
- **Numéro de référence unique d'opération** : une combinaison de lettres, de chiffres ou de symboles qui est définie conformément aux protocoles des systèmes de paiement et de règlement ou des systèmes de messagerie utilisés pour effectuer le virement de fonds et qui assure la traçabilité de la transaction jusqu'au donneur d'ordre et au bénéficiaire.
- **Donneur d'ordre** : toute personne qui autorise un virement de fonds à partir d'un compte ou, en l'absence de ce compte, donne un ordre de virement de fonds.
- **Bénéficiaire** : la personne qui est le destinataire prévu du virement de fonds.
- **Virement qualifié** : tout virement transfrontalier de fonds d'un montant supérieur à la contrevaleur de 1000 dinars.
- **Banque fictive** : toute banque qui a été constituée et agréée dans un pays où elle n'a pas de présence physique et qui n'est pas affiliée à un groupe financier réglementé soumis à une surveillance consolidée et effective. L'expression « présence physique » désigne la présence d'une direction et d'un pouvoir de décision dans un pays. La simple présence d'un agent local ou de personnel subalterne ne constitue pas une présence physique. Cette définition ne s'applique pas à la banque qui ne dispose pas de siège fixe dès lors qu'elle est rattachée à une banque dûment agréée qui dispose d'une présence physique et qui est soumise à un contrôle effectif.
- **Opération ou transaction suspecte** : Est considérée suspecte, toute opération ou transaction susceptible d'être liée directement ou indirectement au produit d'actes illicites qualifiés par la loi de délit ou crime, ou au financement de personnes, organisations ou activités en rapport avec des infractions terroristes, ainsi que sur toute tentative desdites opérations ou transactions.
- **Opération inhabituelle** : Sont considérées inhabituelles, les opérations et transactions revêtant un caractère complexe ou d'un montant anormalement élevé ainsi que les opérations et transactions inhabituelles dont le but économique ou la licéité n'apparaissent pas manifestement (**Article 126 de la Loi 2015-26**).
- **Déclaration de soupçon** : La déclaration d'opérations suspectes permet d'alerter les autorités sur la possibilité qu'une transaction particulière puisse être liée au blanchiment de capitaux et qu'elle mérite par conséquent de faire l'objet d'une enquête approfondi.
- **La Commission Tunisienne des Analyses Financières (CTAF)**, instituée auprès de la Banque Centrale de Tunisie, est chargée de la centralisation et du traitement des déclarations se rapportant aux opérations suspectes parvenues des établissements bancaires.

- **Groupe d'Action Financière (GAFI)** : un organisme intergouvernemental ayant notamment pour objectifs l'élaboration de normes et la promotion de politiques relatives à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme.
- **Le filtrage dynamique en temps réel ou en différé** : correspond à filtrer des noms des personnes ou des sociétés titulaires de transactions de transferts nationaux ou internationaux par rapport à des listes nationales et internationales.
- **Le profilage** : correspond à la détection des opérations inhabituelles ou suspectes provenant des différents traitements générés par les applications de la banque se fait sur la base de différents scénarios paramétrés.
- **GoAML** : Une plateforme professionnelle dédiée à l'activité déclarative et analytique des risques de blanchiment des capitaux et de financement du terrorisme qui a été adoptée à ce jour par plusieurs Cellules de Renseignement Financier (CRF) dans le monde.

L'application GoAML est une solution logicielle entièrement intégrée spécialement conçue pour les Cellules de Renseignement Financier (Financial Intelligence Unit « FIU ») et est l'une des réponses stratégiques de l'ONUDC pour lutter contre la criminalité financière, notamment contre le blanchiment d'argent et le financement du terrorisme. L'application GoAML est spécialement conçue pour répondre aux besoins des « FIU » en termes de collecte de données, gestion des flux / processus, analyses et élaboration de statistiques.

- **Vigilance approfondie à l'égard de la Clientèle (en anglais, Enhanced Due Diligence, ou, encore EDD)** : En lien avec la « due diligence » à l'égard de la clientèle, la vigilance approfondie implique des mesures complémentaires destinées à identifier et à réduire le risque présenté par les clients à haut risque. Selon **l'Article 17 de la circulaire N°2018-09**, les établissements assujettis doivent soumettre leurs relations d'affaires à une vigilance renforcée lorsqu'elles sont :

- ✓ Des associations notamment en matière d'identification des personnes agissant en leurs noms et d'analyse des transactions y afférentes.
- ✓ Des clients présentant un profil de risque élevé dans le cadre du profilage et du filtrage de la clientèle.
- ✓ Des clients jugés à risque élevé par référence à l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme.

En matière de contrôles anti-blanchiment d'argent, cela signifie la mise en place de politiques, de pratiques et de procédures adaptées permettant à la banque de prédire avec une relative certitude les types de transactions dans lesquelles un client est susceptible de s'engager. Une « due diligence » clients inclut non seulement d'établir l'identité des clients, mais également de surveiller l'activité du compte pour identifier les transactions qui ne sont pas conformes aux transactions standards ou prévisibles.

#### IV. L'approche par les risques

La réglementation anti-blanchiment préconise des mesures de vigilance fondées sur une analyse des risques. Cette approche peut s'appliquer également avec pertinence à d'autres réglementations bancaires. Alors que le coût de la mise en conformité ne cesse de s'elever, une approche transversale par les risques permet une allocation des ressources plus efficientes en tenant en compte des facteurs de risques tels que le profil des clients, les pays ou les zones géographiques, les produits, les services, les transactions ou les canaux de distribution (**Article 4 de la Circulaire BCT N°2018-09**).

L'approche par les risques exige que les risques soient identifiés, évalués et classés selon leurs

niveaux avant que des mesures d'atténuation soient mises en place : c'est la classification des risques. En fonction de cette classification, la banque détermine l'étendue des obligations de vigilance qui s'imposent à lui avant d'entrer en relation d'affaires.

Afin de limiter l'exposition de la Banque au risque de blanchiment d'argent et de financement du terrorisme de façon efficace, il faut adopter une approche basée sur les risques en suivant les étapes suivantes :

- L'identification des risques inhérents.
- La quantification des risques : C'est à partir d'une échelle simple établie dans le but de déterminer les zones les plus exposées afin de mesurer ensuite l'exposition de chaque entité au risque. Echelle de risque (Probabilité d'occurrence X).
- Le suivi des risques : identification des zones non suivies et détermination des indicateurs de suivi par type de risque.
- La maîtrise du risque : identification des mesures à mettre en place, renforcement du contrôle, détermination du niveau de tolérance maximale et les nouvelles orientations de maîtrise des risques à mettre dans les dispositifs existants.

Le risque de blanchiment d'argent et de financement du terrorisme est tributaire de ce qui suit :

- ✓ Le risque intrinsèque/inhérent (RI) à l'activité : la quantité de risque de blanchiment d'argent et de financement du terrorisme telle qu'identifiée par les facteurs de risque LAB/FT associés à la nature de l'activité à savoir la nature des clients servis, des produits et services utilisés, des zones géographiques et des canaux de distribution.
- ✓ L'efficacité du dispositif de contrôle mis en place : la qualité de contrôles mis en place pour atténuer les risques intrinsèques/inhérents.

La combinaison du risque inhérent et la qualité de contrôle donne ce qu'on appelle le risque résiduel. Ce dernier représente la cotation ultime du risque de blanchiment d'argent et de financement du terrorisme de la Banque.

L'efficacité du dispositif de lutte contre le blanchiment d'argent et le financement du terrorisme se base sur les préalables suivants :

- L'élaboration d'une cartographie des risques LAB/FT.
- La déclinaison, à partir de la cartographie des risques, d'une matrice d'évaluation des risques de LAB/FT.
- L'établissement d'un plan d'action afin de gérer les risques résiduels liés à la LAB/FT.

Généralement, toutes les catégories de risque peuvent être classifiées comme suit :

- ❖ Interdit ou sanctionné : La banque ne tolérera aucune négociation, quelle que soit, vu le risque.  
Les pays sujets à des sanctions économiques tels que la Corée du Nord, ou désignés en tant qu'États sponsors du terrorisme, tels que l'Iran, sont des candidats de premier ordre pour les transactions interdites. Les banques fictives figureraient parmi les clients interdits.
- ❖ Risque élevé : Ces risques sont significatifs, mais ne sont pas nécessairement interdits. Pour réduire le risque élevé qui se présente, la banque devrait appliquer des contrôles plus stricts, tels que mettre en place une vigilance clients renforcée et une surveillance des transactions plus rigoureuse. Les pays qui sont connus pour être corrompus, ou en lien avec le trafic de drogue, sont généralement réputés comme étant à risques élevés. Les clients à risques élevés peuvent inclure les Personnes Politiquement Exposées, les produits et services à haut risque peuvent inclure la banque correspondante et la banque privée.
- ❖ Risque modéré : Les risques modérés sont plus que des risques faibles ou des risques normaux en matière de blanchiment et méritent une surveillance supplémentaire, mais n'atteignent pas le niveau de risque élevé.
- ❖ Risque faible ou normal : Ceci représente le risque de référence du blanchiment de capitaux. Les règles de pratique courante s'appliquent. Les pays membres du GAFI et les clients nationaux de détail sont fréquemment, mais pas systématiquement, considérés comme de risque modéré ou faible.

### 1. Le facteur de risque « Profil des Clients »

La banque doit tenir compte de la nature et des activités de ses clients et des relations qu'elle entretient avec eux afin de déterminer le niveau de risque de blanchiment d'argent et le financement du terrorisme. Cela signifie qu'elle doit connaître ses clients pour effectuer une évaluation des risques. Connaître les clients ne se limite pas à vérifier leur identité ou à tenir des documents. Il s'agit de comprendre qui sont les clients, y compris les activités qu'ils exercent, le modèle de leurs opérations, comment ils gèrent leurs affaires, et ainsi de suite. Il convient de considérer les clients passagers ou occasionnels comme étant plus risqués que ceux connus.

Le facteur de risque « Profil des clients » se décompose comme suit :

- **Catégorie des clients** : Personnes Physiques, Personnes Morales (sociétés), Associations, Partis Politiques, Patrimoines d'affectation, Correspondants Bancaires, etc....
- **Types des clients**: Inventaire des clients personnes physiques (PPE, Non-résidents, Personnes Physiques résidente par domaine d'activités, etc...), Inventaire des personnes morales (non résidentes, multinationale, domestique publique, domestique privés : PME , Grandes Entreprises, Holding, etc..), et par domaine et nature d'activités (nature de services, nature d'industrie, nature de commerce, nature de conseil en patrimoines, etc...), Inventaire des Associations par vocation (œuvres caritatives, culturelles, scientifiques, religieuses, syndicat, développement, amicales,

mosquées, syndics de copropriétés, etc..., partis politiques, inventaire des fondations, des ONG, des groupements d'intérêt économique, des patrimoines d'affectation relevant d'un droit étranger tels que les trusts et les fiducies et autres constructions similaires, inventaire des correspondants bancaires, etc...).

Les types de clients peuvent se subdiviser à leur tour en sous types de clients (pays de résidence, nationalité, juridiction, structure juridique, etc....).

## 2. Le facteur de risque « Pays et Zones Géographiques Internes »

Certains pays localisés dans des pays et zones géographiques où le blanchiment de capitaux est considéré à haut risque. Toutefois, il n'existe aucun système définitif et indépendant pour évaluer les risques de blanchiment de capitaux des divers territoires et pays. Lorsque l'on considère le risque de blanchiment de capitaux, les listes des terroristes et de sanctions, publiées par les gouvernements et les organisations internationales, peuvent être un point de départ. Elles incluent des listes publiées par le régulateur du Royaume-Uni, l'U.S. Office of Foreign Assets Control, l'U.S. Financial Crimes Enforcement Network, l'Union Européenne, la Banque mondiale et le Comité du Conseil de Sécurité des Nations Unies. Un modèle de cotation devrait également considérer si le pays est un membre du GAFI ou d'une organisation de type GAFI et dispose d'obligations, en matière de LAB/FT, équivalentes aux meilleures pratiques internationales. Procéder à une veille médiatique des principaux journaux est également recommandé, et tout changement concernant toutes les listes de pays, devrait être surveillé. Ainsi, la qualité des lois et régulations anti-blanchiment, et la force du secteur financier peuvent être des facteurs déterminant le risque.

Le Facteur de risque « Pays » se décompose comme suit :

- **Catégorie :** Les pays se distinguent par le degré de risque décidé par le Groupe d'Action Financière GAFI. Ce dernier publie périodiquement ses listes qui sont répartis comme suit :
  - Pays à risque faible nécessitant une vigilance simplifiée en l'absence de soupçon.
  - Pays à risque moyen nécessitant une vigilance standard.
  - Pays à risque élevé nécessitant une vigilance renforcée pour les opérations financières concernant les clients et les établissements financiers provenant de ces pays tiers et ce, afin de mieux détecter les flux des capitaux suspects.
- **Types de Pays étrangers :** inventaire de tous les pays concernés par l'activité de la banque et de ses clients (pays n'ayant jamais figuré sur les listes du GAFI, Pays ne faisant plus partie des juridictions sous surveillance du GAFI, Pays sous surveillance du GAFI ou ne faisant plus partie des juridictions à haut risque et non coopératives ou centres financiers offshores ou paradis fiscaux, pays classés par le GAFI à haut risque et non coopératifs et Pays soumis à des sanctions, des embargos ou des mesures similaires prises par l'ONU, OFAC et UE).

Le Facteur de risque « Zones Géographiques » se décompose comme suit :

- **Catégorie :** zones géographiques locale (Nord, sud ...) Concernées par l'activité de la banque (régions rurales, petites villes, grandes villes, quartiers reconnus par leurs taux élevés de criminalité, postes frontaliers...).

- **Types :** Agences de différentes tailles, petites Agences, succursales Centres d’Affaires de criminalité, Agences situées près d'un poste frontalier (aérien, maritime, etc...).

### 3. Le Facteur de risque « Produits, Services et Transactions »

Cette évaluation du risque, basée sur la nature du produit recherché par le client, est calculée à l'aide d'un certain nombre de critères liés au produit. En premier lieu, cela dépend de la probabilité que le produit soit utilisé à des fins de blanchiment ou de financement du terrorisme. L'évaluation des produits n'est pas universelle, car les institutions financières font face à différents niveaux de risques.

De plus, certaines fonctions ou produits spécifiques de la banque sont considérés à haut risque. Ils comprennent :

- ✓ La banque privée,
- ✓ L'activité internationale extraterritoriale,
- ✓ Le service de dépôt,
- ✓ Les fonctions de virements bancaires et de gestion de la trésorerie,
- ✓ Les transactions dont l'identité du bénéficiaire effectif est dissimulée,
- ✓ Les systèmes de garantie de prêts,
- ✓ Les chèques de voyage,
- ✓ Les mandats,
- ✓ Les opérations de change,
- ✓ Les transactions de financement du commerce à des taux inhabituels,
- ✓ Les comptes de passage.

Il faut donc être vigilant et reconnaître les produits, les services, ou un ensemble des deux, qui peuvent poser un risque élevé de blanchiment d'argent ou de financement du terrorisme. Les produits et les services légitimes peuvent servir à masquer l'origine illicite des fonds, à déplacer des fonds afin de financer des activités terroristes ou à dissimuler la véritable identité des propriétaires ou des bénéficiaires des produits et services. Les produits et services qui peuvent faciliter le mouvement et la conversion de biens par l'entremise du système financier peuvent poser un risque élevé.

Le Facteur de risque « produits, services et transactions » se décompose comme suit :

- **Catégorie des produits, services et transactions :** moyens de paiement, crédits, commerce extérieur, comptes et location de coffres, etc....
- **Types des produits, services et transactions:** Moyens de paiement (transferts électroniques de fonds, cartes monétiques, espèces, chèques, effets, etc..), crédits (crédit garantis par les actifs détenus par des tiers, prêts garantis par des dépôt ou autres actifs facilement négociables tels que les titres, crédits pour le compte de tiers, autres crédits d'investissement, autres prêts de consommation, autres prêts de logement, etc...), comptes (en dinars, en devises, en dinars convertibles, comptes de placement bancaires et titres, comptes épargne à vue, etc...) commerce extérieur (lettres de crédits, aval des traites, financement en devises, etc...). Les types de produits et services peuvent se subdiviser à leur tour en sous types de produits et services (virements électroniques transfrontaliers de fonds qualifiés, virements électroniques transfrontaliers de fonds non qualifiés, télé-virements, dépôt espèces, retrait espèces, mise à disposition, Transferts de fonds par l'intermédiaire de prestataires de services « MSB », cartes nationales, cartes internationales, cartes prépayées, etc...).

#### 4. Le Facteur de risque « Canaux de distribution »

La Banque doit appliquer, pour les clients qui agissent en qualité de donneur d'ordre ou de bénéficiaire des mesures de vigilance renforcée lorsque l'opération est effectuée aux moyens des nouvelles technologies d'information et de communication.

La Banque doit mettre en place un dispositif permettant de prévenir les risques inhérents à l'utilisation des nouvelles technologies à des fins de blanchiment d'argent ou de financement du terrorisme. À cet effet, elle doit se doter de dispositifs de gestion des risques permettant d'identifier et d'évaluer les risques de blanchiment d'argent et de financement du terrorisme pouvant résulter de :

- Développement de nouveaux produits et services, y compris de nouveaux canaux de distribution ; et
- L'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou des produits préexistants.

Le Facteur de risque « Canaux de distribution » se décompose comme suit :

- **Catégorie des canaux de distribution** : face à face, guichets automatiques, intermédiation, contact à distance.
- **Types des canaux de distribution** : face à face (contact direct avec le client à l'agence, etc...), guichets automatiques (libre-service, etc...), intermédiation (mandataires, courtiers, etc..), banque à distance (téléphone, internet, etc...).

### V. LES INDICATEURS D'ALERTE DE BLANCHIMENT D'ARGENT ET DE FINANCEMENT DU TERRORISME

Les indicateurs d'alertes sont des signaux d'alarmes potentiels qui pourraient déclencher des soupçons ou indiquer que quelque chose peut être inhabituelle ou n'ayant pas d'explication raisonnable. Les signaux d'alarme d'une ou plusieurs caractéristiques factuelles, comportements ou autres facteurs révélant des irrégularités liées aux opérations financières. Les indicateurs de blanchiment d'argent combinés à des faits et au contexte peuvent aider à déterminer s'il existe des motifs raisonnables de soupçonner une personne. Il s'agit :

- Des indicateurs de blanchiment d'argent liés aux clients qualifiés à risque élevé notamment :
- Le client insuffisamment identifié ou occasionnel.
  - Le compte dont le fonctionnement est assuré par un mandataire.
  - Le client sans adresse fixe.
  - Les personnes ayant des relations avec des individus connus par leurs activités présumées illicites.
  - Le client ou ses contreparties non-résidents, notamment provenant de pays à haut risque.
  - Les secteurs d'activités ou professions à risques (Agent immobilier, société de promotion immobilière, sociétés offshore, bureaux de change et sous délégataires, les casinos et les établissements de jeux de hasard, les joailliers et commerçants en pierres précieuses, les cabinets de conseils, les avocats, les notaires, les comptables et toute

activité juridique, les sans activités, les travailleurs journaliers, les activités à manipulation d'argent en espèces, etc....).

- Les clients à statuts particulières (PPE, Associations, Partis politiques, etc.,).

➤ Des indicateurs d'alerte liés à la nature de services et produits notamment :

- La location de coffres forts.
- Les opérations de commerce extérieurs.
- Les sociétés de transferts d'argent (MSB).
- La demande de prêts adossés à des garanties tierces.
- Le financement d'acquisition de biens de luxe, objets d'art ou d'antiquité.
- Les cartes prépayées et les cartes de paiement ou les cartes de crédit étrangères.
- Les opérations à distance (internet, smartphone, etc.,).
- Les opérations de paiement utilisant la nouvelle technologie.
- Les banques en ligne.
- Les placements.

➤ Des indicateurs d'alerte liés aux opérations et aux mouvements sur les comptes auxquels il faut être attentif, notamment :

- L'opération ou la transaction qui paraît sans rapport avec la nature de l'activité du client.
- L'opération ou la transaction dont les documents ou informations faisant apparaître sa finalité n'ont pas été produits.
- L'opération ou la transaction qui ne revêt aucune justification économique ou licéité apparente.
- L'opération ou la transaction qui revêt un caractère complexe.
- L'opération ou la transaction qui porte sur un montant anormalement élevé.
- Les versements et les retraits fréquents en espèces.
- Les opérations en espèces et les virements fractionnés.
- Les opérations avec l'étranger.
- Les virements électroniques de fonds.
- Les remises chèques de montant significatif sans rapport avec l'activité économique du client.
- Remise à l'encaissement des chèques tirés sur des banques implantées dans des pays à risque élevé ou dans des paradis fiscaux.
- Les mouvements de fonds sur de comptes dormants.
- Les crédits adossés à des garanties financières.
- Les transactions impliquant de non-résidents ou clients à risque élevé.

➤ Des indicateurs d'alerte liés au fonctionnement de comptes de sociétés, notamment :

- La réticence à fournir des informations ou explications confuses, incohérentes ou invérifiables.
- L'élément de réponse ne justifiant pas l'incohérence entre les transactions réalisées et l'activité de la relation.
- Des explications peu claires ou peu convaincantes sur l'origine de fonds ou le fondement économique des transactions réalisées.
- La modification de l'activité des comptes comme l'utilisation de comptes personnels à des activités professionnelles.

➤ Des indicateurs d'alerte liés au pays ou zones géographiques à risque, notamment :

- Les pays identifiés par des sources crédibles, notamment le GAFI, comme n'étant pas dotés d'un dispositif de LAB/FT présentant de déficiences stratégiques substantielles.
- Les pays soumis à des sanctions, des embargos, ou des mesures similaires, prises notamment, par les NU, l'OFAC ou l'UE.
- Les pays identifiés et classés par des sources crédibles comme l'Interpol ou Transparency International comme caractérisés par un niveau élevé de corruption, de trafic de drogue intensif ou de délinquance financière.
- Les pays identifiés par des sources crédibles, notamment le GAFI, comme apportant un soutien moral et financier aux activités terroristes.
- Les pays classés en tant que paradis fiscaux par des sources crédibles (liste OCDE, etc.).
- Les zones de conflits armés.
- Les zones frontalières terrestres et maritimes.

➤ Des indicateurs d'alerte liés aux opérations de commerce extérieur

Origine ou destination inhabituelle des biens :

- Le pays n'est pas connu pour importer ou exporter ce type de biens.
- Des transactions sont réalisées avec des personnes physiques ou des entités se trouvant dans des pays à risque.

Fournisseur ou acheteur inhabituel :

- Des sociétés récemment créées procèdent à des importations et des exportations massives.
- Le volume ou le type des biens ne correspond pas au profil des fournisseurs ou des acheteurs.
- Les fournisseurs ou les acheteurs sont des sociétés extraterritoriales.

Transport inhabituel de biens :

- Le coût du transport est élevé par rapport à la valeur des biens.
- La dimension et le poids ou la nature des biens ne correspondent pas au mode de transport.

Description inhabituelle des biens :

- On relève des différences importantes entre les déclarations en douane et les factures.
- On relève des différences importantes entre la description des biens sur la facture et les biens réellement transportés.
- On se trouve en présence de biens risqués, à savoir des marchandises de grande valeur.

Prix inhabituels :

- On relève une différence importante entre la valeur déclarée et la valeur de marché.
- On relève une différence importante entre la valeur assurée et le montant facturé.

Financement/paiements inhabituels :

- Des biens sont achetés avec des fonds d'origine inconnue (espèces).
- On relève une différence entre l'origine des biens et la destination des fonds (ou inversement).

- On relève une différence entre le montant de la somme versée et celui de la somme facturée.
- Un paiement a été effectué par une société extraterritoriale ou depuis un compte extraterritorial.
- Une commission a été versée à un tiers sans pièce justificative ou en dehors de toute logique économique.
- Le paiement des biens est (en partie) réalisé par un tiers, et non par l'importateur.

Virement et transfert de fonds :

- Transfert de fonds inhabituel ou sans justification économique apparente en provenance ou à destination de pays étrangers.
- Transfert reçu ou émis d'un pays où le client ne possède aucune activité connue.
- Réception d'un transfert de fonds sans indication du nom, de l'adresse ou du numéro de compte du donneur d'ordre, et sans que ces informations aient pu être obtenues de la banque du donneur d'ordre.
- Compte, sans ou à faible mouvement, activé par des opérations de transfert ou de virement sans motif clair.

**NB :** Les indicateurs ci-dessus mentionnés ne constituent pas une liste exhaustive d'indicateurs de blanchiment d'argent et de financement du terrorisme.

## VI. LES OBLIGATIONS DES BANQUES EN MATIERE DE LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX

Le dispositif tunisien de lutte contre le blanchiment de l'argent et le financement du terrorisme vise à prémunir le système financier contre son utilisation à des fins illicites. De ce fait, le législateur tunisien a misé sur le système bancaire pour lutter contre le blanchiment des capitaux. Ainsi, deux principales obligations ont été imposées aux banques notamment, le devoir de vigilance en termes d'identification des clients et l'obligation de déclaration du soupçon.

De ce fait, la BH Bank a adopté les obligations suivantes :

- Obligation d'identification des clients et les bénéficiaires effectifs.
- Obligation de vigilance vis-à-vis des opérations et des transactions dont les résultats doivent être consignés ; obligation de détecter les opérations et les transactions entachées de soupçons de blanchiment d'argent ou de financement du terrorisme.
- Obligation de collecte et d'archivage des documents liés à l'identification des clients et aux opérations effectuées et de mettre à jour les données d'identification.
- Obligation de déclaration de soupçon des opérations et des faits suspects ayant été détectés.

### 1. Identification des clients et les bénéficiaires effectifs (Article 6 de la circulaire BCT N° 2018-09)

La vigilance au sujet de la clientèle est l'ensemble des procédures permettant de s'assurer que les banques ont une connaissance appropriée de leurs clients, et de leurs activités. (**Loi n°2015-26** telle que modifiée par la **loi 2019-09**, la **circulaire BCT 2017-08** telle que modifiée par la note **circulaire 2018-09**).

### 1.1. Avant l'entrée en relation avec la clientèle

Avant l'entrée en relation d'affaires avec la clientèle, la banque est appelée :

- A Faire un entretien portant sur les données d'identification, l'activité, les revenus, le patrimoine, l'objet social et le courant d'affaires des clients, l'origine géographique et lieu de réalisation de l'activité.
- A collecter les informations sur les clients moyennant des justificatifs et maintenir à jour les informations et les documents.
- A se renseigner sur l'identité des mandataires, des principaux associés et actionnaires, les dirigeants et les bénéficiaires effectifs.
- A consigner les informations recueillies dans une fiche d'entretien.
- A garder des copies des documents officiels présentés par la relation.

A ce titre, le chargé de l'opération doit prendre en compte les principes directeurs suivants :

- Le bénéficiaire effectif est une personne physique. Il n'est pas nécessairement le bénéficiaire déclaré de l'opération ou la transaction. Il importe de distinguer clairement ces deux notions.
- Le bénéficiaire effectif n'est pas nécessairement le client, que ce dernier soit une personne physique, une personne morale ou une construction juridique.
- Le bénéficiaire effectif et le bénéficiaire peuvent être, dans certains cas, une seule et même personne, par exemple lorsque le bénéficiaire effectif d'un client donneur d'ordre d'un virement en est aussi le destinataire.
- Une relation d'affaires, une opération ou une transaction, avec un client occasionnel peut dissimuler un ou plusieurs bénéficiaires effectifs.
- Certaines relations d'affaires ou opérations réalisées avec des clients occasionnels, font ressortir que le bénéficiaire et le bénéficiaire effectif ne sont pas distincts.

### 1.2. A l'entrée en relation d'affaires avec une relation

A l'ouverture des comptes, le chargé de l'opération est tenu de vérifier minutieusement les documents justificatifs de l'identité présentés par le client et ce, conformément à la circulaire BCT N°2018-09 (Article 5) et aux procédures en vigueur.

Ces documents doivent être des documents reconnus par les autorités tunisiennes, soit :

❖ Pour les personnes physiques :

- ✓ Le nom complet, la date et le lieu de naissance ainsi que la nationalité.
- ✓ Carte d'Identité Nationale ou Passeport pour les tunisiens.
- ✓ Passeport ou Carte de Séjour en cours de validité, pour les étrangers, portant la photo d'identité, l'adresse et l'activité de son titulaire et reconnue par les autorités des Etats dont ils relèvent.
- ✓ La profession et son adresse.
- ✓ L'objectif de la relation d'affaires et sa nature.
- ✓ Un exemplaire de signature.
- ✓ Copie de la facture récente STEG, SONEDÉ ou téléphone fixe pour la vérification de l'adresse ou tout autre document probant permettant de s'assurer de l'adresse (contrat de location, etc...).

- ✓ Le numéro de téléphone fixe et portable, Adresse E-mail, etc...

**NB :** Incrire la nature et le numéro de la pièce d'identité ainsi que le lieu et la date de délivrance, sur le contrat d'ouverture compte, le contrat de location de coffre-fort ou de toute autre opération et conserver dans le dossier du client, une photocopie du document présenté. Détecter les anomalies éventuelles figurant sur lesdits documents (grattages, gommages, surcharges, photo d'identité méconnaissable, etc...).

❖ Pour les personnes morales, sur la base de documents officiels attestant :

- ✓ La date de sa constitution, sa raison ou sa dénomination sociale, sa forme juridique et son objet social, son activité, l'adresse de son siège social comportant le code postal, les numéros de téléphone et de fax et l'adresse électronique (E-mail) ainsi que la répartition de son capital. Lorsque les activités principales ne sont pas exercées au sein du siège social, il convient d'indiquer l'adresse effective d'exercice de l'activité.
- ✓ L'identité et le domicile de ses dirigeants, et ceux ayant le pouvoir de mouvementer le(s) compte(s) de la relation et de s'engager en son nom et des personnes physiques qui la contrôlent en exigeant une copie de la pièce d'identité de cette personne (Carte d'Identité Nationale « CIN » ou Passeport pour les personnes physiques, extrait récent du registre national de l'entreprise pour les personnes morales « RNE » ou une pièce équivalente pour les non-résidents).
- ✓ L'identité et le domicile des principaux actionnaires ou associés. Tout actionnaire ou associé détenant 10% ou plus doit faire l'objet d'une identification « KYC » et de la saisie de toutes les données nécessaires au niveau de la Base de Données Clients.
- ✓ L'identité et le domicile de(s) bénéficiaire(s) effectif(s) détenant directement ou indirectement **20% ou plus du capital ou des droits de vote** de la personne morale ou de la construction juridique et d'une manière générale toute personne physique qui en dernier lieu possède ou exerce un contrôle effectif sur le client ou pour le compte de laquelle l'opération est effectuée.
- ✓ **La présence physique** du titulaire du compte ou de son mandataire est obligatoire lors de l'ouverture. Toute ouverture de compte par mandat pour une personne physique doit être suivie par une **signature légalisée** de la fiche de spécimen de signature et de la convention de gestion de compte par le mandant accompagnée d'une copie lisible de la pièce d'identité comportant une photo d'identité fidèle de la personne.
- ✓ L'objectif de la relation d'affaires et sa nature.
- ✓ Enregistrer toutes les mentions relatives à l'identité du client au niveau du système d'information et en assurer une mise à jour permanente des informations recueillis au moment de l'ouverture permettant de prendre en compte tout élément de nature à modifier son profil.
- ✓ Une vigilance constante doit être exercée à l'égard des relations d'affaires et un examen attentif des opérations et transactions effectuées doit être conduit pendant toute la durée de la relation. La vérification n'est pas requise pour le cas des sociétés cotées en Bourse et des entreprises à participation publique. Est considéré entreprise à participation publique, toute entreprise dans laquelle l'Etat détient directement ou indirectement par le biais d'entreprises ou d'établissements publics des participations au capital social.

Les vérifications consistent à s'assurer de l'identité du client, de la régularité et de l'authenticité des documents présentés et de leur cohérence et l'établissement d'une fiche d'identification « **KYC** ».

Le chargé de l'opération doit vérifier la conformité des pièces d'identité par rapport aux originaux. Il doit apposer son visa autorisé en indiquant son matricule sur les documents d'ouverture du compte.

Le chargé de l'opération est tenu de :

- Se renseigner sur la nature des opérations à réaliser sur le compte et des services à demander sur les compte (cartes, crédits, virement...) et le chiffre d'affaires prévisionnel.
- Vérifier que la demande d'ouverture et la fiche d'identification « **KYC** » (Know Your Customer) ont été soigneusement remplis. Toute information utile pourra être portée au verso de la fiche d'identification « **KYC** ».

Une attention particulière est recommandée lorsque le compte est ouvert dans une agence dans le ressort duquel la personne morale n'a ni son Siège, ni son activité, ni une activité significative ou lorsque le client a le statut de non-résident, ou a élu domicile **chez un tiers** dont l'adresse de correspondance est **une boîte postale** ou est **différente de l'adresse fiscale**.

**L'ouverture de comptes sous des noms anonymes est interdite.** Le compte doit être ouvert sous des noms complets. **Les abréviations ne sont pas tolérées.** Une attention particulière doit être donnée à l'orthographe des noms et prénoms qui doit être identique à celle écrite par le client.

Pour les clients qui agissent en qualité de donneur d'ordre ou de bénéficiaire qui sont résidents dans des pays signalés par le GAFI (Groupe d'Action Financière) n'appliquant pas ou appliquant d'une manière insuffisante les normes internationales en matière de lutte contre le blanchiment d'argent et au cas où les documents fournis ne peuvent être authentifiés, le chargé de l'opération doit demander :

- ✓ Une attestation bancaire de confirmation de sa banque indiquant la date d'entrée en relation avec le client,
- ✓ Des informations supplémentaires des correspondants de la Banque à l'étranger pour certification de la copie du document officiel.

### Cas des mandataires

Le chargé de l'opération prend en outre connaissance des pouvoirs de représentation de la personne agissant au nom du client et procède à leur vérification au moyen de documents susceptibles de faire preuve dont il prend copie. Sont notamment visés :

- Les représentants légaux de clients incapables.
- Les personnes autorisées à agir au nom des clients en vertu d'un mandat général ou spécial.
- Les personnes autorisées à représenter les clients qui sont des personnes morales, des fonds ou toutes autres structures juridiques dénuées de personnalité juridique dans leurs relations avec l'agence concernée.

Le chargé d'opération doit vérifier, lors de l'ouverture d'un nouveau compte, si le client dispose déjà d'autres comptes ouverts sur les livres de la banque et vérifier, le cas échéant, l'historique des opérations sur les comptes existants. **Il doit se renseigner sur les raisons pour lesquelles la demande d'ouverture d'un nouveau compte est formulée.**

**NB :** Si à l'ouverture de compte, les documents présentés ne peuvent être identifiés, sont insuffisants ou fictifs, ou si le client ne présente pas les pièces exigées dans la semaine qui suit l'ouverture ou refuse de répondre aux questions relatives à la nature de son activité, à la nature de la relation d'affaires objet du compte, à l'origine de son patrimoine, etc... Le chargé de l'opération doit s'abstenir d'ouvrir le compte, de nouer ou de continuer la relation d'affaires ou d'effectuer l'opération ou la transaction et envisager de faire une déclaration d'opération suspecte à conformité.

### 1.3. Client occasionnel ou passager

Il est entendu par client occasionnel, toute personne qui réalise une opération sans avoir de relation contractuelle ou habituelle avec la banque. Exemple d'opérations : change manuel, location de coffre-fort, les virements électroniques de fonds ou mise à disposition...

Pour toute opération occasionnelle :

- En espèces dont la valeur est égale ou supérieure à **Dix Mille Dinars** (10.000 TND).
- En devises dont la valeur est égale ou supérieure à la contrevaleur en dinars de **Cinq Mille Dinars** (5.000 TND).

Le chargé de l'opération doit présenter une fiche de renseignements au client qui doit la remplir soigneusement. Une copie de sa Carte d'Identité Nationale ou de son Passeport doit être gardée par le chargé de l'opération.

Procéder à la recherche en ligne, envoyer le résultat avec la photocopie de l'identité ou passeport à la Direction de la Conformité qui va demander l'accord de la Direction Générale pour toute opération indépendamment du montant de l'opération

### 1.4. Clients titulaires de comptes à risque élevé

Est considéré à risque élevé, le compte dont le titulaire fait partie de la catégorie de clientèle sensible en vertu du secteur où il exerce son activité professionnelle, de la nature du revenu et des circonstances de l'ouverture. La clientèle sensible comprend surtout :

- Les personnes dont l'activité génère des volumes d'espèces importants (casinos, bureaux de change, objets d'arts, métaux précieux, pierres précieuses, etc,...).
- Les clients sollicitant une ouverture à distance ou moyennant les nouvelles technologies d'informations et de communications (NTIC) à cet effet il est recommandé la confirmation de l'identité du client par une institution financière.
- Les ressortissants de pays non coopérants ou à faible réglementation selon le GAFI.
- Les partis politiques et les associations surtout non-résidentes.
- Les personnes politiquement exposées « PPE ».

### 1.5. Recours à des Tiers pour la connaissance du client « KYC »

Selon l'**Article 9 (nouveau) de la circulaire N°2018-09**, lorsque la Banque fait recours à des tiers pour s'acquitter de l'obligation de connaissance du client, elle doit :

- ✓ Obtenir immédiatement les informations nécessaires concernant les mesures de vigilance relatives à la clientèle.
- ✓ Prendre les mesures adéquates pour s'assurer que le tiers est à même de fournir, sur demande et sans délais des copies des données d'identification et d'autres documents pertinents liés aux devoirs de vigilance relatifs à la clientèle.
- ✓ S'assurer que le tiers est soumis à une réglementation et une surveillance relative à la répression du blanchiment d'argent et à la lutte contre le financement du terrorisme et qu'il a pris des mesures pour respecter les diligences de vigilance relatives à la clientèle et les obligations de conservation des documents.

Le recours à un tiers n'exonère pas l'établissement assujetti de ses responsabilités en matière d'identification du client et dans tous les cas il doit continuer à assurer les obligations mises à sa charge par le cadre légal et réglementaire régissant l'externalisation.

#### **1.6. Anciennes relations d'affaires**

Conformément aux procédures en vigueur, la Direction chargée des Affaires Juridiques et les Agences doivent procéder périodiquement selon le risque de la relation, à la mise à jour des dossiers d'ouverture des anciennes relations ainsi que de la Base de Données Clients et la fiche d'identification « KYC ».

❖ Pour les personnes physiques :

- ✓ Mise à jour de la fiche d'identification « KYC » selon la périodicité prescrite dans les procédures internes en vigueur.
- ✓ Mise à jour de la nouvelle adresse et la nouvelle activité.
- ✓ Mise à jour de l'identité du ou des bénéficiaires effectifs.
- ✓ Vérification de la validité des cartes de séjour et des passeports pour toutes les nationalités.
- ✓ Vérification si le client n'a pas fait le retour définitif et le changement de résidence pour les travailleurs tunisiens résidents à l'étranger « TRE ».
- ✓ Mise à jour des champs informatiques déjà erronés, mal renseignés ou manquantes.

❖ Pour les personnes morales :

- ✓ Mise à jour des fiches d'identification « KYC » selon la périodicité prescrite dans les procédures internes en vigueur.
- ✓ Exiger un extrait récent ne dépassant pas trois mois du registre national des entreprises (RNE).
- ✓ Exiger les justificatifs de changement des statuts, les PV de nomination du mandataire ou du dirigeant, les PV des délibérations du Conseil, les rapports de gestion, éventuellement les rapports de(s) commissaire(s) aux comptes...
- ✓ Exiger les justificatifs d'adresse qui est en principe le lieu où la société a son siège social.
- ✓ Exiger l'identité et le domicile de ses dirigeants, et ceux ayant le pouvoir de mouvementer le(s) compte(s) de la relation.
- ✓ Exiger l'identité et le domicile des principaux actionnaires ou associés.
- ✓ Exiger l'identité du ou des bénéficiaires effectifs.

- ✓ Demander les justificatifs de L'activité (artisan, entrepreneur, salarié secteur public ou secteur privé, profession libérale pour une personne physique), sa surface financière (bilan, comptes de résultats ou états prévisionnels) ou patrimoniale. Se méfier de toute indication vague du style « homme d'affaires », « Intermédiaire » etc, ...

S'assurer, outre de l'activité réelle de l'entreprise, de la cohérence de cette activité avec l'objet social ainsi que de la cohérence des transactions financières ou des mouvements de marchandises avec l'objet social.

#### **1.7.Relations avec les Associations**

Le chargé de l'opération est tenu de se renseigner sur :

- ✓ Le nom de l'Association.
- ✓ L'adresse du siège principal.
- ✓ Noms et prénoms des personnes habilitées à réaliser des opérations financières et les numéros de leurs Cartes d'Identité Nationale (CIN) ou Passeports.
- ✓ Les statuts et la référence de l'extrait du J.O.R.T relatif à la constitution de l'association.
- ✓ Un extrait récent du Registre Nationale de l'Entreprise « RNE ».
- ✓ Tout élément permettant d'apprecier la situation financière notamment les états tenanciers et le cas échéant les rapports de(s) commissaire(s) aux comptes, rapport financier, rapport moral, etc ...
- ✓ Identité du ou des bénéficiaires effectifs.

#### **1.8.Relations d'affaires avec les correspondants bancaires et autres relations similaires (RMA et MSB)**

L'entrée en relation avec un organisme financier (correspondant bancaire, RMA, MSB) n'exonère pas les établissements de toute vigilance :

En premier lieu, il convient de connaître précisément la nature juridique du contractant (établissement bancaire, MSB, etc,) et le régime de supervision auquel il est soumis en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Le principe « Know Your Customer » doit s'exercer sur la composition du capital et sur tout changement susceptible d'intervenir, sur les organes de direction, les principales activités et lieu d'implantation, les procédures de lutte contre le blanchiment et le financement du terrorisme, la finalité du compte, l'identité de tous les utilisateurs des services du correspondant, la réglementation et les modalités d'exercice du contrôle bancaire dans le ou les pays considérés. Il faut de plus pouvoir apporter la preuve que l'organisme contractant est bien soumis à des règles de vigilance identiques à celles en vigueur en Tunisie et qu'il est assujetti au contrôle d'une autorité nationale. Toutes les informations en la matière sont utiles, en particulier pour les établissements qui ne seraient pas notoirement connus. En second lieu, il convient de distinguer les opérations faites par un organisme financier pour son propre compte de celles pouvant être réalisées pour le bénéfice d'un tiers. Relèvent notamment de la seconde catégorie les dépôts fiduciaires, dont la nature s'apparente à la fois à des opérations interbancaires et de clientèle.

L'ensemble des informations recueillies sera regroupé dans un dossier électronique ou sur support papier ouvert au nom de l'établissement.

Pour les correspondants étrangers, la Conformité est tenue de :

- S'assurer que le correspondant est agréé et soumis au contrôle des autorités compétentes de son pays d'origine ou du pays où il est établi.
- Collecter suffisamment de renseignements, en vue de connaître la nature de ses activités et apprécier, sur la base d'informations accessibles au public, sa réputation et l'efficacité du système de contrôle auquel il est soumis.
- Vérifier dans le questionnaire qui a été adressé au correspondant, si celui-ci a fait l'objet d'une enquête ou d'une intervention de l'autorité de contrôle, liée au blanchiment d'argent et au financement du terrorisme.
- Apprécier le système de contrôle auquel est soumis le correspondant dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme. Le correspondant doit répondre au questionnaire approprié qui lui a été adressé par la Banque.
- Obtenir l'avis préalable de la conformité et l'approbation du Conseil d'Administration avant de nouer des relations avec un nouveau correspondant bancaire, RMA ou MSB. Dans ce cadre, le Conseil d'Administration peut mandater la Direction Générale pour statuer sur lesdites relations.
- S'abstenir de nouer ou de poursuivre une relation de correspondant bancaire avec une banque étrangère fictive et de nouer des relations avec des institutions étrangères qui autorisent des banques fictives à utiliser leurs comptes. Est considéré fictive, toute banque ne disposant pas de siège fixe, n'emploie pas une personne ou plus pour exercer l'activité, ne conserve pas les documents relatifs à ses opérations et n'est pas soumise à un contrôle d'une autorité de supervision compétente.

Les obligations des deux parties doivent être établies par écrit (Contrat, convention de compte, convention de partenariat) notamment pour le traitement des cas de virement ou de transferts reçus non accompagnés par les renseignements exigés en matière d'identification du donneur d'ordre en prévoyant l'application progressive des mesures suivantes :

- ✓ La suspension de l'exécution de l'opération jusqu'à l'obtention dans un délai raisonnable, les renseignements manquants.
- ✓ Le rejet de l'opération en cas de non-réceptions des renseignements requis dans le délai imparti.
- ✓ La rupture de la relation d'affaires.
- ✓ La déclaration de l'opération à la CTAF.

Les conventions de partenariat et les conventions de compte doivent être soumises à l'avis préalable de la conformité de la banque.

### 1.6. Identification du bénéficiaire effectif

(Décisions CTAF Mars 2017 et 2018)

Par bénéficiaire effectif, il faut entendre toute personne physique qui possède in fine ou contrôle le client, ou pour le compte duquel l'opération est effectuée sans qu'il soit nécessaire qu'il y ait un pouvoir écrit entre le client et le bénéficiaire effectif (**Article 5 de la directive n°2 de la CTAF**).

En s'appuyant sur l'**Article 6 (nouveau) de la circulaire N02018-09**, les établissements assujettis doivent effectuer les diligences relatives à l'identification du client et du

bénéficiaire effectif de l'opération ou de la transaction et la qualité de celui qui agit pour son compte notamment lorsque :

- ✓ Le client souhaite ouvrir un compte, quelle que soit sa nature, ou louer un coffre-fort;
- ✓ Le client effectue des transactions occasionnelles, dont la valeur est égale ou supérieure à un montant fixé par arrêté du ministre des finances qu'elles soient réalisées en une seule opération ou en plusieurs opérations apparaissant comme liées entre elles.
- ✓ Le client effectue des opérations sous forme de virements électroniques de fonds.
- ✓ Il y a suspicion de blanchiment d'argent ou de financement du terrorisme.
- ✓ Il y a des doutes quant à la véracité de l'opération.

A l'occasion du traitement d'une opération ou transaction, s'il apparaît qu'elle est ou pourrait être effectuée au profit d'un tiers bénéficiaire effectif de l'opération ou de la transaction (ayant droit économique), le chargé de l'opération doit relever l'identité du bénéficiaire effectif, son activité, son adresse et les pouvoirs en remplissant une fiche d'identification « KYC » qui doit être signée par le bénéficiaire effectif, et dans le cas échéant, de celui qui agit pour son compte.

Pour les chargés d'opérations, l'entreprise personne morale, n'est pas l'unique partenaire à prendre en compte, il y a toujours des personnes physiques qui sont les bénéficiaires effectifs et qui doivent faire l'objet d'une identification pour faciliter la compréhension de la propriété et du fonctionnement de la structure de contrôle.

Pour l'identification du bénéficiaire effectif, le chargé d'opération procède à la consultation des informations ou données pertinentes obtenues de source fiables. A cet effet le chargé doit :

- Déterminer, pour l'ensemble des clients, si le client agit pour le compte d'une tierce personne et prendre, si c'est le cas, toutes mesures raisonnables pour obtenir des données d'identification suffisantes permettant de vérifier l'identité de cette tierce personne.
- S'assurer que le client n'est pas un prête nom ou une société écran.
- Prendre lorsque le client est une personne morale ou une construction juridique, toutes les mesures raisonnables pour vérifier l'identité du ou des bénéficiaires effectifs au moyen des éléments d'identification suivants :

**- Lorsqu'il s'agit d'une personne morale :**

Le chargé d'opération est tenu d'identifier :

- La ou les personne(s) physique(s) qui détient/ détiennent, directement ou indirectement, 20% ou plus des parts du capital ou des droits de vote de la société. A cet effet, le chargé doit réclamer les documents nécessaires à l'identification du bénéficiaire effectif à savoir les statuts, l'extrait récent du registre national de l'entreprise « RNE » de la personne morale, contrat de cession d'actions, attestation de propriété d'actions délivrée par la société ou par un intermédiaire en bourse agréée lorsqu'il s'agit d'une société cotée en bourse...

- A défaut de pouvoir identifier le(s) bénéficiaire(s) effectif (s) sur la base du critère du pourcentage de participation ou des droits de vote, le chargé doit identifier la ou les personnes physiques qui exerce(nt), par tout autre moyen, de fait ou de droit, un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction ou sur l'assemblée générale ou sur le fonctionnement de la société.
- A défaut d'identifier le(s) bénéficiaire(s) effectif(s) sur la base des deux critères précédents, le chargé d'opération doit considérer le dirigeant principal en tant que bénéficiaire effectif.

**- Dans le cas d'une construction juridique :**

**Pour les trusts :** le chargé d'opération est tenu d'identifier :

L'identité du constituant du trust, du ou des trustees, du protecteur, des bénéficiaires ou de la catégorie de bénéficiaire et de toute autre personne physique exerçant en dernier ressort un contrôle effectif sur le trust y compris au travers d'une chaîne de contrôle ou de propriété.

**Pour les autres types de constructions juridiques :** le chargé d'opération est tenu d'identifier l'identité des personnes physique exerçant en dernier ressort un contrôle effectif sur la construction juridique y compris au travers d'une chaîne de contrôle ou de propriété.

**Lorsque le client est une société cotée sur un marché financier et est assujettie à des obligations de publication permettant de garantir une transparence satisfaisante des bénéficiaires effectifs, ou une filiale majoritaire de ladite société, le chargé d'opération peut se dispenser de l'obligation d'identifier et de vérifier l'identité des actionnaires ou des bénéficiaires effectifs de cette société pourvu qu'il obtienne les données d'identification pertinentes à partir du registre national de l'entreprise « RNE » ou auprès du client ou d'autres sources fiables.**

**NB :** Si l'identité du bénéficiaire effectif n'est pas connue ou entourée de doutes, le chargé d'opération doit s'abstenir de traiter avec la relation et le cas échéant, faire une déclaration de soupçon à la conformité.

### **1.7. Identification de fournisseurs des biens et services**

Afin d'éviter de conclure de contrat de marché avec des prestataires blacklistés, la banque est tenue d'identifier son fournisseur (Know Your Provider « KYP ») avant toute entrée en relation ou attribution de marché, de commande ou engagement de dépense.

L'identification de fournisseur ou de prestataire consiste à l'établissement du formulaire « KYC » en procédant de la manière suivante :

- Pour les achats objet de marchés écrits, la commission de dépouillement doit procéder à l'identification du fournisseur en consignant le formulaire « KYP » afférent au prestataire retenu et ce, avant de soumettre le rapport de dépouillement à

l'avis de la commission compétente. Le rapport de dépouillement doit mentionner explicitement que le prestataire retenu ne figure dans aucune liste de sanctions.

- Pour les achats par Bons de commande la Direction des Achats, doit procéder à l'établissement du formulaire « KYP » afférent au prestataire proposé de lui attribuer la commande et ce, avant la validation de l'autorisation de dépense correspondante.
- Pour les commandes engagées directement par certaines structures centrales de la Banque (sans passer par la Direction des Achats), la structure concernée doit procéder à l'établissement du formulaire « KYP » afférent au prestataire proposé avant d'engager la dépense.
- Pour les prestataires sollicités directement par les agences, la recherche en ligne et le KYP/KYC sont effectués au niveau de l'agence, quel que soit le montant du service ou du produit fourni.

Le processus d'identification passe par les étapes suivantes :

- Accéder au module de filtrage par et insérer les informations du prestataire (nom, prénom, nationalité...) conformément à la procédure en vigueur.
- Contrôler les similitudes entre les données de leur identification (figurant sur la carte d'identité pour les personnes physiques et sur le certificat du RNE pour les personnes morales), par rapport aux listes de sanctions et des personnes politiquement exposées (PEP).
- Editer le résultat de la recherche en ligne et le formulaire **KYP** et le classer avec la copie de la CIN ou du RNE du prestataire.
- Conserver le dossier du Prestataire pour une période de dix (10) ans.

Deux cas peuvent se présenter :

- Au cas où le prestataire figure sur **une liste de sanctions**, il faut refuser l'entrée en relation et informer sans délai la conformité.
- Au cas où le prestataire existe sur la liste des personnes politiquement exposées (PEP), il faut adresser une demande d'autorisation à la conformité et ce, avant d'entamer toute relation contractuelle.

### 1.8. Identification de l'employé

Afin d'éviter de recruter un employé balacklisté, la banque est tenue d'identifier son employé (Know Your Employee « KYE ») avant son recrutement. L'identification de l'employé consiste à s'assurer de l'identité de candidat, de la régularité et de l'authenticité des documents présentés et de leur cohérence et l'établissement d'une fiche d'identification « KYE ».

Le processus d'identification passe par les étapes suivantes :

- Accéder au module de filtrage par et insérer les informations du prestataire (nom, prénom, nationalité...) conformément à la procédure en vigueur.
- Contrôler les similitudes entre les données d'identification du candidat (figurant sur la carte d'identité), par rapport aux listes de sanctions et des personnes politiquement exposées (PEP).
- Editer le résultat de la recherche en ligne et le formulaire **KYP** et le classer dans le dossier du candidat.

Deux cas peuvent se présenter :

- Au cas où le prestataire figure sur **une liste de sanctions**, il faut refuser la candidature du postulant au poste d'emploi et informer sans délai la conformité.
- Au cas où le candidat existe sur la liste des personnes politiquement exposées (**PEP**), il faut adresser une demande d'autorisation à la conformité et ce, avant le recrutement du candidat au poste d'emploi.

## 2. Vigilance à l'égard des comptes à haut risques

Certains comptes revêtent un caractère particulier qui en fait des comptes à risque. Ils nécessitent une plus grande vigilance et une surveillance particulière. Tout compte ainsi juger, doit être identifié et soumis à vérifications périodiques.

Les chargés d'opérations doivent accorder une attention particulière aux :

- Opérations financières effectuées par des intermédiaires professionnels (tels que les agents des établissements de paiement, les bureaux de change et les sous délégués de change, les intermédiaires en matière de transactions immobilières, les Avocats, Les Huissiers Notaires, les commerçants d'objets d'art et des métaux précieux, les casinos, etc.,) pour leur propre compte ou pour le compte de leurs clients, personnes physiques et personnes morales.
- Nouveaux comptes ouverts au nom des associations et personnes morales nouvellement constituées.
- Opérations exécutées par des personnes dont le courrier est domicilié chez un tiers, dans une boîte postale ou bancaire ou qui changent fréquemment d'adresse.
- Comptes des personnes physiques gérés par des mandataires.
- Clients et opérations effectuées par ou au bénéfice de personnes politiquement exposées (PPE).
- Clients et opérations effectuées par ou au bénéfice de personnes résidents dans des pays présentant un risque élevé de blanchiment d'argent et de financement du terrorisme, notamment ceux listés par des instances internationales habilitées (GAFI).
- Mouvements de fonds d'importance significative.
- Comptes frappés par des mesures administratives ou des jugements judiciaires (gel judiciaire, saisie-arrêt, opposition administrative, etc.,).
- Transactions sur des comptes classés au niveau de la banque.
- Comptes frappés par des mesures de sanctions internationales (embargo, etc.,).

### ❖ Les comptes en dinars et en devises convertibles

Les comptes en Dinars convertibles ou en devises des non-résidents de nationalité tunisienne ou étrangère ou ayant des relations dans des pays désignés non coopératifs par le GAFI : Groupe d'Action Financière sur le blanchiment de capitaux doivent faire l'objet d'une vigilance renforcée.

Aussi et en application de la réglementation de change, l'alimentation des comptes en dinars ou en devises convertibles ne peut être effectuée que sur la base d'une déclaration

d'importation de devises délivrée par les services de douane (**Article 114 de la loi 2005-26 du 07 août 2015**).

❖ **Les comptes indisponibles**

Les Directeurs des Agences doivent porter une attention particulière aux comptes indisponibles (crées pour les sociétés en cours de constitution) et se conformer aux dispositions de la note de service N°14/2009 du 17/02/2009.

❖ **Les comptes ouverts par les Personnalités Politiquement Exposées (PPE) (Décisions CTAF Mars 2017 et juin 2018)**

Conformément à l'article 5 de la circulaire BCT 2018-09 du 08 octobre 2018, Les établissements assujettis doivent, dès l'entrée en relation d'affaires avec un client et/ou, le cas échéant, son mandataire, vérifier son identité et le domaine de son activité ainsi que son environnement bancaire et financier. Ils doivent procéder à un entretien lors du premier contact dont une fiche d'identification de client « KYC » visée par une personne habilitée, doit être versée au dossier du client, permettant :

- D'identifier juridiquement la personne.
- D'avoir une compréhension claire des activités, des revenus et du patrimoine du titulaire du compte.
- D'obtenir, lorsque le client est une personne morale, toute indication sur son courant d'affaires, par la communication, entre autres, des états financiers récents.
- D'obtenir, lorsque le client est une construction juridique toute information sur ses éléments constitutifs, les finalités poursuivies, les modalités de sa gestion et de sa représentation ainsi que l'identité des personnes l'ayant constitué et celles assurant sa gestion et les bénéficiaires effectifs.
- De comprendre et d'obtenir des informations sur l'objet et la nature envisagée de la relation.

A cet effet, les éléments d'information susceptibles d'être recueillis au titre de la connaissance de l'identité et de la situation juridique, professionnelle, économique et financière du client doivent être contenus dans la fiche d'identification de client « KYC » renfermant les informations minimales.

Les éléments d'identification ci-dessus doivent également être recueillis des personnes qui pourraient être amenées à faire fonctionner le compte d'un client en vertu d'une procuration et des gérants des personnes morales qu'ils soient salariés ou non.

Dans ce cadre et conformément à l'article 16 de la circulaire BCT n°2018-09, la banque doit observer une vigilance renforcer sur les Personnes Politiquement Exposées. À cet effet, ils doivent:

- ✓ Mettre en place les systèmes de gestion des risques permettant de déterminer si le client ou le bénéficiaire effectif est une personne politiquement exposée.
- ✓ Obtenir l'autorisation de nouer ou de poursuivre selon le cas une relation d'affaires avec une telle personne, du conseil d'administration ou du directoire ou de toute personne habilitée à cet effet.
- ✓ Prendre des mesures raisonnables pour comprendre l'origine du patrimoine et des fonds des clients et des bénéficiaires effectifs identifiés comme des personnes politiquement exposées.
- ✓ Assurer une surveillance continue et renforcée de cette relation.

Ces mêmes dispositions s'appliquent aux proches des personnes visées au paragraphe premier du présent article ainsi qu'aux personnes ayant des rapports étroits avec celles-ci. Sont considérés, comme personnes proches des personnes susvisées, les membres directs de leur famille: les ascendants et descendants, au premier degré ainsi que leurs conjoints. Est considérée comme personne ayant des rapports avec les personnes susvisées, toute personne physique connue comme entretenant avec celles-ci des liens d'affaires étroits.

- ❖ **Les comptes ouverts par les Partis politiques et les Associations : (régis respectivement par le décret-loi N°2011-87et le décret-loi N°2011-88 du 24/09/2011)**

Le chargé d'opération doit :

- ✓ S'assurer que le Parti n'a pas d'autres comptes ouverts auprès des banques confrères et ce, en consultant le site web de la BCT.
- ✓ Identifier les personnes agissant en leurs noms.
- ✓ Analyser rigoureusement les transactions effectuées sur leur compte notamment les dépenses et recettes d'un montant inférieur à 500 dinars effectuées en espèces.

## **2.1. Vigilance spécifique à l'égard des opérations de virement électronique de fonds**

En application des dispositions de la Circulaire BCT n° 2017-08, la banque est tenue d'appliquer des mesures de vigilance spécifique à l'égard des opérations de virement électronique de fonds.

A cet effet, la banque doit veiller à ce que les virements internationaux qualifiés (supérieur ou égal à 1000DT) comportent les informations exactes et complètes suivant :

### **2.1.1. En tant que banque de donneur d'ordre**

- Les informations exactes et complètes suivantes sur le donneur d'ordre :
  - Le nom et le prénom du donneur d'ordre.
  - Le numéro de compte bancaire du donneur d'ordre dès lors qu'un tel compte est utilisé pour réaliser l'opération, ou un numéro de référence unique d'opération permettant la traçabilité de l'opération ; et
  - L'adresse du donneur d'ordre, son numéro de carte d'identité nationale ou le numéro de passeport pour les non-résidents, leurs dates d'émission et de validité, ainsi que la date et le lieu de naissance.
  - L'objet de l'opération.
- Les informations complètes suivantes sur le bénéficiaire :
  - Le nom et le prénom du bénéficiaire ; et
  - Le numéro de compte bancaire ou postal du bénéficiaire ou en l'absence de compte, un numéro de référence unique d'opération permettant la traçabilité de l'opération.

### **2.1.2. En tant que banque Intermédiaire**

- S'assurer que le virement électronique contient toutes les informations sur le donneur d'ordre et le bénéficiaire.
- La mise en place de procédures appropriées pour détecter si, dans le système de messagerie Swift ou dans le système de paiement et de règlement utilisé pour le virement de fonds, les champs devant contenir les informations sur le donneur d'ordre et le

bénéficiaire ont été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions de ce système.

- Mise en place d'une politique et de procédures fondées sur le risque pour décider :
  - D'exécuter ou de suspendre les virements dont les informations sur les parties font défaut ou sont incomplètes.
  - Demander des informations complémentaires.
  - De rejeter les virements de fonds.
- Lorsqu'un établissement omet de manière répétée de fournir les informations requises sur le donneur d'ordre ou le bénéficiaire, la banque intermédiaire doit :
  - Dans un premier temps émettre un avertissement avec fixation d'échéances,
  - Rejeter tout nouveau virement de fonds provenant de cet établissement ; ou bien
  - Restreindre sa relation d'affaires avec celui-ci ;
  - Ou d'y mettre fin.
- La banque doit déclarer à la BCT cette omission ainsi que les mesures prises ;
- La banque intermédiaire apprécie, en fonction des informations manquantes ou incomplètes si le virement de fonds ou toute opération qui s'y rattache, présente un caractère suspect et doit être déclaré(e) à la CTAF.

#### **2.1.3. En tant que banque du bénéficiaire**

- L'application des procédures appropriées pour détecter si, dans le système de messagerie Swift, les champs devant contenir les informations sur le donneur d'ordre et le bénéficiaire ont été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions de ce système.
- La vérification, avant de créditer le compte du bénéficiaire ou de mettre les fonds à sa disposition, l'exactitude des informations sur son identité sur la base de documents, ou de données obtenues d'une source fiable.
- La conservation des dossiers et des pièces se rapportant aux identités des clients habituels et occasionnels pendant dix ans au moins de la date de la fin de la relation.
- La conservation des dossiers et des pièces se rapportant aux opérations et transactions pendant dix ans au moins de la date de leur réalisation.

Avant d'exécuter l'opération de virement, le chargé d'opération doit vérifier que ni le donneur d'ordre ni le bénéficiaire ne figurent sur une des listes de sanctions et ce, au moyen de l'application SIRON. A cet effet, le service concerné est tenu **de prendre les mesures de gel immédiat des fonds et de s'interdire de réaliser toute opération avec des personnes, organisations ou entités dont le lien avec des crimes terroristes ou des crimes de financement de la prolifération d'armes de destruction massive est établi par les instances onusiennes et l'autorité nationale compétente** et d'en informer la Direction de Contrôle de la Conformité.

Le chargé d'opération doit, aussi, refuser d'exécuter le virement si les informations requises sur le donneur d'ordre et le bénéficiaire font défaut ou sont incomplètes.

Avant d'exécuter un virement le chargé d'opération doit demander les motifs économiques ou licites de cette opération ainsi que les pièces justificatives (factures, contrats, etc...).

En fonction des informations recueillis sur l'opération de virement, le chargé d'opération doit vérifier la cohérence avec le profil du client. En cas d'incohérence ou de refus du client de présenter les documents justificatifs, il y a lieu de s'abstenir d'exécuter l'opération et de la déclarer à la Direction de Contrôle de la Conformité pour analyse et investigation.

La Direction de Contrôle de la Conformité analyse l'opération en fonction des risques et peut prendre les mesures suivantes :

- La suspension de l'exécution de l'opération tout en exigeant de l'établissement du donneur d'ordre, dans un délai raisonnable, les données manquantes.
- Le rejet de l'opération en cas de non réception des données manquantes.
- Proposer à l'organe d'administration ou l'organe de direction la cessation de la relation avec le correspondant concerné au cas où ce dernier ne respecte pas les exigences réglementaires requises en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.
- La déclaration de l'opération à la CTAF.

#### **Devoirs spécifiques en matière de virements émis nationaux :**

Pour tout virement national, il y a lieu d'inclure obligatoirement les renseignements relatifs **au donneur d'ordre et au bénéficiaire** (nom, prénoms et adresse pour les personnes physiques ou dénomination sociale et siège social pour les personnes morales et lorsqu'un compte existe, le numéro de ce compte. En l'absence d'un compte, un numéro de référence unique doit être inclus).

La banque doit aussi inclure l'adresse du donneur d'ordre, son numéro de CIN/ Passeport et leur date d'émission et de validité ainsi que la date et le lieu de naissance.

Ces données peuvent ne pas être incluses, si ces données peuvent être mises à la disposition :

- De l'établissement du bénéficiaire ou de la Banque Centrale de Tunisie par tout autre moyen dans les 3 jours ouvrables à compter de la réception, par l'établissement du donneur d'ordre, de la demande émanant de l'établissement du bénéficiaire ou de la Banque Centrale de Tunisie ; et
- Des autorités judiciaires immédiatement à leurs demandes.

Dans ce cas, l'établissement du donneur d'ordre inclut seulement le numéro de compte ou un numéro de référence unique d'opération permettant de reconstituer le parcours de l'opération jusqu'au donneur d'ordre ou au bénéficiaire.

#### **Devoirs spécifiques en matière de virements reçus :**

En cas de réception d'un transfert de fonds ou lorsque la Banque agit comme banque intermédiaire, une consultation systématique des identités du donneur d'ordre et du bénéficiaire est opérée par le module de filtrage approprié.

En cas de ressemblance d'identité avec celle figurant sur les listes consultées, le message SWIFT correspondant est automatiquement bloqué par ledit module. Son déblocage éventuel sera assuré par la Direction de Contrôle de la Conformité.

En cas de correspondance certaine et après vérification, la Direction de Contrôle de la Conformité doit bloquer l'exécution de l'opération ou de la transaction et déclarer, **immédiatement**, l'opération ou la transaction à la CTAF.

Outre, les vérifications précitées et à la réception du message SWIFT, le chargé de l'opération doit :

- Vérifier que les champs devant contenir les informations sur le donneur d'ordre et le bénéficiaire ont été complétés à l'aide de caractères ou d'éléments admissibles conformément aux conventions du système utilisé (SWIFT ou tout autre système de paiement et règlement utilisé) ;
- S'assurer, lorsque la Banque agit comme une Banque intermédiaire, que toutes les informations sur le donneur d'ordre et le bénéficiaire qui accompagnent un virement électronique y restent attachées. Lorsque des contraintes d'ordre technique font obstacle à ce que les informations requises sur le donneur d'ordre ou le bénéficiaire contenues dans un virement électronique transfrontalier soient transmises avec le virement électronique correspondant, la banque doit conserver pendant au moins dix ans les informations reçues de l'établissement du donneur d'ordre ou d'une autre banque intermédiaire ; s'assurer de l'existence de l'identité du donneur d'ordre sur le message reçu (SWIFT, etc,...). Lorsque l'identité n'y est pas indiquée lorsqu'elle est incomplète ou manifestement fictive ou lorsque les champs concernant ces informations n'ont pas été complétés à l'aide de caractères ou d'éléments admissibles, il y a lieu de s'abstenir d'exécuter l'opération ou de demander des informations complémentaires,
- Vérifier pour les transferts (qualifiés en devises) effectués en une transaction unique ou en plusieurs transactions qui semblent être liées, avant de créditer le compte du bénéficiaire ou de mettre les fonds à sa disposition, et lorsque cela n'a pas été fait précédemment, l'exactitude des informations sur son identité sur la base de documents, de données ou de renseignements obtenus d'une source fiable.
- Vérifier, systématiquement, l'identité du bénéficiaire effectif.
- Demander, au préalable, l'autorisation du Ministre chargé des finances si le virement concerne une personne morale soumise à une restriction conformément à l'article 72 de la loi n°2003-75 du 10 Décembre 2003 telle que modifiée par les textes subséquents.

Les services concernés ne sont pas tenus de vérifier l'exactitude des informations sur le bénéficiaire pour les virements de fonds non qualifiés en devises qui ne semblent pas être liés à d'autres transferts de fonds et dont le montant, cumulé avec celui du virement en question, excède la contrevaleur de 1000 dinars, à moins qu'il :

- Effectue le versement des fonds en espèces
- Ait des motifs raisonnables de suspecter des actes de blanchiment d'argent ou de financement du terrorisme.

Le chargé d'opération doit prendre des mesures raisonnables pour détecter les virements électroniques transfrontaliers pour lesquels il manque les informations requises sur le donneur d'ordre ou sur le bénéficiaire, notamment au moyen d'un contrôle à postérieur ou, lorsque cela est possible, d'un contrôle en temps réel.

Lorsqu'un correspondant omet de manière répétée de fournir les informations requises sur le donneur d'ordre ou le bénéficiaire, la banque peut prendre l'une de ces mesures :

- L'émission d'avertissemens et la fixation d'échéances.
- Le rejet de tout nouveau virement provenant de cet établissement.
- La restriction ou même la rupture de la relation d'affaires avec celui-ci.
- La déclaration à la BCT de cette omission et les mesures prises à cet égard.
- La déclaration ou non à la CTAF en fonction des informations manquantes ou incomplètes.

#### **Devoirs spécifiques en matière de change manuel**

Lorsque l'opération de change manuel (achat / vente de devise), il y a lieu de s'assurer de l'identité du client occasionnel et de porter, obligatoirement, les éléments d'identification du client sur le bordereau d'échange ou sur le reçu et lui remettre une copie.

Les éléments d'identification du client, à mentionner sur le bordereau d'échange ou sur le reçu, sont :

- Pour les personnes physiques : le nom, le prénom et l'adresse, le type et le numéro de la pièce d'identité ainsi que sa date d'émission.
- Pour les personnes morales : la dénomination sociale, le siège social et l'identification du représentant.

En outre et lorsque l'opération de change manuel porte sur un montant dont la contre-valeur est égale ou supérieure à vingt mille (20.000) dinars, il y a lieu d'exiger une déclaration d'importation de devises visée par la Douane.

**Les opérations de change manuel dont la contre-valeur est supérieure ou égale à cinq mille (5000) dinars doivent faire l'objet d'une déclaration à la BCT à travers la**

plateforme du système d'échange des données (SED), au plus tard 15 jours ouvrables, après leur réalisation et ce, conformément aux dispositions de la circulaire BCT n° 2012-11 du 8 août 2012.

### **3.Détection des opérations suspectes**

Dans le cadre de la détection des opérations inhabituelles ou suspectes, le chargé d'opération doit :

- ✓ Prêter une attention particulière aux opérations ou transactions revêtant un caractère complexe ou d'un montant anormalement élevé et aux opérations inhabituelles.
- ✓ Examiner le cadre et le but dans lesquels ces opérations ont été effectuées.
- ✓ Communiquer par écrit le résultat de cet examen à la Direction de Contrôle de la Conformité qui se chargera de le communiquer, après étude, à la CTAF.

Sur le plan pratique, Trois modules sont mis en place :

#### **✿ Le module KYC :**

Permet le filtrage des clients par rapport à des listes de sanction et des PPE.

Cas	Action à entreprendre
Client figurant dans une liste des sanctions	Ne pas ouvrir le compte et soumettre une déclaration de soupçon à la conformité.
PPE, Associations, Partis Politiques, Bureau de change, non-résident, location d'un coffre-fort et tout client présentant un score risque élevé selon la fiche « KYC ».	Informier la conformité pour recueillir l'accord de la Direction Générale ou du Conseil d'Administration.
Client présente un score risque Moyen selon la fiche « KYC ».	Demander l'avis préalable du Directeur d'agence avant d'entamer la procédure d'ouverture de compte.
Client ne figurant sur aucune liste et présente un score risque faible selon la fiche « KYC ».	Entamer la procédure d'ouverture de compte conformément à la réglementation en vigueur

Le module KYC permet également le profilage du client c'est-à-dire la connaissance de la clientèle et l'attribution d'un niveau de risque variant selon l'occurrence d'un nouvel élément et selon le risque attribué, on applique le niveau de vigilance adapté.

#### **✿ Le module AML :**

Déployé au niveau de la Direction de Contrôle de la Conformité, est un module d'analyse avancée permettant de détecter le blanchiment d'argent et le financement du terrorisme.

Il contrôle les clients, les comptes et les transactions avec une précision, à la recherche d'activités suspectes. Des scénarii sont implantés après l'approbation du conseil d'administration au niveau de SIRON AML permettant la détection de ces opérations. Le paramétrage de AML a été fondé sur une approche dynamique et l'attribution d'une classe de risque instantanée.

Cette approche est basée sur 4 niveaux de risques :

- Chaque critère de risque se voit consacrer une cotation (score).
- Plus le score est élevé, plus le client est risqué.

#### Le module EMBARGO :

Permet :

- ✓ L'interfaçage avec SWIFT (Mécanismes complets de recherche pour identifier les transactions en lien avec un terroriste) et la détection des données suspectes d'un émetteur/destinataire d'une transaction.
- ✓ Le contrôle en temps réel des données de l'émetteur/du destinataire sur la base des listes de sanctions nationales et internationales émises par le bureau américain de contrôle des avoirs étrangers (OFAC), les listes UN, UE, etc....

#### Le module GTI-TBML :

C'est un module permet à la banque de contrôler les opérations de commerce extérieur et les transferts à l'international en vue d'identifier les activités et les transactions potentiellement inhabituelles, complexe ou suspectes et de se conformer à la réglementation nationale en matière de Lutte contre le Blanchiment d'Argent et de Financement du Terrorisme (LAB/FT). Les opérations et les transactions présentant un risque élevé en matière de blanchiment d'argent et de financement du terrorisme seront systématiquement acheminées à la conformité pour analyse, contrôle et investigation et ce, selon une matrice risque préalablement définie.

### **3.1. Traitement des alertes générées**

La banque dispose d'un outil de traitement des alertes permettant de détecter les éventuelles opérations suspectes de la manière la plus efficace en adoptant l'approche par les risques et ce, en se basant sur des scénarios préétablis et validée par le Conseil d'Administration.

Les alertes générées par l'outil font l'objet d'un suivi quotidien par la conformité dans le cadre de sa mission de contrôle LAB/FT.

Le suivi consiste à examiner attentivement les opérations et les transactions effectuées tout au long de la relation d'affaire afin de vérifier si ces transactions sont en adéquation avec l'activité habituelle du client et son profil de risque et d'examiner dans la mesure possible, le contexte et l'objet de toute opération inhabituelle ou complexe ou qui n'a pas d'objet économique ou licite apparent.

Le traitement des alertes sur la base d'une analyse documentée, donne lieu à un classement sans suite dûment motivé ou à une déclaration de soupçon à la CTAF.

### **3.2. Balayage de la base de données clients**

L'outil AML permet le filtrage des clients par rapport à liste des sanctions et la liste des personnes politiquement exposées « PPE ». Pour détecter les relations sanctionnées ou politiquement exposées, la Direction chargée des Systèmes Informatiques procède à un **balayage quotidien delta et un balayage total mensuel** de la Base de données. Le rapport de balayage sera communiqué à la conformité pour analyse et traitement.

En cas d'incident ou de dysfonctionnement survenu au moment des opérations de balayage de la base de données clients, la conformité devrait être avisé dans l'immédiat.

## VII. Déclaration des opérations suspectes et inhabituelles

### Désignation d'un correspondant de la CTAF et son suppléant

Selon l'Article 13 de la décision de la Commission Tunisienne des Analyses Financières (CTAF) n°2017-02 du 2 mars 2017 « Les institutions financières doivent désigner parmi leurs dirigeants ou agents ayant au moins le grade de directeur, ou son équivalent, un correspondant de la Commission Tunisienne des Analyses Financières chargé de l'examen des opérations ou transactions suspectes et, le cas échéant, de leur déclaration à la Commission Tunisienne des Analyses Financières. Elles doivent également désigner un correspondant suppléant remplissant la même condition. Les institutions financières doivent communiquer au Secrétariat Général de la Commission Tunisienne des Analyses Financières la décision de désignation du correspondant et de son suppléant avec indication de leur qualité, fonction ainsi que de leurs coordonnées et adresses électroniques. Le correspondant et son suppléant doivent assister aux réunions périodiques des correspondants avec la Commission chaque fois qu'ils y sont conviés. Le correspondant ou son suppléant doivent fournir, dans les meilleurs délais, à la Commission tous les documents et informations qu'elle demande ».

Le premier responsable en charge de la structure de contrôle de la conformité assure le rôle de **correspondant** auprès de la Commission Tunisienne des Analyses Financières (CTAF).

### Déclaration des opérations suspectes

La déclaration d'opérations suspectes permet d'alerter les autorités sur la possibilité qu'une transaction particulière qui puisse être liée au blanchiment de capitaux et qu'elle mérite par conséquent de faire l'objet d'une enquête approfondie.

L'obligation de déclaration est dans le prolongement de l'obligation de diligence. Si l'opération projetée fait naître un soupçon, la banque doit faire une déclaration de soupçon à la CTAF.

Afin que la déclaration de soupçon soit acceptée par l'organisme spécialisé dans la lutte contre le blanchiment d'argent et le financement du terrorisme, soit la CTAF, la banque doit respecter certaines conditions relatives au fonds à savoir les opérations soumises à la déclaration et la confidentialité.

### Opérations soumises à la déclaration

Conformément aux dispositions de la loi organique telle que complétée par la décision de la CTAF n°2017-01, les assujettis sont tenus de déclarer, à la CTAF, toute opération lorsqu'elle porte sur des capitaux paraissant provenir d'une infraction ou semblent être destinés au financement du terrorisme. Ce système de déclaration de soupçon est subjectif. En effet, il appartient à chaque professionnel de se livrer à une analyse personnelle des faits et des caractéristiques intrinsèques des opérations se présentant à lui.

Ainsi, toute opération ou transaction jugée suspecte, initiée au niveau des agences et des services centraux doit faire l'objet d'analyse et d'investigations. Lorsque les agences ou les services centraux disposent d'informations confirmant la suspicion, elles (ils) doivent

remonter à la Conformité, sans délai la suspicion accompagnée des justificatifs de l'opération ou de la transaction et comportant la fiche d'identification « KYC » valide du client. Lorsque l'examen confirme le soupçon, la conformité doit déclarer immédiatement l'opération ou la transaction à la Commission Tunisienne des Analyses Financières (CTAF).

L'obligation de déclaration s'applique même **après** la réalisation de la transaction, lorsque de nouvelles informations sont susceptibles de relier, directement ou indirectement, ladite transaction à des fonds provenant d'actes illicites qualifiés par la loi de délit ou de crime, ou au financement du terrorisme.

#### ❖ Au niveau des structures opérationnelles de la banque :

Le chargé de l'opération doit :

- ✓ Relever tout mouvement suspect pouvant être lié directement ou indirectement à une opération de blanchiment d'argent.
- ✓ S'entretenir le cas échéant, avec le client au sujet de l'opération détectée sans lui faire sentir la suspicion.
- ✓ Juger le bienfondé de cette suspicion avec le responsable hiérarchique.
- ✓ Etablir, le cas échéant, le jour même, une déclaration selon le modèle prévu par la décision n° 01 de la CTAF.
- ✓ Transmettre à la conformité, sans délai, la déclaration préliminaire de soupçon accompagnée des justificatifs relatifs à l'opération, du dossier d'ouverture de compte et de la fiche d'identification « KYC » valide.

#### ❖ Au niveau de la conformité

La conformité est tenue de:

- ✓ Apprécier le bienfondé de la suspicion, par rapport aux critères établis et aux typologies retenues et pousse les investigations sur l'opération et la personne si elle le juge nécessaire.
- ✓ Examiner les alertes détectées par les modules de filtrage et de profilage.
- ✓ Etudier minutieusement les documents parvenus des différentes structures opérationnelles de la Banque et s'assure que la déclaration comprend toutes les informations utiles qu'elle aura à compléter le cas échéant.
- ✓ Procède ensuite à la consultation du fichier des déclarations centralisées à son niveau pour inclure s'il y a lieu les déclarations antérieures enregistrées sur la même relation.
- ✓ Décider du sort des personnes suspectes et des opérations inhabituelles.
- ✓ Etablir et transmettre le cas échéant, la déclaration définitive à la CTAF, en la complétant le cas échéant par l'inclusion des antécédents enregistrés sur le même client, si la suspicion est confirmée.

L'envoi des déclarations à la CTAF se fait à travers l'application web GoAML.

Les types des déclarations de soupçons disponibles sur l'application GoAML sont :

- Déclaration de transaction suspecte (STR).
- Déclaration d'activité suspecte (SAR).
- Déclaration de financement de terrorisme (TFR).

- Déclaration d'activité relative au financement de terrorisme (TAR).

Toute information complémentaire (relevés du compte, nouvelle transaction, pièces comptables, etc...) liée à une déclaration antérieure doit être communiquée ; selon le type d'information qu'il contient ; en tant qu'un rapport de type :

- « Information complémentaire avec transaction » (AIFT)
- « Information complémentaire sans transaction » (AIF)

Le déclarant doit obligatoirement indiquer dans la zone « Référence CTAF » la référence qui lui a été communiquée par la CTAF une fois sa déclaration initiale a été validée.

Une réponse à une demande d'informations émanant de la CTAF doit être fournie en tant qu'un rapport de type :

- « Réponse à une demande d'information avec transaction » (ORDRT)
- « Réponse à une demande d'information sans transaction » (ORDRe).

Dans ces types de rapport, le déclarant doit mentionner dans la zone « Référence CTAF » la référence attribuée par la CTAF à la demande.

Une réponse à un signalement émanant de la CTAF doit être fournie en tant qu'un rapport de type :

- « Réponse à un signalement avec transaction » (RSIGT)
- « Réponse à un signalement sans transaction » (RSIG).

Dans ces types de rapport, le déclarant doit mentionner la référence dans la zone « Référence CTAF » attribuée par la CTAF au signalement.

### **Délai de déclaration de soupçon**

La déclaration de soupçon peut être effectuée au moment de l'exécution de l'opération et peut aussi être effectuée après la réalisation de l'opération.

La déclaration de soupçon après la réalisation de l'opération peut intervenir dans les cas suivants :

- Impossibilité de surseoir à son exécution
- Report pouvant faire obstacle au bon déroulement des investigations portant sur une opération suspectée de blanchiment d'argent ou de financement du terrorisme.
- Soupçon apparu postérieurement à la réalisation de l'opération en cause.

A la demande d'informations sollicitées par la CTAF, la Conformité à son tour demande des Agences ou des structures centrales des documents d'ouverture de compte, les KYC, les dossiers de la transaction (SWIFT, Factures, Titres ...), ces documents doivent être communiqués à la Conformité dans un délai de 48 heures. Pour les dossiers égarés ou inexistant, l'Agence doit fournir une explication écrite validée par la Hiérarchie (Agences incendiées, déménagements, inondations ...)

### **Suivi des décisions de la CTAF**

Deux hypothèses peuvent se présenter :

**Première hypothèse :** Si la suspicion s'avère infondée selon la CTAF, la conformité classe le dossier en indiquant le motif d'infirmation.

**Deuxième hypothèse :** Si la suspicion est confirmée par la CTAF, la conformité procède comme suit :

- La suspension provisoire et préventive de l'opération déclarée au cas où les éléments de suspicion convergent vers une probable décision de gel et que le risque de retirer les fonds objets de la déclaration est très fort.  
A l'expiration d'un délai de 48 heures à partir de la date du dépôt de la déclaration, signifie à l'entité concernée (Agences ou Structure Centrale) la levée de la suspension provisoire et préventive de l'opération détectée après avis de la CTAF et lorsque cette dernière ne statue pas sur la déclaration dans ce délai.
- Le blocage des fonds sur décision de la CTAF, exige de l'entité concernée de geler les fonds relatifs à l'opération déclarée dans le compte d'attente approprié jusqu'à nouvel ordre et de lui retourner sans délais, la justification de gel.

#### **Enregistrement des déclarations de soupçon**

A l'occasion de chaque déclaration de soupçon reçue, qu'elle soit justifiée ou infondée, la conformité procède à l'enregistrement et à la saisie de la suspicion en lui attribuant un numéro d'ordre spécifique et constitue un dossier comprenant :

- ✓ La déclaration préliminaire
- ✓ La déclaration définitive revêtue de la décharge/référence du dossier de la CTAF
- ✓ Les décisions de la CTAF
- ✓ Les correspondances entre la conformité et l'entité déclarante.
- ✓ Toute autre correspondance et tout autre échange de courrier au sujet de la déclaration.

Lorsque sur un même client il est enregistré plusieurs déclarations, le dossier comportera autant de sous-dossiers que de déclarations.

### **VIII. OBLIGATION DE RESERVE ET DE CONFIDENTIALITE**

#### **❖ Obligation de réserve :**

Conformément à la loi N° 2015-26 du 07 Août 2015, il est interdit d'informer le client ou toute autre personne du déroulement de la procédure de déclaration et des décisions de la CTAF. Cette interdiction vise à préserver la confidentialité de la procédure. Le responsable au niveau de l'agence ou de la structure concernée doit en conséquence s'interdire de fournir au client des informations et des renseignements sur le déroulement de l'opération déclarée.

#### **❖ Obligation de confidentialité :**

Les responsables au niveau des structures impliquées dans les opérations de détection et de déclaration en vertu du présent manuel sont tenus d'une obligation de diligence et de vigilance qu'ils s'engagent à accomplir conformément aux dispositions qui précèdent et dans l'esprit de la loi édictée dans le domaine de la lutte contre le blanchiment d'argent. Ils s'engagent, également, à ne pas divulguer les informations relatives aux opérations détectées et aux conséquences de la déclaration.

La déclaration des opérations suspectes ou la communication des documents y relatifs par les assujettis à l'autorité compétente implique nécessairement que ces informations soient

traitées d'une manière confidentielle. Aucune correspondance ou documentation échangée entre les différentes structures de banque ne doit être communiquée au clients de la banque. De même l'identité des personnes chargées de faire des analyses et des investigations ne doit aucun cas communiqué aux clients de la Banque notamment, l'identité et les coordonnées des collaborateurs de la conformité.

Les membres de la Commission Tunisienne des Analyses Financières (CTAF), leurs collaborateurs et tout autre agent appelés en vertu de leurs fonctions à accéder aux informations objet des déclarations concernant les opérations ou transactions suspectes sont tenus au respect du secret professionnel. Ils ne peuvent de ce fait, même après cessation de leurs fonctions, utiliser les renseignements dont ils ont eu connaissance à des fins autres que celles exigées par la mission qui leur est dévolue.

Les collaborateurs de la Banque sont aussi tenus de ne pas divulguer au client ou à quiconque la déclaration ainsi établie. Dès que la CTAF est informée, le banque ne doit plus informer la personne concernée de la déclaration dont elle a fait l'objet et des mesures qui en ont résulté.

La banque doit définir les règles de déontologie et de professionnalisme en matière de déclaration de soupçon notamment celles relatives à l'obligation de confidentialité. Et elle doit se doter de procédures internes claires et précises en vue d'assurer la bonne application et le respect des dispositions légales et réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Ces procédures doivent être portées à la connaissance de tout le personnel principalement celui en contact avec la clientèle.

Il importe de souligner qu'une **rupture de l'obligation de secret** dans le but de permettre à l'auteur de l'opération de blanchiment de capitaux ou de financement du terrorisme de se soustraire aux conséquences de la déclaration effectuée ou à effectuer pourrait, en fonction des circonstances, constituer en outre **un acte de complicité** de blanchiment de capitaux ou de financement du terrorisme.

## IX. Responsabilité des déclarants

Conformément à l'article **137 de la loi N°2015-26 du 07 août 2015** : « Aucune action en dommage ou en responsabilité pénale ne peut être admise contre toute personne physique ou morale pour avoir accompli, de bonne foi, le devoir de déclaration prévu à l'article 125 de la loi ».

## X. Suivi des déclarations

Le suivi de la déclaration de soupçon ne doit pas être oublié. Si de nouveaux éléments sérieux apparaissent tendant à renforcer le soupçon initial ou au contraire à l'infirmer le déclarant doit avertir immédiatement la CTAF.

### ❖ Au niveau de la conformité

- Tenir un registre d'arrivée des déclarations parvenues à la conformité.
- Tenir un fichier des déclarations qui doit comporter :
  - ✓ La référence
  - ✓ La date et heure de la déclaration parvenue des différentes structures de la Banque
  - ✓ La date et l'heure de la réception de la déclaration
  - ✓ Structures concernées

- ✓ Le déclarant
- ✓ Le numéro du compte
- ✓ Le nom et prénom du client
- ✓ La nature de l'opération
- ✓ Le montant
- ✓ Tiers (bénéficiaire, donneur d'ordre)
- ✓ Soupçons
- ✓ La date et l'heure de communication de soupçon à la CTAF
- ✓ Le sort réservé au soupçon
- ✓ La date de communication du sort par la CTAF
- ✓ Observations.
- Suivi des deux comptes d'attente (dinars et devises) relatifs aux sommes gelées ouverts au niveau des Agences.
- Envoi à la BCT (Direction Générale de la Supervision Bancaire) au plus tard un mois après la clôture de l'exercice un état indiquant :
  - ✓ Le nombre total des déclarations effectuées à la CTAF au cours de l'exercice clôturé
  - ✓ Le montant total des opérations déclarées au cours de l'exercice clôturé réparti par nature d'opération et par catégorie de clientèle (personnes physiques et personnes morales).

❖ **Au niveau de l'agence ou du Service Central**

- Tenir un registre des déclarations transmises à la conformité pour consigner les suites qui leur sont réservées.

## XI. Devoir de gel des avoirs

### 1. Gel des personnes ou d'organisation dont le lien avec des crimes terroristes est établi par des instances nationales et onusiennes compétentes

En application des dispositions de l'article 103 de la loi n°2015-26 du 07/08/2015 et du décret gouvernemental n°2019-72 du 1<sup>er</sup> février 2019 portant sur les procédures de mise en œuvre des résolutions prises par les instances onusiennes compétentes liées à la répression du financement du terrorisme et de la prolifération des armes de destruction massive, les responsables concernés au niveau des agences sont tenus de procéder au gel, sans délai et sans notification préalable, des avoirs des personnes ou d'organisations dont le lien avec des crimes terroristes ou des crimes de financement de la prolifération d'armes de destructions massives est établi par la Commission Nationale de Lutte Contre le Terrorisme (CNLCT) ou des instances onusiennes compétentes et ce dès réception de la décision de gel communiquer par la conformité.

### 2. Gel et levée de gel des avoirs sur instruction d'une instance judiciaire compétente

#### Réception de la décision de gel au niveau de l'agence

Dès réception de la décision de gel de la part d'une instance judiciaire compétente, l'Agence ou toute autre Direction concernée, doit :

- S'abstenir de mettre les fonds à la disposition du client sanctionné
- Procéder immédiatement et sans délai au gel des fonds existants au niveau de tout type de comptes détenus par le client (l'étendue du gel est fixée dans la décision).

- Virer instantanément les montants bloqués des clients sanctionnés dans les comptes d'attente appropriés prévus à cet effet selon la réglementation en vigueur.
- Procéder au blocage et virement dans le compte d'attente approprié, tout montant venant alimenter le compte du client après le premier blocage.
- Transmettre **immédiatement après exécution**, à la conformité les décisions de gel.
- Communiquer le jour même, à la conformité, un extrait de compte d'attente retraçant les opérations de gel exécutées dans ces comptes.

#### Réception de la décision de gel au niveau de Direction de contrôle de la Conformité

Dès réception de la décision de gel, la conformité doit :

- Procéder à l'intégration manuelle, sans délai, de la nouvelle liste des personnes sanctionnées au niveau de l'applicatif SIRON
- Procéder aux recherches nécessaires, par le biais des applicatifs mis à sa disposition ou en sollicitant les directions concernées et agences de la Banque, en vue de déceler l'existence éventuelle, parmi les relations d'affaires de la banque, de personnes ou d'organisations concernées par les décisions de gel.
- Ordonner à toute agence ou autre structure concernée l'exécution immédiate de la décision du gel des avoirs.
- Déclarer à l'instance nationale de lutte contre le terrorisme toutes les opérations de gel effectuées lorsqu'il s'agit de personnes ou d'organisation dont le lien avec des crimes terroristes est établi par des instances onusiennes compétentes ou nationales.
- Informer l'autorité judiciaire compétente de l'exécution de la décision de gel lorsqu'il s'agit d'une décision judiciaire.

A la réception des extraits des comptes d'attente des Points de vente, la conformité doit :

- S'assurer que les comptes bloqués sont conformes aux listes des clients sanctionnés ;
- Notifier **instantanément** par courrier électronique les justificatifs de blocage aux émetteurs de décisions de Gel ;
- Transmettre par courrier ordinaire les justificatifs de blocage aux émetteurs de décisions de gel dans un délai ne dépassant pas **3 Jours ouvrables** ;
- Suivre les comptes gelés par décision de la CTAf et de la CNLCT.

#### Réception de la décision de levée de gel

Aussi et dès la réception des décisions de levée totale ou partielle de gel ou de confiscation, la conformité est tenue de :

- Transmettre, le jour même, une copie de ces décisions aux agences concernées, pour **exécution immédiate et crédit des comptes des clients**;
- Suivre les opérations de levée de gel effectuées par les agences sur la Base de l'extrait des comptes d'attente débités.

**Remarque :**

- Les comptes gelés ne doivent faire l'objet **d'aucun mouvement débit sous aucun motif quel qu'il soit.**
- Tout déblocage sans autorisation préalable de la conformité est susceptible de sanctions pénales au sens de la **loi organique n°2015-26.**

### 3. Gel des avoirs sur instructions de la CTAF

En application des dispositions des articles 127, 128 et 131 de la loi n°2015-26 du 07/08/2015, la banque est tenue de procéder, sur instructions de la CTAF, au gel provisoire des fonds résultant d'une transaction ayant fait l'objet d'une déclaration de soupçon.

Sur instructions de la conformité, l'agence ou toute autre structure concernée doit loger les montants ayant fait l'objet d'une décision de gel dans un compte de gestion ouvert à l'occasion (Compte d'attente approprié) pendant un délai maximum de six (06) jours à compter de la date du gel.

En l'absence d'une décision judiciaire confirmant le gel et à l'expiration du délai ci-dessus mentionné, le gel est considéré comme nul et non avenu et l'agence est tenue de reloger les fonds gelés au compte du client.

Il demeure entendu qu'il y a lieu de s'abstenir d'informer la personne concernée de la décision du gel provisoire et des mesures qui en ont résulté.

## XII. Echange d'informations entre le groupe BH

Les entités du groupe BH Bank sont tenues, sous réserve du respect de la réglementation en matière de secret professionnel et protection des données à caractère personnel, de mettre en œuvre des politiques et des procédures :

- ✓ De partager les informations requises relatif à la clientèle aux fins de devoir de vigilance en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.
- ✓ De la mise en place d'une base mutualisée et interfacée avec leurs systèmes d'information permettant l'échange d'informations relatives aux clients, aux comptes et aux opérations, lorsqu'ils sont nécessaires aux fins de vigilance en matière LAB/FT.

Les entités du groupe définissent les procédures à adopter entre eux en matière d'échange des données au niveau de la base mutualisée.

Les échanges d'informations à des fins de vigilance LAB/FT ne peuvent être effectués qu'entre les fonctions de conformité des entités concernées. Chaque entité du groupe désigne nominativement la personne habilitée à échanger et/ou à avoir accès aux informations mutualisées au niveau de la base des données.

### XIII. Conservation des documents

#### ❖ Obligation de conservation

Les Agences et les Services Centraux concernés doivent conserver le dossier du client et les pièces se rapportant à son identité pendant **dix ans (10) au moins** à compter de la date de la fin de la relation.

De même, ils doivent conserver les documents et informations relatifs aux opérations et transactions effectuées par leurs soins sur support électronique et/ou sur support papier pendant dix ans (10) au moins à compter de la date de leur réalisation. En effet, les responsables sont tenus de conserver les documents relatifs aux ouvertures de compte, et aux opérations nécessitant des justificatifs.

Aussi, la banque est tenue de conserver toute correspondance avec la CTAF, ainsi que chaque décision de gel publié au JORT et les mesures prises pour son exécution.

D'après l'**Article 113 de la Loi 2015-26**, « Les personnes visées à l'article 107 de la loi doivent conserver pendant **dix ans à compter de la date de la réalisation de l'opération ou de la clôture du compte**, les registres, livres comptables, et autres documents qu'ils détiennent sur support matériel ou électronique aux fins de consultation, le cas échéant et pour les besoins de traçabilité des différentes phases des transactions et opérations financières effectuées par leur soins ou par leur intermédiaire et identifier tous les intervenants et de s'assurer de leur véracité ».

#### ❖ Au niveau de la Direction Régionale ou du Service central

Les responsables des Directions Régionales ou des Services Centraux sont tenus de la conservation des documents relatifs :

- ✓ Aux ouvertures de compte telle que régies par les procédures d'ouverture de compte en vigueur.
- ✓ Aux opérations nécessitant des justificatifs. A cet effet, la conservation doit s'effectuer par la tenue de dossier comportant les justificatifs de l'opération. Les références à porter sur le dossier sont : la date et la référence de la transaction attribuée par le système.

Le classement de ces dossiers se fait par :

- ✓ Identifiant : pour les clients ayant une relation contractuelle avec la Banque.
- ✓ Type et numéro de la pièce d'identification (CIN, CS, P) : pour les clients occasionnels.
- ✓ Aux opérations déclarées à la Direction de Contrôle de la Conformité, ainsi que des pièces relatives aux suites données à ces déclarations.

#### ❖ Au niveau de la conformité

La conformité est tenue de procéder à la création d'un dossier pour :

- ✓ Chaque déclaration reçue, comportant les documents s'y rapportant ainsi que toute correspondance avec la CTAF.
- ✓ Chaque décision de gel publié au JORT ainsi que les mesures prises pour son exécution (gel des fonds et déclaration au Ministère chargé des Finances).

#### ❖ Obligation de Mise à jour des dossiers Juridiques des clients

Le chargé d'opération est tenu de procéder à une mise à jour périodique des dossiers juridiques de leurs relations d'affaires personnes physiques et personnes morales.

La mise à jour des données nécessite :

- La collecte des documents et justificatifs y relatifs.
- La conservation des documents actualisés dans le dossier juridique tenu au niveau de l'agence.
- La mise à jour de la fiche d'identification du client « KYC » et la saisie des nouvelles données sur le système d'information de la banque.

La périodicité de la mise à jour des dossiers juridiques dépend du score risque affecté à la relation :

- Pour les relations d'affaires dont le niveau **score risque est élevé**, la mise à jour doit être effectué **chaque année**.
- Pour les relations d'affaires dont le niveau **score risque est moyen**, la mise à jour doit être effectuée tous les **deux (02) ans**.
- Pour les relations d'affaires dont le niveau **score risque est faible**, la mise à jour doit être effectuée tous les **trois (03) ans**.

Lors de la constatation de toute nouvelle information affectant l'identification client ; par exemple du fait d'un changement d'actionnaire majoritaire au sein de la société, changement de dirigeants, le changement de mandataire, le changement d'adresse, le changement d'activité, etc... la mise à jour du dossier doit être effectuée instantanément.

En cas de doute quant à la véracité ou à la pertinence des informations fournies sur l'identité du client ou lorsqu'il y a soupçon de blanchiment d'argent ou de financement du terrorisme, une nouvelle identification doit être effectuée.

#### XIV. Formation et veille interne

La Direction chargée de la formation doit arrêter annuellement en collaboration avec la conformité, un programme de formation continue au profit des employés de la banque comprenant des informations sur les techniques, méthodes et tendances en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Cette formation doit porter sur tous les aspects de la réglementation en la matière et notamment, les obligations relatives au devoir de vigilance à l'égard des clients et des opérations et de déclaration des opérations et des transactions suspectes.

La banque doit mettre en place un programme permanent de formation préparant convenablement son personnel à la connaissance des dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme. Le calendrier et le contenu des séances organisées devront être adaptés aux nécessités spécifiques de la banque.

La banque doit s'assurer que les procédures sont communiquées à tout le personnel et permettre à chaque collaborateur de rapporter toute opération suspecte au responsable de la conformité en matière de lutte contre la blanchiment d'argent et le financement du terrorisme.

La conformité doit définir dans un document les critères de déontologie et de professionnalisme en matière de déclaration. Ce document est obligatoirement porté à la connaissance de tout personnel de la Banque.

Les actions de formation et de sensibilisation doivent se dérouler comme suit :

- ✓ Au moment de recrutement des nouveaux collaborateurs.
- ✓ Périodiquement pour les opérationnels concernés par la lutte contre le blanchiment d'argent et le financement du terrorisme.
- ✓ A l'occasion de l'évolution du dispositif réglementaire en matière de lutte contre le blanchiment d'argent et le financement du terrorisme et à l'évolution de l'activité de la banque.

Les modules de formation et ceux de la sensibilisation en matière LAB/FT, doivent être conçus et préparés sous la responsabilité de la conformité.

## XV. DISPOSITIF DE CONTROLE INTERNE EN MATIERE LAB/FT

Le dispositif de lutte contre le blanchiment d'argent repose sur sa parfaite intégration dans le dispositif de contrôle interne mis en place par l'organisation et qui constitue le premier rempart dans la prévention et la maîtrise des risques. Le dispositif de contrôle interne est constitué du dispositif de contrôle de la conformité, de gestion de risque et de l'audit. Ces structures sont distinctes et indépendantes l'une de l'autre, tout en étant complémentaires et coordonnées.

Le système de contrôle interne au sein de la Banque est conçu sur la base du modèle des trois lignes de défense relatif aux systèmes de contrôle interne et de management des risques :

- **La première ligne de défense** ou de maîtrise des activités est constituée par les managers et les opérationnels seuls responsables de l'évaluation et de la réduction des risques dans les processus dont ils ont la charge et ce à travers des contrôles opérationnels réalisés au fil de l'eau sur les opérations traitées et des contrôles hiérarchiques opérés par les responsables sur les travaux réalisés par les opérationnels. La première ligne de défense est assurée par les chargés de métiers dont ont la charge de contrôler au fil de l'eau les opérations de débit et de crédit dépassant un seuil fixé et d'informer la conformité pour les opérations suspectes ou inhabituelles.
- **La deuxième ligne de défense** est constituée par les fonctionnels et qui ont pour objectifs de coordonner et de structurer le dispositif de maîtrise des risques de l'organisation, ces actions comprennent l'assistance des opérationnels dans l'identification et l'évaluation des principaux risques, l'élaboration de la politique et la contribution à la conception des contrôles plus robustes ainsi que le développement des meilleures pratiques et le compte rendu sur l'état de fonctionnement effectif des processus. En matière de LAB/FT, la deuxième ligne de défense est pilotée par la fonction de contrôle de la conformité selon une approche

par les risques en utilisant les outils informatiques dédiés SIRON Embargo (filtrage des opérations par SWIFT par rapport aux listes de sanctions et liste des pays à haut risque ou les pays dont sa juridiction présentant de insuffisances selon le GAFI).

Il reste entendu que la conformité est une instance de contrôle permanent de 2ème niveau en matière LAB/FT chargée de veiller au respect des lois et des exigences réglementaires et déontologiques au niveau de la Banque. Elle est indépendante des fonctions commerciales et opérationnelles.

- **La troisième ligne de défense** concerne l'évaluation globale et indépendante du dispositif de maîtrise des risques, ces évaluations sont réalisées par l'audit interne qui donne aux organes de gouvernance une assurance que la maîtrise des risques est efficiente et efficace. C'est la direction de l'audit de la Banque qui assure l'audit du dispositif LAB/FT tous les deux ans et ce, selon l'article 50 de la circulaire BCT 2017-08 qui stipule que « ...Le dispositif de contrôle interne pour la gestion du risque blanchiment d'argent doit être audité selon une périodicité qui tient compte de la nature, du volume et de la complexité des opérations de l'établissement et dans tous les cas au moins une fois tous les 2 ans... ».

## XVI. SANCTIONS

Le non-respect des dispositions mentionnées dans le présent manuel de lutte contre le blanchiment d'argent et le financement du terrorisme est sanctionné par des mesures disciplinaires et pénales à l'encontre des contrevenants.

En effet et selon l'article 140 de la loi 2015-26 du 07 août 2015, « Est puni de six mois à trois ans d'emprisonnement et d'une amende de cinq mille dinars à dix mille dinars les personnes citées à l'article 107 de la présente loi, les dirigeants, les représentants, les agents et les associés des personnes morales dont la responsabilité personnelle est établie pour avoir enfreint ou ne pas obtempérer aux dispositions des articles 99, 100, et 102, et l'alinéa 3 de l'article 103 et les articles 106, 113, 124 et 126 et l'alinéa 2 de l'article 127 et l'article 135 de la présente loi. La peine est de trois mois à deux ans d'emprisonnement et de mille à cinq mille dinars d'amende, si une relation d'affaires est nouée ou continuée ou une opération ou transaction occasionnelle réalisée dont la valeur est supérieure ou égale à un montant qui sera fixé par le ministre chargé des finances ou qui comprend des virements électroniques, est réalisée sans respecter les obligations de :

- Vérifier, au moyen de documents officiels ou autres documents émanant de source fiable et indépendante, l'identité des clients habituels ou occasionnels et d'enregistrer toutes les données nécessaires à leur identification.
- Vérifier, au moyen de documents officiels ou autres documents émanant de source fiable et indépendante, l'identité du bénéficiaire de l'opération ou de la transaction, la qualité de celui qui agit pour son compte et de la constitution de la personne morale, de sa forme juridique, de son siège social, de la liste des actionnaires ou associés, de l'identité de ses dirigeants et de ceux qui ont le pouvoir de s'engager en son nom.
- Obtenir du client des informations sur l'objet et la nature de la relation d'affaires.

- S'abstenir d'ouvrir un compte, de nouer ou continuer une relation d'affaires ou de réaliser une opération ou une transaction si les informations s'y rapportant sont insuffisantes ou manifestement fictives. Cela n'empêche pas les poursuites contre les personnes morales qui encourrent une amende égale à cinq fois le montant de l'amende prévue pour l'infraction originale ».

## XVII. Application du manuel de procédure LAB/FT

Le présent manuel de procédure LAB/FT entre en vigueur après validation du Comité d'Audit et approbation par le Conseil d'Administration de la Banque. Il sera communiqué à l'ensemble du personnel dès son approbation par le Conseil d'Administration et sera affiché sur le Site Intranet de la Banque.

Sous réserves de leurs missions et attribution, les fonctions inspection, contrôle permanent et audit interne sont chargées du contrôle du respect des dispositions du présent manuel de procédure LAB/FT dans le cadre de leurs missions.

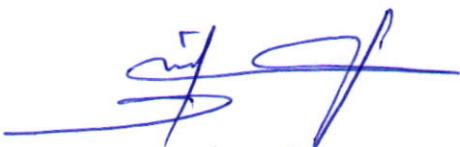
## XVIII. Mise à jour du manuel de procédure LAB/FT

La mise à jour du manuel se fait périodiquement, en fonction de l'évolution de la réglementation nationale et internationale en matière de lutte contre la blanchiment d'argent et le financement du terrorisme et en fonction de l'évolution de l'activité de la banque.

La mise à jour du manuel de procédure LAB/FT est autorisée par le Conseil d'Administration, sur proposition Direction de la Conformité.

Le présent document, une fois validé par le Conseil d'Administration, sera diffusé sur le site Intranet de la Banque.

Le Président du Conseil d'Administration



Mohamed Salah Chebbi El Ahssen