uexo \ Myrtle Ltd \ FSC

Manuel de conformité AML-CFT

v1.0

Table des matières

1. Introduction

La marque uexo est autorisée et réglementée dans plusieurs juridictions, l'entité mauricienne étant détenue et gérée par Myrtle Limited. Myrtle Limited (ci-après dénommée " uexo " ou " la société ") a son adresse à Suite 803, 8th Floor, Hennessy Tower, Pope Hennessy Street, 11328, Port Louis, Maurice. La société est réglementée par la Mauritius Financial Services Commission (FSC) en tant que courtier en valeurs mobilières (Broker) avec le numéro de licence GB21026300.

En 2002, la loi sur le renseignement financier et la lutte contre le blanchiment d'argent (FIAMLA) a été promulguée à Maurice afin de prévenir le blanchiment d'argent et le financement du terrorisme. Le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme à Maurice a été établi par la FIAMLA et, plus tard, par les Financial Intelligence and Anti Money Laundering Regulations 2003. Les règlements de 2003 ont été modifiés en 2018 et sont maintenant connus sous le nom de Financial Intelligence and Anti Money Laundering Regulations 2018.

La société répond à la définition d'une personne déclarant telle que définie à l'article 2 de la FIAMLA 2002. La société doit veiller au respect permanent des exigences pertinentes de la FIAMLA 2002, des règlements FIAML 2018, de la loi des Nations unies (interdictions financières, embargo sur les armes et interdiction de voyager) 2019 et d'autres règles, règlements, lettres circulaires, codes ou lignes directrices publiés par le CSF de temps à autre.

La société s'engage à veiller à ce que ses activités commerciales soient menées dans le respect des normes juridiques et réglementaires applicables. Le Manuel de conformité sur la lutte contre le blanchiment d'argent et le financement du terrorisme (ci-après dénommé le Manuel LAB-CFT ou le Manuel de conformité ou le Manuel) vise à assurer la conformité avec les exigences énoncées dans la FIAMLA, le Règlement 2018 sur le renseignement financier et la lutte contre le blanchiment d'argent, la Loi sur les sanctions des Nations Unies 2019 et toutes les autres lois et législations subsidiaires applicables. L'objectif du Manuel AML-CFT est de permettre à la Société et à ses employés d'appliquer les mesures prescrites par son régulateur, la FSC, en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (AML-CFT), et donc de prévenir toute violation.

Le présent manuel de conformité LBC/FT reflète l'état de la législation à cette date. Il doit donc être révisé au moins une fois par an, afin de s'assurer de son adéquation et de son efficacité et de refléter toute modification de la législation et de la réglementation applicables.

Le présent manuel de conformité AML-CFT s'applique à la Société et à toutes ses filiales, actuelles et futures. Les employés, y compris les représentants/agents, qui participent à la prestation des services prescrits sont censés connaître et comprendre le contenu de la présente politique et respecter les normes qu'elle contient. Tout employé en infraction avec la présente politique fera l'objet de mesures disciplinaires jugées appropriées par le conseil d'administration.

Tous les employés concernés de l'entreprise sont tenus de signer le formulaire de reconnaissance figurant à l'annexe 9 afin de démontrer que le manuel leur a été distribué et qu'ils l'ont lu, compris et se sont engagés à respecter les exigences qu'il contient.

2. Définitions et interprétations

1. **AML-CFT**
   Signifie lutte contre le blanchiment d'argent et le financement du terrorisme.

2. **Client**
   désigne toute personne physique ou morale ou toute construction juridique qui cherche à établir une relation d'affaires ou à effectuer une transaction ponctuelle avec/par l'intermédiaire de l'entreprise.

3. **Bénéficiaire effectif**
   désigne la personne physique qui détient ou contrôle en dernier ressort une personne morale ou une construction juridique et/ou la personne physique pour le compte de laquelle une transaction est effectuée. Elle comprend la personne physique qui exerce le contrôle ultime sur une personne morale ou une construction juridique et les autres personnes physiques spécifiées ci-dessous :
   a. détenant une participation de contrôle ultime dans une personne morale
   b. en cas de doute concernant le point (A), la personne physique détenant une participation majoritaire ou la personne physique exerçant un contrôle sur la personne morale par d'autres moyens
   c. lorsqu'aucune personne physique n'est identifiée au titre des points (A) ou (B), l'identité de la personne physique qui occupe le poste de haut fonctionnaire dirigeant.

4. **Relations d'affaires**
   Relation contractuelle entre l'entreprise et un client pour la fourniture de produits ou de services par l'entreprise au client sur une base fréquente, habituelle, régulière ou ponctuelle.

5. **CDD**
   Signifie diligence raisonnable à l'égard du client.

6. **Partie désignée**
   Toute personne, groupe, entreprise ou entité déclarée comme partie désignée par le secrétaire aux affaires intérieures sur instruction du comité national des sanctions en vertu de l'article 9 ou 10 de la loi sur les sanctions de l'ONU.

7. **EDD**
   Signifie qu'il faut faire preuve d'une diligence accrue.

8. **FIAMLA**
   La loi de 2002 sur le renseignement financier et la lutte contre le blanchiment d'argent.

9. **FIAMLR**
   désigne la réglementation de 2018 relative au renseignement financier et à la lutte contre le blanchiment d'argent.

10. **FIU**
    Des moyens la cellule de renseignement financier a été créée en vertu de l'article 9 de la FIAMLA.

11. **Manuel du FSC**
    désigne le Manuel LAB/CFT publié par le CSF

12. **Personne morale**
    Moyens
    a. toute entité, autre qu'une personne physique, qui peut établir une relation d'affaires permanente avec la société ou posséder des biens ;
    b. et comprend une société, une fondation, une association, une société à responsabilité limitée ou toute autre entité prescrite par la CRF ou une autorité réglementaire/autoritaire compétente.

13. **Arrangement juridique**
    désigne une fiducie ou un accord similaire.

14. **Partie inscrite**
    Toute personne, groupe, entreprise ou entité figurant sur la liste récapitulative du Conseil de sécurité des Nations unies - également connue sous le nom de liste des sanctions des Nations unies - établie par le Conseil de sécurité des Nations unies ou sous son autorité.

15. **MLRO**
    Signifie responsable de la déclaration de blanchiment d'argent.

16. **ML/TF**
    Signifie blanchiment d'argent, financement du terrorisme et financement de la prolifération.

17. **Individuel**
    désigne un être humain vivant légalement capable de conclure un contrat contraignant avec l'entreprise (ou ses filiales).

18. **NRA**
    Signifie l'évaluation nationale des risques de blanchiment d'argent et de financement du terrorisme à Maurice, rapport public publié par le ministère des services financiers et de la bonne gouvernance en août 2019.

19. **PEP**
    désigne une personne politiquement exposée. Les personnes politiquement exposées sont des individus qui exercent ou ont exercé des fonctions/positions publiques importantes (par exemple, des chefs d'État ou de gouvernement, des hommes politiques de haut rang, des hauts fonctionnaires gouvernementaux/judiciaires/militaires, des cadres supérieurs

d'entreprises publiques et des responsables de partis politiques importants), ainsi que leur famille et leurs associés. Il s'agit notamment des personnes suivantes

a. les personnes qui répondent à la définition d'un PEP à Maurice (PEP domestique),
b. les personnes qui répondent à la définition d'une PPE dans un pays étranger (PPE étrangère) et
c. les personnes qui se sont vu confier une fonction/un poste important par une organisation internationale, y compris les membres de la direction générale ou d'autres fonctions équivalentes à celles de directeur, de directeur adjoint et de membre du conseil d'administration (PPE d'une organisation internationale).
d. Sont également concernés les proches collaborateurs et les membres de la famille des PPE, tels que définis ci-dessous :
    i. Membres de la famille
        1. une personne qui a un lien de parenté avec une PPE, soit directement par consanguinité, soit par mariage ou toute autre forme de partenariat civil ; et
        2. toute autre personne spécifiée par une autorité de contrôle ou un organisme de réglementation après consultation du Comité national.
    ii. Proches collaborateurs
        1. une personne étroitement liée à un PEP, que ce soit sur le plan social ou professionnel ; et
        2. toute autre personne spécifiée par une autorité de contrôle ou un organisme de réglementation après consultation du Comité national.

20. **Directeurs d'école**

Toute personne, physique ou morale, qui, directement ou indirectement :

a. est en mesure de contrôler ou d'exercer une influence significative sur les activités commerciales ou financières d'une personne morale ou d'une construction juridique,
b. a le pouvoir de nommer ou de révoquer un membre de l'organe de direction de la personne morale ou de la construction juridique,
c. peut nommer ou révoquer une personne en tant que membre de l'organe de direction de la personne morale ou de la construction juridique,
d. est un bénéficiaire effectif de la personne morale ou de la construction juridique,
e. a doté une personne morale ou une construction juridique de ses actifs initiaux,
f. a transféré des biens ou pris des dispositions testamentaires en faveur d'une personne morale ou d'une construction juridique.

Pour éviter toute ambiguïté, lorsque le client est une société, les mandants sont les directeurs, les actionnaires, le(s) bénéficiaire(s) effectif(s) et les représentants autorisés.

Lorsque le client est une société de personnes, les mandants sont le(s) commandité(s), le(s) commanditaire(s), le(s) bénéficiaire(s) effectif(s) et les représentants autorisés.

Lorsque le client est un trust, les mandants sont le constituant, le trustee, le(s) bénéficiaire(s), l'exécuteur et/ou le protecteur (le cas échéant) et les représentants autorisés du trustee.

Lorsque le client est une fondation, les mandants sont le fondateur, les membres du conseil, le(s) bénéficiaire(s) et les représentants autorisés.

Lorsque le client est une société, on entend par Principaux : le gérant, les associés, le bénéficiaire effectif et les représentants autorisés.

21. **Règlement**
    Désigne la réglementation en vertu des Financial Intelligence and Anti-Money Laundering Regulations 2018 (règlements sur le renseignement financier et la lutte contre le blanchiment d'argent).

22. **STR**
    Signifie déclaration de transaction suspecte.

23. **Loi sur les sanctions de l'ONU**
    désigne la loi de 2019 sur les sanctions des Nations unies (interdictions financières, embargo sur les armes et interdiction de voyager).

24. **UN**
    Signifie que l'Organisation des Nations unies a été fondée en 1945.

25. **Liste des sanctions de l'ONU**
    La liste récapitulative du Conseil de sécurité des Nations unies.

Dans la présente politique, l'utilisation du masculin, du féminin ou du neutre doit être interprétée comme incluant les autres genres, et l'utilisation du singulier doit être interprétée comme incluant le pluriel et vice versa.

3. Blanchiment de capitaux, financement du terrorisme et financement de la prolifération

Le blanchiment de capitaux peut être décrit comme le processus consistant à déguiser l'origine des produits du crime, par exemple en les faisant passer par une séquence complexe de virements bancaires ou de transactions commerciales, dans le but ultime de faire paraître légaux les produits illicitement gagnés. Le blanchiment de capitaux est souvent considéré, à tort, comme une activité associée uniquement à la criminalité organisée et au trafic de stupéfiants. Or, il y a blanchiment d'argent chaque fois qu'une personne (physique ou morale) utilise le produit direct ou indirect d'un acte ou d'une omission contraire à la loi, qu'il s'agisse de chantage, de vol, de fraude, d'évasion fiscale, d'enlèvement, de corruption, de violation des droits d'auteur, de comptabilité créative, etc. Même si l'infraction est qualifiée de "blanchiment d'argent", elle concerne toutes les formes de biens matériels ou immatériels, et pas seulement l'argent liquide, qui représentent directement ou indirectement le produit d'un crime.

Le blanchiment d'argent est généralement décrit comme un processus en trois étapes:

1. **Placement**
   La première étape consiste à injecter des fonds illicites dans le système financier légitime. Par exemple, en déposant de petites sommes sur des comptes bancaires ou en utilisant de fausses méthodes de facturation. Cette étape a deux objectifs : (i) elle dispense le criminel de détenir et de garder de grandes quantités d'argent liquide, et (ii) elle introduit les fonds illicites dans le système financier légitime.

2. **Superposition**
   L'objectif principal de cette étape est de séparer les fonds illicites du crime initial en utilisant des structures et des transactions complexes (couches) pour masquer la piste d'audit. Par exemple, les blanchisseurs de capitaux peuvent commencer par transférer les fonds par voie électronique d'un pays à l'autre, convertir les espèces en instruments monétaires ou conclure des accords de prêt-retour.

3. **Intégration**
   L'étape finale du système de blanchiment d'argent. Les fonds ont été entièrement assimilés à l'économie légitime, ce qui permet au criminel de les récupérer dans le cadre d'une transaction apparemment légitime. Par exemple, en achetant des biens immobiliers ou en investissant sur les marchés des valeurs mobilières.

Financement du terrorisme

Le financement du terrorisme, quant à lui, est le processus qui consiste à collecter ou à fournir des fonds ou un soutien non financier à des organisations terroristes. Ces organisations ont besoin de fonds non seulement pour financer des opérations terroristes spécifiques, mais aussi pour couvrir les coûts organisationnels liés au développement et au maintien d'un groupe terroriste et pour créer un environnement favorable nécessaire à la poursuite de leurs activités. Les organisations terroristes peuvent se procurer des fonds auprès de sources légitimes, notamment en abusant d'entités caritatives ou d'entreprises légitimes, ou en s'auto-finançant. Les terroristes tirent également leur financement de diverses activités criminelles.

Les principales différences entre le blanchiment de capitaux et le financement du terrorisme sont les suivantes :

- ★ Dans le cas du blanchiment de capitaux, les fonds/actifs proviennent toujours d'activités illégales, alors que dans le cas du financement du terrorisme, les fonds/actifs peuvent provenir de sources légales ou criminelles ; et

- ★ L'objectif sous-jacent du blanchisseur de capitaux est de dissimuler la source des fonds/actifs illicites, tandis que les personnes impliquées dans le financement du terrorisme cherchent à dissimuler qu'elles financent des actes de terreur ou des organisations terroristes

Il existe également des similitudes entre le blanchiment de capitaux et le financement du terrorisme :

- ★ Activité criminelle - Les terroristes se livrent également à d'autres formes de criminalité, comme le trafic de drogue ou d'êtres humains, par exemple, pour financer leurs activités ;

- ★ Les blanchisseurs d'argent et les financiers du terrorisme utilisent tous deux des institutions financières et des professionnels des services financiers.

Financement de la prolifération

La prolifération fait référence au développement et à l'utilisation d'armes nucléaires, chimiques ou biologiques - également connues sous le nom d'armes de destruction massive - et de leurs vecteurs, en violation des accords internationaux et des régimes de contrôle des exportations.

Le financement de la prolifération désigne le financement de la prolifération des armes de destruction massive, y compris, mais sans s'y limiter, le transfert ou l'exportation de technologies, de biens, de logiciels, de services ou d'expertise pouvant être utilisés dans des programmes impliquant des armes nucléaires, biologiques ou chimiques et leurs vecteurs. Les personnes qui participent à des systèmes de prolifération et de financement de la prolifération utilisent des réseaux complexes de sociétés écrans et des techniques de détournement copiées sur les blanchisseurs d'argent pour accéder au système financier mondial et échapper aux mesures de plus en plus strictes de lutte contre le financement de la prolifération.

3.1 Infractions liées au blanchiment de capitaux et au financement du terrorisme

Les principales législations traitant des infractions de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération à Maurice sont respectivement la loi de 2002 sur le renseignement financier et la lutte contre le blanchiment d'argent, la loi de 2002 sur la prévention du terrorisme et la loi de 2019 sur les sanctions des Nations unies (interdictions financières, embargo sur les armes et interdiction de voyager).

3.1.1 Loi de 2002 sur le renseignement financier et la lutte contre le blanchiment de capitaux (FIAMLA)

Section 3:

1. Toute personne qui

a. effectue une transaction portant sur des biens qui, en tout ou en partie, directement ou indirectement, représentent le produit d'un crime ; ou

b. reçoit, est en possession, dissimule, déguise, transfère, convertit, cède, enlève de Maurice ou introduit à Maurice tout bien qui, en tout ou en partie, directement ou indirectement, représente le produit d'un crime, lorsqu'il soupçonne ou a de bonnes raisons de soupçonner que le bien provient ou est réalisé, en tout ou en partie, directement ou indirectement, d'un crime, commet une infraction.

2. Un déclarant qui ne prend pas les mesures raisonnablement nécessaires pour s'assurer que ni lui, ni aucun service qu'il propose, n'est susceptible d'être utilisé par une personne pour commettre ou faciliter la commission d'une infraction de blanchiment de capitaux ou de financement du terrorisme commet une infraction.

3. La dissimulation ou le déguisement de biens qui sont, en tout ou en partie, directement ou indirectement, le produit d'une infraction comprend la dissimulation ou le déguisement de leur véritable nature, de leur origine, de leur localisation, de leur disposition, de leur mouvement, de leur propriété ou des droits y afférents.

Section 8:
Toute personne condamnée en vertu de la FIAMLA est passible d'une amende n'excédant pas 2 millions de roupies et d'une peine de servitude pénale n'excédant pas 10 ans.

3.1.2. Loi de 2002 sur la prévention du terrorisme (POTA)

Section 6:

1. Toute personne qui, de quelque manière ou sous quelque forme que ce soit
    a. sollicite un soutien pour un acte de terrorisme ou offre un soutien en relation avec un tel acte, ou
    b. sollicite un soutien ou apporte un soutien à une organisation interdite, commet une infraction.

2. Aux fins du paragraphe (1), le terme "soutien" comprend
    a. l'incitation à la cause du terrorisme ;
    b. l'offre d'une assistance matérielle, d'armes, de faux documents ou de fausses pièces d'identité ;
    c. la fourniture ou la mise à disposition de tels services financiers ou autres services connexes.

Section 15 :

1. Toute personne qui conclut ou participe à un accord facilitant la détention ou le contrôle de biens terroristes par une autre personne ou en son nom, de quelque manière que ce soit, y compris
    a. par dissimulation ;
    b. par la soustraction à la juridiction ; ou
    c. par transfert à une autre personne, commet une infraction.

Section 32:
Toute personne qui commet une infraction en vertu des articles 6 ou 15 est passible, sur déclaration de culpabilité, d'une peine de servitude pénale d'une durée de 3 ans au moins et de 20 ans au plus.

3.1.3. Loi de 2019 sur les sanctions contre les Nations unies (interdictions financières, embargo sur les armes et interdiction de voyager) (loi sur les sanctions contre les Nations unies)

Section 23 (1):

1. Sous réserve des dispositions de la présente loi, il est interdit d'effectuer des opérations sur les fonds ou les actifs d'une partie désignée ou d'une partie inscrite sur la liste, y compris
    a. Tous les fonds ou autres actifs détenus ou contrôlés par la partie désignée ou la partie inscrite sur la liste, et pas seulement ceux qui peuvent être liés aux éléments suivants
        i. un acte, un complot ou une menace terroriste particulier ;
        ii. un acte, un complot ou une menace de prolifération en particulier ;
    b. les fonds ou autres actifs qui sont entièrement ou conjointement détenus ou contrôlés, directement ou indirectement, par la partie désignée ou la partie inscrite sur la liste ;
    c. les fonds ou autres actifs dérivés ou générés à partir de fonds ou autres actifs détenus ou contrôlés, directement ou indirectement, par la partie désignée ou la partie inscrite sur la liste, et
    d. les fonds ou autres actifs d'une partie agissant pour le compte ou sur instruction de la partie désignée ou de la partie cotée en bourse.

Section 23 (5):

Toute personne qui ne se conforme pas au paragraphe (1) commet un délit et est passible, en cas de condamnation, d'une amende n'excédant pas 5 millions de roupies ou le double de la valeur des fonds ou autres actifs, le montant le plus élevé étant retenu, et d'une peine d'emprisonnement n'excédant pas 3 ans.

3.2 Comprendre le risque

L'activité criminelle génère des quantités massives de fonds illicites qui doivent être intégrés dans le système économique et financier légitime afin de profiter aux criminels sans attirer l'attention sur le crime sous-jacent.

À la suite de l'évaluation nationale des risques (ENR), les courtiers en valeurs mobilières titulaires d'une licence de courtier en valeurs mobilières ont été classés comme présentant un risque moyen en termes de vulnérabilité au blanchiment d'argent. Il a également été indiqué dans l'évaluation nationale des risques que les activités des courtiers en valeurs mobilières se caractérisent par un grand nombre de clients de détail et que la complexité des produits ainsi que les types de clients (PPE ou clients provenant de juridictions à haut risque) peuvent présenter des risques du point de vue de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Comme indiqué précédemment, les organisations terroristes collectent des fonds auprès de sources légitimes et criminelles pour soutenir leurs activités. Par conséquent, le financement du terrorisme peut également impliquer le blanchiment de capitaux.

4. Obligation de conformité

Étant donné que la société répond à la définition d'une personne déclarant en vertu de la FIAMLA, elle a l'obligation légale de se conformer aux exigences énoncées à la fois dans la FIAMLA et dans la FIAMLR.

L'article 3, paragraphe 2, de la FIAMLA stipule qu'une personne déclarante qui ne prend pas les mesures raisonnablement nécessaires pour s'assurer que ni elle ni aucun des services qu'elle propose n'est susceptible d'être utilisé par une personne pour commettre ou faciliter la commission d'une infraction de blanchiment de capitaux ou de financement du terrorisme commet une infraction.

La peine applicable en cas de condamnation est une amende n'excédant pas 10 millions de roupies et une peine de servitude pénale n'excédant pas 20 ans.

4.1 Violation par un employé

Tous les employés et dirigeants de l'entreprise doivent veiller à respecter rapidement les dispositions pertinentes du présent manuel. Si un employé ou un dirigeant enfreint les exigences définies dans le présent manuel, l'entreprise peut, à sa discrétion et en fonction de certains facteurs (tels que la gravité et les conséquences de l'infraction), prendre des mesures incluant, sans s'y limiter, l'ouverture de procédures disciplinaires et/ou le signalement de l'affaire aux autorités compétentes, entre autres.

5. Principaux responsables de la lutte contre le blanchiment d'argent et le financement du terrorisme

L'entreprise a pour politique de veiller à ce que ses activités commerciales soient menées dans le respect des normes légales et réglementaires applicables. En sa qualité de personne déclarante, l'entreprise se conforme aux obligations qui lui incombent en vertu de la FIAMLA et de la FIAMLR.

Par conséquent, l'entreprise doit nommer un responsable de la conformité, un MLRO et un MLRO adjoint et établir des procédures comprenant, sans s'y limiter, les éléments suivants:

1. Identifier et vérifier l'identité des clients ;
2. Veiller à ce que les transactions suspectes soient dûment signalées ;
3. Assurer un contrôle adéquat des clients et des employés potentiels ;
4. Mettre en place une fonction d'audit indépendante pour tester le programme de lutte contre le blanchiment d'argent et le financement du terrorisme.
5. Fournir une formation appropriée aux employés en matière de lutte contre le blanchiment d'argent et le financement du terrorisme ; et
6. Conserver les preuves documentaires du respect des exigences légales et réglementaires en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

5.1 Responsable de la conformité

Conformément aux Règlements 22 (1) (a), 22 (2) et 22 (3), et aux dispositions pertinentes du Manuel LAB/CFT, la Société a l'obligation de nommer un Responsable de la conformité qui aura les fonctions décrites au paragraphe 5.1.1 ci-dessous. La Société doit demander l'approbation préalable du CSF avant de nommer un Compliance Officer.

5.1.1 Fonctions de l'agent de conformité

Le responsable du respect des dispositions est chargé

a. Veiller au respect permanent des exigences de la FIAMLA et de la FIAMLR, sous la supervision continue du conseil d'administration et de la direction générale,
b. Assurer la gestion quotidienne du programme de lutte contre le blanchiment d'argent et le financement du terrorisme de la société,
c. faire régulièrement rapport au conseil d'administration sur l'état de la conformité et/ou de la non-conformité,
d. contribuer à la conception, à la mise en œuvre et à la maintenance des manuels, politiques et systèmes internes de la société en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

En d'autres termes et d'un point de vue pratique, le Compliance Officer est la personne de référence responsable de la conformité AML/CFT de l'entreprise.

La société s'assure à tout moment que le responsable de la conformité

a. a accès en temps utile et sans restriction aux documents de l'institution financière ;
b. dispose de ressources suffisantes pour exercer ses fonctions ;
c. bénéficie de la pleine coopération du personnel de l'institution financière ;
d. est pleinement conscient de ses obligations et de celles de l'institution financière ; et
e. rend compte directement au conseil d'administration et a des contacts réguliers avec lui afin de permettre au conseil d'administration de s'assurer que toutes les obligations statutaires et les dispositions de la FIAMLA et des règlements FIAML 2018, ainsi que du présent manuel, sont respectées et que l'institution financière prend des mesures suffisamment solides pour se protéger contre le risque potentiel d'être utilisée à des fins de blanchiment d'argent et de financement du terrorisme.

En outre, la société doit demander l'approbation préalable de la CSF conformément à la section 24 de la loi de 2007 sur les services financiers (Financial Services Act 2007) avant de le nommer. La Société doit également s'assurer que, même après avoir nommé le Compliance Officer, ce dernier reste apte à exercer ses fonctions.

5.2 MLRO

Conformément à la règle 26 (1), la société doit nommer un MLRO auquel toutes les déclarations internes de transactions suspectes doivent être adressées, ainsi qu'un MLRO adjoint qui remplit les fonctions du MLRO en son absence.

Conformément à la règle 26(4) du règlement FIAMLA et aux dispositions pertinentes des lignes directrices, le MLRO et le MLRO adjoint de la société doivent :

1. être suffisamment haut placé dans l'entreprise ou avoir une expérience et une autorité suffisantes, et
2. avoir un droit d'accès direct au conseil d'administration de l'entreprise et disposer de suffisamment de temps et de ressources pour s'acquitter efficacement de ses fonctions.

La même personne peut être nommée aux postes de MLRO et de Compliance Officer, à condition (i) qu'elle le juge approprié au regard des exigences respectives des deux rôles et (ii) que la personne à nommer dispose de suffisamment de temps et de ressources pour remplir efficacement les deux rôles.

Le MLRO et le DMLRO doivent être enregistrés en tant qu'utilisateurs actifs sur la plateforme GoAML de la cellule de renseignement financier (CRF) dès qu'ils ont été approuvés en cette qualité et tout au long de leur mandat.

5.2.1 Fonctions du MLRO

Le MLRO doit avoir accès à toutes les informations ou à tous les registres pertinents pour déterminer si une transaction déclarée est suspecte ou non. Aux fins de l'enquête, le MLRO doit prendre en compte toutes les informations pertinentes dont il dispose pour déterminer si la transaction déclarée est suspecte ou non. Le MLRO est également le point de contact de la CRF.

Le MLRO et le DMLRO sont enregistrés sur la plateforme GoAML de la CRF et la preuve de cet enregistrement est conservée et mise à la disposition de l'autorité de régulation sur demande.

Traitement des déclarations de transactions suspectes

Dès que le MLRO ou le DMLRO reçoit une DOD interne, il doit la consigner dans le journal des DOD (voir annexe 3) avec tous les détails. Conformément à la règle 27 (e), le MLRO doit avoir accès à toutes les informations ou à tous les dossiers pertinents pour déterminer si la transaction est suspecte ou non.

La section 14(1) de la FIAMLA prévoit que la personne déclarante doit faire une déclaration de transaction suspecte (STR) à la CRF dès que possible et **au plus tard dans les 5 jours ouvrables** à compter du jour où elle a eu connaissance de la transaction suspecte. Le MLRO documente les informations qui ont été examinées pour évaluer la transaction déclarée. Conformément à l'article 30 (3) du règlement, la date à laquelle la déclaration d'opérations suspectes a été transmise à la CRF doit être consignée dans le registre des déclarations d'opérations suspectes. Dans les cas où l'entreprise est en train de déposer une déclaration de soupçon, elle peut demander conseil à la CRF sur la manière de traiter le client ou sur la possibilité d'interrompre les transactions sans alerter cette dernière.

Si, après examen, le MLRO considère que la transaction déclarée n'est pas suspecte, il doit documenter les informations qui ont été examinées pour évaluer la transaction ainsi que les raisons pour lesquelles il n'a pas fait de déclaration à la CRF dans le registre des DOD. La documentation des informations peut inclure la constitution d'un dossier (physique ou électronique) auquel seul le MLRO ou le MLRO adjoint a accès et l'enregistrement des documents/informations suivants dans ce dossier :

a. Faits relatifs à l'activité/transaction suspecte présumée
b. Documents/évidences/informations relatifs à l'enquête interne menée par le MLRO ou le MLRO adjoint
c. les conclusions de l'enquête interne
d. Procès-verbaux des réunions tenues avec les employés au cours des enquêtes internes (le cas échéant)
e. Analyse écrite du MLRO / MLRO adjoint justifiant la décision de déposer ou non une DOD auprès de la CRF

Il convient de noter que la liste ci-dessus n'est pas exhaustive.

Le MLRO de l'entreprise doit être le principal point de contact de l'entreprise avec la CRF. Il est strictement interdit aux dirigeants et aux employés de la société de divulguer à quiconque des informations ou tout autre élément susceptible de nuire à une enquête sur une transaction suspecte.

Tous les employés doivent être informés de l'identité du Compliance Officer, du MLRO et du DMLRO. En cas de changement de MLRO ou de DMLRO, les dirigeants et les employés de la société doivent en être informés. Le MLRO adjoint assumera les fonctions et responsabilités du MLRO en ce qui concerne la déclaration des transactions suspectes et se verra accorder le même accès aux informations et à la documentation pour lui permettre d'exercer ses fonctions en l'absence du MLRO.

6. Évaluation des risques liés à la lutte contre le blanchiment de capitaux et le financement du terrorisme

L'article 17 de la loi de 2002 sur le renseignement financier et la lutte contre le blanchiment de capitaux ("FIAMLA") exige que chaque personne déclarante prenne les mesures appropriées pour identifier, évaluer et comprendre les risques de blanchiment de capitaux et de financement du terrorisme pour les clients, les pays ou les zones géographiques et les produits, les services, les transactions ou les canaux de distribution. L'article 17 oblige les personnes déclarantes à prendre en compte tous les facteurs de risque pertinents avant de déterminer le niveau de risque global, le niveau approprié et le type d'atténuation à appliquer. La nature et l'étendue de l'évaluation doivent correspondre à la nature et à la taille de l'activité du déclarant et doivent prendre en compte les éléments suivants

a. tous les facteurs de risque pertinents, y compris
    i. la nature, l'échelle et la complexité des activités du déclarant ;
    ii. les produits et services fournis par le déclarant ;
    iii. les personnes auxquelles les produits et services sont fournis et la manière dont ils le sont ;
    iv. la nature, l'échelle, la complexité et la localisation des activités du client ;
    v. le recours à des tiers pour certains éléments du processus de vigilance à l'égard des clients ; et
    vi. les évolutions technologiques ; et

b. le résultat de toute évaluation des risques effectuée au niveau national et toute orientation émise.

Les personnes déclarantes sont également tenues, en vertu de la section 17, d'identifier et d'évaluer les risques de blanchiment de capitaux ou de financement du terrorisme susceptibles de survenir lors du lancement d'un nouveau produit ou d'une nouvelle pratique commerciale ou de l'utilisation d'une technologie nouvelle ou en cours de développement.

Selon l'article 17 de la FIAMLA, l'évaluation du risque commercial est le processus par lequel une personne déclarante détermine et évalue sa vulnérabilité au blanchiment de capitaux et au financement du terrorisme afin de mettre en œuvre des contrôles et des mesures appropriés pour minimiser et gérer ces risques. L'évaluation des risques professionnels vise à aider le déclarant à déterminer dans quelle mesure son activité, ses produits et ses services sont exposés au blanchiment de capitaux et au financement du terrorisme. Une évaluation appropriée des risques commerciaux devrait permettre à l'entreprise de s'assurer que son dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme est équivalent et adapté aux risques de blanchiment de capitaux et de financement du terrorisme auxquels elle est confrontée.

6.1 Évaluation des risques de l'entreprise

L'objectif d'une évaluation du risque commercial est d'identifier dans quelle mesure les activités, les produits et les services de la société sont exposés au blanchiment d'argent et au financement du terrorisme. En vertu de l'article 17 (2) de la FIAMLA, six domaines clés doivent être pris en considération lors de l'évaluation du risque commercial, parmi d'autres facteurs de risque:

a. la nature, l'échelle et la complexité des activités de l'institution financière ;

b. les produits et services fournis par l'institution financière ;
c. les personnes auxquelles les produits et services sont fournis et la manière dont ils le sont ;
d. la nature, l'échelle, la complexité et la localisation des activités du client ;
e. le recours à des tiers pour certains éléments du processus de vigilance à l'égard de la clientèle ; et
f. les évolutions technologiques.

En outre, les déclarants sont également tenus de prendre en compte les résultats de toute évaluation des risques effectuée au niveau national et de toute orientation émise. Les conclusions du rapport national d'évaluation des risques doivent donc être prises en considération.

6.1.1 Lignes directrices pour l'évaluation des risques des entreprises

Par conséquent, la société, en sa qualité de personne soumise à déclaration et donc de personne soumise à déclaration, doit prendre les mesures appropriées pour procéder à une évaluation du risque d'entreprise comme l'exige la section 17 de la FIAMLA.

La méthodologie d'évaluation du risque d'entreprise a été incluse dans le même document que l'évaluation du risque d'entreprise elle-même. Veuillez vous référer à ce document en conséquence (voir l'annexe 7).

Dans le cadre de l'évaluation du risque d'entreprise, les facteurs de risque ci-dessous doivent être pris en considération :

1. La nature, l'ampleur et la complexité des activités
    a. Examiner les services fournis par l'entreprise et la manière dont ces services pourraient être détournés à des fins de blanchiment d'argent et de financement du terrorisme.

    b. Impliquer activement tous les membres de la direction dans la détermination des risques (menaces et vulnérabilités) posés par le blanchiment d'argent et le financement du terrorisme dans les domaines dont ils sont responsables.

    c. Tenir compte de tout facteur organisationnel susceptible d'accroître l'exposition au risque de blanchiment de capitaux et de financement du terrorisme, par exemple le volume d'activité et les aspects liés à l'externalisation des activités réglementées ou des fonctions de conformité.

    d. Tenir compte de la nature, de l'échelle et de la complexité de ses activités, notamment de la diversité de ses opérations, du volume et de la taille de ses transactions, ainsi que du degré de risque associé à chaque domaine d'activité. Les transactions volumineuses et complexes peuvent présenter un risque plus élevé de blanchiment de capitaux que les transactions moins complexes et volumineuses. Toutefois, cela dépendra également de l'évaluation du domaine d'activité et de la nature de l'entreprise. Dans l'ensemble, les facteurs doivent être pris en compte afin d'obtenir une évaluation plus complète.

    e. Il convient de prendre en compte les juridictions dans lesquelles l'entreprise opère, toute menace particulière provenant de ces juridictions et toute vulnérabilité particulière au sein de l'organisation dans ces juridictions. Le

règlement 24(1) du règlement FIAML 2018 indique comment les pays tiers à haut risque doivent être identifiés.

2. La nature, l'ampleur et la complexité des activités
    a. Examiner les services fournis par l'entreprise et la manière dont ces services pourraient être détournés à des fins de blanchiment d'argent et de financement du terrorisme.

    b. Impliquer activement tous les membres de la direction dans la détermination des risques (menaces et vulnérabilités) posés par le blanchiment d'argent et le financement du terrorisme dans les domaines dont ils sont responsables.

    c. Tenir compte de tout facteur organisationnel susceptible d'accroître l'exposition au risque de blanchiment de capitaux et de financement du terrorisme, par exemple le volume d'activité et les aspects liés à l'externalisation des activités réglementées ou des fonctions de conformité.

    d. Tenir compte de la nature, de l'échelle et de la complexité de ses activités, notamment de la diversité de ses opérations, du volume et de la taille de ses transactions, ainsi que du degré de risque associé à chaque domaine d'activité. Les transactions volumineuses et complexes peuvent présenter un risque plus élevé de blanchiment de capitaux que les transactions moins complexes et volumineuses. Toutefois, cela dépendra également de l'évaluation du domaine d'activité et de la nature de l'entreprise. Dans l'ensemble, les facteurs doivent être pris en compte afin d'obtenir une évaluation plus complète.

    e. Il convient de prendre en compte les juridictions dans lesquelles l'entreprise opère, toute menace particulière provenant de ces juridictions et toute vulnérabilité particulière au sein de l'organisation dans ces juridictions. Le règlement 24(1) du règlement FIAML 2018 indique comment les pays tiers à haut risque doivent être identifiés.

3. Produits et services fournis par les institutions financières
    a. Examiner les vulnérabilités des services ou produits offerts et la manière dont ils pourraient être utilisés à des fins de blanchiment d'argent ou de financement du terrorisme. Certaines caractéristiques des produits et l'existence éventuelle de vulnérabilités accrues, telles que des volumes importants d'argent liquide, des monnaies virtuelles ou des supports non traçables/anonymes.

    b. Si les paiements à des tiers inconnus ou non associés sont autorisés. De tels paiements comporteraient des risques plus élevés.

    c. Si les produits/services/structures sont d'une complexité particulière ou inhabituelle.

4. Les personnes auxquelles et la manière dont les produits et services sont fournis
    a. Examinez les menaces posées par les types de clients. Il peut s'agir, par exemple, de personnes politiquement exposées ("PEP"), de personnes fortunées, de personnes originaires ou exerçant leurs activités dans une juridiction à haut risque, ou encore d'entreprises qui ne sont pas en contact direct avec le client.

b. Le type de produit doit être pris en considération ; les produits ou services à haut risque sont plus susceptibles d'être ceux dont la valeur et le volume sont élevés, où des fonds illimités de tiers peuvent être librement reçus et ceux où des fonds peuvent être régulièrement versés à des tiers sans qu'il soit nécessaire d'obtenir une CDD sur les tiers.

c. La rapidité avec laquelle les produits et services peuvent être livrés ou les transactions effectuées.

d. La section 17A(b) de la FIAMLA prescrit que toute personne soumise à déclaration doit régulièrement revoir, mettre à jour et, le cas échéant, améliorer les politiques, les contrôles et les procédures mis en place. Par conséquent, l'évaluation des risques de l'entreprise doit être revue au moins une fois par an afin de déterminer le degré d'exposition de l'entreprise aux risques de blanchiment d'argent et de financement du terrorisme.

5. La nature, l'échelle, la complexité et la localisation des activités des clients
   a. si la clientèle est impliquée dans des activités susceptibles d'être les plus vulnérables à la corruption, telles que le pétrole, la construction ou les ventes d'armes.

   b. Tenir compte de facteurs juridictionnels tels que les niveaux élevés de criminalité organisée, les vulnérabilités accrues à la corruption et les cadres inadéquats pour prévenir et détecter le blanchiment d'argent et le financement du terrorisme dans les pays où l'entreprise peut avoir des clients.

   c. Les pays, territoires et zones géographiques avec lesquels les clients (et les bénéficiaires effectifs des clients) ont un lien pertinent.

6.2 Évaluation du risque client

Les risques associés à un client sont déterminés par l'importance des indicateurs de risque. Conformément à l'article 17(1) de la FIAMLA, sur la base des documents d'identification recueillis et du résultat de l'examen, une évaluation du risque client en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme doit être effectuée. À cette fin, une évaluation du risque client est effectuée à l'aide de l'outil d'évaluation du risque client afin de déterminer le niveau de risque de blanchiment de capitaux et de financement du terrorisme associé à l'exercice d'activités avec le client. Veuillez vous référer à l'outil d'évaluation du risque client (voir annexe 8).

6.2.1 Processus d'évaluation du risque client

Sur la base des informations recueillies lors de la procédure de vérification de l'identité et des détails saisis lors de l'interaction avec le client, l'utilisateur de l'outil d'évaluation du risque client devra évaluer les risques en remplissant le formulaire.
Les niveaux d'évaluation des risques seront classés selon les catégories ci-dessous :

Niveau de risque	**Fréquence d'examen**
Faible	Tous les 3 ans

Moyen	Tous les 2 ans
Élevée	Tous les ans

Facteurs de risque

Différents facteurs de risque ont été pris en considération dans la matrice d'évaluation du risque client. Des conseils (qui font également partie de la méthode d'évaluation des risques utilisée) sont fournis ci-dessous pour une meilleure compréhension :

Les catégories de facteurs de risque de base sont les suivantes :

1. Risques clients (individus/entités)
2. Risques géographiques
3. Risques liés aux produits/services

Risques clients

Le risque client est associé à tout facteur lié à l'activité, à la réputation, à la nature ou au comportement du client susceptible d'accroître les risques de blanchiment d'argent et de financement du terrorisme.

Lors de l'identification du risque associé aux clients, l'entreprise prend en compte l'activité commerciale ou professionnelle, la réputation, la structure, la nature et le comportement du client et de son bénéficiaire effectif.

Facteurs de risque à prendre en compte en fonction d'activité des clients :

- ★ Le client ou le bénéficiaire effectif a-t-il des liens avec des secteurs généralement associés à un risque de corruption plus élevé, tels que la construction, les produits pharmaceutiques, les soins de santé, le commerce des armes et la défense, les industries extractives ou les marchés publics ?
- ★ Le client ou le bénéficiaire effectif a-t-il des liens avec des entreprises liées à des produits ou à des activités jugés illégaux en vertu des lois ou des réglementations du pays d'accueil ou des conventions et accords internationaux, y compris, mais sans s'y limiter, les exigences du pays d'accueil en matière d'environnement, de santé, de sécurité et de travail ?
- ★ Le client ou le bénéficiaire effectif a-t-il des liens directs avec des entreprises qui ne correspondent pas à l'appétit pour le risque de la société ? Par exemple, il est lié à des entreprises de crypto-monnaie par le biais d'une structure de propriété ou d'un partenariat, à des entreprises sans licence qui nécessitent une licence, etc.
- ★ Le client ou le bénéficiaire effectif a-t-il des liens avec des secteurs associés à un risque de blanchiment d'argent et de financement du terrorisme plus élevé, par exemple certaines institutions financières, les jeux d'argent, les paris, les casinos ou les opérations de change ?
- ★ Le client ou le bénéficiaire effectif a-t-il des liens avec des activités qui impliquent des montants importants d'argent liquide (l'argent liquide représente plus de 30 % de toutes les transactions) ?
- ★ Lorsque le client est une personne morale ou une construction juridique, quel est l'objet de son établissement ? Par exemple, quelle est la nature de son activité ?
- ★ Le client a-t-il des liens politiques, par exemple s'agit-il d'une personne politiquement exposée ("PEP") ou son bénéficiaire effectif est-il une PEP ? Le client ou le bénéficiaire effectif a-t-il d'autres liens pertinents avec une PPE, par

exemple des PPE de parents ou d'associés proches ? Certains des administrateurs du client sont-ils des PPE et, dans l'affirmative, ces PPE exercent-elles un contrôle significatif sur le client ou l'ayant droit économique ?

- ★ Une personne physique ou morale est-elle soumise à des obligations d'information exécutoires qui garantissent que des informations fiables sur le bénéficiaire effectif du client sont accessibles au public, par exemple les sociétés cotées en bourse qui font de cette divulgation une condition d'admission à la cote ?
- ★ Le client est-il une institution financière agissant pour son propre compte et relevant d'une juridiction dotée d'un régime efficace de lutte contre le blanchiment d'argent et le financement du terrorisme, et est-il contrôlé quant au respect des obligations locales en matière de lutte contre le blanchiment d'argent et le financement du terrorisme ?
- ★ Existe-t-il des preuves que le client a fait l'objet de sanctions prudentielles ou de mesures d'exécution pour non-respect des obligations en matière de LBC/FT ou de règles de conduite plus larges au cours des dernières années ?
- ★ Le client est-il une administration publique ou une entreprise d'une juridiction où le niveau de corruption est faible, moyen ou élevé ?
- ★ Les antécédents du client ou du bénéficiaire effectif sont-ils cohérents avec ce que la société sait de son activité commerciale passée, actuelle ou prévue, du chiffre d'affaires de son entreprise, de l'origine des fonds et de la source de richesse du client ou du bénéficiaire effectif ?
- ★ Si le client est une personne morale dont le profil d'activité est lié à l'argent, les entreprises disposent de politiques et de procédures de lutte contre le blanchiment d'argent et le financement du terrorisme suffisantes pour contrôler leurs propres clients.

Facteurs de risque à prendre en compte en fonction de la **réputation** des clients :

- ★ Existe-t-il des rapports médiatiques défavorables ou d'autres sources d'information pertinentes concernant le client, par exemple des allégations de criminalité, de corruption, de terrorisme et d'autres délits financiers à l'encontre du client ou du bénéficiaire effectif ? Dans l'affirmative, ces sources sont-elles fiables et crédibles ? La société doit déterminer la crédibilité des allégations sur la base de la qualité et de l'indépendance de la source des données et de la persistance des rapports sur ces allégations, entre autres considérations. L'absence de condamnation pénale peut ne pas suffire à elle seule à écarter les allégations d'actes répréhensibles.
- ★ Le client, le bénéficiaire effectif ou toute personne publiquement connue pour être étroitement associée à ces personnes a-t-elle vu ses avoirs gelés en raison de procédures administratives ou pénales ou d'allégations de terrorisme ou de financement du terrorisme ? La société a-t-elle des motifs raisonnables de soupçonner que le client, le bénéficiaire effectif ou toute personne publiquement connue pour lui être étroitement associée a, à un moment donné dans le passé, fait l'objet d'un tel gel des avoirs ?
- ★ Le client ou le bénéficiaire effectif a-t-il fait l'objet d'une déclaration de transaction suspecte dans le passé ?
- ★ Existe-t-il des informations internes sur l'intégrité du client ou du bénéficiaire effectif, obtenues, par exemple, dans le cadre d'une relation d'affaires de longue date ?
- ★ Existe-t-il d'autres problèmes de comportement du client, tels que le refus de fournir ou la fourniture de fausses informations ou de faux documents sur l'entreprise ?

Facteurs de risque à prendre en compte en fonction **de la nature et du comportement** du client :

- ★ Le client a-t-il des raisons légitimes de ne pas pouvoir fournir des preuves solides de son identité, par exemple parce qu'il est demandeur d'asile ?
- ★ Existe-t-il des doutes quant à la véracité ou à l'exactitude de l'identité du client ou du bénéficiaire effectif ?

- ★ Existe-t-il des signes indiquant que le client pourrait chercher à éviter l'établissement d'une relation d'affaires ? Par exemple, le client envisage-t-il d'effectuer une ou plusieurs opérations ponctuelles pour lesquelles l'établissement d'une relation d'affaires serait plus judicieux d'un point de vue économique ?
- ★ La structure de propriété et de contrôle du client est-elle transparente et logique ? Si la structure de propriété et de contrôle du client est complexe ou opaque, existe-t-il une justification commerciale ou légale évidente ?
- ★ Le client émet-il des actions au porteur ?
- ★ Le client a-t-il des actionnaires désignés ?
- ★ Le client est-il une personne morale ou un arrangement qui pourrait être utilisé comme véhicule de détention d'actifs ?
- ★ Existe-t-il une raison valable de modifier la structure de propriété et de contrôle du client ?
- ★ Les informations et la documentation fournies par le client correspondent-elles aux informations fournies par une source publique indépendante ?
- ★ Le client demande-t-il des niveaux de secret inutiles ou déraisonnables ? Par exemple, le client est-il réticent à partager des informations CDD (nom du client, photographie sur un document officiel et adresse résidentielle), ou semble-t-il vouloir dissimuler la véritable nature de ses activités ?
- ★ La source de richesse ou de fonds du client, du bénéficiaire effectif ou de la personne morale peut-elle être facilement expliquée, par exemple par sa profession, son héritage, ses documents financiers ou ses investissements ? L'explication est-elle plausible ?
- ★ Le client utilise-t-il les produits et services qu'il a souscrits comme prévu lors de l'établissement de la relation d'affaires ?
- ★ Si le client est un non-résident, ses besoins pourraient-ils être mieux satisfaits ailleurs ? La demande du client pour le type de service financier recherché est-elle justifiée par des raisons économiques et juridiques valables ?
- ★ Il est de notoriété publique que l'entreprise cliente a reçu des avertissements d'amendes. Dans l'affirmative, ces amendes ou avertissements étaient-ils liés à des délits financiers ou au financement du terrorisme ? Y avait-il des liens possibles avec des activités criminelles ou s'agissait-il simplement d'une violation involontaire de la loi ? Comment l'entreprise a-t-elle agi ? Quelles ont été les actions/réactions ultérieures de cette entreprise après la réception des avertissements/amendes ? Exemple : a-t-elle accepté et suivi les recommandations fournies pour se conformer aux exigences légales ?
- ★ Le site web officiel du client est-il actif et semble-t-il légitime compte tenu de la nature de l'activité du client ?

Facteurs possibles que l'entreprise utilise/met en œuvre pour atténuer le risque le risque pour les produits de monnaie électronique :

- ★ Afin d'éviter toute atteinte financière ou à la réputation de l'entreprise qui pourrait être causée par ses clients, chaque nouveau client (personne physique ou morale) fait l'objet de plusieurs niveaux de mesures de protection. En commençant par l'identification électronique et la soumission de documents, toutes les informations sur le client sont soigneusement vérifiées par la procédure CDD et le contrôle des informations sur le client par rapport aux listes PEP/Sanctions, la recherche de médias défavorables, l'évaluation du risque client, effectuée par le spécialiste AML et un deuxième niveau d'examen effectué par le MLRO avant d'autoriser l'accès d'un client aux systèmes de l'entreprise. Après l'intégration du client dans la catégorie de risque qui lui a été attribuée, ses données KYC et ses activités sont évaluées périodiquement (faible - tous les 3 ans, moyen - tous les 2 ans, élevé - tous les 1 an ou moins) par les spécialistes AML et, en fonction des résultats obtenus, certaines mesures sont prises (par exemple, mises à jour KYC, demandes d'explications du client, exclusion du client) ; en outre, les informations sur le client sont vérifiées quotidiennement par rapport aux listes de sanctions et de PEP ;

- ★ Dans le cadre de la procédure CDD au cours du processus d'accueil des clients, il est obligatoire pour tout client potentiel lié à une activité financière de prouver l'existence de processus et de procédures efficaces de lutte contre le blanchiment d'argent appliqués à ses clients et d'en fournir la preuve ;
- ★ Les règles correctes appliquées au système de surveillance des transactions des clients qui déclenchent tout changement d'activité du client ou tout comportement inattendu (utilisation soudaine de produits tels que les cartes prépayées à l'étranger, montants significatifs de transactions juste en dessous du seuil, transactions d'un montant élevé, transactions provenant de ou envoyées vers de nombreux comptes différents, etc ;

Souvent, les modifications des données personnelles du client (identification, comptes bancaires liés), comme toute autre modification des informations relatives au client, sont enregistrées et les pistes d'audit contenant des informations sur les modifications mentionnées sont visibles pour les spécialistes de la lutte contre le blanchiment d'argent qui procèdent à des examens périodiques des clients. Si les changements sont très fréquents, les clients peuvent être contactés et invités à mettre à jour leur profil KYC.

Risques géographiques

Le risque pays fait référence à toute localisation géographique, juridiction ou relation avec des juridictions susceptibles de présenter un risque de blanchiment d'argent ou de financement du terrorisme.

- ★ Lors de l'identification des risques associés aux pays et aux zones géographiques, l'entreprise prend en compte les juridictions dans lesquelles le client et le bénéficiaire effectif sont basés, les lieux où les affaires sont menées, les affiliations, les autres liens personnels pertinents, les informations de source publique sur les juridictions où des affaires liées à toute forme de criminalité financière, de terrorisme, de pots-de-vin et de corruption ont récemment eu lieu. L'entreprise dispose de ses propres évaluations internes du risque pays, établies à partir de multiples sources fiables et crédibles (Wolfsberg, GAFI, Indice de corruption pays, Indice TF, KYC, etc.) Selon ces évaluations, tous les risques mentionnés sont pris en compte en fonction de la juridiction (blanchiment d'argent, financement du terrorisme, corruption/évasion fiscale) et des procédures de diligence raisonnable sont mises en place à l'intention des clients.

Afin d'évaluer les risques, des règles générales doivent être prises en compte :

- ★ Lorsque les fonds utilisés dans la relation d'affaires ont été générés à l'étranger, le niveau des infractions préalables au blanchiment d'argent et l'efficacité du système juridique d'un pays seront particulièrement pertinents ;
- ★ Lorsque des fonds sont reçus de, ou envoyés vers, des juridictions où des groupes commettant des infractions terroristes sont connus pour opérer, l'entreprise examine dans quelle mesure on peut s'attendre à ce que cela donne lieu à des soupçons, sur la base de ce que l'entreprise sait de l'objectif et de la nature de la relation d'affaires ;
- ★ Lorsque le client est une institution financière ou de crédit, l'Entreprise accorde une attention particulière à l'adéquation du régime LAB/CFT du pays et à l'efficacité de la supervision LAB/CFT ;
- ★ Lorsque le client est une personne morale ou un trust, la société prend en compte la mesure dans laquelle le pays dans lequel le client et, le cas échéant, le bénéficiaire effectif sont enregistrés se conforme effectivement aux normes internationales en matière de transparence fiscale.

Facteurs de risque à prendre en compte en fonction de la **juridiction**.

- ★ Lors de l'identification de l'efficacité des obligations d'une juridiction en matière de lutte contre le blanchiment d'argent et le financement du terrorisme :

- Le pays a-t-il été identifié comme présentant des déficiences stratégiques au regard de ses obligations en matière de LBC/FT (pays tiers à haut risque) ?
- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables sur la qualité des contrôles LAB/CFT de la juridiction, y compris des informations sur la qualité et l'efficacité de l'application de la réglementation et de la surveillance ? Parmi les sources possibles, on peut citer les rapports d'évaluation mutuelle du Groupe d'action financière (GAFI) ou des organismes régionaux de type GAFI (un bon point de départ est un résumé et les principales conclusions, ainsi que l'évaluation de la conformité aux recommandations 10 (vigilance à l'égard de la clientèle et conservation des documents), 26 (réglementation et surveillance des institutions financières), 27 (pouvoirs des autorités de surveillance) et les résultats immédiats 3 (surveillance) et 4 (mesures préventives), la liste du GAFI des juridictions à haut risque et non coopératives, les évaluations du Fonds monétaire international (FMI) et les rapports du Programme d'évaluation du secteur financier (PESF). L'appartenance au GAFI ou à un FSRB (par exemple MoneyVal) ne signifie pas en soi que le régime de lutte contre le blanchiment de capitaux et le financement du terrorisme de la juridiction est adéquat et efficace.

★ Lors de l'identification du niveau de risque de financement du terrorisme associé à une juridiction:
- Existe-t-il des informations, provenant par exemple des services répressifs ou de sources médiatiques ouvertes crédibles et fiables, suggérant qu'une juridiction fournit un financement ou un soutien à des activités terroristes ou que des groupes commettant des infractions terroristes sont connus pour opérer dans le pays ou le territoire ?
- La juridiction fait-elle l'objet de sanctions financières, d'embargos ou de mesures liées au terrorisme, au financement du terrorisme ou à la prolifération, imposés par exemple par les Nations unies ou l'Union européenne ?

★ Lors de l'identification du niveau de transparence et de conformité fiscale d'une juridiction :
- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables selon lesquelles le pays a été jugé conforme aux normes internationales en matière de transparence fiscale et d'échange d'informations ? Existe-t-il des preuves que les règles pertinentes sont effectivement mises en œuvre dans la pratique ? Parmi les exemples de sources possibles, on peut citer les rapports du Forum mondial sur la transparence et l'échange de renseignements à des fins fiscales de l'Organisation de coopération et de développement économiques (OCDE), qui évalue les juridictions à des fins de transparence fiscale et d'échange de renseignements ; les évaluations de l'engagement de la juridiction à l'égard de l'échange automatique de renseignements sur la base de la Norme commune de déclaration ; les évaluations de la conformité aux recommandations 9 (lois sur le secret des institutions financières), 24 (transparence et propriété effective des personnes morales) et 25 (transparence et propriété effective des constructions juridiques) du GAFI et aux résultats immédiats 2 (coopération internationale) et 5 (personnes morales et constructions juridiques) du GAFI ou des FSRB ; et les évaluations du FMI (par exemple, les évaluations des services du FMI sur les institutions financières offshore). les évaluations des centres financiers offshore par les services du FMI).
- La juridiction s'est-elle engagée à appliquer effectivement la Norme commune de déclaration sur l'échange automatique d'informations, adoptée par le G20 en 2014 ?
- La juridiction a-t-elle mis en place des registres de propriété effective fiables et accessibles ?

★ Lors de l'identification du risque associé au niveau des infractions préalables au blanchiment de capitaux :

- Existe-t-il des informations provenant de sources publiques crédibles et fiables sur le niveau des infractions préalables au blanchiment de capitaux, par exemple la corruption, la criminalité organisée, la criminalité fiscale et la fraude grave ? Il peut s'agir, par exemple, d'indices de perception de la corruption, de rapports nationaux de l'OCDE sur la mise en œuvre de la convention anti-corruption de l'OCDE ou du rapport mondial sur les drogues de l'Office des Nations unies contre la drogue et le crime (ONUDC).
- Existe-t-il des informations provenant de plusieurs sources crédibles et fiables sur la capacité du système d'enquête et du système judiciaire de la juridiction à mener des enquêtes et des poursuites efficaces sur ces infractions ?

Facteurs possibles mis en œuvre par L'ENTREPRISE pour atténuer le risque lié aux produits de monnaie électronique :

★ L'entreprise accorde une attention particulière aux juridictions connues pour fournir un financement ou un soutien à des activités terroristes ou dans lesquelles des groupes commettant des infractions terroristes sont connus pour opérer, ainsi qu'aux juridictions soumises à des sanctions financières, des embargos ou des mesures liées au terrorisme, au financement du terrorisme ou à la prolifération.

★ Le client doit fournir un document prouvant sa citoyenneté et son lieu de résidence, ses lieux de constitution et d'activité au cours d'une procédure d'intégration afin d'atténuer le risque découlant d'une éventuelle affiliation à un pays potentiellement dangereux.

Risques liés aux produits/services

Le risque lié aux produits, services et transactions concerne tous les produits, services et transactions susceptibles de créer des conditions propices à l'apparition de risques de blanchiment d'argent et de financement du terrorisme.

Lors de l'identification des risques associés aux produits, aux services et aux transactions, l'entreprise prend principalement en compte les facteurs énumérés ci-dessous :

★ le niveau de transparence ou d'opacité du produit, du service ou de la transaction ;
★ la complexité du produit, du service ou de la transaction
★ la valeur ou la taille du produit, du service ou de la transaction.

Pour les produits de monnaie électronique :

★ Les seuils ;
★ la méthode de financement ;
★ l'utilité et la négociabilité.

Facteurs de risque à prendre en compte sur la base de la **transparence**:

★ Dans quelle mesure les produits ou services permettent-ils au client, au bénéficiaire effectif ou aux structures bénéficiaires de rester anonymes ou facilitent-ils la dissimulation de leur identité ? Parmi ces produits et services, on peut citer les actions au porteur, les dépôts fiduciaires, les véhicules offshore et certains trusts, ainsi que les entités juridiques telles que les fondations qui peuvent être structurées de manière à tirer parti de l'anonymat et à permettre des transactions avec des sociétés fictives ou des sociétés dont les actionnaires sont des prête-noms ;

- ★ Dans quelle mesure un tiers qui ne fait pas partie de la relation d'affaires peut-il donner des instructions ?

Facteurs de risque à prendre en compte en fonction de la **complexité**:

- ★ Dans quelle mesure la transaction est-elle complexe et implique-t-elle plusieurs parties ou plusieurs juridictions, par exemple dans le cas de certaines transactions de financement commercial ? Les transactions sont-elles simples, par exemple des paiements réguliers sont-ils effectués aux fournisseurs des entreprises pour des matériaux fournis ?
- ★ Dans quelle mesure les produits ou services autorisent-ils les paiements de tiers ou acceptent-ils des paiements en trop alors qu'on ne s'y attendrait pas normalement ? Lorsque des paiements de tiers sont attendus, l'entreprise connaît-elle l'identité du tiers, par exemple s'agit-il d'une autorité publique ou d'un garant ? Les produits et services sont-ils financés exclusivement par des transferts de fonds à partir du compte du client dans une autre institution financière ?
- ★ L'entreprise comprend-elle les risques associés à son produit ou service nouveau ou innovant, en particulier lorsqu'il implique l'utilisation de nouvelles technologies ou méthodes de paiement ?

Facteurs de risque à prendre en compte en fonction **de la valeur ou de la taille**:

- ★ Dans quelle mesure les produits ou services sont-ils gourmands en liquidités ?
- ★ Dans quelle mesure les produits ou services facilitent-ils ou encouragent-ils les transactions de grande valeur ? Existe-t-il des plafonds pour la valeur des transactions ou des niveaux de primes qui pourraient limiter l'utilisation du produit ou du service à des fins de blanchiment d'argent ou de financement du terrorisme ?

Facteurs éventuels mis en œuvre dans l'entreprise pour atténuer le risque.

- ★ Seuils: le produit
  - fixe des limites de faible valeur pour les paiements, les chargements ou les remboursements, y compris les retraits d'espèces (bien qu'un seuil peu élevé puisse ne pas suffire à réduire le risque de TF) ;
  - limite le nombre de paiements, de chargements ou de remboursements, y compris les retraits d'espèces, au cours d'une période donnée ;
  - limite le montant des fonds pouvant être stockés sur le produit/compte de monnaie électronique à tout moment.

- ★ Financement: le produit
  - exige que les fonds destinés à l'achat ou au rechargement soient tirés de manière vérifiable d'un compte détenu au nom unique ou conjoint du client auprès d'un établissement de crédit ou d'une institution financière de l'EEE ;

7. Diligence raisonnable à l'égard des clients

D'une manière générale, l'entreprise applique des mesures de vigilance normales à l'égard des clients potentiels ou des mesures de vigilance renforcées en cas de relations avec des clients à haut risque. Si le risque de blanchiment d'argent est faible, l'entreprise peut appliquer les mesures de vigilance simplifiées mentionnées ci-dessous.

Diligence raisonnable simplifiée

L'application d'une diligence simplifiée ne signifie pas qu'il ne faut pas appliquer de mesures CDD, mais plutôt qu'il faut appliquer des mesures réduites qui doivent être proportionnelles au risque posé par le client ou la situation spécifique.

Lorsqu'une institution financière décide d'adopter les mesures simplifiées à l'égard d'un demandeur particulier, elle doit

1. documenter cette décision de manière à expliquer les facteurs qu'elle a pris en compte (y compris en conservant tout document justificatif pertinent) et les raisons pour lesquelles elle a adopté les mesures en question ; et
2. réexaminer la relation avec le demandeur (y compris l'opportunité de continuer à utiliser les mesures simplifiées) et mettre en œuvre des politiques, des procédures et des contrôles appropriés à cet effet.

La CDD simplifiée ne s'applique jamais lorsqu'une institution financière sait, soupçonne ou a des motifs raisonnables de savoir ou de soupçonner qu'un client ou un candidat à l'activité est impliqué dans le blanchiment de capitaux ou le financement du terrorisme ou que la transaction effectuée par le client ou le candidat à l'activité est effectuée pour le compte d'une autre personne impliquée dans le blanchiment de capitaux ou lorsqu'il existe d'autres indicateurs de risque de blanchiment de capitaux ou de financement du terrorisme. Lorsque des mesures simplifiées de vigilance à l'égard de la clientèle sont adoptées, les institutions financières doivent appliquer une approche fondée sur le risque pour déterminer s'il convient d'adopter les mesures simplifiées de vigilance à l'égard de la clientèle dans une situation donnée et/ou de continuer à appliquer les mesures simplifiées, bien que les comptes de ces clients soient toujours soumis à des obligations de surveillance des transactions.

7.1 Vérification de l'identité

L'entreprise a l'obligation légale d'identifier ses clients, qu'ils soient permanents ou occasionnels, et de vérifier leur identité à l'aide de documents, de données ou d'informations fiables et de source indépendante, spécifiés par son organisme de réglementation. En d'autres termes, la vérification de l'identité consiste à s'assurer que les clients sont bien ceux qu'ils prétendent être.

Les documents types à demander aux clients pour vérifier leur identité sont énumérés dans les tableaux 1 à 3 ci-dessous. La collecte des informations requises à l'aide des documents spécifiés permettra à l'entreprise de :

1. établir un profil du client
2. évaluer tout risque de blanchiment de capitaux et de financement du terrorisme associé au client,
3. décider d'entrer ou non en relation d'affaires avec le client en fonction de son profil et de l'évaluation du risque qu'il présente.

7.1.1 Individus

Lorsque la relation d'affaires est établie entre la société et une personne agissant en son nom propre, les documents énumérés dans le tableau 1 ci-dessous sont demandés au client pour se conformer au règlement 4:

Tableau 1 - Documents à demander aux clients - particuliers

Informations requises	**Document source**	**Détails**
• Nom complet (y compris les noms antérieurs) • Date et lieu de naissance, • nationalité, • le sexe • Numéro d'identification personnel délivré par le gouvernement ou autre identifiant unique délivré par le gouvernement	• Carte d'identité nationale, ou • Passeport en cours de validité, • Un document officiel attestant du changement de nom (le cas échéant, par exemple un acte de mariage, un certificat de changement de nom),	Le passeport ou la carte d'identité doit comporter une photographie et la signature de la personne. Si le client a plus d'une nationalité, il convient de demander un passeport ou une carte d'identité nationale pour la nationalité supplémentaire.
• Adresse actuelle et permanente	• Une facture de services publics (facture de téléphone fixe/ facture de gaz/ facture d'électricité/ facture d'eau) émise au cours des 3 derniers mois, ou • un relevé bancaire émis au cours des trois derniers mois, ou • un relevé de carte de crédit émis au cours des trois derniers mois, ou • une lettre d'un professionnel, tel qu'un avocat, un comptable agréé, un banquier ou un notaire, qui connaît la personne. La lettre doit indiquer l'adresse du domicile permanent de la personne.	Les adresses de boîtes postales ne sont pas acceptables en tant qu 'adresses résidentielles permanentes et peuvent ne pas être acceptées. Les factures de services publics doivent être au nom du client. Si le document est au nom d'un parent (mère ou père), l'acte de naissance du client doit être fourni. Si la facture est au nom d'un tiers, une lettre du tiers doit être fournie, certifiant que le client réside à l'adresse indiquée sur la facture, ainsi qu'une copie certifiée de la carte d'identité du tiers.
• Profession et nom de l'employeur	• Titre du poste et nom de l'employeur, ou • un CV, ou • Informations sur les antécédents professionnels • Nature et détails de l'activité indépendante, le cas échéant. • Pour les indépendants, licence professionnelle et carte d'immatriculation.	La période (c'est-à-dire les dates) d'emploi et le nom de l'employeur doivent être indiqués dans le CV. Les informations sur le parcours professionnel peuvent également être saisies lors de la procédure d'enregistrement du client.
• Source des fonds utilisés par le client pour financer l'acquisition	• Justificatifs pertinents (le cas échéant).	Tous les champs du formulaire doivent être remplis. Le formulaire doit être

ou la location		signé et daté par le client. Il est également possible de demander des informations sur l'origine des fonds au cours de la procédure d'enregistrement.

7.1.2 Personnes morales ou constructions juridiques

Si la relation d'affaires est établie entre l'entreprise et une personne morale ou une construction juridique, lorsque la proposition est acceptée par le client, l'entreprise est tenue de vérifier les éléments suivants :

1. Le nom, la forme juridique et la preuve d'existence du client ;
2. Les pouvoirs qui régissent et lient le client (c'est-à-dire qui gère le client et qui a le droit de le représenter et de signer en son nom) ;
3. les noms des personnes occupant des postes de direction au sein du client ; et
4. l'adresse du siège social ou de l'établissement principal du client.

La société doit également comprendre et documenter la nature de l'activité et la structure de contrôle de la propriété d'un client qui est une personne morale ou une structure juridique.

Par conséquent, les documents de vérification de l'identité énumérés dans le tableau 2 ci-dessous doivent être demandés au client.

Le tableau 2 ci-dessous énumère les documents standard de vérification de l'identité qui doivent être obtenus des clients en général. Lors de l'intégration d'un nouveau client, il lui sera demandé de remplir et de signer les conditions générales et de soumettre les informations et les documents KYC demandés sur le site web.

Tableau 2 - Documents à demander aux clients - Personnes morales ou constructions juridiques

Type de personne morale/dispositif juridique	**Document à demander**
Société	● Certificat de constitution ou d'enregistrement, ● l'acte constitutif et les statuts de l'entreprise (selon le cas), ● Recherche dans le registre des sociétés ● Certificat de bonne réputation délivré par un organisme national compétent, ● Carte d'enregistrement de l'entreprise (le cas échéant), ● Tableau de la structure de l'actionnariat jusqu'au bénéficiaire effectif, ● Dernier registre des administrateurs, ● Dernier registre des membres/actionnaires, ● Adresse du siège social et principal lieu d'activité (s'il diffère du siège social), ● Derniers états financiers vérifiés ou rapport annuel, le

	cas échéant, ● Documents de vérification de l'identité des administrateurs, des actionnaires importants et du bénéficiaire effectif, ● Preuve d'identité et adresse résidentielle des personnes autorisées à représenter la société aux fins de la transaction et à signer les documents requis.
Partenariat	● Le contrat de société ou l'acte de société, ● Certificat d'enregistrement de la société de personnes si elle est enregistrée, ● Preuve que la société de personnes continue d'exister (certificat de bonne réputation délivré par le registraire) ● Derniers états financiers vérifiés ou rapport annuel, ● Documents de vérification de l'identité du gérant/associé général, ● Dernier registre (ou document équivalent) indiquant les noms, adresses et pourcentages d'intérêt des commanditaires, ● L'adresse du siège social et le principal lieu d'activité (s'il est différent du siège social), ● Documents de vérification de l'identité des commanditaires et du bénéficiaire effectif, ● la preuve de l'identité et de l'adresse résidentielle des personnes autorisées à représenter la société aux fins de la transaction et à signer les documents, et
Société	● Acte de société ou document équivalent établissant la société, ● Si la société est enregistrée, le certificat d'enregistrement, ● Preuve que la société continue d'exister, ● Structure de propriété/détention jusqu'au bénéficiaire effectif, ● Preuve de l'identité et de l'adresse résidentielle de la personne autorisée à signer les documents requis, ● Documents de vérification de l'identité des administrateurs ou des gérants de la société, ● Dernier registre (ou document équivalent) indiquant le nom, l'adresse et la participation des membres ou des associés, ● Documents de vérification de l'identité des membres ou des associés de la société, ● Documents de vérification de l'identité du bénéficiaire effectif, ● les derniers états financiers ou le rapport annuel, s'ils sont disponibles, et

Trust	● Acte de fiducie ou extraits pertinents indiquant les noms du constituant, du fiduciaire, des bénéficiaires, du protecteur, de l'exécuteur et de la loi applicable à la fiducie, ● L'information du trustee selon laquelle le trust continue d'exister, ● Des informations sur le type et l'objet du trust, ● des informations sur l'origine des actifs du trust, ● Documents de vérification de l'identité du constituant, du fiduciaire, des bénéficiaires, du protecteur (le cas échéant) et de l'exécuteur (le cas échéant), ● une preuve de l'identité et de l'adresse résidentielle de la personne autorisée à signer les documents requis pour l'acquisition ● Coordonnées du siège social et du lieu d'activité du fiduciaire ● le dernier résumé financier ou les derniers états financiers de la fiducie, s'ils sont disponibles, et
Foundation	● Charte et/ou statuts de la fondation, ● Si la fondation est enregistrée, le certificat d'enregistrement, ● une attestation du conseil de la fondation certifiant que la fondation continue d'exister, ● Registre ou document équivalent indiquant les noms et adresses des membres du conseil de la fondation, du fondateur et de toute personne ayant fait une donation à la fondation, ● Les coordonnées du siège social et du lieu d'activité de la fondation, ● Documents de vérification de l'identité du fondateur, des membres du conseil et des bénéficiaires de la fondation, ● le dernier résumé financier ou les derniers états financiers, s'ils sont disponibles, et

Propriété effective

La Société identifie et vérifie l'identité des bénéficiaires effectifs des personnes morales ou des constructions juridiques. Conformément à la Réglementation 6 du Règlement FIAML 2018, l'identification des bénéficiaires effectifs se fait en demandant des informations sur :

1. l'identité de toutes les personnes physiques qui détiennent en dernier ressort une participation majoritaire dans la personne morale ;
2. en cas de doute, au titre du point a), sur la question de savoir si la personne détenant le contrôle est le bénéficiaire effectif ou si aucune personne physique n'exerce de contrôle par le biais de participations, l'identité de la personne

physique exerçant un contrôle sur la personne morale par d'autres moyens spécifiés par l'organisme de réglementation ou l'autorité de surveillance compétent ; et

3. lorsqu'aucune personne physique n'est identifiée au titre des points a) ou b), l'identité de la personne physique qui occupe le poste de haut fonctionnaire dirigeant.

L'identité de la personne physique qui détient ou contrôle en dernier ressort le client (c'est-à-dire le bénéficiaire effectif) doit dans tous les cas être établie et vérifiée.

7.1.3 Personnes autorisées ou signataires autorisés

Certains clients (en particulier ceux qui sont des personnes morales) seront représentés par des personnes autorisées à agir en leur nom. La Société a l'obligation légale de vérifier l'identité et l'adresse permanente et résidentielle actuelle de toute personne qui prétend agir au nom d'un client. Elle doit également vérifier que cette personne est dûment autorisée à représenter le client ou à agir en son nom. Par conséquent, les informations énumérées dans le tableau 3 ci-dessous devront être obtenues de toute personne qui prétend agir au nom d'un client.

Tableau 3 - Documents à demander aux personnes autorisées

Informations	**Source du document**	**Recommandation**
● Nom complet (y compris les noms antérieurs) ● Date et lieu de naissance, ● nationalité, ● le sexe ● Numéro d'identification personnel délivré par le gouvernement ou autre identifiant unique délivré par le gouvernement	● Carte d'identité nationale, ou ● Passeport en cours de validité, ● Un document officiel attestant du changement de nom (le cas échéant, par exemple un certificat de mariage, un certificat de changement de nom), ● Le document gouvernemental pertinent tel que, mais sans s'y limiter, toute licence commerciale délivrée ou le numéro de compte fiscal (TAN) de l'individu.	Le passeport ou la carte d'identité doit comporter une photographie et la signature de la personne. Si le client a plus d'une nationalité, le passeport ou la carte d'identité nationale de la nationalité supplémentaire doit être demandé.
● Adresse actuelle et permanente	● une facture de services publics (facture de téléphone fixe/ facture de gaz/ facture d'électricité/ facture d'eau) émise au cours des trois derniers mois, ou ● un relevé bancaire émis au cours des trois derniers mois, ou ● un relevé de carte de crédit émis au cours des trois derniers	Les adresses de boîtes postales ne sont pas acceptables en tant qu 'adresses résidentielles permanentes et peuvent ne pas être acceptées. Les factures de services publics doivent être au nom du client. Si le document est au nom d'un parent (mère ou père), l'acte de naissance du client doit être fourni.

	mois, ou ● une lettre d'un professionnel, tel qu'un avocat, un comptable agréé, un banquier ou un notaire, qui connaît la personne. La lettre doit indiquer l'adresse du domicile permanent de la personne.	Si la facture d'électricité est au nom d'un tiers, il convient de fournir une lettre du tiers certifiant que le client réside à l'adresse indiquée sur la facture d'électricité, ainsi qu'une copie certifiée de la carte d'identité du tiers.
● Preuve écrite que la personne est autorisée à agir au nom du client	● Résolution écrite signée autorisant la personne à représenter le client	Le document doit préciser le nom de la personne, son lien avec le client et mentionner le bien à acquérir, le prix et le fait que la personne est autorisée à représenter le client pour la transaction et à signer tout document nécessaire à la transaction.

7.2 Original ou copies certifiées conformes des documents de vérification de l'identité

Comme indiqué précédemment, la société doit identifier et vérifier l'identité de ses clients à l'aide de documents, de données ou d'informations de source fiable et indépendante. L'entreprise doit donc s'assurer que les documents sur lesquels elle s'appuie pour vérifier l'identité sont exacts et qu'ils se rapportent effectivement au client.

Dans les cas où un employé ou un dirigeant de l'entreprise a eu un contact direct avec un client et a vérifié les documents originaux, ce dernier peut certifier les documents de diligence raisonnable. Par ailleurs, les documents de vérification du client doivent être certifiés par une personne appropriée, telle qu'un avocat, un comptable qualifié ou un autre professionnel. Les professionnels peuvent être

- ★ Notaire,
- ★ un actuaire,
- ★ un comptable qualifié,
- ★ un membre du pouvoir judiciaire (un officier de police, un juge, un magistrat),
- ★ un employé d'une ambassade ou d'un consulat du pays de citoyenneté de la personne,
- ★ un gérant, un dirigeant, un administrateur ou un secrétaire d'une institution financière réglementée aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Le certificateur doit indiquer que la copie est une copie conforme du document original. Le certificateur doit signer la copie et y apposer son cachet (s'il en a un), et indiquer clairement son nom, son adresse et sa fonction/profession ainsi que ses coordonnées (c'est-à-dire un numéro de téléphone ou une adresse).

7.3 Dépistage

Dans le cadre de la procédure de vérification de l'identité, un contrôle doit être effectué sur les clients et leurs mandants (lorsque les clients sont des personnes morales ou des constructions juridiques). Le filtrage s'effectue en effectuant des recherches dans des bases de données indépendantes et fiables sur la base des informations recueillies dans les documents de vérification d'identité obtenus. La Société utilisera un moteur de filtrage approprié pour effectuer son filtrage, y compris le filtrage continu.

L'objectif du filtrage est de vérifier si les clients (ou leurs mandants dans le cas de clients qui sont des personnes morales ou des constructions juridiques) :

- ★ sont des personnes politiquement exposées ; ou
- ★ ont des liens avec la criminalité organisée, le trafic de drogue, le trafic d'armes, la traite des êtres humains, la corruption de fonctionnaires étrangers, la criminalité violente ou le terrorisme ; ou
- ★ font ou ont fait l'objet de condamnations ou d'allégations d'activités frauduleuses, criminelles ou douteuses.

Dans le cas où les documents d'identité complets n'ont pas encore été obtenus, afin de ne pas perturber le déroulement normal des activités, le filtrage peut être effectué sur la base des informations énumérées ci-dessous. Toutefois, une fois les documents de vérification de l'identité obtenus, les résultats du contrôle doivent être vérifiés par rapport aux documents pour s'assurer qu'il n'y a pas d'incohérence :

Pour les particuliers :

- ★ Nom (y compris tout nom antérieur, tout autre nom utilisé et tout autre pseudonyme)
- ★ Nationalité (y compris toute nationalité supplémentaire)
- ★ Pays de résidence

Pour les personnes morales ou les constructions juridiques :

- ★ Nom (y compris tout nom antérieur, tout autre nom commercial ou nom d'entreprise utilisé)
- ★ Pays d'enregistrement
- ★ Pays où l'entreprise/l'activité est exercée

Les résultats du contrôle effectué doivent être conservés dans les dossiers de vérification de l'identité du client (sur support papier ou électronique) pendant toute la durée de la relation d'affaires et pendant une période d'au moins sept ans après la fin de celle-ci.

Si le dépistage indique que le client (ou l'un de ses mandants) :

- ★ est une personne politiquement exposée ; ou
- ★ a des liens avec la criminalité organisée, le trafic de drogue, le trafic d'armes, la traite des êtres humains, la corruption de fonctionnaires étrangers, la criminalité violente ou le terrorisme ; ou
- ★ fait ou a fait l'objet de condamnations ou d'allégations d'activités frauduleuses, criminelles ou douteuses,

L'entreprise doit considérer la relation d'affaires comme présentant un risque élevé et appliquer les mesures de détection et de réduction des risques (EDD) expliquées plus loin dans ce manuel. Si l'on soupçonne que le client tente d'utiliser les produits/services de l'entreprise pour commettre des opérations de blanchiment d'argent ou de financement du terrorisme, une déclaration d'opérations suspectes interne (voir le modèle à l'annexe 3) doit être adressée au MLRO, qui déterminera alors s'il y a lieu de déposer une déclaration d'opérations suspectes auprès de la CRF.

Tous les rapports de dépistage seront conservés dans les dossiers des clients respectifs.

7.4 Moteur de criblage

SumSub

Le département "Conformité et gestion des risques" utilisera l'outil Sumsub, fourni par la Commission européenne, comme principal outil d'assistance. Sumsub détient des informations qui aident les institutions financières, les entreprises, les sociétés de services professionnels, les gouvernements, les organismes chargés de l'application de la loi, les régulateurs et d'autres clients et sociétés à effectuer des contrôles préalables et d'autres activités de sélection conformément à leurs obligations légales ou réglementaires et aux procédures de gestion des risques mises en œuvre dans l'intérêt public, y compris, mais sans s'y limiter, à des fins de lutte contre le blanchiment d'argent ou de connaissance du client, de lutte contre la corruption ou d'autres contrôles de conformité réglementaire, ou pour prévenir, enquêter, détecter ou poursuivre la criminalité financière, la fraude et les fautes graves ou la malhonnêteté, ou d'autres activités criminelles ou illégales (par exemple, l'esclavage moderne, le trafic illégal, les crimes contre l'environnement, etc.) et toute conduite contraire à l'éthique.

En outre, Sumsub fournit des solutions telles que la vérification des utilisateurs, le suivi des transactions, la vérification des entreprises et la prévention des fraudes.

De cette manière, les responsables de la conformité peuvent effectuer rapidement des contrôles pour chaque client, fournisseur, partenaire commercial ou toute autre contrepartie en fonction de trois domaines principaux de sources :

1. Sources officielles avec mots-clés - listes de sanctions, application de la réglementation, application de la loi
2. Sources médiatiques et médias défavorables - rapports d'actualité, articles de journaux, agrégateurs de nouvelles archivées, sources médiatiques réputées.
3. Sources gouvernementales et officielles - dossiers judiciaires, résultats d'élections, documents déposés par les entreprises, sites web officiels des entreprises et communiqués de presse.

Comme toujours, l'entreprise ne souhaite pas s'appuyer uniquement sur des outils automatiques en raison des lacunes potentielles ou de l'incompréhension de la machine qu'une personne (responsable de la conformité) pourrait comprendre facilement. Par conséquent, chaque correspondance est vérifiée manuellement par un agent de conformité qualifié (et formé), ce qui permet d'obtenir une certitude totale quant au résultat.

Essai du moteur de criblage

Afin de garantir la fiabilité et l'intégrité du moteur de filtrage, la Société effectue un test/une évaluation du moteur de filtrage avant la souscription et conserve le résultat du test/de l'évaluation dans ses dossiers. Il s'agit d'une étape importante, étant donné que l'entreprise s'appuie sur le moteur de filtrage pour déterminer si un client ou un client potentiel est un PPE ou si des informations défavorables ou des sanctions correspondent à son profil.

7.5 Vérification de l'origine des fonds

Le fait que les fonds nécessaires à la transaction soient versés à partir d'un compte bancaire ou d'une carte de crédit/débit n'exempte pas la société de son obligation, en vertu de l'article 3, paragraphe 2, de la FIAMLA, de prendre les mesures raisonnablement nécessaires pour s'assurer que ni elle ni aucun des services qu'elle offre n'est susceptible d'être utilisé par une personne pour commettre ou faciliter la commission d'un délit de blanchiment d'argent ou de financement du terrorisme.

La source des fonds est définie comme les activités qui ont généré les fonds à utiliser pour l'achat du terrain, par exemple :

- ★ Revenus du travail
- ★ Revenus de l'activité professionnelle
- ★ Prêt
- ★ Vente de biens
- ★ Vente d'investissements
- ★ Donation
- ★ Héritage
- ★ Vente d'entreprise
- ★ Paiement d'une indemnité
- ★ Retour sur investissement/épargne
- ★ Gain à la loterie/au jeu

L'origine des fonds peut être établie à partir d'une combinaison de sources telles que les informations fournies par le client, les informations fournies par les professionnels réglementés qui connaissent le client (avocats, notaires, comptables, banques) ou les informations accessibles au public (registres de propriété, registres des sociétés, couverture médiatique, recherches sur Internet, etc.) Des exemples sont présentés dans le tableau ci-dessous:

Provenance des fonds destinés à financer la transaction	**Exemples de documents justificatifs qui peuvent s'appliquer au cas par cas**
Revenus de l'emploi	• CV avec historique de l'emploi, y compris les détails de l'entreprise et des postes occupés, ou • Informations sur les revenus de l'employeur, ou • Comptes récents si vous êtes indépendant, ou • Relevés bancaires montrant clairement la réception des paiements réguliers des trois derniers mois de la part de l'employeur désigné, ou • Déclaration d'impôts.
Revenu de l'activité professionnelle	• Les états financiers ou les comptes, • les relevés bancaires de l'entreprise en question. • Informations indépendantes obtenues de sources publiques corroborant les informations.
Prêt	• Contrat de prêt

Vente de biens	● Contrat de vente, ou ● Relevé bancaire indiquant le montant du prix de vente, ou ● Lettre d'un comptable ou d'un notaire confirmant la vente, ou ● Couverture médiatique (le cas échéant) relative à la vente.
Vente d'investissements	● Certificats, notes de contrat ou relevés au nom du client démontrant la vente.
Donation	● un document juridique attestant du don, si possible ; ou ● Déclaration écrite du donateur confirmant le don.
Héritage	● un document juridique fournissant tous les détails de la succession héritée ; ou ● Relevé bancaire s'il indique clairement le nom complet du client, son adresse et l'origine des fonds.
Vente d'entreprise	● Contrat de vente, ou ● Document juridique attestant de la vente, ou ● Couverture médiatique (le cas échéant) relative à la vente, ou ● Lettre signée d'un comptable ou d'un notaire confirmant la vente.
Paiement d'une indemnité	● Lettre de l'organisme d'indemnisation ; ou ● Documents judiciaires exposant les détails de la demande ; ou ● document juridique attestant du paiement de l'indemnité.
Retour sur investissement/épargne	● Certificats, notes de contrat ou relevés au nom du demandeur ; ou ● une confirmation de la société d'investissement concernée ; ou ● un relevé bancaire attestant de la réception des fonds de la société d'investissement.
Gain à la loterie/au jeu	● Lettre de l'organisation concernée (siège de la loterie ● siège de la loterie/boutique de paris/casino), ou ● Relevé bancaire indiquant les fonds déposés par l'organisation concernée, ou ● Couverture médiatique (le cas échéant) relative au gain.

Toutes les informations obtenues dans le cadre de la vérification de l'origine des fonds d'un client doivent être enregistrées de manière appropriée. Les questions posées et les réponses données par le client, ainsi que les mesures prises pour vérifier objectivement les informations, doivent être documentées. Les documents conservés doivent permettre à un examinateur indépendant, tel qu'un enquêteur, de comprendre comment l'entreprise a établi l'origine des fonds du client.

Ouverture minimale du compte

Le montant minimum de dépôt accepté pour l'ouverture d'un compte est de 50 dollars.

En ce qui concerne les autres catégories de clients, y compris, mais sans s'y limiter, les gestionnaires de fonds, les conseillers financiers, les gestionnaires de fonds institutionnels et importants et les entités similaires, la Société doit mener un exercice complet de diligence raisonnable à leur égard conformément au processus de diligence raisonnable à l'égard de la clientèle souligné ci-dessus et vérifier qu'ils sont dûment réglementés du point de vue de la LBC/FT par un régulateur/une autorité dans une juridiction ayant au moins des lois LBC/FT équivalentes à celles de l'île Maurice. En outre, dans les cas où ces entités souhaitent utiliser la plateforme pour gérer individuellement les portefeuilles des clients (c'est-à-dire que les comptes sont ouverts au nom des clients), la Société doit s'assurer que tous ces clients sont dûment identifiés et que leur identité est vérifiée conformément à la procédure de vigilance à l'égard de la clientèle décrite dans le présent manuel, y compris la vérification de l'origine des fonds.

7.6 Évaluation des risques liés à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC-FT) pour les clients

Conformément à l'article 17(1) de la FIAMLA, sur la base des documents d'identification recueillis et des résultats de l'examen, une évaluation du risque client en matière de lutte contre le blanchiment d'argent et le financement du terrorisme doit être effectuée. À cette fin, une évaluation du risque client est effectuée à l'aide de l'outil d'évaluation du risque client afin de déterminer le niveau de risque de blanchiment de capitaux et de financement du terrorisme associé à l'exercice d'activités avec le client.

7.6.1 Clients à haut risque et mesures de vigilance renforcée

Lorsqu'un client est classé comme présentant un risque élevé, par exemple si le client ou son bénéficiaire effectif ou l'un de ses mandants est une PPE, la société est tenue, en vertu des règlements 12 et 15 du règlement relatif à l'application de la réglementation sur les marchés financiers, d'appliquer des mesures de diligence raisonnable renforcées. La diligence raisonnable renforcée (DDR) implique de prendre des mesures supplémentaires par rapport à la vérification régulière de l'identité généralement effectuée. Comme le prévoient les règlements susmentionnés, les mesures de diligence raisonnable renforcée impliquent

1. obtenir des informations supplémentaires sur le client (par exemple, profession, volume des actifs, informations disponibles dans les bases de données publiques, sur Internet, etc.) et mettre à jour plus régulièrement les données d'identification du client et du bénéficiaire effectif
2. l'obtention d'informations supplémentaires sur la nature prévue de la relation d'affaires ;
3. obtenir des informations sur l'origine des fonds et la source du patrimoine du client ;
4. obtenir des informations sur les raisons des transactions envisagées ou effectuées ;
5. obtenir l'approbation de la direction générale pour entamer ou poursuivre la relation d'affaires ;

6. renforcer la surveillance de la relation d'affaires, en augmentant le nombre et le calendrier des contrôles appliqués et en sélectionnant les types de transactions qui nécessitent un examen plus approfondi ;

Pour les clients à haut risque, il faudra obtenir l'approbation de la direction générale pour commencer (s'il s'agit d'un nouveau client), poursuivre (s'il s'agit d'un client existant) ou mettre fin à la relation d'affaires (voir le modèle à l'annexe 1). À cette fin, des informations complètes concernant la disponibilité des documents de vérification de l'identité, les résultats de la vérification et les documents de CED disponibles devront être fournies pour permettre une décision en connaissance de cause.

7.6.2 EDD sur l'individu

Lorsque le client est une personne physique agissant en son nom propre et qu'il est considéré comme un client à haut risque, par exemple s'il s'agit d'une PPE ou d'un membre de la famille ou d'un associé proche d'une PPE, la Société doit obtenir davantage d'informations sur l'origine de la richesse et d'autres informations/documents, y compris, mais sans s'y limiter, une référence bancaire émise au cours des trois derniers mois, dans le cadre d'une mesure de détection précoce de l'abus de confiance. En outre, tant que la relation d'affaires dure avec le client, la société doit s'assurer, dans le cadre d'un contrôle continu, que les documents de vérification de l'identité du client sont à jour et valides. Par exemple, la copie du passeport figurant dans les dossiers n'a pas expiré, la preuve d'adresse figurant dans les dossiers est exacte (c'est-à-dire que l'adresse et le nom du client n'ont pas changé entre-temps). La société effectue également des recherches et des analyses approfondies sur les facteurs à haut risque, qui sont consignées dans le dossier, afin d'atténuer davantage les risques. Il convient de noter que les mesures susmentionnées ne sont pas exhaustives et dépendent principalement du type de risque que représente le client ou le client potentiel.

La source de richesse et la source de fonds sont deux choses distinctes. La source de richesse est définie comme l'activité ou l'événement qui a généré la valeur nette de l'individu (et pas seulement les fonds à utiliser pour la transaction en question). La source du patrimoine peut également être vérifiée par une combinaison de sources telles que les informations fournies par le client, la confirmation de professionnels réglementés qui connaissent le client (avocats, notaires, comptables, banques) ou des informations accessibles au public (registres de propriété, registres des sociétés, couverture médiatique, recherches sur Internet, etc.)

Une lettre de référence bancaire prouve que (i) l'identité et l'adresse du client ont été vérifiées par une institution indépendante, et (ii) que le client est également client d'une institution financière soumise à la réglementation en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

La référence bancaire doit être délivrée sur le papier à en-tête de la banque et indiquer clairement la date à laquelle la lettre a été délivrée, le nom et le titre du responsable de la banque, ainsi que les coordonnées de la banque. La lettre de référence bancaire doit indiquer la période pendant laquelle la personne a été cliente de la banque et confirmer que la relation bancaire a été acceptable, sans aucune défaillance de la part de la personne. En outre, l'entreprise doit effectuer des recherches approfondies et documenter les résultats obtenus sur la personne.

Les mesures de contrôle approfondi varient en fonction de la nature du risque élevé posé et il n'existe donc pas de liste sur mesure des documents qui seraient généralement exigés.

7.6.3 EDD sur la personne morale ou la construction juridique

Lorsque le client est une personne morale ou une construction juridique, la mesure de l'EDD dépend de la raison pour laquelle la personne morale ou la construction juridique a été classée comme présentant un risque élevé. Par exemple :

- ★ lorsque le client est une personne morale et qu'il est classé comme présentant un risque élevé en raison du résultat de l'examen de son actionnaire (ou d'une fonction équivalente au sein de la personne morale ou de la construction juridique) ou de son bénéficiaire effectif, l'EDD est appliquée en établissant et en documentant la source de richesse de l'actionnaire ou du bénéficiaire effectif en question et en fournissant toute autre information qui serait raisonnablement nécessaire pour documenter et atténuer le risque;

- ★ lorsque le client est classé comme présentant un risque élevé en raison du résultat de l'examen de son administrateur (ou d'une fonction équivalente au sein de la personne morale ou de l'arrangement), l'EDD est appliquée en s'assurant (i) qu'aucun fonds ou bien de l'administrateur en question ne sera impliqué dans une transaction avec la société et (ii) que l'administrateur en question n'est pas le bénéficiaire effectif de la personne morale. La nature du risque élevé présenté par l'administrateur sera également examinée en effectuant des recherches supplémentaires;

- ★ Dans les cas où le client est classé comme présentant un risque élevé en raison d'informations défavorables trouvées sur le client lui-même, l'EDD sera appliqué en obtenant des informations supplémentaires pour établir l'objectif légitime de la transaction avec la société. La société prend également toutes les mesures raisonnables pour s'assurer que ses services ne seront pas utilisés à des fins illicites, si elle décide d'établir une relation d'affaires avec le client.

Dans le cas de nouveaux clients, les documents relatifs à l'EDD doivent être obtenus avant d'établir la relation avec le client. Plus important encore, les documents et/ou les informations relatifs à l'EDD doivent être obtenus avant d'accepter un dépôt ou une remise de fonds de la part du client. Si le client a déjà été intégré, les documents relatifs à l'EDD doivent être obtenus avant de poursuivre la transaction.

Toutes les informations relatives au contrôle préalable de l'identité d'un client doivent être enregistrées de manière appropriée. Les documents conservés doivent être suffisants pour démontrer à un examinateur indépendant, tel qu'un enquêteur de la CRF ou d'une autorité compétente, la manière dont la société a procédé à la vérification de l'identité du client afin de s'assurer que ses services ne sont pas utilisés à des fins illégales.

7.6.4 Personnes politiquement exposées (PPE)

Les personnes politiquement exposées sont des individus qui exercent ou ont exercé des fonctions/positions publiques importantes (par exemple des chefs d'État ou de gouvernement, des hommes politiques de haut rang, des hauts fonctionnaires gouvernementaux/judiciaires/militaires, des cadres supérieurs d'entreprises publiques et des responsables de partis politiques importants), ainsi que leur famille et leurs associés.

Il s'agit notamment de

1. les personnes qui répondent à la définition d'un PEP à Maurice (c'est-à-dire un PEP national),
2. les personnes qui répondent à la définition d'une PPE dans un pays étranger (c'est-à-dire une PPE étrangère) et

3. les personnes qui se sont vu confier une fonction/un poste important par une organisation internationale, y compris les membres de la direction générale ou d'autres fonctions équivalentes à celles de directeur, de directeur adjoint et de membre du conseil d'administration (c'est-à-dire les PPE d'organisations internationales).

La définition des PPE inclurait également les membres de la famille et les proches collaborateurs des PPE. Les proches et les membres de la famille sont définis ci-dessous :

"proches collaborateurs" -

1. désigne une personne étroitement liée à un PEP, que ce soit sur le plan social ou professionnel ; et
2. toute autre personne spécifiée par une autorité de contrôle ou un organisme de réglementation après consultation du Comité national;

"membres de la famille" -

1. une personne qui a un lien de parenté avec une PPE, soit directement par consanguinité, soit par mariage ou par une forme de partenariat civil similaire ; et
2. inclut toute autre personne pouvant être spécifiée par une autorité de contrôle ou un organisme de réglementation après consultation du Comité national..

Les PPE présentent un risque plus élevé du point de vue du blanchiment de capitaux et du financement du terrorisme parce qu'elles sont plus susceptibles de bénéficier des produits de la corruption et aussi parce qu'elles peuvent potentiellement (en raison de leurs fonctions et de leurs relations) dissimuler les produits de la corruption ou d'autres délits.

Lorsqu'un client ou un bénéficiaire effectif a été identifié (que ce soit par le biais d'une vérification ou d'informations disponibles) comme étant une PPE, en plus des mesures de DED mentionnées ci-dessus, une approbation spécifique de la direction générale doit être obtenue avant d'établir ou de poursuivre la relation d'affaires en utilisant le formulaire joint à l'annexe 1.

En outre, chaque fois qu'un client ou un mandant d'un client (dans le cas d'une personne morale ou d'un arrangement) est identifié comme étant un PPE (par le biais de l'examen des mesures CDD reçues, au cours de la procédure de filtrage etc), le registre PPE (annexe 10) doit être complété en conséquence.

7.6.5 Clients interdits

Aucune relation d'affaires ne doit être établie avec un client classé comme interdit à la suite de l'évaluation du risque client. La société doit immédiatement cesser ses relations avec le client et une déclaration de transaction suspecte doit être déposée auprès de la CRF, le cas échéant. Une liste des clients interdits est fournie ci-dessous:

1. Liste des clients interdits (applicable aux personnes physiques et aux personnes morales ou constructions juridiques)
    a. Les personnes figurant sur les listes de sanctions (par exemple la liste des sanctions des Nations unies ou la liste émise par le Comité national des sanctions) dans le cadre du processus de sélection ;
    b. Les personnes dont les avoirs ont été gelés en vertu de la loi sur les drogues dangereuses (Dangerous Drugs Act) ;
    c. Les personnes qui ont été condamnées pour blanchiment d'argent et/ou financement du terrorisme à Maurice ou à l'étranger ;

d. Les personnes qui font actuellement l'objet d'une enquête par une autorité locale ou étrangère pour des accusations liées au blanchiment d'argent, au financement du terrorisme, à la corruption, aux pots-de-vin, à la fraude ou à tout autre crime financier.

7.6 Calendrier de la vérification de l'identité, de la sélection et de l'évaluation du risque client

Les documents de vérification de l'identité doivent être demandés au client au cours de la phase d'accueil. Toutes les mesures raisonnables doivent être prises pour obtenir tous les documents de vérification d'identité requis, procéder à une vérification et à une évaluation du risque client avant d'établir la relation avec le client et d'ouvrir un compte.

7.6.1 S'il n'est pas possible d'obtenir des documents de vérification de l'identité ou des documents EDD

En vertu de la Réglementation 13 du Règlement FIAML 2018, aucune relation d'affaires ne doit être établie/aucune transaction ne doit être effectuée/la relation doit être interrompue et une DOD doit être déposée auprès de la CRF si la société ne peut pas obtenir toutes les informations nécessaires pour établir l'identité du client.

En vertu de la règle 12(3) de la réglementation FIAML 2018, la société est tenue de mettre fin à la relation d'affaires et de déposer une DOD auprès de la CRF lorsqu'elle n'est pas en mesure de mettre en œuvre les mesures d'EDD requises. Par conséquent, une DOD interne doit être adressée au MLRO lorsque

1. les documents de vérification de l'identité du client et de l'un de ses mandants ne peuvent être obtenus de manière satisfaisante (dans le cas où le client est une personne morale/une construction juridique), et/ou
2. Des mesures de vérification de l'identité doivent être appliquées, mais les documents/informations de vérification de l'identité requis ne peuvent être obtenus du client.

8. Acceptation du client

Approche fondée sur les risques

Afin d'atténuer et d'éviter que les dispositions prises par une entreprise ne deviennent un fardeau restrictif ou encombrant, celle-ci doit veiller à ce que son approche et ses contrôles intégrés suivent et reflètent les éléments essentiels de toute approche fondée sur le risque à cet égard. Il s'agit notamment d'être satisfait et rassuré de savoir (tant sur le plan juridique que bénéficiaire) qui sont les clients, ainsi que la nature et l'objectif/les attentes autour desquels les clients cherchent à nouer et à entreprendre une ou des relations d'affaires. Mais les entreprises réglementées devront également appliquer et utiliser des mesures appropriées ainsi que des sources et des documents indépendants pour identifier tout client et vérifier séparément cette identité, tout en exerçant une diligence raisonnable fondée sur le risque à l'égard de leur(s) client(s) sur une base initiale et continue. Pour la société, cela peut aller jusqu'à l'application de mesures d'investigation et de contrôle pour déterminer et vérifier la source sous-jacente et légitime des fonds (SoF) et/ou l'origine de la richesse concernant la manière et l'origine des fonds d'investissement pour le dépôt sur le compte et les transactions, par exemple un revenu réaliste, un héritage ou un investissement/épargne antérieur, etc. Toutefois, cela peut également signifier que les entreprises doivent faire preuve de souplesse et de pragmatisme quant aux documents demandés et acceptés pour remplir leurs obligations réglementaires et légales et permettre aux relations avec les clients de se dérouler sans heurts.

Les éléments clés de l'identification des clients sont les suivants:

- ★ Vérification de l'identité : Pour ouvrir un nouveau compte, les personnes doivent fournir une pièce d'identité valide délivrée par le gouvernement, telle qu'un passeport, un permis de conduire ou une carte d'identité nationale, afin de confirmer leur identité.
- ★ Vérification de l'adresse : Un justificatif de domicile, tel que des factures de services publics ou des relevés bancaires, est nécessaire pour confirmer le lieu de résidence du client.
- ★ Contrôle préalable du client : L'entreprise doit faire preuve de diligence raisonnable à l'égard de ses clients. Il s'agit notamment d'évaluer le profil de risque du client, ses activités commerciales, ses bénéficiaires effectifs et l'origine de ses fonds.
- ★ Contrôle continu : L'identification des clients n'est pas un processus ponctuel. L'entreprise est tenue de surveiller en permanence les transactions effectuées dans les dossiers des clients (en fonction de la cote de risque attribuée) afin d'identifier et de signaler toute activité suspecte.

Identification et vérification électroniques

Lorsque l'entreprise adopte un système permettant la vérification électronique de l'identité d'une personne physique, elle doit évaluer la véracité des contrôles inhérents au système afin de déterminer si elle peut se fier aux résultats obtenus ou si des mesures supplémentaires sont nécessaires pour compléter les contrôles existants. Les mesures supplémentaires prises par l'entreprise peuvent consister à demander à un représentant de l'entreprise ou à un tiers désigné, par exemple un avocat, un notaire ou un comptable, d'être présent avec la personne physique lors de l'utilisation du logiciel d'intégration.

Dans tous les cas, l'Entreprise adoptera une approche basée sur le risque pour s'assurer que les documents reçus permettent de vérifier que le client est bien celui qu'il prétend être et que l'Entreprise est convaincue de l'authenticité de ces documents. L'entreprise vérifiera le type de fichier et s'assurera qu'il est inviolable, elle pourrait vérifier l'adresse électronique à partir de laquelle elle est reçue pour s'assurer qu'elle semble légitime et qu'elle correspond au client qui envoie les documents, si le document a été certifié, qu'il s'agit d'un certificateur approprié, etc.

Lorsque l'entreprise n'est pas certaine de l'authenticité des documents sur la base des moyens électroniques de collecte, ou que les documents concernent effectivement le client, il convient d'adopter une approche cumulative et de prendre des mesures ou de procéder à des vérifications supplémentaires pour se rassurer. Si la vérification de l'identité ou de l'adresse n'est toujours pas satisfaisante, la relation d'affaires ne doit pas aller plus loin, l'entreprise mettra fin à la relation d'affaires et envisage de procéder à une divulgation interne.

8.1 Processus d'accueil du client

8.1.1 Demande de documents de vérification d'identité

Les clients proposés qui s'inscrivent sur le site web de la société pour utiliser les services de la société doivent, au cours de la phase d'inscription, fournir les informations pertinentes et soumettre les documents de vérification demandés.

8.1.2 Effectuer un dépistage

Une fois que le client proposé s'est inscrit sur le site web de la société et a soumis les informations et documents pertinents, l'équipe chargée de l'intégration reçoit ces informations et documents et procède à la sélection.

8.1.3 Effectuer une évaluation du risque client

Une fois l'examen préalable terminé, le service de conformité (l'agent concerné) procède à l'évaluation du risque client à l'aide de l'outil d'évaluation du risque client conçu à cet effet. Les documents de vérification de l'identité et les rapports de contrôle devront être pris en considération lors de l'évaluation. Dans le cas d'un client à haut risque, des mesures d'EDD seront appliquées en conséquence.

Une fois ces étapes franchies, le client est accepté et les documents sont téléchargés dans le système de gestion de la relation client de l'entreprise.

Clients à haut risque

Pour les clients à haut risque et les relations d'affaires impliquant des PPE, comme mentionné précédemment, l'approbation de la haute direction devra être obtenue. À cette fin, il doit prendre en considération l'évaluation du risque client et:-

1. évaluer les documents de vérification de l'identité, les résultats de la sélection, l'évaluation du risque client et les documents relatifs à l'EDD obtenus sur le client,
2. prendre en considération les services proposés au client, et
3. prendre la décision de poursuivre ou non en signant le document figurant à l'annexe 1.

9. Canal de dépôt

Compte tenu des risques de blanchiment d'argent et de financement du terrorisme, la Société n'accepte les dépôts des clients que par transfert bancaire direct à partir d'un compte bancaire détenu au nom du client, par carte de crédit/débit/carte prépayée/solution de paiement régionale au nom du client. La Société n'accepte pas les dépôts provenant de tiers. En outre, la Société accepte également les dépôts effectués via Skrill et Neteller.

Les dépôts seront traités par l'intermédiaire de fournisseurs de services de paiement ("PSP") appropriés qui fourniront des services de passerelle de paiement. En pratique, les fonds sont crédités sur le compte du PSP qui, après déduction des frais de transaction convenus, dépose les fonds sur le compte client de la Société pour que les activités de négociation puissent avoir lieu.

Le montant minimum acceptable pour un dépôt est de 50 USD et le montant maximum acceptable par dépôt est de 5000 USD (ce qui constitue une limite journalière pour les dépôts).

10. Contrôle continu

Conformément au règlement 3 (1) (e), la société a l'obligation légale d'effectuer un suivi continu d'une relation d'affaires jusqu'à ce que la relation d'affaires avec un client ait pris fin. Le processus de contrôle permanent est mené selon une approche fondée sur le risque afin de garantir une affectation adéquate des ressources.

10.1 Contrôle continu du CDD

Le contrôle continu du CDD est effectué selon les modalités ci-dessous :

10.1.1 Pour les clients à haut risque - Au moins une fois par an

Le processus de surveillance continue est mené chaque année à compter de la date de la précédente évaluation du risque client.

Pour les clients à haut risque :

- ★ Demander au client des documents d'identification à jour et procéder à une nouvelle vérification avant d'effectuer une autre transaction (y compris l'acceptation d'un autre dépôt).
- ★ Mise à jour des informations sur le client, telles que sa profession et toute autre information pertinente.
- ★ Nouvelle évaluation du risque client afin de réévaluer les risques posés par le client.
- ★ Remplir le formulaire de suivi permanent (annexe 2).
- ★ En fonction de différents aspects (par exemple, les schémas/activités de transaction), d'autres documents peuvent être demandés aux clients.
- ★ Évaluation des facteurs de risque élevé et recherches/analyses approfondies de ces facteurs

Le contrôle continu du CDD est effectué chaque année.

10.1.2 Pour les clients à risque moyen - Tous les 2 ans

Le processus de surveillance continue est mené tous les deux ans à compter de la date de la précédente évaluation du risque client.

Pour les clients à risque moyen :

- ★ Des documents d'identification à jour doivent être demandés au client et un nouveau contrôle doit être effectué avant toute autre transaction (y compris l'acceptation d'un autre dépôt).
- ★ Nouvelle évaluation du risque client afin de réévaluer les risques posés par le client.
- ★ Mise à jour des informations relatives au client, telles que sa profession et toute autre information pertinente.
- ★ Remplir le formulaire de suivi permanent (annexe 2).
- ★ En fonction de différents aspects (par exemple, les schémas/activités de transaction), d'autres documents peuvent être demandés aux clients.

La surveillance continue est effectuée tous les deux ans.

10.1.3 Pour les clients à faible risque - Tous les 3 ans

Le processus de surveillance continue est mené tous les trois ans à compter de la date de la précédente évaluation du risque client.

Pour les clients à faible risque :

- ★ Des documents d'identification à jour doivent être demandés au client et un nouveau contrôle doit être effectué avant toute autre transaction (y compris l'acceptation d'un autre dépôt).
- ★ Nouvelle évaluation du risque client afin de réévaluer les risques posés par le client.
- ★ Remplir le formulaire de suivi permanent (annexe 2).
- ★ Mise à jour des informations relatives au client, telles que sa profession et toute autre information pertinente.
- ★ En fonction de différents aspects (par exemple, les schémas/activités de transaction), d'autres documents peuvent être demandés aux clients.

Un contrôle continu du CDD est effectué chaque année.

10.1.4 Tableau de suivi du CDD en cours

Niveau de risque	**Fréquence de la surveillance continue**
Faible	Tous les 3 ans
Moyenne	Tous les 2 ans
Élevée	Tous les ans

10.2 Suivi des transactions

Le suivi des transactions est un élément essentiel du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme, dans la mesure où il permet d'identifier rapidement les transactions suspectes. Le processus de surveillance des transactions doit être mené comme décrit ci-dessous :

1. Surveillance des dépôts
   La Société surveille les dépôts effectués par les clients en vue de transactions futures. En particulier, la Société doit tenir compte des éléments suivants
   a. Le montant des dépôts est-il en adéquation avec le profil du client ?
   b. Le schéma/fréquence des dépôts est-il en adéquation avec le profil du client et les dépôts attendus ?
   c. Les dépôts sont-ils effectués directement à partir d'un compte bancaire ou d'une carte de crédit/débit/prépayée au nom du client ?

2. Surveillance des échanges
   La Société assure un suivi adéquat des activités de négociation des clients sur la plateforme de négociation. En particulier, l'Entreprise prend en compte :
   a. si la structure des transactions ne semble pas avoir d'objectifs légaux ou économiques
   b. si la structure des transactions ne semble pas correspondre au profil du client et à tout objectif d'investissement

3. Suivi des retraits/rachats
   La Société assure un suivi adéquat de tout retrait/rachat demandé par les clients. En particulier, l'entreprise doit tenir compte des éléments suivants
   a. si l'activité globale du client jusqu'au retrait a un sens économique
   b. si les fonds dont le retrait est demandé sont envoyés sur un compte bancaire ou une carte de crédit enregistrés au nom du client
   c. si le modèle de retrait est adapté au profil du client et à ses objectifs d'investissement

La vérification doit être effectuée en effectuant des recherches dans des bases de données indépendantes et fiables à l'aide des documents de vérification d'identité obtenus afin de s'assurer qu'entre-temps (c'est-à-dire entre le moment de la vérification initiale et le paiement des acomptes finaux), le client ou l'un de ses directeurs (si le client est une personne morale) n'a pas été signalé comme étant une personne physique ou morale:

- ★ une PPE, un membre de la famille ou un associé proche d'une PPE ; ou
- ★ n'a aucun lien avec la criminalité organisée, le trafic de drogue, le trafic d'armes, la traite des êtres humains, la corruption de fonctionnaires étrangers, la criminalité violente ou le terrorisme ; ou
- ★ n'a pas fait l'objet de condamnations ou d'allégations d'activités frauduleuses, criminelles ou douteuses.

Si les résultats de l'examen montrent de manière irréfutable que le client ou l'un de ses directeurs (dans le cas où le client est une personne morale ou une construction juridique) :

- ★ est une PPE, un membre de la famille ou un associé proche d'une PPE ; ou
- ★ a des liens avec la criminalité organisée, le trafic de drogue, le trafic d'armes, la traite des êtres humains, la corruption de fonctionnaires étrangers, la criminalité violente ou le terrorisme ; ou
- ★ fait ou a fait l'objet de condamnations ou d'allégations d'activités frauduleuses, criminelles ou douteuses,

L'entreprise a l'obligation légale d'appliquer des mesures de CED. Une décision doit être prise par le conseil d'administration (voir le modèle à l'annexe 1), afin de déterminer s'il convient de poursuivre ou de mettre un terme à la relation d'affaires. À cette fin, des informations complètes concernant la disponibilité des documents de vérification de l'identité et les résultats du contrôle devront être fournies pour permettre une décision éclairée.

Si, à l'issue de l'examen, il s'avère qu'un client ou un de ses principes figure sur la liste des sanctions des Nations unies ou sur une liste établie par le Comité national des sanctions, la société doit **immédiatement en informer** le Secrétariat national des sanctions et la CSF, et **soumettre une déclaration d'opérations suspectes à la CRF**, comme indiqué dans le chapitre du présent manuel intitulé "Sanctions financières ciblées".

Lorsque l'on soupçonne raisonnablement que le client tente d'utiliser les services de l'entreprise pour commettre des actes de blanchiment d'argent ou de financement du terrorisme, une déclaration d'opérations suspectes interne doit être déposée auprès du MLRO.

10.3 Registres des contrôles continus

Tous les rapports de sélection, le rapport d'évaluation du risque client et la fiche de suivi permanent doivent être conservés et versés au dossier du client concerné (sur support papier ou électronique) pendant toute la durée de la relation d'affaires et pendant une période d'au moins sept ans après la fin de celle-ci.

11. Sanctions financières ciblées

Le Conseil de sécurité des Nations unies (CSNU) a imposé des sanctions pour prévenir et contrer la prolifération et son financement. Il s'agit notamment de sanctions financières ciblées à l'encontre de personnes et d'entités spécifiques qui ont été identifiées comme étant liées à la prolifération des armes de destruction massive. Tous les États membres des Nations unies sont tenus de mettre en œuvre ces mesures.

La loi sur les sanctions de l'ONU a été promulguée en mai 2019 à Maurice pour permettre la mise en œuvre des mesures de sanctions financières ciblées imposées par le Conseil de sécurité de l'ONU.

En vertu de l'article 41 de la loi sur les sanctions de l'ONU, la société doit mettre en œuvre des contrôles internes et d'autres procédures pour lui permettre de se conformer efficacement à ses obligations en vertu de la loi sur les sanctions de l'ONU. Ces obligations peuvent être classées comme suit:

- ★ Contrôle des sanctions
  - Filtrage des clients
  - Contrôle des transactions
  - Correspondance des sanctions et résolution des faux positifs
- ★ Obligations de déclaration

11.1 Obligations de dépistage des sanctions

11.1.1 Filtrage des clients

L'article 25 de la loi sur les sanctions de l'ONU exige que toute personne déclarante vérifie si les coordonnées d'une partie inscrite sur la liste correspondent à celles d'un client et, dans l'affirmative, qu'elle détermine si le client possède des fonds ou d'autres actifs à l'île Maurice. Tous les clients et toutes les transactions doivent donc être examinés à la lumière des listes de sanctions afin de déceler d'éventuelles correspondances.

Lors de l'établissement d'une nouvelle relation d'affaires, dans le cadre du processus de filtrage, la société doit donc vérifier si le client potentiel et ses mandants (le cas échéant) figurent sur la liste des sanctions de l'ONU ou sur la liste publiée par le Comité national des sanctions, ou s'ils sont liés à des personnes figurant sur ces listes.

Ce qui précède s'applique également lors de la mise en place d'un contrôle continu au cours de la relation d'affaires avec un client. Par conséquent, dans le cadre du processus de sélection aux fins de la surveillance continue, la société vérifie si le client et ses mandants (le cas échéant) figurent sur la liste des sanctions des Nations unies ou sur une liste publiée par le Comité national des sanctions, ou s'ils sont liés à des personnes figurant sur de telles listes.

11.1.2 Suivi des transactions

Le contrôle de la liste des sanctions des Nations unies et de la liste émise par le comité national des sanctions doit également être effectué pour chaque transaction entrante et sortante avant d'effectuer la transaction sur les parties impliquées dans la transaction (c'est-à-dire sur le remettant, le bénéficiaire, les intermédiaires et toute autre partie impliquée dans la transaction).

En outre, les points de données suivants doivent être vérifiés lors du contrôle des transactions :

1. Les parties impliquées dans la transaction (c'est-à-dire le remettant, le bénéficiaire, les intermédiaires et les autres parties impliquées dans la transaction),
2. les noms des banques, les codes d'identification des banques et autres codes d'acheminement, et
3. les champs de texte libre (tels que la référence du paiement/le détail de l'objet).

Comme indiqué précédemment dans le manuel, conformément à la section 23(1) de la loi sur les sanctions de l'ONU, le fait de traiter les fonds/autres actifs d'une personne figurant sur la liste des sanctions de l'ONU ou sur une liste publiée par le comité national des sanctions établi en vertu de la loi sur les sanctions de l'ONU constitue un délit.

L'article 24 interdit de mettre des fonds ou d'autres actifs ou des services financiers ou autres services connexes à la disposition, directement ou indirectement, entièrement ou conjointement, d'une personne ou d'un groupe de personnes:

1. une personne figurant sur la liste des sanctions des Nations unies ou sur une liste établie par le Comité national des sanctions
2. une partie agissant au nom ou selon les instructions d'une personne décrite au point a) ci-dessus ; ou
3. une entité détenue ou contrôlée, directement ou indirectement, par une personne décrite au point a) ci-dessus.

Le non-respect de l'article 23 (1) et de l'article 24 constitue un délit et entraîne, en cas de condamnation, une amende n'excédant pas 5 millions de roupies ou le double de la valeur des fonds ou autres actifs, le montant le plus élevé étant retenu, et une peine d'emprisonnement d'au moins 3 ans.

11.1.3 Correspondance des sanctions et résolution des faux positifs

Au cours du processus de filtrage, si une correspondance est détectée (c'est-à-dire s'il s'avère qu'un client, le mandant d'un client ou une partie à une transaction figure sur la liste des sanctions des Nations unies ou sur une liste émise par le Comité national des sanctions, ou est lié à une telle personne), l'entreprise doit immédiatement :

- ★ interrompre la transaction en question pour éviter de commettre une infraction au titre de l'article 23 de la loi sur les sanctions de l'ONU, et
- ★ poursuivre l'enquête sur la base des informations dont dispose la société et des informations d'identification fournies dans la liste des sanctions afin de confirmer la concordance.

L'entreprise tient un registre des faux positifs (en mettant en place un registre des faux positifs) qui est mis à la disposition des autorités compétentes ou des tiers appropriés (tels que l'auditeur indépendant LBC/FT et le CSF) sur demande.

11.2 Obligations de déclaration

Si la société détecte une correspondance positive confirmée (c'est-à-dire que les coordonnées d'un client ou du mandant d'un client correspondent à celles d'une personne figurant sur la liste des sanctions des Nations unies ou sur une liste publiée par le Comité national des sanctions), elle est tenue, en vertu de l'article 25(2) de la loi sur les sanctions des Nations unies, de faire un rapport au Secrétariat national des sanctions en utilisant le modèle à télécharger sur le site web du Secrétariat national des sanctions - http://nssec.govmu.org - à l'adresse électronique suivante : nssec@govmu.org

L'absence de déclaration constitue un délit et entraîne, en cas de condamnation, une amende n'excédant pas 5 millions de roupies et une peine d'emprisonnement n'excédant pas 10 ans.

Lorsque la société fait une déclaration au Secrétariat national des sanctions en vertu de l'article 25(2), elle doit également la faire à la CSF.
Si la société détient, contrôle ou a en sa possession des fonds ou d'autres actifs d'une personne figurant sur la liste des sanctions des Nations unies ou sur une liste établie par le Comité national des sanctions, elle doit, en vertu de l'article 23(4), informer immédiatement le Secrétariat national des sanctions de ce qui suit

1. les détails des fonds ou autres actifs en question,
2. le nom et l'adresse de la personne figurant sur la liste des sanctions des Nations unies ou sur la liste établie par le comité national des sanctions,
3. les détails de toute tentative de transaction impliquant les fonds ou autres actifs, y compris
    a. le nom et l'adresse de l'expéditeur ;
    b. le nom et l'adresse du destinataire prévu ;
    c. l'objet de la tentative de transaction ;
    d. l'origine des fonds ou autres actifs ; et
    e. le lieu où les fonds ou autres actifs devaient être envoyés.

La notification doit être faite en utilisant le modèle à télécharger sur le site web du Secrétariat national aux sanctions - http://nssec.govmu.org et soumise à l'adresse électronique suivante: nssec@govmu.org.

Le non-respect de l'article 23, paragraphe 4, constitue une infraction et, en vertu de l'article 45 de la loi sur les sanctions des Nations unies, entraîne, en cas de condamnation, une amende n'excédant pas 1 million de roupies et une peine d'emprisonnement n'excédant pas 10 ans.

11.2.1 Dépôt d'une DOD

Conformément à l'article 39 de la loi sur les sanctions de l'ONU, la société doit immédiatement soumettre une déclaration d'opérations suspectes à la CRF si elle dispose d'informations relatives à une personne figurant sur la liste des sanctions de l'ONU ou sur une liste publiée par le Comité national des sanctions. Par conséquent, après vérification, s'il s'avère qu'un client ou un mandant d'un client figure sur la liste des sanctions des Nations unies ou sur une liste publiée par le Comité national des sanctions, une déclaration d'opérations suspectes interne doit être soumise au MLRO de la société pour suite à donner.

11.2.2 Amendements à la liste des sanctions de l'ONU

La liste des sanctions de l'ONU est dynamique et peut être modifiée de temps à autre, y compris par des ajouts. Dans ce cas, la CRF envoie un avis à tous les MLRO/DMLRO/Senior Management personnel reporting persons enregistrés, selon le cas. Dès réception de ces avis, l'agent de conformité doit :

1. vérifier rapidement si l'un de ses clients correspond au nouvel ajout (une preuve appropriée de cette vérification doit être conservée)
2. tester le moteur de filtrage utilisé par l'entreprise pour s'assurer que ses bases de données sont rapidement mises à jour
3. En cas de non-concordance avec la liste des sanctions de l'ONU après réception des avis de modification de la liste des sanctions de l'ONU de la CRF, l'entreprise doit soumettre un rapport NIL au SSN et envoyer une copie au CSF dans l'e-mail envoyé.

12. Déclaration de transactions suspectes

Conformément à l'article 14 de la FIAMLA, la société a l'obligation légale de faire une déclaration à la CRF dès que possible et au plus tard dans les cinq jours ouvrables suivant le jour où elle a connaissance d'une transaction dont elle a des raisons de penser qu'elle peut être une transaction suspecte.

12.1 Qu'est-ce qu'une transaction suspecte ?

La section 2 de la FIAMLA définit une transaction suspecte comme une transaction qui :

1. donne lieu à un soupçon raisonnable qu'il peut impliquer
    a. le blanchiment d'argent ou le produit de tout crime ; ou
    b. des fonds liés ou apparentés au financement du terrorisme ou au financement de la prolifération ou à toute autre activité ou transaction liée au terrorisme telle que spécifiée dans la loi sur la prévention du terrorisme ou dans tout autre texte législatif, que ces fonds représentent ou non le produit d'un crime ;
2. est effectuée dans des circonstances d'une complexité inhabituelle ou injustifiée ;
3. ne semble pas avoir de justification économique ou d'objectif licite ;
4. est effectuée par ou pour le compte d'une personne dont l'identité n'a pas été établie à la satisfaction de la personne avec laquelle la transaction est effectuée ; ou
5. donne lieu à des soupçons pour toute autre raison.

Il convient de noter que, conformément à l'article 2 de la FIAMLA, une transaction comprend une proposition ou une tentative de transaction.

Les transactions suspectes sont des transactions pour lesquelles il existe des motifs raisonnables de soupçonner qu'elles sont liées à la commission d'un blanchiment d'argent ou d'un financement du terrorisme. Les motifs raisonnables de suspicion sont déterminés par ce qui est raisonnable compte tenu des pratiques et systèmes commerciaux normaux dans le cadre des activités de l'entreprise et du secteur dans lequel elle opère. Une transaction suspecte peut impliquer plusieurs facteurs qui, en soi, peuvent sembler insignifiants, mais qui, pris ensemble, peuvent faire soupçonner que la transaction est liée à la commission ou à la tentative de commission d'une opération de blanchiment d'argent ou de financement du terrorisme.

Il n'y a pas de seuil monétaire pour faire une déclaration concernant une transaction suspecte. Toutefois, l'article 5 de la FIAMLA érige en infraction le fait d'effectuer ou d'accepter un paiement en espèces supérieur à 500 000 roupies ou à un montant équivalent en devises étrangères. Il est obligatoire de déclarer tout paiement en espèces dépassant 500 000 roupies ou un montant équivalent en devises étrangères.

Lorsque deux ou plusieurs transactions d'un montant total de 500 000 roupies ou d'un montant équivalent en devises étrangères sont effectuées pour le compte d'un même client dans un court laps de temps, et que la société sait que ces transactions ou transferts sont effectués par le même client ou pour son compte, elles doivent être traitées comme une seule transaction et être déclarées à la CRF.

12.2 Indicateurs de transactions suspectes

L'entreprise doit être attentive et veiller à l'identification rapide de tout indicateur suspect. Certains de ces indicateurs sont décrits ci-dessous :

1. Impossibilité d'identifier de manière satisfaisante la source des fonds
2. Les dépôts sont effectués à partir de sources (par exemple des comptes bancaires) qui ne sont pas au nom du client et au nom d'un tiers non identifié, sans justification.
3. La structure des transactions ne semble pas avoir de justification légale ou économique, et/ou ne correspond pas au profil du client.
4. Impossibilité d'obtenir des informations actualisées sur un client

12.3 Obligation de déclaration

Une DOD doit être déposée auprès de la CRF si la société ne peut pas obtenir toutes les informations nécessaires pour établir l'identité du client. La société est tenue de déposer une DOD auprès de la CRF lorsqu'elle n'est pas en mesure d'exécuter les mesures d'EDD requises.

Il incombe au MLRO (ou au DMLRO en son absence) de déposer les DOD auprès de la CRF. Aucun autre employé ou dirigeant de la société ne peut déposer de DOD auprès de la CRF. Pour que le MLRO puisse déposer des DOD auprès de la CRF, il doit être mis au courant ou informé de la transaction suspecte. À cette fin, les employés ou les dirigeants doivent déclarer les transactions suspectes au MLRO en soumettant une DOD interne (voir le modèle à l'annexe 3). En l'absence du MLRO, le MLRO adjoint est chargé d'enquêter et de soumettre les déclarations de soupçon, le cas échéant.

12.4 Quand soumettre une déclaration d'insolvabilité interne au MLRO ?

Une déclaration de soupçon interne (modèle à l'annexe 3) doit être adressée au MLRO par un employé ou un fonctionnaire qui est confronté aux cas suivants :

- ★ Les documents de vérification de l'identité (au cours du processus CDD) ne peuvent pas être obtenus pour le client et l'un de ses principaux (dans le cas où le client est une personne morale/une construction juridique),
- ★ les mesures de vérification de l'identité doivent être appliquées, mais les documents de vérification de l'identité requis ne peuvent être obtenus,
- ★ À la suite de l'évaluation du risque client, le client est classé dans la catégorie des personnes interdites.
- ★ Tout soupçon qu'une transaction puisse être liée au blanchiment d'argent, au financement du terrorisme ou au financement de la prolifération, directement ou indirectement.

Les déclarations de soupçon internes peuvent être remises en personne au MLRO dans une enveloppe scellée ou en envoyant une pièce jointe au format PDF par courrier électronique. Les DOD internes et les DOD doivent être traitées de manière strictement confidentielle.

Lorsque le MLRO / DMLRO reçoit une DOD, il en accuse réception en envoyant un courriel à l'employé concerné.

12.4.1 Le pourboire

Une fois que l'employé a fait une déclaration d'opérations suspectes interne au MLRO, il doit demander conseil au MLRO sur la manière de traiter le client pour lequel/par lequel la transaction suspecte est proposée ou a été effectuée, afin d'éviter d'alerter le client sur le fait que la transaction a été déclarée. Les dirigeants et les employés de la société ne doivent pas informer ou alerter le client ou toute autre personne qu'une déclaration de soupçon interne a été transmise au MLRO. Le MLRO est le principal point de contact de l'entreprise avec la CRF.

Il est strictement interdit aux dirigeants et aux employés de la société de divulguer à quiconque des informations ou tout autre élément susceptible de nuire à une enquête sur une opération suspecte. Dans le cas contraire, cela pourrait constituer un délit (Tipping Off) en vertu de la FIAMLA.

En vertu de la section 16(1) de la FIAMLA, l'entreprise et ses dirigeants ne doivent pas divulguer à **une personne non autorisée** (y compris leurs collègues) qu'une déclaration d'insolvabilité est ou a été déposée, ou que des informations connexes sont ou ont été demandées, fournies ou soumises à la CRF.) Toute personne qui ne se conforme pas à l'article 16 (1) commet une infraction et, en cas de condamnation, est passible d'une amende n'excédant pas 5 millions de roupies et d'une peine d'emprisonnement n'excédant pas 10 ans (article 16(3A) de la FIAMLA).

12.4.2 Traitement des déclarations internes de transactions suspectes

Dès que le MLRO reçoit une DOD interne, il la consigne dans le journal des DOD (voir annexe 4) avec tous les détails, et en accuse réception par courriel à la personne qui a soumis la DOD interne.

Le MLRO aura accès à toutes les informations ou dossiers pertinents pour évaluer si la transaction est suspecte ou non. Après enquête, si le MLRO estime que la transaction est suspecte, il soumettra une DOD à la CRF dès que possible et au plus tard dans les 5 jours ouvrables à compter du jour où le soupçon est apparu.

Le MLRO doit documenter les informations qui ont été examinées pour évaluer la transaction déclarée et la date à laquelle la DOD a été transmise à la CRF dans le journal des DOD. Si le cas le justifie, le MLRO doit demander conseil à la CRF sur la manière de procéder ou de traiter la relation client.

Si, après examen, le MLRO considère que la transaction déclarée n'est pas suspecte, il doit également documenter les informations qui ont été examinées pour évaluer la transaction ainsi que les raisons pour lesquelles il n'a pas fait de déclaration à la CRF dans le journal des DOD. La documentation des informations comprend l'établissement d'un dossier (physique ou électronique) auquel seul le MLRO ou le MLRO adjoint a accès et l'enregistrement des documents/informations suivants dans ce dossier :

- ★ Faits relatifs à l'activité ou à la transaction suspecte présumée
- ★ Documents / preuves / informations relatifs à l'enquête interne menée par le MLRO ou le MLRO adjoint
- ★ les conclusions de l'enquête interne
- ★ Procès-verbaux des réunions tenues avec les employés au cours des enquêtes internes (le cas échéant)
- ★ Analyse écrite du MLRO / MLRO adjoint justifiant la décision d'introduire ou non une DOD auprès de la CRF.

Il convient de noter que la liste ci-dessus n'est pas exhaustive.

En résumé, les différentes étapes pour le MLRO sont les suivantes lorsqu'une déclaration de soupçon est reçue de la part d'un employé :

- ★ Mettre à jour le registre des DOD (modèle à l'annexe 4) en y indiquant la date de réception de la DOD, sa nature et d'autres détails pertinents ;
- ★ poursuivre l'enquête, y compris, le cas échéant, en demandant des documents/informations supplémentaires au client (en évitant de le renseigner), en organisant des réunions avec l'employé qui s'occupe du client, etc ;
- ★ Décider de déposer ou non la DOD auprès de la CRF à l'issue de l'enquête ; et
- ★ Mettre à jour le registre des DOD en conséquence.

12.4.3 Soumission de la DOD à la CRF

Les déclarations de soupçon peuvent être transmises à la CRF par voie électronique ou manuellement.

12.4.3.1 Soumission électronique des DOD

La soumission électronique des DOD peut se faire via le site web de la CRF (goAML) selon les deux modalités suivantes:

1. au format XML ;
2. en remplissant un formulaire STR en ligne sur la plateforme GoAML

Pour pouvoir soumettre des DOD via le site Internet de la CRF, le MLRO/DMLRO doit être enregistré sur la plateforme GoAML auprès de la CRF. La preuve de cet enregistrement doit être conservée.

Une fois que la société a été enregistrée, vérifiée et acceptée par la CRF, le MLRO peut soumettre des DOD en ligne.

L'enregistrement doit être effectué sur le site web de la CRF par le biais de l'application goAML ou sur www.mrugoaml.fiumauritius.org en cliquant sur le guide de l'utilisateur web pour plus de détails sur l'enregistrement. Le MLRO et le DMLRO doivent être enregistrés en tant qu'utilisateurs actifs sur la plateforme GoAML à tout moment.

12.4.3.2 Soumission des DOD sur papier

Si l'entreprise n'a pas la capacité technique de transmettre les DOD par voie électronique, l'agent de liaison avec les organismes de blanchiment d'argent doit :

1. télécharger un formulaire STR vierge sur le site de la CRF ou en suivant le lien ci-dessous :
2. http://www.fiumauritius.org/English/Reporting/Documents/STR_FORM_FINAL_VERSION.pdf le compléter, et
3. le remettre en main propre à la réception de la CRF au 10ème étage, SICOM Tower, Wall Street, Ebene Cybercity, Ebene 72201, République de Maurice, ou le soumettre par fax au +230 466 2431.

13. Sélection et formation des employés

13.1 Contrôle des employés :

L'entreprise a pour politique, lorsqu'elle recrute des employés ou avant de nommer un administrateur ou un dirigeant (au sens de la loi de 2007 sur les services financiers), de procéder à une sélection des candidats afin de s'assurer qu'ils sont compétents et aptes à occuper le poste à pourvoir. Les mesures de sélection peuvent inclure

1. obtenir et confirmer les détails des antécédents professionnels, des qualifications et des affiliations professionnelles ;
2. obtenir et confirmer les références appropriées
3. obtenir et confirmer les détails de toute mesure réglementaire ou de toute mesure prise par un organisme professionnel à l'encontre de l'employé potentiel ;
4. obtenir et confirmer les détails de toute condamnation pénale, y compris la vérification du casier judiciaire de l'employé potentiel ; et
5. vérifier que les employés ne figurent pas sur la liste des personnes désignées par les Nations unies dans le cadre des sanctions financières ciblées sur le financement du terrorisme et de la prolifération.

Les registres des contrôles effectués sont conservés dans le cadre des données relatives à l'emploi de chaque travailleur.

13.1.1 Dépistage continu

L'entreprise adopte un programme de contrôle continu pour s'assurer que les employés existants ne représentent pas un risque pour l'entreprise pendant toute la durée de leur emploi/engagement. Il peut être important de savoir, par exemple, si un employé existant a été condamné pour un délit ou s'il a été impliqué dans un comportement susceptible de nuire à l'entreprise ou à ses activités. Dans ce contexte, les mesures ci-dessous s'appliquent aux employés existants:

- ★ Tous les trois ans, un nouveau contrôle est effectué sur les bases de données des médias défavorables et sur la liste des sanctions des Nations unies concernant les employés existants.

13.2 Formation des employés :

Tous les employés dont les fonctions sont liées au traitement des relations d'affaires ou des transactions doivent être sensibilisés à la législation pertinente et aux normes relatives à la lutte contre le blanchiment d'argent et le financement du terrorisme. L'entreprise s'efforcera donc de former ses dirigeants et employés impliqués dans le traitement des relations d'affaires ou des transactions liées aux activités de l'entreprise.

Les employés reçoivent une formation qui couvre au moins les points suivants

- ★ les obligations légales de la Société en vertu de la législation, des réglementations et des directives relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme ;
- ★ les vulnérabilités des produits et services offerts par la Société en matière de blanchiment d'argent et de financement du terrorisme ;
- ★ Les contrôles et procédures de LBC-FT de l'entreprise ;
- ★ L'identité et les responsabilités du MLRO ;
- ★ l'identification et la déclaration des transactions suspectes ;
- ★ Les sanctions pénales en vigueur en cas de non-déclaration de transactions suspectes ;

- ★ Les nouveaux développements, y compris les informations sur les techniques, méthodes, tendances et typologies actuelles en matière de blanchiment d'argent et de financement du terrorisme ; et
- ★ Informations sur l'évolution du comportement et des pratiques des blanchisseurs de capitaux et des personnes qui financent le terrorisme.

Les nouveaux employés impliqués dans les activités commerciales de la Société recevront une formation de sensibilisation à la LAB-FT sur les mesures en place au sein de la Société concernant la LAB-FT et leur obligation en tant qu'employé/responsable d'une institution financière, conformément aux dispositions applicables de la loi. Le nouvel employé reçoit une formation à la LAB-FT dès que cela est raisonnablement possible et, en tout état de cause, dans un délai d'un mois à compter du début de son emploi/contrat. La formation doit garantir que le nouvel employé/agent est conscient des obligations légales et réglementaires qui lui incombent et lui permettre de reconnaître une transaction suspecte et les procédures à suivre pour signaler de manière adéquate une transaction suspecte.

En outre, la société doit fournir une formation spécifique aux membres du conseil d'administration et aux employés faisant partie de la direction générale. Cette formation doit porter sur les points suivants

13.2.1 Pour le conseil d'administration et le personnel de direction

- ★ les infractions et les sanctions applicables en cas de non-déclaration ou d'assistance aux blanchisseurs de capitaux ou aux personnes impliquées dans le financement du terrorisme
- ★ les exigences en matière de CDD, y compris la vérification de l'identité et la conservation des documents ; et
- ★ En particulier, l'application de la stratégie et des procédures de l'institution financière fondées sur le risque.

13.2.2 Pour le responsable de la conformité, le MLRO et le MLRO adjoint

1. les exigences législatives et réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme
2. les normes et exigences internationales sur lesquelles la stratégie de Maurice est fondée, à savoir les 40 recommandations du GAFI et les rapports typologiques sur le blanchiment de capitaux et le financement du terrorisme qui sont pertinents pour leurs activités ;
3. l'identification et la gestion des risques de blanchiment d'argent et de financement du terrorisme ;
4. la conception et la mise en œuvre de systèmes internes de contrôle de la LBC/FT ;
5. la conception et la mise en œuvre de programmes de contrôle et de suivi de la conformité en matière de LBC/FT ;
6. l'identification et le traitement des activités et accords suspects et des tentatives d'activités et d'accords suspects ;
7. les vulnérabilités en matière de blanchiment d'argent et de financement du terrorisme des services et produits concernés ;
8. le traitement et la validation des divulgations internes ;
9. le processus de soumission d'une divulgation externe ;
10. la liaison avec les organismes chargés de l'application de la loi ;
11. les tendances et typologies en matière de blanchiment d'argent et de financement du terrorisme ; et
12. la gestion du risque de dénonciation.

Toutes les informations relatives à la formation sont consignées dans le journal de formation (modèle à l'annexe 5).

13.2.3 Participation obligatoire à une session de sensibilisation

Comme mentionné ci-dessus, les sessions de sensibilisation des employés sont l'une des méthodes choisies par la Société pour atteindre son objectif de maintenir ou d'accroître les connaissances des employés en matière de lutte contre le blanchiment d'argent et le financement du terrorisme afin de lui permettre de se conformer pleinement à ses obligations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. En outre, l'assiduité et la performance des employés lors des sessions de sensibilisation/formation seront contrôlées. Par conséquent, la participation aux sessions de sensibilisation est obligatoire et la non-participation sans excuse raisonnable peut entraîner des mesures disciplinaires appropriées de la part de l'entreprise.

13.3 Formation des agents de conformité, des MLRO et des MLRO adjoints

Le MLRO/DMLRO étant responsable du traitement, de l'évaluation et de la déclaration des transactions suspectes à la CRF, il doit recevoir une formation appropriée lui permettant de s'acquitter de ses devoirs et obligations.

Le Compliance Officer est un autre employé clé dans la mesure où il est responsable de la supervision quotidienne du cadre de conformité AML/CFT. Dans ce contexte, il est de la plus haute importance que le Compliance Officer, le MLRO et le DMLRO reçoivent un minimum de 10 heures de formation sur une base annuelle qui se concentrera sur son rôle et ses devoirs spécifiques comme le prévoit la Réglementation FIAML 2018. Cette formation est conforme aux exigences des normes de compétence.

14. Tenue de registres

14.1 Vérification de l'identité et relevés de transactions

Le règlement 14 (1) exige que la société tienne et conserve tous les registres relatifs aux transactions sous une forme qui permette de reconstituer rapidement chaque transaction individuelle.

L'entreprise doit tenir des registres de toutes les transactions dans lesquelles elle est impliquée ainsi que des registres de tous les clients. En conséquence, l'entreprise doit être tenue :

1. Les documents relatifs à l'identification des clients et des bénéficiaires effectifs (par exemple, les copies ou les enregistrements des documents d'identification officiels tels que les passeports, les cartes d'identité, les permis de conduire ou des documents similaires) ainsi que la correspondance commerciale pendant au moins sept ans après la fin de la relation d'affaires,
2. Les dossiers concernant les transactions, tant nationales qu'internationales, pendant une période de 7 ans après la fin de la transaction.
3. les enregistrements de toutes les déclarations d'opérations suspectes, y compris les documents d'accompagnement
4. les détails de tous les enregistrements de toutes les modifications apportées au présent manuel conformément à la section 17A de la FIAMLA 2002.

La société conservera donc les documents énumérés ci-dessous pendant une période d'au moins sept ans après la fin de la relation d'affaires ou sa résiliation dans le dossier du client concerné (sur support papier ou électronique) :

- ★ Conditions générales signées
- ★ Documents de vérification de l'identité (y compris tous les documents EDD), résultats du screening et évaluation du risque client effectuée ;
- ★ les informations relatives à la transaction
- ★ les correspondances relatives à la transaction.

Dans tous les cas, des informations suffisantes sont enregistrées pour permettre la reconstitution d'une transaction avec un client.

14.2 Rapports internes et externes sur les transactions suspectes

Conformément à la section 17F de la FIAMLA et à la politique de lutte contre le blanchiment d'argent et le financement du terrorisme de la société, l'agent de liaison pour le blanchiment d'argent doit conserver les informations suivantes sur les déclarations de soupçon internes reçues et les déclarations de soupçon déposées pendant une période d'au moins sept ans à compter de la date à laquelle la déclaration a été faite:

- ★ les déclarations d'opérations suspectes internes reçues par le MLRO ;
- ★ les documents relatifs aux mesures prises à la suite de la réception des déclarations internes de transactions suspectes ;
- ★ les relevés des mesures prises pour déterminer si les transactions déclarées sont suspectes ou non ;
- ★ les documents relatifs aux informations examinées pour déterminer si les transactions signalées sont suspectes ou non ;
- ★ lorsque, après examen, le MLRO a décidé de ne pas faire de déclaration à la CRF, un enregistrement du motif de la décision de ne pas faire de déclaration à la CRF ; et

- ★ toutes les déclarations faites par le MLRO à la CRF.

Ces dossiers peuvent être conservés sous forme de copies papier et/ou électroniques.

Il convient de noter que, conformément à l'article 13(5) de la FIAMLA, lorsqu'une déclaration de soupçon a été faite à la CRF, le directeur de la CRF doit, par avis écrit, exiger de la société qu'elle conserve les documents relatifs à cette transaction suspecte pendant la période spécifiée dans l'avis.

14.3 Dossiers de formation

La Société doit conserver une trace de toutes les formations AML-CFT dispensées aux employés, comme indiqué ci-dessous, dans le registre de formation (voir le modèle à l'annexe 5) :

- ★ les dates auxquelles la formation à la lutte contre le blanchiment de capitaux et le financement du terrorisme a été dispensée ;
- ★ la nature de la formation, y compris les détails du contenu et du mode de prestation ;
- ★ les noms des employés qui ont reçu la formation ; et
- ★ des copies des dossiers de formation professionnelle continue (CPD) pour le Compliance, le MLRO et le MLRO adjoint.

14.3.1 Modifications des politiques et procédures

La société doit conserver une trace écrite de toute modification apportée aux politiques et procédures de LBC/FT, conformément à la FIAMLA 2002. Ces informations sont consignées dans un registre des modifications de la politique (modèle à l'annexe 6).

15. Contrôle et vérification de la conformité

Comme le prévoit le règlement 31 du FIAMLR, la société doit disposer d'une politique et d'une procédure appropriées pour le suivi et le contrôle de la conformité de la société et de ses activités avec les exigences pertinentes en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Le contrôle et la vérification du niveau de conformité doivent inclure :

- ★ Des tests et un suivi sont effectués pour déterminer si la société dispose de dispositifs solides et documentés pour gérer les risques identifiés par l'évaluation des risques de l'entreprise ;
- ★ Des actions rapides sont prises pour remédier à toute déficience identifiée en termes de AML-CFT.

La vérification et le contrôle de la conformité de la société aux exigences applicables en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme doivent être effectués de manière continue et l'exercice doit porter sur les points suivants :

- ★ l'adéquation de son évaluation des risques de blanchiment d'argent et de financement du terrorisme
- ★ l'adéquation des politiques, procédures et processus en matière de CDD, et leur conformité avec les exigences internes,
- ★ l'adéquation de son approche fondée sur le risque par rapport aux services offerts aux clients et aux implantations géographiques,
- ★ l'adéquation de la formation, y compris son exhaustivité, l'exactitude des supports, le calendrier de la formation,
- ★ la conformité avec les lois applicables,
- ★ la capacité du système à identifier les activités inhabituelles,
- ★ l'adéquation de la tenue des dossiers et
- ★ l'examen de ses systèmes de déclaration d'opérations suspectes (STR), qui devrait comprendre une évaluation de la recherche et de l'orientation des opérations inhabituelles, entre autres.

Le responsable de la conformité est chargé de contrôler et de vérifier le respect des exigences en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, comme l'exige le règlement 31. En outre, les résultats de l'exercice de contrôle et de vérification doivent être consignés et communiqués au conseil d'administration afin de garantir que ce dernier exerce un contrôle approprié sur la conformité et l'efficacité des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme mises en œuvre.

16. Audit indépendant de la lutte contre le blanchiment d'argent et le financement du terrorisme

Conformément au règlement 22(1)(d) du règlement FIAML 2018, la société est tenue de mettre en place une fonction d'audit indépendante pour examiner et vérifier la conformité et l'efficacité des mesures prises conformément à la FIAMLA et au règlement FIAML 2018.

16.1 Portée de l'audit

Au minimum, l'exercice d'audit doit couvrir les points suivants :

1. l'adéquation de son évaluation des risques de blanchiment d'argent et de financement du terrorisme
2. l'adéquation des politiques, procédures et processus en matière de CDD, et leur conformité avec les exigences internes,
3. l'adéquation de son approche fondée sur le risque par rapport aux services offerts aux clients et aux implantations géographiques,
4. l'adéquation de la formation, y compris son exhaustivité, l'exactitude des supports, le calendrier de la formation,
5. la conformité avec les lois applicables,
6. la capacité du système à identifier les activités inhabituelles,
7. l'adéquation de la tenue des dossiers et
8. l'examen de ses systèmes de déclaration d'opérations suspectes (STR), qui devrait comprendre une évaluation de la recherche et de l'orientation des opérations inhabituelles, entre autres.

16.2 Indépendance du contrôleur des comptes

L'audit est réalisé par un auditeur interne ou externe indépendant des fonctions de contrôle de la conformité et ne doit pas être réalisé par le responsable de la conformité.

16.3 Résultat de l'audit

À l'issue de l'exercice d'audit, l'auditeur soumet un rapport d'audit à l'attention du conseil d'administration. Le rapport couvre le champ d'application susmentionné, fournit les observations relatives à toute déficience constatée et formule des recommandations de qualité en vue de la prise rapide de mesures correctives.

Après réception du rapport d'audit, un plan d'action est élaboré pour remédier à toute déficience observée par l'audit dans un délai maximum d'un mois.

16.4 Fréquence de l'audit

L'audit indépendant est réalisé au moins une fois par an et tous les rapports sont conservés et fournis à la CRF sur demande. Cette fréquence peut être révisée par le conseil d'administration en fonction des risques de blanchiment d'argent et de financement du terrorisme auxquels l'entreprise est confrontée.

Les rapports d'audit sont soumis au conseil d'administration pour examen, approbation et suite à donner.

17. Confiance des tiers

Conformément à la règle 21 du FIAMLR 2018, la Société peut faire appel à un tiers pour la prospection commerciale ou l'exécution des mesures CDD pour le compte de la Société. Si la Société fait appel à un tiers pour la prospection commerciale ou l'exécution des mesures CDD en son nom, la Société doit:

1. prendre des mesures pour s'assurer que des copies des données d'identification et d'autres documents pertinents relatifs aux exigences CDD sont disponibles sur demande et sans délai auprès du tiers ;
2. s'assurer que le tiers est réglementé et supervisé ou contrôlé aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, et qu'il a mis en place des mesures pour se conformer aux exigences en matière de CDD et de tenue de registres, conformément à la Loi et au présent règlement.

L'Entreprise ne doit pas faire appel à un tiers situé dans un pays à haut risque.

Même lorsque l'entreprise fait appel à un tiers pour mettre en œuvre tout ou partie des mesures de CDD en son nom, l'Entreprise doit avoir rapidement accès à tous les documents de CDD qui doivent être conservés dans les dossiers en conséquence.

Toutes les mesures prises en vertu du présent paragraphe (par exemple l'évaluation du statut réglementaire du tiers) doivent être conservées dans les dossiers afin de pouvoir démontrer la conformité avec le règlement 21 du FIAMLR 2018.

17.1 Évaluation des risques et diligence raisonnable à l'égard des prestataires de services tiers

La société procède à une évaluation des risques et à une procédure de diligence raisonnable à l'égard des prestataires de services tiers qui fournissent des services essentiels à la société, y compris des fonctions externalisées telles que la fonction de conformité, le MLRO et le DMLRO. Le processus d'évaluation des risques et de diligence raisonnable a pour principal objectif de

1. Identifier et vérifier l'identité des prestataires de services tiers en obtenant des informations et des documents pertinents auprès de sources indépendantes.
2. Effectuer un contrôle sur le prestataire de services tiers afin de vérifier s'il existe des occurrences.
3. Procéder à une évaluation des risques liés au prestataire de services tiers.
4. Procéder à une évaluation continue des risques et à un exercice de diligence raisonnable à l'égard du prestataire de services tiers.

18. Pays à haut risque

Conformément à l'article 12(1)(c) du Règlement FIAML 2018, une personne soumise à déclaration doit appliquer des mesures CDD renforcées telles que décrites dans le présent document. En outre, le règlement 24(1) prévoit qu'il convient de tenir dûment compte des éléments ci-dessous lors de l'identification des pays à haut risque :

1. des lacunes stratégiques dans le cadre juridique et institutionnel de la lutte contre le blanchiment de capitaux et le financement du terrorisme, en particulier en ce qui concerne
    a. l'incrimination du blanchiment de capitaux et du financement du terrorisme ;
    b. les mesures relatives à la CDD ;
    c. les exigences relatives à la tenue de registres ;
    d. les exigences relatives à la déclaration des transactions suspectes ;
    e. la mise à disposition des autorités compétentes d'informations précises et opportunes sur la propriété effective des personnes morales et des constructions juridiques ;

2. les pouvoirs et procédures des autorités compétentes du pays aux fins de la lutte contre le blanchiment de capitaux et le financement du terrorisme, y compris les sanctions efficaces, proportionnées et dissuasives, ainsi que les pratiques du pays en matière de coopération et d'échange d'informations avec les autorités compétentes d'outre-mer ;

3. l'efficacité du système national de lutte contre le blanchiment de capitaux et le financement du terrorisme pour faire face aux risques de blanchiment de capitaux ou de financement du terrorisme.

En vue d'identifier les pays à haut risque et conformément au règlement 24(3) de la réglementation FIAML 2018, la Société appliquera des mesures de diligence raisonnable renforcées à l'égard de tous les pays identifiés par le Groupe d'action financière (GAFI) sur leur liste de juridictions faisant l'objet d'une surveillance accrue. Il est à noter que la Société n'entretient aucune relation avec les pays figurant sur la liste des juridictions faisant l'objet d'un appel à l'action du GAFI.

Annexe 1 - Formulaire d'approbation de la direction générale (clients à haut risque)

Nom du client	
Date d'intégration (le cas échéant)	
Évaluation du risque	Haut
Raisons du risque élevé	
Autres commentaires	

L'établissement ou la poursuite de la relation d'affaires se fait par la présente :
Veuillez cocher la case appropriée

Approuvé ☐ **Refusé** ☐

Nom : _____

Signature: _____

Date: _____

Annexe 2 - Formulaire de suivi continu

Voir séparément

Annexe 3 - Déclaration de transaction suspecte interne

Déclaration de transaction suspecte (DTS) interne

Détails de la relation d'affaires suspectée

Nom du client : _____

Type de service offert au client: _____

Date du début de la relation d'affaires (jj/mm/aa**) :** _____

Détails des soupçons (veuillez joindre les pièces justificatives pertinentes)

Transaction suspectée:

_____

Motifs de suspicion:

_____

Le fait d'informer le client ou toute autre personne de votre suspicion et de ce rapport constitue un délit. Ce rapport doit être traité de manière strictement **CONFIDENTIELLE.**

Signature du rapporteur :_____ Date (dd/mm/yy):_____

Nom du rapporteur:_____

FOR MLRO's USE

Date received: **Time**:

Details of Action: (*please attach relevant documents*)

Date assessment completed:
STR submitted to FIU (*please indicate YES/NO*):

Annexe 4 - Registre des déclarations de transactions suspectes

Interne - Registre des déclarations d'opérations suspectes								
Date	**STR Rempli le** (Nom du dossier du client)	**Nom de l'employé qui remplit le STR** (inclure le poste)	**Raisons d'être de l'internat STR**	**Reçu par le MLRO ou le DMLRO**	**MLRO a déposé une DOD auprès de la CRF** (Oui / Non)	**Raisons de l'enregistrement auprès de la CRF** (le cas échéant)	**Date de dépôt auprès de la CRF** (le cas échéant)	**Retour d'information de la CRF** (le cas échéant)

Annexe 5 - Journal de formation

Voir séparément

Annexe 6 - Journal des modifications de la politique

Voir séparément

Annexe 7 - Évaluation des risques d'entreprise et méthodologie

Voir séparément

Annexe 8 - Évaluation du risque client et méthodologie

Voir séparément

Annexe 9 - Formulaire d'accusé de réception

Please See Separately

Annexe 10 - Registre des personnes politiquement exposées (PEP)

Please See Separately