الجمهورية الجزائرية الديمقراطية الشعبية

Commission d'Organisation et de Surveillance des Opérations de Bourse – COSOB -

Cellule de Lutte Contre le Blanchiment des Capitaux le Financement du Terrorisme et le Financement de la Prolifération des Armes de Destruction Massive

لجنة تنظيم عمليات البورصة ومراقبتها

خلية مكافحة تبييض الأموال وتمويل الإرهاب

وتمويل انتشار أسلحة الدمار الشامل

LIGNES DIRECTRICES N° 02-2025 DU 27 MARS 2025

RELATIVES AUX MESURES DE VIGILENCE A PRENDRE VIS-A-VIS DES CLIENTS

V 1.0

COSOB – MARS 2025

Introduction :

Ces lignes directrices font partie d'une stratégie globale visant à renforcer la sensibilisation et l'orientation des assujettis soumis au contrôle de la Commission d'Organisation et de Surveillance des Opérations de Bourse « COSOB », dans le but d'assurer une conformité effective et durable aux procédures nécessaires de vigilance financière. Ces mesures sont étroitement liées à la prévention et la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive.

L'objectif de ces lignes directrices est de définir les mesures nécessaires pour mettre en œuvre les actions de vigilance appropriées à prendre, en pleine conformité avec les recommandations du groupe d'action financier (GAFI), en particulier les recommandations (10), (11), (16), (18), (19) et (34).

Le but principal de ces lignes directrices est d'assurer une mise en œuvre efficace de ces mesures, contribuant à renforcer la sécurité financière contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive au travers du système financier, conformément aux normes internationales des meilleures pratiques dans ce domaine.

I. Références légales et réglementaires

- Ordonnance n° 66-156 du 18 Safar 1386, correspondant au 8 juin 1966, portant code pénal, modifiée et complétée ;
- Loi n° 05-01 du 27 Dhou El Hidja 1425, correspondant au 6 février 2005, relative à la prévention et à la lutte contre le blanchiment de capitaux et le financement du terrorisme, modifiée et complétée ;
- Décret exécutif n° 25-101 du 12 Ramadhan 1446 correspondant au 12 mars 2025 relatif à la procédure de gel et/ou de saisie des fonds dans le cadre de la prévention et de la lutte contre le financement du terrorisme et le financement de la prolifération des armes de destruction massive
- Décret exécutif n° 23-429 du 15 Joumada El Oula 1445, correspondant au 29 novembre 2023, relatif au registre public des bénéficiaires effectifs des personnes morales de droit algérien ;
- Décret exécutif n° 25-102 du 12 Ramadhan 1446 correspondant au 12 mars 2025, fixant la composition, l'organisation et le fonctionnement du comité de suivi des sanctions internationales ciblées ;
- Décret exécutif n° 25-103 du 12 Ramadhan 1446 correspondant au 12 mars 2025 fixant les modalités d'inscription et de radiation de la liste nationale des personnes et entités terroristes et les effets qui en découlent ;
- Règlement COSOB n°24-01 du 11 Moharram 1446 correspondant au 17 juillet 2024 relatif à la prévention et à la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive ;
- Instruction COSOB n° 24-07 du 21 novembre 2024 portant mesures de vigilance à l'égard des clients dans le cadre de la prévention et de la lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive.

II- Définition : au sens de présente ligne directrice, on entend par :

Les assujettis : les intermédiaires en opérations de bourse, les teneurs de comptes conservateurs de titres, les organismes de placement collectif en valeurs mobilières, la bourse d'Alger, le dépositaire central (Algérie Clearing), les sociétés de capital investissement et les gérants de plates-formes de financement participatif (Crowd-Funding) ;

Client : la personne physique ou morale qui traite avec l'assujetti ;

Client occasionnel : Le client qui n'est pas lié à l'institution financière par une relation d'affaire continue.

Relation d'affaire : La relation qui s'établit entre le Client et toute institution financière, liée à toute activité.

Le bénéficiaire effectif : La ou les personnes physiques qui, in fine :

1. Détiennent ou contrôlent le client, l'agent du client ou le bénéficiaire des contrats d'assurance-vie ;
2. La personne physique pour laquelle une transaction est réalisée ou pour laquelle une relation d'affaire est conclue ;
3. Des personnes qui, ultimement, exercent un contrôle effectif sur la personne morale.

La Personne Politiquement Exposée : Tout Algérien, étranger, élu ou nommé, qui a exercé ou exerce en Algérie ou à l'étranger de hautes fonctions législatives, exécutives, administratives ou judiciaires, ainsi que les hauts responsables des partis politiques, et les personnes qui exercent ou ont exercé des fonctions importantes au sein ou pour le compte d'une organisation internationale.

Le Groupe financier : Un groupe constitué d'une société mère ou d'un autre type de personnes morales qui détiennent des actions majoritaires et coordonnent leurs fonctions avec le reste du groupe pour appliquer ou mettre en œuvre un contrôle sur le groupe en vertu des principes fondamentaux, conjointement avec les succursales et/ou les filiales soumises à des politiques et procédures de lutte contre le blanchiment d'argent et le financement du terrorisme au niveau du groupe.

Les assujettis doivent se conformer au devoir de vigilance et, à ce titre, ils doivent mettre en œuvre un programme écrit de prévention, de détection et de lutte contre le blanchiment d'argent, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Et prendre en compte la dimension commerciale et les risques associés au blanchiment d'argent et au financement du terrorisme, qui comprennent notamment :

- Les politiques,
- Les procédures,
- La contrôle interne.

III. Mesures de vigilance à prendre avant d'établir une relation d'affaires ou d'exécuter des transactions

A. Identification des clients et de leurs mandataires

- Vérification et confirmation : Les assujettis doivent vérifier l'identité du client à l'aide d'un ensemble de documents officiels fiables (tels que la carte d'identité nationale, le

passeport, les registres d'entreprises ou les licences commerciales). Elles doivent également vérifier l'identité des mandataires ou des représentants du client en utilisant des documents officiels, tels que des mandats légaux.

- Contrôle des mandataires : Les assujettis doivent vérifier rigoureusement les personnes prétendant agir pour le compte des clients à l'aide de moyens de vérification indépendants, comme les registres commerciaux ou la vérification des mandats légaux enregistrés.

B. Définir l'objet et la nature de la relation

- Analyse des données : Chaque dossier client doit comporter une analyse complète de l'objet de la relation (est-elle commerciale, d'investissement, ou financière ?) et des activités attendues. Par exemple, si un client demande des services financiers complexes, il faut enquêter sur l'objet de ce service et documenter les intentions financières.
- Analyse des activités futures : Il est nécessaire d'anticiper le type de transactions attendues dans le cadre de la relation (s'agit-il de transactions importantes ou périodiques ?).

C. Traitement des informations suspectes

- Vérification indépendante : En cas de doute sur la précision ou l'exhaustivité des informations fournies par le client, des investigations indépendantes doivent être menées à l'aide de moyens fiables, tels que les données bancaires, les informations actualisées des autorités financières, ou les audits effectués par des tiers.
- Mesures préventives : En cas de persistance des doutes après vérification, des mesures renforcées peuvent être prises, telles que la demande de documents supplémentaires ou même la suspension de la relation d'affaires jusqu'à clarification de la situation.

D. Vérification de la conformité des opérations avec des objectifs légitimes

- Consultation des listes de sanctions : Les assujettis doivent mettre en place des procédures pour vérifier que les clients ne figurent pas sur les listes de sanctions nationales ou internationales liées au blanchiment d'argent, au financement du terrorisme, ou à la prolifération des armes de destruction massive.
- Vérification périodique : Les noms figurant sur ces listes doivent être vérifiés régulièrement.

E. Mesures en cas de soupçon d'opérations illégales

- Suspension des opérations : En cas de doute concernant une opération liée au blanchiment d'argent, au financement du terrorisme ou à la prolifération des armes de destruction massive, l'entité soumise doit suspendre immédiatement l'opération et enquêter sur celle-ci.
- Signalement des soupçons : Un signalement de suspicion doit être envoyé à l'unité de traitement des informations financières et/ou aux autorités compétentes conformément aux lois locales.

F. Vérification continue des données

- Mise à jour régulière : Les assujettis doivent mettre à jour les informations des clients de manière régulière, en tenant compte des risques associés à chaque client.
- Fréquence de la mise à jour : La mise à jour doit être annuelle au minimum, mais peut être effectuée plus fréquemment si des changements importants surviennent dans les activités ou les risques associés au client.

IV. Mesures nécessaires pour identifier et vérifier l'identité du client

A. Mesures de base

- Collecte d'informations détaillées : Il est nécessaire de collecter toutes les informations requises du client (qu'il soit une personne physique ou morale) à l'aide d'un formulaire "Connaître son client" validé.

B. Rapports et documents

- Vérification de l'authenticité des documents : La vérification de l'authenticité des documents officiels fournis par le client doit être réalisée, en utilisant des technologies telles que l'analyse biométrique ou les outils de vérification numérique pour garantir l'exactitude des informations.

V. Collecte d'informations sur le client avant l'établissement de la relation

A. Analyse des informations avant la relation d'affaires

- Les assujettis doivent analyser toutes les données disponibles (comme les informations sur l'activité commerciale, la situation financière du client, les sources de fonds) et s'assurer qu'elles sont conformes aux normes légales.
- Les clients doivent être classés en fonction du niveau de risque associé à leur profil (faible, moyen, élevé) avant d'établir une relation d'affaires.

B. Dossier de connaissance du client

- Un dossier complet doit être constitué pour chaque client, indiquant ses informations personnelles ou juridiques, l'objet et la nature de la relation, ainsi que le niveau de risque associé.

VI. Mesures de vigilance pour les relations d'affaires à distance

A. Vérification des informations à distance

- **Utilisation de technologies avancées :** L'utilisation de la vérification par vidéo, d'entretiens numériques ou d'outils de vérification biométrique est essentielle pour garantir l'exactitude de l'identité du client.
- **Analyse des données fournies :** Il est nécessaire de comparer les données fournies par le client avec celles disponibles dans les bases de données publiques ou privées.

B. Entretiens et examens

- **Entretiens en ligne :** En cas de doute, des entretiens directs via des plateformes de communication visuelle peuvent être nécessaires.

VII. Mise à jour de la connaissance du client et de ses données

A. Révision périodique des données

- Les assujettis doivent mettre à jour les informations sur le client en fonction de périodes spécifiques en fonction des risques associés. La mise à jour annuelle est le minimum, mais pour les clients à haut risque, des mises à jour peuvent être exigées plus fréquemment.

B. Vérification des changements dans la relation

- Les informations doivent être mises à jour en cas de modification de la relation d'affaires, comme un changement dans la structure de propriété ou l'ajout de nouveaux services financiers.

VIII. Analyse des informations mises à jour et réévaluation des risques

- Après la mise à jour des données, une réévaluation complète du dossier client doit être effectuée pour garantir que les risques associés restent faibles ou sous contrôle.

IX. Système de surveillance interne efficace pour une vérification continue

Les assujettis doivent mettre en place un système de surveillance interne solide qui assure la mise à jour régulière des informations et l'intégration de ces données dans les systèmes approuvés.

X. Mesures en cas de difficulté de mise à jour

- Si l'entité ne peut pas mettre à jour les données d'un client, elle doit fermer immédiatement le compte et informer les autorités compétentes.
- **Procédures de signalement :** L'entité doit informer les autorités compétentes, telles que l'unité de traitement des informations financières, et mettre fin à la relation commerciale si nécessaire.

XI. Vigilance continue pendant la relation d'affaires

A. Surveillance des opérations de manière continue

- Les opérations effectuées pendant la durée de la relation doivent être surveillées en permanence et de manière intégrée.
- **Révision continue :** Les opérations doivent être examinées régulièrement en prenant en compte la mise à jour des informations sur le client et les ajustements des politiques administratives en fonction des évaluations des risques.
- Des systèmes automatisés doivent être utilisés pour surveiller les opérations suspectes ou inhabituelles.

B. Utilisation des outils technologiques

- Si les opérations sont effectuées en ligne ou à distance, des systèmes automatisés doivent être utilisés pour détecter rapidement les opérations inhabituelles.
- Les outils de surveillance doivent être basés sur des informations fiables et actualisées sur les clients pour identifier les transactions non conformes de manière précise.

XII. Établissement des critères pour les opérations atypiques

A. Définition claire des critères

- Des critères précis doivent être établis pour identifier les opérations atypiques, telles que les opérations à valeur élevée, les opérations complexes, celles effectuées dans des circonstances exceptionnelles ou celles présentant des ambiguïtés économiques.
- Les assujettis doivent appliquer des critères flexibles permettant de détecter les opérations susceptibles d'être liées au blanchiment d'argent ou au financement du terrorisme.

B. Analyse basée sur les risques

- Les seuils d'importance doivent être adaptés à la nature du client et à l'environnement de travail. Par exemple, les opérations effectuées dans des pays ou zones à risque élevé doivent être surveillées plus attentivement.

XIII. Système de surveillance des opérations

A. Mise en place de systèmes automatisés de surveillance

- Un système de surveillance des opérations automatisé est préférable, couvrant toutes les activités financières de l'entité, afin de détecter rapidement et efficacement les opérations inhabituelles.
- Pour les opérations simples ou de petite taille, des systèmes manuels peuvent être utilisés pour réduire les coûts tout en garantissant l'efficacité de la surveillance.

B. Révision continue du système

- Le système doit être révisé périodiquement pour évaluer son efficacité, et les critères utilisés doivent être mis à jour pour refléter l'évolution des affaires et des risques.
- **Analyse des alertes :** En cas de détection d'une opération inhabituelle, l'alerte doit être examinée minutieusement pour déterminer si l'opération est liée au blanchiment d'argent ou au financement du terrorisme.

XIV. Ressources humaines pour l'analyse des alertes

- L'entité doit disposer de personnel spécialisé et bien formé pour analyser les alertes générées par le système de surveillance des opérations.
- Ces employés doivent avoir accès à toutes les informations internes nécessaires pour garantir l'efficacité du processus.

XV. 1Application de mesures renforcées pour les relations d'affaires avec des pays à haut risque

A. Mise en place de mesures supplémentaires pour les clients des pays à haut risque

- Les assujettis doivent appliquer des mesures de vigilance renforcée pour les clients provenant de pays classés à haut risque en matière de blanchiment d'argent et de financement du terrorisme.
- Elles doivent suivre les directives des autorités compétentes concernant le traitement de ces pays, y compris la collecte et l'analyse de données supplémentaires.

B. Mesures renforcées

- Des mesures contre les risques, telles que la demande d'informations supplémentaires sur les activités commerciales du client ou la réalisation de contrôles plus approfondis sur les transactions financières, doivent être appliquées.
- **Audit approfondi :** Un examen approfondi des flux financiers doit être effectué pour identifier toute activité suspecte.

XVI. Dispositions juridiques

A. Vérification des arrangements juridiques étrangers

- Il est nécessaire de vérifier les détails des arrangements juridiques tels que les fonds fiduciaires ou les entités étrangères ayant des structures complexes.
- Cela nécessite la collecte de documents spécifiques concernant la structure organisationnelle, les personnes qui contrôlent les arrangements et les bénéficiaires.

B. Vérification de l'authenticité des documents

- Il faut vérifier l'authenticité des documents relatifs aux arrangements juridiques à l'aide de documents fiables, tels que des registres officiels ou des documents validés.

XVII. Renforcement du contrôle des relations à haut risque

A. Surveillance stricte des clients à haut risque

- Les clients classés comme à haut risque doivent faire l'objet d'une surveillance continue, et des données supplémentaires doivent être collectées sur leurs activités.

B. Gestion des opérations à haut risque :

- Les opérations de grande envergure ou celles effectuées dans des zones géographiques à risque élevé doivent être surveillées de manière spéciale.

XVIII. Application de mesures simplifiées pour les clients à faible risque

A. Réduction du niveau de diligence en cas de faible risque :

- Les assujettis doivent appliquer des mesures simplifiées lorsque les transactions ou les clients présentent un faible risque (par exemple, les institutions financières agréées ou les entreprises cotées en bourse).

B. Définition claire des clients à faible risque

- Les clients appartenant à des secteurs spécifiques ou des pays ayant des systèmes efficaces de lutte contre le blanchiment d'argent doivent être classés comme à faible risque.

XIX. Conservation des documents

A. Durée de conservation :

- Les assujettis doivent conserver les documents relatifs aux mesures de vigilance et aux transactions exécutées pendant au moins cinq ans après la fermeture du compte ou la fin de la relation d'affaires.

B. Accès rapide aux documents :

- Les documents doivent être facilement accessibles par les autorités compétentes en cas de besoin, tout en garantissant la confidentialité et la sécurité des données.

C. Conservation sécurisée des registres :

- Les assujettis doivent conserver les archives de manière sécurisée, y compris des copies de sauvegarde des données stockées dans des endroits sûrs.

D. Maintien de registres précis :

- Les registres doivent être suffisamment détaillés pour reconstruire clairement les transactions si cela est demandé par les autorités.

XX. Dispositions finales

Il est essentiel que les procédures relatives aux mesures de vigilance appropriées soient claires et précises à tous les niveaux pour les assujettis à ces règles, afin d'assurer une conformité effective et d'éviter toute sanction ou mesure légale en cas de non-conformité.