



**AUTORITE DE REGULATION DU MARCHE
DES CAPITAUX DU BURUNDI**

**REGLEMENT N° 009/2026 DU 23 / 2 / 2026 PORTANT LUTTE CONTRE LE
BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME**

FEVRIER 2026

AS

Vu la Constitution de la République du Burundi ;

Vu la loi n° 1/02 du 18 janvier 2005 portant Ratification par la République du Burundi de la Convention de l'Union Africaine sur la Prévention et la lutte contre la Corruption ;

Vu la loi n° 1/03 du 18 janvier 2005 portant Ratification par la République du Burundi de la Convention des Nations unies contre la Corruption ;

Vu la loi n°1/12 du 18 avril 2006 portant Mesures de Prévention et de Répression de la corruption et des infractions connexes ;

Vu la loi n°1/09 du 30 mai 2011 portant code des Sociétés privées et à participation publique ;

Vu la loi n°1/01 du 16 janvier 2015 portant révision de la loi n°1/07 du 26 avril portant Code de commerce

Vu la loi n°1/12 du 28 juin 2017 régissant les sociétés coopératives au Burundi

Vu la loi n°1/17 du 22 août 2017 régissant les activités bancaires

Vu la loi n°1/27 du 29 décembre 2017 portant révision du Code pénal ;

Vu la loi n°1/05 du 23 janvier 2018 portant insolvabilité du commerçant au Burundi ;

Vu la loi n°1/07 du 11 mai 2018 portant système national de paiement ;

Vu la loi n°1/09 du 11 mai 2018 portant modification du Code de procédure pénale ;

Vu la loi n°1/05 du 27 février 2019 régissant le Marché des capitaux du Burundi

Vu la loi n°1/08 du 29 octobre 2020 régissant l'Autorité de Régulation du Marché des Capitaux du Burundi ;

Vu la loi n°1/19 du 17 juin 2021 portant modification de la n°1/24 du 10 septembre 2008 portant Code des investissements du Burundi ;

Vu la loi n°1/10 du 16 mars 2022 portant prévention et répression de la cybercriminalité au Burundi ;

Vu la loi n°1/08 du 27 mars 2025 portant modification de la loi n°1/02 du 04 février 2008 portant lutte contre le blanchiment de capitaux et le financement du terrorisme ;

Décret n°100/085 du 25 juillet 2018 portant cadre national de collecte, de diffusion, d'accès, d'archivage et de sécurisation des données et des micro-données ;

Vu la réglementation de change de la Banque de la République du Burundi du 28 décembre 2023 ;

Vu le règlement n° 02/2026 du 30 janvier 2026 de la Banque Centrale édicté en application de la loi n°1/08 du 27 mars 2025 portant modification de la loi n°1/02 du 04 février 2008 portant lutte contre le blanchiment de capitaux et le financement du terrorisme

L'Autorité de Régulation du Marché des Capitaux du Burundi, ci-après désigné « Autorité », édicte le présent Règlement.

CHAPITRE I. DES DISPOSITIONS GENERALES

Article 1 : Champ d'application

Les dispositions du présent règlement sont applicables à toute personne (physique ou morale) agréée pour opérer sur le marché des capitaux du Burundi.

Article 2 : Objet

Le présent Règlement est édicté pour :

1. définir les règles et les stratégies visant à prévenir, détecter et réprimer toutes les activités/opérations liées au blanchiment des capitaux et au financement du terrorisme ;
2. exiger aux acteurs agréés d'établir et de maintenir des politiques, des procédures et outils spécifiques pour se prémunir contre l'utilisation du marché des capitaux à des fins de blanchiment des capitaux et financement du terrorisme ;
3. instruire les acteurs opérant sur le marché des capitaux du Burundi à identifier les opérations suspectes, à les documenter et à transmettre aux autorités habilitées les rapports et les informations relatives auxdites opérations suspectes ;
4. promouvoir la transparence sur le marché des capitaux du Burundi.

Article 3 : Sigles et Définitions

Au sens du présent Règlement, on entend par :

1. **autorité compétente**, toute autorité administrative ou de poursuite chargée de lutter contre le blanchiment de capitaux et le financement du terrorisme ;
2. **ayant-droit économique**, toute personne physique ou morale représentée de quelque manière que ce soit, tout signataire de comptes bancaires ou financiers ou tout bénéficiaire de droits ou d'avantages économiques résultant du compte ;
3. **bénéficiaire effectif**, la ou les personnes physiques qui en dernier ressort possèdent ou contrôlent un client et/ou la personne physique pour laquelle une opération est réalisée. Cela inclut les personnes qui exercent en dernier ressort un contrôle effectif sur une personne morale ou une construction juridique ;

4. **blanchiment de capitaux**, processus par lequel une personne physique ou morale dissimule ou déguise la nature ou l'origine du produit d'activités illicites de manière à ce qu'il paraisse provenir de sources licites notamment par :
 - I. la conversion ou le transfert de biens, dans le but de dissimuler ou de déguiser l'origine illicite des biens ou d'aider toute personne qui est impliquée dans la commission de l'infraction principale à échapper aux conséquences juridiques de ses actes ;
 - II. la dissimulation ou le déguisement de la nature, de l'origine, de l'emplacement, de la disposition, du mouvement de la propriété réelle de bien ou de droits y relatifs par toute personne en sachant que ceux-ci proviennent d'un crime, d'un délit ou à une participation à un crime ou délit ;
 - III. l'acquisition, la détention ou l'utilisation de biens par toute personne en sachant que ceux-ci proviennent d'un crime ou d'un délit ou d'une participation à un crime ou délit ;
5. **CDD**, Customer Due Diligence (Diligence raisonnable à l'égard des clients ou contrôle préalable des clients) ;
6. **Cellule Nationale de Renseignement Financier**, « CNRF » en sigle, organe chargé de lutter contre le blanchiment de capitaux et le financement du terrorisme au Burundi ;
7. **la diligence raisonnable renforcée « EDD-Enhanced Due Diligence »** est une procédure KYC approfondie, cruciale dans la lutte contre le blanchiment d'argent (LCB/FT), appliquée aux clients, transactions ou juridictions à haut risques ;
8. **fiducie**, opération par laquelle un ou plusieurs individus (constituants) transfèrent des biens, des droits ou des sûretés ou un ensemble de biens, de droits, de sûretés, présents ou futurs, à un ou plusieurs gestionnaires (fiduciaires) qui, les tenant séparés de leurs patrimoines propre, agissent dans un but déterminé au profit d'un ou plusieurs autres individus (bénéficiaires) ;
9. **financement du terrorisme**, tout acte commis par une personne physique ou morale qui, par quelque moyen que ce soit, directement ou indirectement, par elle-même ou par personne interposée, a délibérément fourni ou réuni, ou tente de fournir ou de réunir des biens, fonds et autres ressources financières dans l'intention de les utiliser ou sachant qu'ils seront utilisés, en tout ou partie, en vue de la commission d'un ou plusieurs actes terroristes ;
10. **fonds**, avoirs de toute nature, corporel ou incorporel, meuble ou immeuble, tangible ou intangible, fongible ou non fongible ainsi que tout document ou instrument juridique sous toute forme, y compris électronique ou numérique, prouvant la propriété des avoirs ou des droits y afférents ainsi que les intérêts sur lesdits avoirs, notamment les crédits, les chèques de voyage, les chèques bancaires, les mandats, les actions, les valeurs mobilières, les obligations, les

traites, les lettres de crédits ainsi que les éventuels intérêts, dividendes ou autres revenus ou valeurs tirés ou générés par de tels avoirs ;

11. **GAFI** (Groupe d'Action Financière), Organisme mondial de surveillance du blanchiment de capitaux et du financement du terrorisme et définit des normes internationales visant à prévenir ces activités illégales ;
12. **intermédiaire de marché**, toute entité agréée et exerçant les activités sur le marché des capitaux du Burundi ;
13. **KYC, Know Your Customer** (Obligation d'identification du client)
14. **LBC/FT**, Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme ;
15. **pays à haut risque**, pays identifié par le Groupe d'Action Financière comme présentant des lacunes importantes stratégiques dans ses mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
16. **placement illicite**, conversion des sommes d'argent en numéraires issues des trafics ou des activités illicites par leur introduction dans le système bancaire ou dans le circuit économique notamment les dépôts d'espèces en comptes bancaire ou l'acquisition de cartes de paiement prépayées ;
17. **personne politiquement exposée (PPE) nationale**, personnes physique qui exerce ou qui a exercé d'importantes fonctions publiques au Burundi , notamment : les chefs d'Etat ou de Gouvernement, les députés, les Sénateurs, les membres du gouvernement et les personnes de même rang, les gouverneurs de province, les administrateurs communaux, les commissaires généraux, les fonctionnaires occupant de postes de haute responsabilité de niveau égal ou supérieur à celui de Directeur au ministère, les magistrats, les présidents des cours et tribunaux, les comptables publics, les militaires et policiers de haut rang (officiers généraux et officiers supérieur de l'armée et de la police), les inspecteurs de l'armée et de la police, les responsables des partis politiques et de confessions religieuses, les personnes associées à une personne politiquement exposée (membre de la famille en lignée directe ou par alliance, personne proche ou toute personne liée par des relations d'affaires) ;
18. **personne politiquement exposée des organisations internationales**, personne qui exerce ou qui a exercé d'importantes fonctions au sein de ou pour le compte d'une organisation internationale notamment les membres de la haute direction (directeurs, directeurs adjoint) et les membres du comité national consultatif et toute personne exerçant des fonctions équivalentes ;
19. **standards internationaux**, les recommandations du GAFI ;
20. **transaction importante**, toute opération d'un montant supérieur ou égal à quarante millions de francs Burundi (BIF 40.000.000) ou l'équivalent en devises étrangères ou en valeurs mobilières correspondantes à ce montant ;
21. **terroriste**, toute personne physique qui :
 - I. commet ou tente de commettre des actes de terroristes par tout moyen, directement ou indirectement et délibérément ;

- II. participe en tant que complice à des actes terroristes ou au financement du terrorisme ;
- III. organise ou donne l'ordre à d'autres de commettre des actes terroristes ;
- IV. contribue à la commission d'actes terroristes par un groupe de personnes agissant dans un but commun, lorsque ladite contribution est intentionnelle et vise à favoriser la commission de l'acte terroriste ou en ayant connaissance de l'intention du groupe de commettre un acte terroriste.

CHAPITRE II. DES STRATEGIES ET DE LA POLITIQUE INTERNE DE CONFORMITE

Article 4 : Les stratégies de lutte contre le blanchiment des capitaux et financement du terrorisme.

Toute entité agréée pour exercer des activités sur le marché des capitaux du Burundi est tenue d'établir des stratégies de LBC/FT.

Ces stratégies comprennent les éléments suivants :

1. les politiques, les procédures et les contrôles internes y compris les dispositifs de contrôle de la conformité et des procédures appropriées lors du recrutement du personnel de façon à s'assurer de son honorabilité et sa compétence ;
2. les règles et procédures d'identification et de reconnaissance de leur client « *KYC ou EDD* » ;
3. l'identification et la déclaration des opérations suspectes à la CNRF ;
4. la tenue et conservation des documents relatifs aux cas suspects ;
5. la formation du personnel ;
6. la mise en place du dispositif de contrôle interne et de conformité et celui de surveillance et détection des transactions suspectes ainsi que la désignation des responsables chargés de la LBC/FT ;
7. la coopération entre l'Autorité, la CNRF et les intermédiaires de marché.

Article 5 : Mise en place de la politique interne de lutte contre le blanchiment des capitaux et le financement du terrorisme

Toute personne autorisée ou agréé opérant sur le marché des capitaux du Burundi doit élaborer, adopter et mettre en œuvre la politique interne, les procédures et contrôles internes afin de prévenir et détecter toute infraction relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Elle doit élaborer et mettre en œuvre des contrôles internes et d'autres procédures visant à dissuader les criminels d'utiliser ses installations à des fins de blanchiment de capitaux et de financement du terrorisme et à garantir que les activités soient menées conformément à la loi et à des normes éthiques élevées et que le service n'est pas fourni lorsqu'il existe de bonnes raisons de supposer que les transactions sont associées à des activités de blanchiment de capitaux ou de financement du terrorisme.

Toute personne agréée ou autorisée doit coopérer pleinement avec les organismes chargés de l'application de la loi relative à la LBC/FT et les organismes de réglementation compétents, et prendre les mesures appropriées pour divulguer les informations à l'Autorité, à la CNRF et aux autres autorités compétentes.

Les programmes, les politiques, les procédures et les contrôles internes doivent comprendre les éléments suivants :

1. l'établissement de procédures garantissant des normes élevées d'intégrité de ses employés ou des personnes agissant en leur nom ;
2. des programmes de formation continue et des sessions de renforcement des capacités afin de garantir la bonne compréhension et la mise en œuvre des exigences de la loi, des règlements et des lignes directrices relatifs à la LBC/FT ;
3. une fonction de conformité en matière de lutte contre le blanchiment d'argent, dirigée par le responsable des signalements de blanchiment de capitaux ;
4. une fonction d'audit indépendante chargée de vérifier le respect des exigences légales ;
5. un dispositif de contrôle interne pour vérifier la conformité, l'observance et l'efficacité des mesures prises en vue d'appliquer la loi, des règlements et des lignes directrices relatifs à la LBC/FT ;
6. un système de contrôle interne solide et fiable.

Toute personne agréée ou autorisée doit maintenir une fonction d'audit indépendante et dotée de ressources suffisantes, capable d'évaluer régulièrement l'efficacité de ses politiques, procédures et contrôles internes, ainsi que sa conformité aux exigences réglementaires.

Il est tenu de réviser ses politiques, procédures et contrôles au moins une fois tous les deux (2) ans afin de garantir leur efficacité, conformément à la réglementation et de désigner un responsable.

Article 6 : Désignation d'un responsable chargé de la lutte contre le blanchiment des capitaux et le financement du terrorisme

Tout intermédiaire du marché est tenu de désigner un (1) ou plusieurs responsables de la prévention du blanchiment des capitaux et financement du terrorisme chargé(s) généralement de veiller à la cohérence et à l'efficacité du dispositif de prévention du blanchiment des capitaux et financement du terrorisme.

Le(s) responsable(s) de la prévention du blanchiment des capitaux et financement du terrorisme est (sont) chargé(s) en particulier de :

1. la transmission des déclarations à la CNRF ;
2. l'établissement des politiques et procédures applicables et des contrôles internes à mettre en place ;
3. suivi des opérations considérées comme suspectes ;

4. la centralisation des informations afin d'identifier et de prévenir la réalisation des opérations liées au blanchiment des capitaux et financement du terrorisme ;
5. l'information régulière à la hiérarchie sur les clients suspectés ou plus risqués ;
6. veiller à ce que tout le personnel concerné dispose des connaissances requises pour détecter et signaler des opérations liées au blanchiment des capitaux et financement du terrorisme ;
7. établir des relations entre l'intermédiaire du marché, l'Autorité, la CNRF et toute autorité compétente en cas de besoin.

Tout responsable de la prévention du blanchiment des capitaux et financement du terrorisme est désigné sur base des critères d'honorabilité, expérience professionnelle, intégrité morale et doit être investi de niveau hiérarchique adéquat et disposer des moyens et de l'indépendance nécessaires à l'exercice des missions lui confiées.

Le responsable de la prévention du blanchiment des capitaux et financement du terrorisme et la partie du personnel concerné doivent avoir accès à l'ensemble des informations jugées nécessaires pour l'exercice des missions qui leur sont confiées. Leur mission doit être formalisée.

Article 7 : Formation du personnel

Tout intermédiaire du marché est obligé de mettre en place un programme de formation continue du personnel pour lui permettre de détecter les opérations et agissements susceptibles d'être liés au blanchiment des capitaux ou financement du terrorisme et les instruire sur les procédures à suivre dans de cas pareils.

Le calendrier et le contenu des formations destinées aux différents secteurs du personnel doivent être adaptés par chaque intermédiaire de marché à ses propres besoins.

Les points suivants doivent être pris en compte en ce qui concerne la fréquence et le contenu des formations :

1. une compréhension générale de la réglementation relative au blanchiment des capitaux et financement du terrorisme et de la nécessité ultérieure de signaler toute transaction suspecte au responsable des déclarations de blanchiment de capitaux doit être dispensée à tous les nouveaux employés susceptibles d'être en contact avec des clients ou leurs transactions, de préférence dès le premier mois de leur embauche. Ils doivent être sensibilisés à l'importance accordée à la déclaration des soupçons par l'intermédiaire de marché, à l'obligation légale de déclaration et à l'obligation personnelle ;
2. les membres du personnel en contact direct avec le public sont les premiers points de contact avec les personnes potentiellement impliquées dans le blanchiment de capitaux ou financement du terrorisme et leurs efforts sont donc essentiels au système de déclaration des transactions par l'intermédiaire de marché. Une formation doit être dispensée sur les facteurs susceptibles

AB

d'éveiller des soupçons et sur les procédures à adopter lorsqu'une transaction est jugée suspecte ;

3. une formation complémentaire doit être dispensée sur la nécessité de vérifier l'identité des clients et de l'évaluation des risques des clients propres à l'entreprise. Ils doivent également être familiarisés avec les procédures de déclaration des transactions suspectes de l'entreprise ;
4. une formation plus poussée couvrant tous les aspects des procédures de lutte contre le blanchiment de capitaux devrait être dispensée aux personnes chargées de superviser ou de gérer le personnel. Cela comprendra les infractions et sanctions en cas de non-déclaration et d'assistance aux personnes impliquées dans le blanchiment de capitaux et financement du terrorisme, les procédures relatives à la signification des injonctions de produire et de bloquer, les procédures de signalement interne et les exigences de vérification d'identité, de conservation des documents et de divulgation des déclarations d'opérations suspectes ;
5. le responsable du signalement des infractions de blanchiment de capitaux doit suivre une formation approfondie couvrant tous les aspects de la législation et des politiques internes. De plus, il doit bénéficier d'une formation initiale et continue approfondie sur la validation, l'enquête et le signalement des transactions suspectes, ainsi que sur les mécanismes de retour d'information et les nouvelles tendances et schémas d'activité criminelle.

De plus, toute personne agréée ou autorisée est tenue de dispenser à tout le personnel chargé d'exécuter les différentes opérations une formation sur l'identification des clients, l'appréciation générale de la détection du blanchiment des capitaux ou de financement du terrorisme, la conservation des dossiers relatifs aux opérations suspectes et sur la déclaration obligatoire de toute opération suspecte au moins une (1) fois par an.

CHAPITRE III. DE L'IDENTIFICATION DES CLIENTS

Article 8 : Obligation d'identification des clients

Toute entité agréée pour opérer sur le marché des capitaux du Burundi est tenue de procéder préalablement à l'identification de ses clients aussi bien habituels que potentiels et le cas échéant, l'identité et les pouvoirs des personnes agissant pour son compte ou de ceux des ayants-droits économiques, sur base de documents, sources, données, ou de renseignement indépendants et fiables. Des règles et procédures y relatives doivent être mise en place et communiquées aux employés concernés.

L'identification des clients entraîne, pour tout intermédiaire de marché, l'obligation de :

1. connaître, de façon permanente, l'identité de ses clients à l'aide des documents, données, informations de source fiable et indépendante afin de détecter les opérations anormales ou suspectes ;

2. découvrir le bénéficiaire effectif du compte ouvert et prendre les mesures nécessaires pour vérifier son identité ;
3. effectuer un contrôle renforcé dans le cadre des personnes politiquement exposées ;
4. renforcer les mesures de vigilance normales dans une situation de relation d'affaires avec les acteurs du marché des capitaux étrangers ;
5. en cas de relation d'affaires avec les entités ou personnes, vérifier qu'elles ne sont pas impliquées dans le blanchiment des capitaux et/ou le financement du terrorisme ou qu'elles ne figurent pas sur la liste de celles qui sont sanctionnées, publiée par les Nations Unies.

Les vérifications ci-dessus doivent être effectuées au début et pendant la relation d'affaires.

Il est interdit à tout intermédiaire de tenir de comptes anonymes ou de comptes sous des noms fictifs pour ses clients.

Article 9 : Procédure d'identification des clients

En tant qu'une étape importante dans la prévention du blanchiment des capitaux et /ou le financement du terrorisme, l'identification des clients se fait comme suit :

1. la collecte des informations de base : Ces informations varient selon qu'il s'agit d'une personne morale ou d'une personne physique ;
 - i. Pour les personnes physiques : Nom et prénom, date et lieu de naissance, sexe, nationalité, adresse physique complète, numéro de téléphone et e- mail, profession/employeur/source de revenu, photo, pays d'origine ou de résidence ; pièce d'identité (Carte Nationale d'Identité ou passeport) et tout autre information jugée nécessaire ;
 - ii. Pour les personnes morales : Dénomination sociale, forme juridique, objet social, numéro du Registre de Commerce (RC), Numéro d'Identification Fiscal (NIF), adresse du siège social, statuts et actes constitutifs, liste des dirigeants, liste des bénéficiaires effectifs, activité principale et source des fonds ;
2. la vérification des documents : L'intermédiaire de marché doit vérifier les documents fournis afin de savoir qu'ils sont fiables et authentiques et qu'il y a conformité entre les informations figurant sur les documents et celles énoncées au point a) du présent article.
3. détermination du bénéficiaire effectif : Toute entité exerçant les activités sur le marché des capitaux du Burundi doit déterminer toute personne qui exerce un contrôle effectif sur la société ou les décisions importantes (même sans être actionnaire direct) et les actionnaires détenant au moins vingt-cinq pour cent (25 %) du capital ou des droits de vote d'une société. Elle doit identifier les vraies personnes derrière une société ou une

46

transaction et ce, pour lutter contre le blanchiment des capitaux et le financement du terrorisme ;

4. évaluation du profil de risque : Elle consiste en l'analyse du niveau de risque qu'un client ou une opération peut représenter, notamment en matière de blanchiment des capitaux ou de financement du terrorisme. Elle permet de déterminer si un client doit faire l'objet d'un suivi normal, d'une diligence renforcée, ou d'une diligence simplifiée.

Pour évaluer le profil risque du client, les intermédiaires de marché doivent se baser sur les critères suivants :

- i. l'identité et statut du client : Ils doivent vérifier si le client est une Personne Politiquement Exposée (PPE) ainsi que son casier judiciaire ou sa réputation ;
 - ii. le pays d'origine ou de résidence : S'il s'agit d'un pays à haut risque (sanctionnés, non coopérants, conflits...) ;
 - iii. la nature de l'activité professionnelle ou économique : Les activités qu'exercent les clients sont des activités fortement exposées aux flux financiers ou en espèces ;
 - iv. les produits ou services demandés : Titres très liquides, instruments complexes, comptes à l'étranger, etc. ;
 - v. le volume et la fréquence des opérations : Les montants investis, le volume des opérations, les opérations inhabituelles ou non justifiées ;
 - vi. la présence de signes de blanchiment de capitaux ou financement du terrorisme.
5. la conservation des documents : toute entité exerçant les activités sur le marché des capitaux doit conserver pendant dix (10) ans les documents d'identification des clients et ceux de relations d'affaires avec ses clients. Elle doit les mettre à jour en cas de survenance de changements des informations des clients ou en cas de besoin. Elle doit veiller à ce que :
 - i. toutes les exigences légales relatives aux registres et à la documentation soient respectées ;
 - ii. tous les registres des clients, des relations d'affaires et des transactions restent à jour, pertinents et accessibles ;
 - iii. toute transaction effectuée par l'intermédiaire de marché puisse être reconstituée afin de fournir, si nécessaire, des preuves pour des poursuites pénales ; et
 - iv. les dossiers peuvent être consultés et partagés dans un délai raisonnable ou dans le délai imposé par la loi, lorsqu'une enquête ou une ordonnance est émise par l'Autorité, la CNRF ou toute autre autorité compétente chargée de l'application de la loi relative à la LBC/FT.

Article 10 : Eléments d'identification

Lors de l'identification des clients, toute personne agréée ou autorisée doit prendre en compte les éléments suivants :

1. informations d'identité « KYC » pour les clients personnes physiques ou morales ;
2. les objectifs d'investissement des clients ;
3. la détermination du bénéficiaire effectif ;
4. l'évaluation du profil de risque ;
5. la vérification des documents ;
6. la surveillance et suivi continu des clients.

Les détails sur l'identification des clients sont repris à l'annexe I du présent Règlement.

Article 11 : Identification lors des opérations effectuées pour le compte d'autrui

Dans les cas où un mandataire ouvre un compte pour le compte d'une autre personne dont l'identité n'a pas été préalablement identifiée par l'intermédiaire de marché, l'identité de ce mandataire ou de toute autre personne qui aura le contrôle du compte doit être vérifiée. L'intermédiaire doit, par tous les moyens, se renseigner sur l'identité de la personne pour qui le mandataire agit.

Après vérification, si des doutes persistent sur le mandant ou l'ayant-droit économique, l'intermédiaire de marché doit mettre fin à la relation d'affaires et procéder, dans les conditions prévues par la loi relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme, à la déclaration de soupçon à la CNRF.

Les comptes fiduciaires, ceux de mandataire et de tiers sont des instruments privilégiés par les criminels souhaitant échapper aux procédures d'identification et masquer l'origine des fonds issus d'activités criminelles qu'ils souhaitent blanchir. De ce fait, Une prudence particulière est de mise lorsque les comptes sont ouverts dans des lieux soumis à des règles strictes de secret bancaire ou de confidentialité. Lorsque l'intermédiaire de marché n'a pas préalablement vérifié l'identité d'un fiduciaire ou n'entretient aucune relation avec un fiduciaire, la vérification de l'identité du fiduciaire, ou lorsqu'il existe plusieurs fiduciaires, de l'identité de tous les fiduciaires, doit être effectuée conformément aux procédures normales définies dans la réglementation sur la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Dans le cas de sociétés de personnes, de fonds communs de placement et d'autres entreprises non constituées en sociétés dont les associés n'ont pas été préalablement vérifiés par l'intermédiaire de marché, l'identité de tous les associés et signataires du compte doit être vérifiée. De plus, le contrat de société, l'acte de fiducie ou tout autre document pertinent doit être obtenu. Lorsqu'un accord formel de société existe, un mandat de la société autorisant l'ouverture d'un compte et conférant l'autorité à ceux qui le géreront doit être obtenu.

Le gestionnaire de fiducie ou tout mandataire est tenu de divulguer son statut lors de l'établissement d'une relation d'affaire ou de l'exécution d'une transaction/opération d'un montant égal ou supérieur à un montant fixé par la réglementation en vigueur ou d'un montant équivalent en monnaie étrangère.

Article 12 : Identification des clients lors des opérations effectuées à distance

Toute personne agréée ou autorisée offrant la possibilité à ses clients de faire des opérations à distance doit mettre en place des mesures adaptées garantissant l'identification de la clientèle. Il doit établir des politiques et des procédures pour gérer les risques spécifiques liés à l'utilisation des nouvelles technologies et aux relations ou transactions à distance. Ces politiques et procédures doivent être documentées et facilement accessibles aux employés de l'intermédiaire de marché.

Lors de la vérification des transactions à distance, l'intermédiaire de marché doit adopter des procédures plus rigoureuses que celles prévues pour la vérification en face à face afin de confirmer l'identité du client et de prévoir des mesures raisonnables pour éviter les demandes fictives uniques ou multiples, les substitutions (usurpation d'identité) ou les fraudes à des fins de blanchiment de capitaux.

Les procédures adoptées doivent garantir que :

1. une personne portant le nom du client existe et réside à l'adresse indiquée ; et
2. le client est bien cette personne.

Toute personne agréée ou autorisée doit prendre une ou plusieurs des mesures suivantes pour atténuer le risque accru lié à l'impossibilité d'établir un contact en personne lors de l'établissement de relations commerciales :

1. contacter le client par téléphone à un numéro résidentiel ou professionnel vérifiable de manière indépendante ;
2. confirmation de l'adresse du client par un échange de correspondance ou par tout autre moyen approprié ;
3. sous réserve du consentement du client, confirmation téléphonique de sa situation professionnelle auprès du service du personnel de son employeur, au numéro d'entreprise indiqué ;
4. confirmation du salaire du client ou de toute autre source de revenus en exigeant la présentation de relevés bancaires récents ;
5. authentification des documents présentés, demande des documents supplémentaires et vérification indépendante de la situation des clients par un tiers de réputation confirmée
6. certification des pièces d'identité par des magistrats, des commissaires à l'assermentation ou des notaires présentés par le client ; ou
7. tout autre moyen de vérification fiable adopté par l'intermédiaire de marché pour les relations d'affaires à distance.

Un intermédiaire de marché peut utiliser les éléments suivants comme moyens de vérification :

1. une facture de services publics récente, un numéro d'identification fiscal, une référence bancaire ; ou
2. un système informatisé, pour des vérifications internes ou externes des bases de données des applications, afin de détecter toute incohérence dans les informations fournies.

Article 13 : Recours aux tiers pour l'identification des clients

Toute personne agréée ou autorisée peut recourir à des tiers (les ambassadeurs, les employeurs, des personnes de confiance, l'OBR, la Banque, Services fonciers et cadastre national...) pour l'identification de ses clients. Ces derniers doivent transmettre ces informations dans un délai raisonnable et, en tout état de cause, avant les opérations ou les relations d'affaires.

Article 14 : Enregistrement et conservation des documents

Conformément aux dispositions de la loi relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme, tout intermédiaire du marché doit tenir et conserver les documents qui ont servi à l'identification des clients pendant une période de dix (10) ans au moins après la fin des relations d'affaires.

Tous ces documents ci-haut mentionnés doivent être conservés sous forme physique et électronique afin de constituer l'historique des transactions et les preuves en cas d'éventuelles poursuites pénales.

L'intermédiaire doit veiller à ce que :

1. toutes les exigences légales relatives aux registres et à la documentation soient respectées ;
2. tous les registres des clients, des relations d'affaires et des transactions restent à jour, pertinents et accessibles ;
3. toute transaction effectuée par l'intermédiaire de marché puisse être reconstituée afin de fournir, si nécessaire, des preuves pour des poursuites pénales ; et
4. les dossiers peuvent être consultés et partagés dans un délai raisonnable ou dans le délai imposé par la loi, lorsqu'une enquête ou une ordonnance est émise par l'Autorité, la CNRF ou toute autre autorité compétente chargée de l'application de la loi relative à la LBC/FT.

Toute personne agréée ou autorisée doit procéder à des examens périodiques ou ponctuels des dossiers des clients existants.

Toute personne agréée ou autorisée doit conserver les documents et dossiers relatifs à une affaire faisant l'objet d'une enquête ou ayant fait l'objet d'une enquête de la CNRF, de l'Autorité ou de toute autre autorité compétente pendant la période plus longue nécessaire conformément à toute demande ou ordonnance de l'Autorité, de la CNRF ou d'autres autorités compétentes.

Toute personne agréée ou autorisée doit conserver les enregistrements de toutes les transactions pendant une période minimale de dix (10) ans à compter de la date de conclusion de l'opération ou de la transaction concernée ou de la résiliation d'un compte ou d'une relation d'affaires. La conservation peut se faire sous forme de documents originaux, stockés sur disque dur ou sous toute autre forme électronique.

CHAPITRE IV. DE LA SURVEILLANCE ET DETECTIONS DES TRANSACTIONS INHABITUELLES

Article 15 : Surveillance et détection des transactions inhabituelles

Toute personne agréée ou autorisée doit disposer de systèmes et de mécanismes de surveillance conçus pour détecter les activités et/ou transactions susceptibles de résulter d'une manipulation de marché (les ventes fictives, les opérations de dumping ou les délits d'initiés, etc.) qui constituent des infractions sous-jacentes au blanchiment d'argent et financement du terrorisme. Sur ce, il doit élaborer et mettre en œuvre des contrôles internes et d'autres procédures visant à dissuader les criminels d'utiliser ses installations à des fins de blanchiment de capitaux et de financement du terrorisme, et à garantir que les activités sont menées conformément à la loi et à des normes éthiques élevées, et que le service n'est pas fourni lorsqu'il existe de bonnes raisons de supposer que les transactions sont associées à des activités de blanchiment de capitaux ou de financement du terrorisme.

La typologie des opérations suspectes et la description des mécanismes de détection des opérations suspectes sont prévues aux annexe II et III du présent Règlement.

Article 16 : Traçabilité des opérations

Toute personne agréée ou autorisée doit enregistrer et conserver toutes les informations permettant de suivre le cheminement complet d'une opération et ce, depuis l'ordre initial jusqu'à son exécution, afin de garantir la transparence, la conformité et la détection des risques de LBC/FT. Pour tracer les opérations, toute personne agréée ou autorisée doit prendre en compte les éléments suivants :

1. enregistrement de l'identité du client (KYC) : Données d'identification, Profil de risque, Documents justificatifs (Carte Nationale d'Identité, statuts, justificatifs de revenus, etc.) ;
2. journalisation des ordres : Détermination de la date, heure et nature de chaque ordre (achat/vente de titres, souscription, etc.), le montant et instrument financier concerné, le canal utilisé (en ligne, agence, mandataire...) ;
3. données de l'exécution : La date d'exécution de l'opération, la contrepartie (acheteur/vendeur) et le prix et les modalités de règlement ;
4. archivage sécurisé : Les données et pièces doivent être conservés pendant au moins dix (10) ans et l'accès doit être réservé aux personnes autorisées ;
5. outils numériques/technologiques adaptés : L'utilisation de systèmes de gestion intégrés (ERP, plateformes boursières, logiciels de conformité et la traçabilité automatisée des mouvements de fonds et titres).

Article 17 : Transparence dans les opérations financières

Pour garantir la transparence dans les opérations, Toute personne agréée ou autorisée est tenu de :

1. communiquer clairement et régulièrement aux investisseurs sur les risques, les frais, caractéristiques des produits et services financiers, etc. ;
2. identifier rigoureusement chaque client ;
3. vérifier l'origine des fonds ;
4. déclaration du bénéficiaire effectif réel ;
5. tenir un registre des opérations afin de garantir la traçabilité complète des ordres et transactions ;
6. la conservation des données et documents pendant dix (10) ans ;
7. établir des rapports à transmettre à l'Autorité et à la CNRF en cas de besoin.

Article 18 : Conformité aux normes internationales

Toute personne agréée ou autorisée est tenue de se conformer aux normes internationales en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme (les normes du GAFI, etc.). Il est tenu de prendre en considération les conventions internationales relatives à la LBC/FT ratifiées par le Burundi ainsi que les traités, résolutions, recommandations, et directives en la matière.

Tout intermédiaire du marché doit :

1. tenir informer des différentes résolutions adoptées par le Conseil de Sécurité des Nations Unies (CSNU) sur les mesures de lutte contre le terrorisme et toute autre résolution pertinente exigeant des sanctions contre les personnes et entités appartenant ou liées aux Talibans et à l'organisation Al-Qaïda, etc. ;
2. tenir une base de données contenant les noms et coordonnées des personnes inscrites sur la Liste récapitulative des Nations Unies et sur les listes qui pourraient être publiées en vertu du Règlement de 2013 relatif à la prévention du terrorisme ou la liste nationale établie par le Comité consultatif de lutte contre le financement du terrorisme ;
3. s'assurer que les informations contenues dans la base de données sont à jour et pertinentes, et facilement accessibles à leurs employés au siège social, dans leurs succursales ou filiales ;
4. vérifier régulièrement les noms des nouveaux clients, ainsi que ceux des clients existants et potentiels, par rapport aux noms figurant dans la base de données, dès réception de la liste des désignations ou des sanctions de l'Autorité de Régulation du marché des capitaux. En cas de correspondance, les intermédiaires de marché prennent des mesures raisonnables et appropriées pour vérifier et confirmer l'identité de leurs clients.

Une fois la confirmation obtenue, les intermédiaires de marché ont l'obligation d'(e) :

- i. geler immédiatement les fonds du client ou bloquent la transaction, le cas échéant, s'il s'agit d'un client existant, sans délai et sans préavis à l'entité ;
- ii. dans les vingt-quatre (24) heures suivant la détection et le gel des fonds, déposer une déclaration d'opération suspecte auprès de la CNRF ;
- iii. rejeter le client potentiel si la transaction n'a pas encore commencé ; et
- iv. informer l'Autorité et les autres organismes compétents.

40

5. soumettre une déclaration d'opération suspecte en cas de tentative d'opération par l'une des personnes figurant sur la liste consolidée ou sur les listes publiées par les autorités compétentes en vertu des textes légaux relatifs à la prévention du terrorisme et répression du terrorisme ;
6. vérifier les correspondances potentielles avec la liste consolidée afin de confirmer leur exactitude et d'éliminer les faux positifs. Ils doivent s'enquérir auprès du client ou, le cas échéant, de la contrepartie afin de déterminer si la correspondance est exacte ;
7. consolider leur base de données avec les autres listes reconnues de personnes ou d'entités désignées, publiées par d'autres juridictions.

CHAPITRE V. DE L'EVALUATION DES RISQUES ET DE LA DECLARATION

Article 19 : Obligation d'évaluer les risques

Toute personne agréée ou autorisée est tenue de prendre des mesures appropriées pour identifier, évaluer et comprendre les risques de blanchiment de capitaux et financement du terrorisme pour les clients, les pays ou les zones géographiques et les produits, services et/ ou transactions.

Il est tenu également d'examiner tous les facteurs de risque pertinents avant de déterminer le niveau de risque global et le type d'atténuation à appliquer. Il doit éviter de faire une approche cloisonnée lors de l'évaluation de la relation entre les risques.

En cas d'évaluation, lorsque les clients sont considérés comme présentant un risque élevé de blanchiment de capitaux ou de financement du terrorisme, toute personne agréée ou autorisée doit prendre des mesures renforcées pour gérer et atténuer ces risques et lorsque les risques sont moindres, des mesures simplifiées peuvent être appliquées (la réduction de la fréquence des mises à jour d'identification des clients ou la réduction du degré de surveillance et d'examen continu des transactions, sur la base d'un seuil monétaire raisonnable).

Article 20 : Facteurs d'évaluation des risques

Toute personne agréée ou autorisée peut évaluer les risques de blanchiment de capitaux et/ou de financement de terrorisme de ses clients individuels en leur attribuant une note de risque de blanchiment de capitaux et/ou de financement du terrorisme. Pour ce faire, il doit prendre en compte les facteurs suivants :

1. la nature, l'ampleur et la complexité des opérations ;
2. les produits et les services de l'intermédiaire de marché ;
3. les personnes à qui, les produits et les services sont fournis et la manière dont ils sont fournis ;
4. la nature, l'échelle, la complexité et la localisation des activités du client ;

5. le recours à des tiers pour rassembler des informations afin de prendre des mesures appropriées à l'égard de la clientèle.

En cas d'évaluation des risques pays, on doit prendre en compte les facteurs suivants :

1. les clients résidant ou ayant des liens avec des juridictions à haut risque notamment :
 - i. celles identifiées par le Groupe d'action financière comme présentant des lacunes stratégiques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ;
 - ii. les pays soumis à des sanctions, embargos ou mesures similaires édictés par les Nations Unies ;
 - iii. les pays vulnérables à la corruption ; ou les pays soupçonnés d'entretenir des liens étroits avec des activités terroristes.
2. les données disponibles auprès des Nations Unies, du Fonds Monétaire International, de la Banque Mondiale et du Groupe d'Action Financière (GAFI), entre autres, ainsi que l'expérience de l'intermédiaire de marché ou celle d'autres entités du groupe, lorsque l'intermédiaire de marché fait partie d'un groupe multinational, peuvent être prises en compte, ce qui peut révéler des faiblesses dans d'autres juridictions.

Pour des clients susceptibles d'être considérés comme présentant un risque de blanchiment de capitaux plus faible, on peut prendre en compte les cas :

1. des clients salariés ou disposant d'une source de revenus régulière provenant d'une source légitime connue soutenant l'activité entreprise ;
2. la réputation positive du client : une entreprise publique ou privée réputée et bénéficiant d'une longue histoire et bien documentée par des sources indépendantes, y compris des informations concernant sa propriété et son contrôle.

Certains clients, de par leur nature ou leur comportement, peuvent présenter un risque accru de blanchiment d'argent ; l'intermédiaire du marché doit prendre en compte les facteurs suivants pour expliquer ce risque :

1. une personne politiquement exposée, ou le profil public du client indiquant une implication ou un lien avec des personnes politiquement exposées ;
2. la complexité de la relation, notamment le recours à des structures d'entreprise, à des fiducies et à des comptes nominatifs en l'absence de justification commerciale légitime ;
3. une demande d'utilisation de comptes numérotés ou un niveau de confidentialité excessif pour une transaction ;
4. l'implication dans des activités à forte intensité de liquidités ;
5. la nature, la portée et la localisation des activités commerciales générant les fonds ou les actifs, compte tenu des activités sensibles ou à haut risque ;
6. lorsque l'origine du patrimoine ne peut être facilement vérifiée, ou ;
7. les acteurs de détail qui ont tendance à être exposés à un risque de blanchiment de capitaux plus élevé que les clients de gros qui ont généralement un Statut réglementaire et activité établie.

Article 21 : Evaluation des nouveaux produits ou nouvelle technologie

Avant le lancement d'un nouveau produit ou l'utilisation d'une nouvelle technologie, Toute personne agréée ou autorisée doit identifier et évaluer les risques de blanchiment des capitaux et financement du terrorisme qui peuvent survenir en relation avec ces nouveaux produits ou nouvelles technologies et doit prendre les mesures appropriées pour gérer et atténuer ces risques.

Article 22 : Mesures d'atténuation des risques

Toute personne agréée ou autorisée doit :

1. mettre en place des mesures, des contrôles et procédures pour atténuer et gérer efficacement les risques de blanchiment de capitaux et de financement du terrorisme. Il doit surveiller leur mise en place, réviser régulièrement, mettre à jour et si nécessaire, les améliorer ;
2. tenir un registre indiquant les mesures, contrôles et procédures ci-haut mentionnés, toutes les modifications y apportées suite à l'examen et la mise à jour requis ainsi que les dispositions de leur communication prises.

Pour atténuer le risque accru lié à l'impossibilité d'établir un contact en personne lors de l'établissement de relations commerciales, toute personne agréée ou autorisée doit prendre une ou plusieurs des mesures prévues à l'article 12 du présent Règlement

Les mesures, contrôles et procédures adoptés doivent être proportionnés à la taille et à la nature de l'activité d'un intermédiaire de marché.

Article 23 : Mesures de vigilance

L'intermédiaire de marché doit mettre en œuvre les mesures de vigilance à l'égard de la clientèle appropriées à ses clients existants, compte tenu de sa propre évaluation de l'importance relative et des risques.

Toute personne agréée ou autorisée est tenue de mettre en œuvre des mesures de vigilance à l'égard de la clientèle qui est en relation d'affaire avec ce dernier et ce, en tenant compte du résultat d'évaluation des risques. Ces mesures de vigilances doivent être simplifiées en cas de risques moindres et en cas de suspicion de blanchiment de capitaux ou de financement du terrorisme, des mesures de vigilances renforcées doivent être prises.

Tout gestionnaire d'un organisme de placement collectif doit mettre en œuvre des mesures de vigilance à l'égard de la clientèle lorsque des porteurs de parts souscrivent ou participent à l'OPC ou lorsqu'il entame des négociations avec une entité en vue de la signature d'un acte de fiducie en vue de sa création.

Lorsqu'un client est identifié comme « à haut risque », l'intermédiaire de marché doit mettre en œuvre des procédures de EDD concernant ce client, notamment :

1. s'enquérir de l'objet de l'ouverture d'un compte, du niveau et de la nature des activités de négociation envisagées ; des bénéficiaires effectifs et de l'origine des fonds ;
2. obtenir l'approbation de la direction générale pour l'ouverture d'un compte ; et assurer un suivi continu renforcé de la relation d'affaires.

La EDD doit également être mise en œuvre lorsque :

1. une transaction significative est effectuée, compte tenu du mode de fonctionnement habituel du compte ;
2. une modification substantielle des normes de documentation client de l'intermédiaire de marché ;
3. une modification substantielle de la manière dont les relations commerciales avec le client sont menées ;
4. l'intermédiaire de marché prend conscience qu'il pourrait manquer d'informations d'identification adéquates sur un client ; et
5. l'intermédiaire de marché prend connaissance d'un éventuel changement de propriété ou de constitution du client ou de la personne autorisée à agir en son nom dans le cadre de ses relations commerciales avec lui.

Article 24 : Surveillance continue

Toute personne agréée ou autorisée doit surveiller en permanence ses relations d'affaires avec ses clients, observer la gestion du compte du client et examiner attentivement les transactions effectuées afin de s'assurer qu'elles sont cohérentes avec les informations qu'il détient du client, de son activité, de son profil de risque et, le cas échéant, de l'origine des fonds.

Il doit vérifier périodiquement l'adéquation des informations d'identification du client et veiller à leur mise à jour, notamment pour les clients à haut risque.

L'étendue de la surveillance doit être liée au profil de risque du client, déterminé lors de l'évaluation des risques et pour une efficacité optimale, les ressources doivent être ciblées sur les relations d'affaires présentant un risque élevé de blanchiment d'argent.

Pour des relations d'affaires présentant un risque plus élevé et celles à haut risque et impliquant des personnes politiquement exposées ou des clients non en face à face, les intermédiaires de marché doivent prendre des mesures supplémentaires et réaliser des surveillances plus fréquentes et intensives, et ce, en prenant en compte les points pertinents suivants :

- a) la mise en place de procédures ou de systèmes d'information de gestion adéquats pour fournir au personnel concerné (par exemple, responsable de la conformité, responsable des signalements de blanchiment d'argent, personnel de première ligne, chargés de clientèle, personnel chargé des ouvertures de comptes et responsables des opérations) des informations en temps opportun, notamment, suite à la mise en place d'une EDD ou d'autres mesures supplémentaires, toute information sur les

comptes ou relations liés ; et les modalités de surveiller les sources de financement, de patrimoine et de revenus des clients à haut risque et comment tout changement de situation sera enregistré.

- b) la mise en place de politiques internes, conformité et formation : Toute personne agréée ou autorisée doit élaborer, adopter et mettre en œuvre des programmes, politiques, procédures et contrôles internes afin de prévenir et de détecter les cas de blanchiment de capitaux et de financement du terrorisme notamment :
 - i. l'établissement de procédures garantissant des normes élevées d'intégrité de ses employés ou des personnes agissant en leur nom ;
 - ii. des programmes de formation continue et des sessions de renforcement des capacités afin de garantir la bonne compréhension et la mise en œuvre des exigences de la Loi, des Règlements et des Lignes directrices relatifs à la LBC/FT ;
 - iii. une fonction de conformité en matière de LBC/FT, dirigée par le responsable des signalements de blanchiment d'argent ;
 - iv. une fonction d'audit indépendante chargée de vérifier le respect des exigences légales ;
 - v. un système de contrôle interne solide et fiable.
- c) élaboration des calendriers et contenus des formations destinées aux différents secteurs du personnel adaptés par chaque intermédiaire de marché à ses propres besoins et ce, conformément à l'article 7 du présent règlement
- d) l'intermédiaire de marché doit mettre en place des dispositifs appropriés de gestion de la conformité, comprenant au minimum la nomination d'un responsable du signalement des infractions de blanchiment d'argent.
- e) une fonction d'Audit : Un intermédiaire de marché doit maintenir une fonction d'audit indépendante et dotée de ressources suffisantes, capable d'évaluer régulièrement l'efficacité de ses politiques, procédures et contrôles internes, ainsi que sa conformité aux exigences réglementaires.
- f) une bourse de valeurs mobilières ou de produits dérivés doit disposer de systèmes et de mécanismes de surveillance conçus pour détecter les activités susceptibles de résulter d'une manipulation de marché, par exemple les ventes fictives, les opérations de dumping ou les délits d'initiés, qui constituent des infractions sous-jacentes au blanchiment d'argent.

Le personnel de surveillance d'une bourse de valeurs mobilières ou de produits dérivés, lorsqu'il constate une activité susceptible de constituer une manipulation de marché, un délit d'initié ou toute autre anomalie, doit alerter l'intermédiaire de marché impliqué dans cette transaction afin de vérifier si la transaction peut être qualifiée de suspecte, nécessitant ainsi une enquête plus approfondie.

Article 25 : Conservation des documents d'évaluation

Toute personne agréée ou autorisée doit conserver les registres et documents pertinents relatifs à l'évaluation des risques pendant au moins dix (10) ans à compter de leur date officielle de création ou d'émission, selon le cas, afin de pouvoir démontrer à la CNRF, à l'Autorité ou aux autres autorités compétentes sa manière

d'évaluer les risques de blanchiment de capitaux et de financement du terrorisme du client ainsi que l'étendue de la vigilance à l'égard de la clientèle et du suivi continu est appropriée au regard du risque de blanchiment de capitaux ou de financement du terrorisme du client.

Article 26 : Déclaration des soupçons

Toute personne agréée ou autorisée doit déclarer sans délai tout soupçon de blanchiment de capitaux ou financement du terrorisme lié à un client ou à toute opération effectuée à la CNRF.

Toute personne agréée ou autorisée doit signaler comme transactions suspectes les cas suivants :

1. transactions financières atypiques :

- i. achat ou vente de titres financiers avec des sommes très élevées sans justification économique.
- ii. achat/revente rapide d'actions sans logique ou perte volontaire
- iii. souscriptions massives en espèces ou via des comptes offshores
- iv. rachat ou transfert soudain de placement à perte
- v. multiples transactions fractionnées
- vi. transactions vers des zones à risque ou sous sanctions

2. comportement suspect du client :

- i. profil client incohérent
- ii. refus d'identification « KYC » (refus de fournir des pièces d'identité ou masque le bénéficiaire effectif)
- iii. refus de fournir des justificatifs de revenus
- iv. complication de compte ou d'opérations sans cohérence avec le profil déclaré
- v. utilisation de prête-noms, personnes morales opaques ou sociétés écrans

3. structures ou montages complexes :

- i. utilisation de fonds d'investissement, holding ou fiducies non justifiées
- ii. entrée ou sortie des fonds via des pays ou juridictions à risques

4. transactions répétitives ou fractionnées :

- i. transferts de montants proches des seuils de déclaration, fractionnés volontairement
- ii. multiples opérations dans une courte période, sans lien apparent
- iii. petites transactions fréquentes vers ou depuis des zones sensibles ou sous sanctions

5. des activités suspectes :

- i. collecte de fonds (dons, plateforme) sans traçabilité claire
- ii. investissement dans des produits financiers peu liquides, puis retraits rapides

6. origine de fonds douteuse : Fonds venant de pays sous sanctions ou paradis fiscaux

Si un intermédiaire de marché a eu connaissance d'activités ou de transactions suspectes indiquant de possibles activités de blanchiment de capitaux ou de financement du terrorisme, il doit les signaler à la CNRF immédiatement ou, en tout

état de cause, dans les sept (7) jours suivant la date de la transaction ou de l'activité considérée comme suspecte. Il doit :

1. divulguer suffisamment d'informations indiquant la nature et le motif du soupçon, et s'il dispose de pièces justificatives supplémentaires, celles-ci doivent également être mises à la disposition de la CNRF ;
2. mettre en place des mécanismes rigoureux de déclaration des transactions suspectes ;
3. conserver un enregistrement de toutes les transactions signalées à la CNRF, ainsi que de toutes les constatations et analyses internes les concernant.

CHAPITRES VI : DES SANCTIONS

Article 27 : Infractions et sanctions applicables

Au sens du présent Règlement, commet l'infraction toute personne qui viole l'une des dispositions du présent Règlement et est passible des sanctions.

Une liste des infractions et des sanctions applicables est annexée au présent règlement.

CHAPITRE V : DES DISPOSITIONS FINALES

Article 28 : Secret professionnel

Il est interdit à tout intermédiaire de marché, ses administrateurs, dirigeants et employés d'informer ou avertir les clients sur une transaction suspecte les concernant et déclarée à la CNRF.

Article 29 : Entrée en vigueur

Le présent Règlement entre en vigueur le jour de sa signature et publication sur le site de l'Autorité et dans le Bulletin officiel du Burundi. Un délai de six (6) mois, après l'entrée en vigueur du présent Règlement, est accordé à toute personne agréée ou autorisée pour mettre en place des systèmes et l'élaboration des différents documents ainsi que la formation du personnel afin d'observer les dispositions du présent règlement.

Fait à Bujumbura, le 23 / 02 / 2026

LE DIRECTEUR GENERAL DE L'AUTORITE DE REGULATION
DU MARCHE DES CAPITAUX DU BURUNDI



ANNEXE I

ELEMENTS D'IDENTIFICATION ET DE CONNAISSANCE DU CLIENT (KYC) (En vertu de l'article 10 du règlement n° 649/2002 relatif à la lutte contre le blanchiment des capitaux et le financement du terrorisme)

Partie I. Informations d'identité « KYC » des clients

I.. 1. Clients personnes physiques

Les informations d'identification à collecter comprennent obligatoirement mais pas exclusivement:

Types d'informations	Observation
Nom et prénom	
Date et lieu de naissance	
Nationalité	
Adresse de résidence principale	
Numéro et type de documents d'identification officielle	
Date de délivrance et autorité émettrice du document	
Situation principale	
Source principale des revenus	
Numéro de téléphone	
Adresse électronique	

I.. 2. Clients personnes morales

Les informations d'identification à collecter comprennent obligatoirement mais pas exclusivement :

Types d'informations	Observation
Dénomination sociale	
Forme juridique	
Nationalité	
Numéro d'immatriculation et registre de commerce	
Adresse du siège social et des établissements principaux	
Date de délivrance et autorité émettrice du document	
Objet social et nature des activités	
Source principale des revenus	
Numéro de téléphone	
Adresse électronique	

Identité des dirigeants, représentants légaux ou personne habilitée	
Structure de l'actionnariat	

Partie II. Objectifs et nature de la relation d'affaires

Avant l'entrée en relation, l'établissement identifie et documente les objectifs poursuivis par le client. Cette identification concerne obligatoirement les éléments suivants :

Objectif poursuivi	Observation
La finalité de la relation d'affaire	
Les objectifs d'investissement	
L'horizon d'investissement	
Le volume et la nature provisionnelle des opérations	
La tolérance au risque	
Les contraintes éventuelles	

Partie 3. Détermination du bénéficiaire effectif

Types de bénéficiaires	Observations
Personne détenant directement ou indirectement un pourcentage significatif du capital ou des droits de vote 8	
Personne exerçant un contrôle effectif sur le client ou la structure juridique	
Les bénéficiaires finaux des opérations ou des actifs	

Partie 4. Évaluation du profil de risque du client

Types de risques	Observations
Risque lié à l'identité du client	
Le risque géographique	
Le risque lié aux produits, services et canaux de distribution	
Le comportement transactionnel attendu	
La qualité des informations fournies	
La transparence des informations fournies	
Niveau du risque	Faible ☐ Modéré ☐ Elevé ☐

Partie 5. Vérification de la validité des documents

Types de documents	Observation
Pièces d'identités officielles en cours de validité	
Documents légaux et statuts pour les personnes morales	
Justificatifs de domiciles	
Documents attestant la source des fonds, le cas échéant	

Les documents sont conservés conformément aux exigences réglementaires en vigueur.

Partie 6. Surveillance et suivi continu des clients

Types	Observation
Cohérence des opérations avec le profil du client	
Détection de toute opération inhabituelle ou suspecte	
Mise à jour périodique des informations KYC	
Réévaluation du profil de risque en cas d'évaluation significative	

Toute opération suspecte fait l'objet d'une analyse approfondie et, le cas échéant, d'une déclaration aux autorités compétentes.

Partie 7. Conservation des données

Les informations et documents relatifs à l'identification, à la vérification et au suivi des clients sont conservés pendant une période de dix ans après la fin de la relation d'affaires, dans des conditions garantissant leur confidentialité et leur intégrité.

ANNEXE III: MÉCANISMES DE DÉTECTION DES OPÉRATIONS SUSPECTES SUR LE MARCHÉ DES CAPITAUX

1. Objet de l'annexe

La présente annexe a pour objet de définir les mécanismes et procédures que doivent mettre en place les acteurs du marché des capitaux agréés par l'Autorité de Régulation du Marché des Capitaux (ARMC) pour la détection des opérations suspectes de blanchiment de capitaux et de financement du terrorisme, conformément à la législation burundaise en vigueur et aux normes internationales applicables.

2. Principe de l'approche fondée sur les risques

Les acteurs du marché des capitaux appliquent une approche fondée sur les risques, tenant compte:

- de la nature des produits et services offerts ;
- du profil et de la catégorie des clients ;
- de la zone géographique d'activité et de provenance des fonds.

Les mesures de détection sont renforcées lorsque le niveau de risque est élevé.

3. Connaissance du client comme mécanisme central de détection

Les acteurs sont tenus de mettre en œuvre des mesures de vigilance à l'entrée en relation et tout au long de la relation d'affaires, notamment :

- a. l'identification et la vérification de l'identité du client et du bénéficiaire effectif ;
- b. la compréhension de l'activité professionnelle ou économique du client ;
- c. l'identification de l'origine des fonds investis sur le marché des capitaux burundais ;

Tout écart significatif entre le profil établi et les opérations réalisées constitue un indice d'opération suspecte.

4. Surveillance continue des opérations

Les acteurs assurent une surveillance continue des opérations effectuées par leurs clients, portant notamment sur :

- a. la fréquence et le volume des transactions ;
- b. la nature des instruments financiers utilisés ;
- c. la cohérence économique des opérations au regard de la situation financière du client.

Cette surveillance est adaptée à la taille, à la complexité et au niveau de risque de l'acteur concerné.

5. Indicateurs d'alerte propres au contexte burundais

Sans préjudice d'autres indicateurs définis par la CNRF ou l'Autorité, constituent notamment des signaux d'alerte :

a) Indicateurs liés au client

- refus ou retard injustifié à fournir les documents exigés par la réglementation burundaise ;
- informations incomplètes, contradictoires ou manifestement inexactes ;
- recours injustifié à des tiers ou mandataires pour effectuer des opérations.

b) Indicateurs liés aux opérations

- opérations d'un montant disproportionné par rapport aux revenus ou à l'activité déclarée du client ;
- mouvements fréquents d'achats et de ventes de titres sans logique économique apparente ;
- opérations impliquant des pays ou territoires identifiés comme présentant un risque élevé de BC/FT ;
- utilisation inhabituelle du marché des capitaux à des fins de simple transfert de fonds.

c) Indicateurs liés à l'origine des fonds

- origine des fonds non justifiée ou difficilement vérifiable ;
- utilisation de fonds provenant de comptes n'ayant pas de lien économique avec le client ;
- transferts répétés de fonds vers ou depuis l'étranger sans justification économique.

6. Examen renforcé des opérations inhabituelles

Lorsqu'une opération est identifiée comme inhabituelle, l'acteur concerné est tenu de :

- a. procéder à un examen approfondi de ladite opération ;
- b. recueillir, le cas échéant, des informations complémentaires auprès du client ;
- c. analyser la cohérence économique et financière de l'opération ;
- d. documenter l'ensemble du processus d'analyse.

Lorsque les soupçons persistent, l'opération est qualifiée de suspecte.

7. Déclaration des opérations suspectes

Toute opération suspecte doit être déclarée sans délai à la Cellule Nationale de Renseignements Financiers (CNRF), conformément à la législation burundaise relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

8. Désignation et rôle du responsable LBC/FT

Chaque acteur du marché des capitaux désigne un responsable LBC/FT chargé notamment de :

- a. superviser les mécanismes de détection ;
- b. centraliser et analyser les alertes internes ;
- c. assurer les déclarations à la CNRF ;
- d. servir de point focal avec l'ARMC et les autorités compétentes.

9. Conservation des documents

Les acteurs conservent, conformément aux délais prévus par la réglementation burundaise :

- a. les documents relatifs à l'identification des clients ;
- b. les informations sur les opérations effectuées ;
- c. les rapports internes d'analyse des opérations suspectes.

10. Formation et sensibilisation

Les acteurs mettent en place des programmes de formation continue à l'intention de leur personnel afin de :

- a. renforcer la capacité de détection des opérations suspectes ;
- b. tenir compte des typologies de BC/FT observées au Burundi et dans la sous-région.

11. Supervision et contrôle par l'ARMC

L'ARMC, en tant qu'autorité de régulation du marché des capitaux, exercera un contrôle régulier sur l'application des mécanismes de détection des opérations suspectes par les acteurs du marché, conformément à ses compétences légales et réglementaires.

ANNEXE II : TYPOLOGIE DES OPERATIONS SUSPECTES

1. Objet et portée de l'annexe

La présente annexe a pour objet de fournir aux intermédiaires de marché, aux entités assujetties et aux acteurs opérant sur le marché des capitaux du Burundi une typologie indicative et non exhaustive des opérations, comportements et schémas susceptibles de constituer des indices de blanchiment de capitaux et/ou de financement du terrorisme.

Cette typologie vise à faciliter :

- la détection précoce des opérations suspectes ;
- l'analyse et l'évaluation du risque LBC/FT ;
- la déclaration des soupçons à la Cellule Nationale de Renseignement Financier (CNRF).

La présence d'un ou plusieurs indicateurs ne signifie pas automatiquement qu'une infraction est constituée, mais impose un examen renforcé de l'opération ou de la relation d'affaires.

2. Typologie des opérations suspectes liées au profil et au comportement du client

2.1. Incohérences dans le profil du client

- Profil économique, professionnel ou financier incompatible avec le volume ou la nature des opérations effectuées ;
- Client sans activité connue ou avec une activité déclarée à faible revenu réalisant des investissements importants ;
- Modifications fréquentes et injustifiées des informations d'identification ou du bénéficiaire effectif ;
- Refus, retard ou réticence à fournir les documents requis dans le cadre du KYC ou de la diligence renforcée.

2.2. Comportements suspects

- Insistance inhabituelle sur la rapidité d'exécution des opérations sans justification économique ;
- Tentatives d'influence ou de pression sur le personnel pour éviter les contrôles internes ;
- Utilisation de prête-noms ou de représentants sans justification claire ;
- Désintérêt manifeste pour la performance financière ou le risque des investissements réalisés.

3. Typologie des opérations suspectes liées aux transactions financières

3.1. Transactions inhabituelles ou atypiques

- Achats ou ventes de titres pour des montants très élevés sans lien apparent avec la stratégie d'investissement du client ;
- Souscriptions ou investissements massifs suivis de rachats rapides, notamment à perte ;
- Transactions répétitives sans justification économique ou financière identifiable ;
- Opérations effectuées en dehors des pratiques normales du marché.

3.2. Fractionnement des opérations

- Fractionnement intentionnel des transactions afin d'éviter les seuils de déclaration ;
- Multiples opérations de montants proches du seuil réglementaire sur une courte période ;
- Utilisation de plusieurs comptes ou intermédiaires pour réaliser des opérations similaires.

4. Typologie des opérations suspectes liées à l'origine et à la destination des fonds

4.1. Origine douteuse des fonds

- Fonds provenant de juridictions à haut risque ou non coopératives identifiées par le GAFI ;
- Utilisation de comptes offshore ou de structures situées dans des paradis fiscaux sans justification économique ;
- Origine des fonds incompatible avec les revenus déclarés du client ;
- Recours excessif aux espèces ou aux instruments financiers anonymes.

4.2. Destination des fonds

- Transferts de fonds vers des zones géographiques sensibles, sous sanctions ou à risque terroriste ;
- Mouvements de fonds complexes sans justification économique claire ;
- Réinvestissements circulaires visant à dissimuler l'origine réelle des fonds.

5. Typologie des opérations suspectes liées aux instruments et produits du marché des capitaux

5.1. Utilisation abusive des instruments financiers

- Utilisation d'instruments financiers complexes sans compréhension apparente par le client ;
- Opérations fréquentes sur des titres peu liquides suivies de sorties rapides ;
- Manipulation de titres à faible capitalisation ou faible volume de transactions ;
- Opérations de type « aller-retour » sans objectif d'investissement.

5.2. Organismes de placement collectif et fonds d'investissement

- Souscriptions importantes suivies de rachats rapides et répétés ;
- Utilisation de fonds d'investissement comme intermédiaires pour masquer l'origine des fonds ;
- Entrées et sorties de fonds non cohérentes avec l'objet et la politique d'investissement du fonds.

6. Typologie des opérations suspectes liées aux structures juridiques et montages complexes

- Utilisation de sociétés écrans, holdings ou fiducies sans activité économique réelle ;
- Structures de détention opaques rendant difficile l'identification du bénéficiaire effectif ;
- Changements fréquents de structure juridique ou d'actionnariat sans justification légitime ;
- Relations d'affaires impliquant plusieurs intermédiaires dans différentes juridictions.

7. Typologie spécifique au financement du terrorisme

- Collecte ou transfert de fonds au profit d'organisations ou de personnes liées à des activités terroristes ;
- Transactions de faible montant mais répétées vers des zones à risque ;
- Utilisation d'organisations à but non lucratif ou de plateformes de collecte de fonds sans traçabilité claire ;
- Refus de fournir des informations sur l'objet réel des transferts ou investissements.

8. Obligations des intermédiaires de marché

Lorsqu'une opération ou un comportement correspond à une ou plusieurs typologies décrites ci-dessus, l'intermédiaire de marché est tenu de :

- procéder à un examen approfondi de l'opération ;
- documenter l'analyse et les conclusions ;
- appliquer, le cas échéant, des mesures de vigilance renforcées ;
- déclarer sans délai toute opération suspecte à la Cellule Nationale de Renseignement Financier (CNRF), conformément aux dispositions du Règlement sur la LCB/FT.

9. Caractère évolutif de la typologie

La présente typologie est évolutive. Elle peut être complétée ou mise à jour par l'Autorité de Régulation du Marché des Capitaux afin de tenir compte de l'évolution des techniques de blanchiment de capitaux, du financement du terrorisme et des pratiques du marché.

ANNEXE IV LES INFRACTIONS ET LES SANCTIONS APPLICABLES DANS LE CADRE DE LA LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX ET LE FINANCEMENT DU TERRORISME

I. Objet de l'annexe

La présente annexe a pour objet de définir les infractions administratives et disciplinaires liées au non-respect des obligations de lutte contre le blanchiment des capitaux et le financement du terrorisme (LBC/FT) par les acteurs opérant sur le marché des capitaux du Burundi, ainsi que les sanctions y afférentes, sans préjudice des sanctions pénales prévues par la législation en vigueur.

II. Catégories d'infractions

Constituent des infractions aux dispositions du présent règlement, notamment :

1. Infractions liées à l'identification et à la connaissance de la clientèle (KYC/CDD)

- Absence d'identification du client ou du bénéficiaire effectif ;
- Identification incomplète, inexacte ou non mise à jour ;
- Défaut d'application des mesures de vigilance renforcée à l'égard des personnes politiquement exposées (PPE) ;
- Ouverture ou maintien de relations d'affaires anonymes ou sous des identités fictives.

2. Infractions liées à la surveillance et à la détection des opérations suspectes

- Défaut de surveillance des opérations effectuées par les clients ;
- Absence de mécanisme de détection des transactions inhabituelles ;
- Non-examen ou examen insuffisant des opérations suspectes ;
- Fractionnement intentionnel des opérations pour contourner les seuils réglementaires.

3. Infractions liées à la déclaration des opérations suspectes

- Non-déclaration à la CNRF des opérations suspectes ou inhabituelles ;
- Déclaration tardive ou incomplète ;
- Communication d'informations fausses ou trompeuses ;
- Violation de l'obligation de confidentialité liée à la déclaration de soupçon.

4. Infractions liées à l'organisation interne et à la conformité

- Absence de politique interne LBC/FT ;
- Non-désignation d'un responsable chargé de la LBC/FT ;
- Insuffisance ou absence de formation du personnel ;
- Absence ou défaillance du dispositif de contrôle interne et de conformité ;
- Non-conservation des documents et données requis par la réglementation.

5. Infractions liées à l'entrave au contrôle et à la coopération

- Refus de communiquer les informations requises par l'Autorité ou la CNRF ;
- Obstruction aux missions de contrôle ou d'inspection ;
- Destruction, falsification ou dissimulation de documents.

III. Sanctions administratives applicables

Sans préjudice des poursuites pénales prévues par la loi, les infractions ci-dessus exposent leurs auteurs aux sanctions administratives suivantes, selon la gravité des manquements constatés :

1. Avertissement écrit ;
2. Blâme ;
3. Injonction de mise en conformité dans un délai déterminé ;
4. Sanction pécuniaire, dont le montant est fixé par l'Autorité conformément à la réglementation en vigueur ;
5. Suspension temporaire de l'agrément pour tout ou partie des activités ;
6. Retrait de l'agrément ou de l'autorisation d'exercer ;
7. Interdiction temporaire ou définitive d'exercer des fonctions de direction ou de responsabilité sur le marché des capitaux.

IV. Critères de détermination des sanctions

Pour déterminer la nature et le niveau des sanctions, l'Autorité tient notamment compte :

- de la gravité et de la durée de l'infraction ;
- du caractère intentionnel ou non du manquement ;
- du degré de coopération de l'entité concernée ;
- des avantages tirés de l'infraction ;
- des antécédents disciplinaires de l'entité ou de la personne concernée ;
- de l'impact du manquement sur l'intégrité et la réputation du marché des capitaux.

V. Responsabilité des dirigeants

Les dirigeants, administrateurs et responsables de conformité peuvent voir leur responsabilité personnelle engagée lorsque les infractions résultent d'une carence manifeste dans l'organisation, la supervision ou le contrôle interne des dispositifs LBC/FT.

VI. Articulation avec les sanctions pénales

Les sanctions prévues par la présente annexe s'appliquent sans préjudice des sanctions pénales prévues par la loi relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ainsi que par le Code pénal en vigueur.

VII. Publication des sanctions

L'Autorité peut décider de rendre publiques les sanctions prononcées, dans le respect des dispositions légales relatives à la protection des données et au secret professionnel, lorsque cette publication est jugée nécessaire à des fins dissuasives ou de protection du marché.