INSTRUCTION N° 006/2007-CSBF
relative à la prévention et à la lutte contre le blanchiment de capitaux
et le financement du terrorisme

La Commission de Supervision Bancaire et Financière (CSBF),

Vu la loi n° 95-030 du 22 février 1996 relative à l'activité et au contrôle des établissements de crédit, telle qu'amendée,

Vu la loi n° 2005-016 du 29 septembre 2005 relative à l'activité et au contrôle des institutions de microfinance,

Vu la loi n° 2004-020 du 19 août 2004 sur le blanchiment, le dépistage, la confiscation et la coopération internationale en matière de produits du crime,

Vu le décret n° 2007-510 du 4 juin 2007 portant création, organisation et fonctionnement du Service des Renseignements Financiers dénommé Sampana Malagasy Iadiana amin'ny Famotsiam-bola ou SAMIFIN,

Vu l'instruction n° 006/2000-CSBF du 10 novembre 2000 relative au contrôle interne des établissements de crédit,

Considérant les 40 recommandations du Groupe d'Action Financière sur le Blanchiment de capitaux (GAFI) ainsi que ses 9 recommandations spéciales sur le financement du terrorisme, comme références internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme,

Après avis des sections banque et microfinance, composant l'Association Professionnelle des Etablissements de Crédit en vertu de l'article 36, dernier alinéa de la loi n° 95-030 susvisée,

DECIDE

Article 1^{er}. – Sont assujettis à la présente instruction les établissements de crédit visés par la législation bancaire et toute institution financière soumise à la supervision de la CSBF, dont les bureaux de change.

Article 2. – Les établissements assujettis doivent faire preuve d'une vigilance constante et se doter d'une organisation et de procédures internes propres à assurer le respect des prescriptions de la loi n° 2001-020 du 19 août 2004, généralement de toute disposition légale et réglementaire relative à la lutte contre le blanchiment* de capitaux et le financement du terrorisme, et de la présente instruction, notamment en ce qui concerne les mesures préventives ainsi que celles assurant la déclaration des opérations suspectes* stipulées aux articles 4, 7 à 13 et 19 à 20.

* Voir glossaire

Titre I. MESURES PREVENTIVES EN MATIERE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

Chapitre.1 -Mesures préalables

§ 1 - Information sur les correspondants du Service des Renseignements Financiers dénommé Sampana Malagasy Iadiana amin'ny Famotsiam-bola (SAMIFIN) et de la Commission de Supervision Bancaire et Financière (CSBF)

Article 3 -. Tout établissement assujetti doit communiquer au SAMIFIN* et à la CSBF l'identité de ses dirigeants et préposés habilités à faire la Déclaration d'Opérations Suspectes (DOS)* prévue aux articles 19 et 20 de la loi n° 2001-020.

Article 4 - Chaque établissement assujetti communique au SAMIFIN et à la CSBF l'identité de ses dirigeants ou préposés chargés de répondre à toute demande émanant du SAMIFIN ou de la CSBF, de recevoir les accusés de réception des DOS et d'assurer la diffusion aux membres concernés du personnel des informations, avis ou recommandations de caractère général en provenance du SAMIFIN ou de la CSBF.

§ 2 - Obligation de se doter d'une organisation et de procédures internes appropriées

Article 5 – Les établissements assujettis doivent faire preuve de vigilance constante et se doter d'une organisation et de procédures internes propres à assurer le respect de leurs obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. En particulier :

- chaque établissement assujetti doit adopter des règles écrites décrivant les diligences à accomplir en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et donnant des indications sur les types de clients ainsi que les sommes et la nature des opérations qui doivent faire l'objet d'une vigilance particulière ;
- les règles internes relatives aux diligences à accomplir peuvent être adaptées à la nature des clients de l'établissement assujetti, notamment lorsque lesdits clients sont eux-mêmes régis par la présente instruction ;
- un système de surveillance permettant de vérifier le respect des procédures internes prévues ci-dessus doit être mis en place dans chaque établissement assujetti ;
- les informations sur l'identité des clients, donneurs d'ordre, bénéficiaires et titulaires de procuration, mandataires, ayants droit économiques* et sur les transactions suspectes doivent être centralisées par les établissements assujettis ;
- les informations, déclarations et documents relatifs aux opérations importantes et suspectes doivent être conservés selon des modalités propres à en assurer la confidentialité et à en faciliter la communication dans les meilleurs délais au SAMIFIN et à la CSBF ;
- les attributions de la ou des personnes correspondantes du SAMIFIN et de la CSBF doivent être clairement formalisées.

Ils doivent assurer l'information et la formation de tous les membres concernés de leur personnel, conformément aux dispositions de l'article 10 ci-après.

Article 6 - Les règles internes doivent préciser la procédure à suivre au cas où une somme ou une opération paraît susceptible de faire l'objet d'une DOS.

Cette procédure doit notamment prévoir les modalités :

- de transmission au SAMIFIN des caractéristiques de l'opération déjà exécutée ou à exécuter, le délai d'exécution devant être indiqué dans ce dernier cas ;
- d'enregistrement et de conservation des documents se rapportant aux opérations ayant donné lieu à déclaration ;

Article 7 - Les établissements assujettis mettent en place des politiques et procédures au niveau de la maison mère ou, le cas échéant, de celui de l'organe central garantissant que leurs filiales, succursales et établissements affiliés se prémunissent efficacement contre les risques de blanchiment de capitaux et de financement du terrorisme. Ces politiques et procédures font l'objet d'adaptations afin de tenir compte des spécificités propres à chaque filiale, succursale et établissement affilié : pays d'implantation, nature des activités exercées... Elles incluent des dispositions permettant de communiquer au siège ou à l'organe central les informations nécessaires à la prévention effective du blanchiment de capitaux et du financement du terrorisme dans l'ensemble du groupe.

Les succursales et filiales implantées à l'étranger communiquent à leur siège social les dispositions du pays d'accueil qui s'opposent à la mise en œuvre de tout ou partie de ces politiques et procédures. Le siège en informe le SAMIFIN et la CSBF.

Les établissements assujettis doivent être particulièrement attentifs à toutes transactions avec les organismes dont les normes ne sont pas adéquates et tenir compte de la liste des pays et organismes dont le cadre juridique et administratif est jugé non conforme aux recommandations du GAFI*.

Article 8 - L'ensemble des règles internes actualisées relatives à la prévention du blanchiment de capitaux et du financement du terrorisme est organisé de manière à être accessible, sur simple demande, à toute personne ayant qualité à en connaître, notamment le SAMIFIN et la CSBF.

Les établissements affiliés à un organe central doivent transmettre à ce dernier, qui en valide le bien fondé, leurs règles écrites internes actualisées.

§ 3 - Service interne de la lutte contre le blanchiment de capitaux et le financement du terrorisme

Article 9 - Chaque établissement assujetti désigne un responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme qui veille à la cohérence et à l'efficacité de son dispositif de prévention et rend directement compte de sa mission à la direction. A cet effet, il lui incombe notamment de conseiller la direction ainsi que, le cas échéant, les employés de l'établissement dans l'élaboration et la mise en œuvre des politiques et procédures mises en place en application de la loi n° 2001-020, généralement de toute disposition légale et réglementaire relative au blanchiment de capitaux et au financement du terrorisme, et de la présente instruction, dans la formation du personnel, dans l'appréciation des cas suspects ainsi que, de manière générale, sur toutes les questions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Le responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme doit disposer des ressources et de l'indépendance nécessaires à l'exercice des missions qui lui sont attribuées au premier alinéa de cet article. A cet effet, l'ensemble de ses attributions ainsi que celles de ses collaborateurs doivent être formalisées précisément et prévenir tout conflit d'intérêt avec les missions définies au premier alinéa. Le responsable ainsi que ses collaborateurs doivent avoir accès aux données d'identification des clients ainsi qu'à l'ensemble des informations qu'ils estiment nécessaires à l'exercice de leurs missions.

Lorsqu'un établissement assujetti dispose de filiales, succursales ou affiliés, il désigne un responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme compétent pour l'ensemble du groupe et chargé spécialement de la bonne application des dispositions de la présente instruction.

Lorsque la taille de l'établissement assujetti ne justifie pas de confier la responsabilité du dispositif de prévention en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme à une personne spécialement désignée, l'organe exécutif* assure, sous le contrôle du Conseil d'administration, la coordination de tous les dispositifs qui concourent à l'exercice de cette mission.

§ 4 - Formation du personnel

Article 10 – Chaque établissement assujetti doit disposer d'un programme de formation de ses employés affectés à la prévention en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Le contenu et la périodicité de ces formations doivent être adaptés à la nature des risques encourus par l'établissement ainsi qu'à la sensibilité des fonctions occupées par les différents employés. Une attention particulière doit être portée aux employés nouvellement embauchés ainsi qu'à ceux en contact avec la clientèle.

§ 5 - Recours aux services des tiers

Article 11 - Un établissement assujetti peut, dans les conditions définies à l'article 12, recourir à des tiers* pour assurer l'identification de certains de ses clients. Dans tous les cas, l'établissement assujetti reste tenu de la responsabilité de l'identification de sa clientèle.

Article 12 - Les établissements assujettis doivent :

- demander aux tiers visés à l'article 11 des informations relatives à l'identification de chaque client, bénéficiaire réel et à l'objet et la nature de chaque relation d'affaires ainsi nouée, ainsi que des copies des données d'identification et autres documents pertinents liés au devoir de vigilance relatif à la clientèle ;
- s'assurer que les tiers sont soumis à une réglementation et à une surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme au moins équivalente à celle de l'établissement assujetti et qu'ils l'appliquent effectivement.

§ 6 - Information sur le dispositif de prévention en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

Article 13 - Dans le cadre de la mise en œuvre de la mission de contrôle confiée à la Commission de Supervision Bancaire et Financière par l'article 33 de la loi n° 2001-020 du 19 août 2004, les établissements assujettis doivent remettre les états annexés à la présente instruction :

- **Annexe 1** - « Identité des correspondants du SAMIFIN et de la Commission de Supervision Bancaire et Financière », un document comportant la liste des dirigeants et préposés habilités à correspondre avec le SAMIFIN et la CSBF ;
- **Annexe 2** - « Informations relatives au dispositif de prévention en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme », un document de synthèse décrivant les procédures internes et le fonctionnement du dispositif en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Article 14 - Les informations fournies sur les états précités sont arrêtées au 31 décembre de l'année civile.

Article 15 - Les états sont établis sous la responsabilité de l'organe exécutif, dont l'un au moins signe chacun des états mentionnés aux articles 13 et 38. Ils sont adressés, sur support papier, au plus tard à la fin du mois de février de chaque année au Secrétariat Général de la CSBF.

Pour les institutions affiliées à un même organe central, ce dernier établit également un rapport de synthèse concernant l'ensemble du réseau qui est adressé, sur support papier, au plus tard à la fin du mois d'avril de chaque année au Secrétariat Général de la CSBF.

Article 16 - En cas de changement d'un ou de plusieurs correspondants du SAMIFIN et de la Commission de Supervision Bancaire et Financière en cours d'année, un nouvel état – annexe 1- est adressé au Secrétariat Général de la CSBF, au plus tard 1 mois après le changement.

Chapitre.2 - Mesures de vigilance à l'égard de la clientèle

§ 1 - Identification des clients

Article 17 - Les établissements assujettis doivent s'assurer de l'identité et de l'adresse de leurs clients, ainsi que de leurs ayants droit économiques dans les situations suivantes :

- avant de nouer une relation contractuelle,
- dès que possible pour les clients existants, et à tout le moins lorsqu'une transaction significative intervient, quand les normes relatives aux documents d'identification des clients changent substantiellement, lorsqu'une modification importante se produit dans la façon dont le compte fonctionne et quand l'établissement s'aperçoit qu'il ne dispose pas d'information sur un client existant ;
- lorsqu'ils ont des doutes quant à la véracité ou la pertinence des données précédemment obtenues.

Article 18 - La vérification de l'identité d'une personne physique est opérée par le contrôle d'une carte d'identité nationale ou de tout document officiel original en tenant lieu, en cours de validité et comportant une photographie, dont il est pris une copie.

La vérification de son adresse professionnelle et domiciliaire est effectuée par le contrôle de tout document de nature à en rapporter la preuve. S'il s'agit d'une personne physique commerçante, cette dernière est tenue de fournir, en outre, toute pièce attestant de son immatriculation au Registre du Commerce.

Article 19 - L'identification d'une personne morale ou d'une entité juridique ne disposant pas de la personnalité morale est effectuée sur la base de l'original ou de la copie certifiée conforme de tout acte ou extrait de registre officiel constatant sa dénomination, sa forme juridique et son siège social, ainsi que les pouvoirs des personnes agissant en son nom. Les établissements assujettis s'assurent dans les mêmes conditions que celles fixées à l'alinéa 2 du précédent article de l'identité et de l'adresse véritables des personnes habilitées à agir au nom de la personne morale ou de la structure juridique à identifier.

Les établissements assujettis doivent disposer des informations nécessaires pour comprendre la propriété et la structure de contrôle de la personne morale et de l'entité juridique ne disposant pas de la personnalité morale et déterminer les personnes physiques qui, in fine, les possèdent ou les contrôlent.

§ 2 - Politique d'acceptation des nouveaux clients

Article 20 - Les établissements assujettis doivent définir des politiques et procédures claires d'acceptation des nouveaux clients, comprenant notamment la description des différents types de clientèle susceptibles de représenter pour eux un risque supérieur à la moyenne*.

Ces différents types de clientèle doivent être distingués en tenant compte de la nature et de l'importance du risque de blanchiment de capitaux et de financement du terrorisme encouru. Des facteurs tels que les antécédents des clients, leur pays d'origine ou de résidence, l'origine de leurs fonds, les liens entre comptes, les types de transactions qu'ils effectuent sur leurs comptes bancaires ou leurs activités professionnelles peuvent être utilisés à cet effet.

L'admission de tout nouveau client doit être approuvée par un supérieur hiérarchique du chargé de relations avec la clientèle.

Article 21 - Les établissements assujettis doivent être dotés de systèmes de gestion des risques adéquats afin de déterminer si un client potentiel ou son ayant droit économique est une personne politiquement exposée*.

L'autorisation de l'organe exécutif est nécessaire avant de nouer une relation d'affaires avec une personne politiquement exposée.

Article 22 - Les établissements assujettis doivent prendre toutes mesures raisonnables* pour identifier l'origine du patrimoine* et des fonds des clients et ayants droit économiques des clients identifiés comme des personnes politiquement exposées.

Ils doivent appliquer des mesures de vigilance renforcées vis-à-vis des personnes politiquement exposées, en particulier à l'égard de celles détenant des fonctions publiques de premier plan au niveau national.

Article 23 - Lorsqu'un établissement assujéti offre la possibilité d'ouvrir un compte ou d'effectuer toute autre opération à distance, il doit mettre en place des mesures adaptées permettant de garantir l'identification de sa clientèle. Ces mesures peuvent notamment prévoir l'authentification des documents d'identification présentés, la demande de documents supplémentaires, la possibilité d'une vérification indépendante de la situation du client par un tiers de réputation confirmée, l'exigence d'un premier paiement par l'intermédiaire d'un compte ouvert au nom du client auprès d'une banque soumise aux recommandations du GAFI ou l'envoi d'un courrier avec accusé de réception à l'adresse du client.

Article 24 - Les établissements assujéti doivent procéder à la clôture des comptes sur lesquels apparaissent, en cours de fonctionnement, des problèmes d'identification qui ne peuvent pas être résolus dans un délai de 20 jours après constatation, et faire une DOS auprès du SAMIFIN.

Article 25 - Les établissements assujéti ne sont pas autorisés à tenir de comptes anonymes, ni de comptes sous des noms fictifs.

En application de l'article 4 de la loi n° 2001-020 du 19 août 2004, tout paiement d'un bon de caisse anonyme supérieur à 10 millions Ariary est interdit.

Les bons de caisse peuvent être au porteur, la souscription doit toujours être nominative.

§ 3 - Identification des clients occasionnels

Article 26 - L'identification des clients occasionnels s'effectue dans les conditions prévues aux articles 18 et 19 :

- pour toute opération portant sur une somme supérieure à 3 millions MGA et en cas de répétition dans un court laps de temps* d'opérations distinctes entre lesquelles un lien semble exister pour un montant cumulé supérieur ou égal à 3 millions MGA ;
- lorsque l'établissement a un soupçon de blanchiment de capitaux et de financement du terrorisme même pour une transaction de moindre importance.

§ 4 - Identification de l'ayant droit économique

Article 27 - En application de l'article 9 de la loi n° 2001-020 du 19 août 2004, au cas où le client ne paraîtrait pas agir pour son propre compte, l'établissement assujéti se renseigne par tous moyens sur l'identité de la personne pour le compte de laquelle il agit. Après vérification, si le doute persiste sur l'identité de l'ayant droit économique, il doit mettre fin à la relation bancaire et procéder à la déclaration d'opérations suspectes visée aux articles 19 et 20 de la loi n° 2001-020 du 19 août 2004.

Article 28 - Conformément aux dispositions de l'article 27 de la loi n° 2001-020 du 19 août 2004, aucun client ne peut invoquer le secret professionnel pour refuser de communiquer l'identité de l'ayant droit économique.

Chapitre.3 - Mesures de contrôle des transactions

Article 29 – Toute opération portant sur des sommes dont le montant unitaire ou total est supérieur à une somme de 50 millions MGA et qui, sans entrer dans le champ d'application de l'article 41 de la présente instruction, se présente dans des conditions inhabituelles de complexité et ne paraît pas avoir de justification économique ou d'objet licite, requiert de la part de l'établissement assujetti un examen particulier. Dans ce cas, l'établissement assujetti se renseigne auprès du client sur l'origine et la destination de ces sommes ainsi que sur le motif de la transaction, l'identité et le domicile du client et de la personne qui en bénéficie.

Article 30 - Les caractéristiques de l'opération sont consignées par écrit dans un document devant faire état des renseignements recueillis, concernant en particulier :

- l'origine et la destination des sommes ainsi que l'objet de la transaction ;
- l'identité du donneur d'ordre* et du ou des ayants droit économiques avec indication du nom, de l'adresse, de la profession... ;
- les caractéristiques de l'opération au regard des critères énoncés à l'article 29 ;
- le cas échéant, les modalités et conditions de fonctionnement du compte, avec précision de la date d'ouverture, celle de fermeture ou des derniers mouvements, le nom des mandataires et les références des comptes sans mouvement.

Le rapport confidentiel établi à cet effet doit être conservé par les établissements assujettis. Le SAMIFIN et la CSBF peuvent obtenir communication de ce document et des pièces qui s'y rattachent.

Article 31 – Les établissements assujettis doivent avoir en permanence une bonne compréhension des activités normales et raisonnables attendues sur les comptes de leurs différents types de clientèle, de façon à identifier les transactions atypiques. Ils devront à cet effet disposer de systèmes permettant de déceler les opérations concernées, en recourant entre autres à des limites par catégorie de comptes ou en identifiant les opérations répétitives. Le dispositif de surveillance doit être adapté au niveau du risque encouru.

Article 32 - Une vigilance particulière visant notamment à établir l'origine des sommes en cause doit être exercée à l'égard de :

- toute opération portant sur une somme d'un montant unitaire ou total supérieur à 10 millions MGA ;
- tous les transferts de fonds, quel que soit le support de réception ou d'exécution de l'ordre ou le procédé technique utilisé ;
- toutes les opérations en provenance ou à destination d'institutions financières qui ne sont pas soumises à des obligations au moins équivalentes à celles prévues par la présente instruction en matière d'identification des clients ou de contrôle des transactions ou qui sont situées dans les pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI.

Les transferts de fonds, de titres ou de valeurs doivent être exécutés dans le strict respect des textes en vigueur et en particulier de la réglementation des changes.

Chapitre.4 - Obligations de vigilance en matière de monnaie électronique

Article 33 - Les établissements assujettis doivent disposer d'un système automatisé de surveillance des transactions inhabituelles ayant comme support la monnaie électronique.

Les anomalies constatées ayant un lien avec la circulation de la monnaie électronique doivent être communiquées à l'établissement émetteur, au SAMIFIN ainsi qu'à la CSBF.

Chapitre.5 - Obligations de vigilance relatives aux virements électroniques*

Article 34 – Pour l'ensemble des virements, les établissements assujettis du donneur d'ordre doivent obtenir et conserver les renseignements relatifs au donneur d'ordre du virement, appelés renseignements complets et énumérés ci-après, et vérifier l'exactitude de ces renseignements :

- son nom ;
- son relevé d'identité bancaire ;
- et son adresse.

Article 35 - Concernant les virements transfrontaliers*, les établissements assujettis du donneur d'ordre doivent faire figurer les renseignements complets sur ce dernier dans le message ou le formulaire de paiement accompagnant le virement.

Article 36 - Concernant les virements nationaux*, les établissements assujettis du donneur d'ordre doivent, soit faire figurer les renseignements complets sur le donneur d'ordre dans le message ou le formulaire de paiement accompagnant le virement, soit faire figurer uniquement son relevé d'identité bancaire dans le message ou le formulaire de paiement en communiquant les renseignements complets à l'établissement bénéficiaire dans un délai de 3 jours ouvrés à compter de la réception d'une demande.

Chapitre.6 - Obligations de vigilance en matière de relations de correspondant bancaire transfrontalier et relations similaires

Article 37 – Préalablement à toute opération avec un correspondant bancaire situé à l'étranger, un établissement assujetti doit prendre les mesures adéquates pour rassembler suffisamment d'informations sur ce correspondant bancaire afin de bien comprendre la nature de ses activités et d'évaluer, sur la base d'informations publiquement disponibles, la réputation de l'institution et la qualité de sa surveillance, et également si l'institution concernée a fait l'objet d'une enquête ou d'une intervention de l'autorité de surveillance ayant trait au blanchiment de capitaux et au financement du terrorisme ou de toute autre opération illicite.

Il doit, en outre, évaluer les contrôles mis en place par le correspondant bancaire en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et préciser par écrit les responsabilités respectives de chaque institution.

L'autorisation de l'organe exécutif est nécessaire avant d'entretenir de nouvelles relations avec un correspondant bancaire.

Article 38 – Une liste mise à jour des correspondants des établissements assujettis doit être transmise au SAMIFIN et à la CSBF avec les états cités à l'article 13.

Chapitre.7 - Mesures de vigilance vis-à-vis des banques fictives

Article 39 – Les établissements assujettis ne doivent pas lier ou poursuivre des relations de correspondant bancaire avec des banques dites fictives qui sont constituées et agréées dans des pays et territoires où elles n’ont aucune présence physique, sans appartenir à un groupe financier soumis à une surveillance effective sur base consolidée en matière de prévention du blanchiment de capitaux et du financement du terrorisme.

Article 40 - Les établissements assujettis doivent s'assurer que les institutions financières qui font partie de leur clientèle à l'étranger n'autorisent pas des banques fictives à utiliser leurs comptes.

Titre II. MESURES D'INFORMATION EN CAS DE DOUTE PERSISTANT OU DE SOUPÇON DE BLANCHIMENT DE CAPITAUX ET DU FINANCEMENT DU TERRORISME

Chapitre.1 - Obligations des établissements assujettis

Article 41 - Les établissements assujettis sont tenus de déclarer dans les plus brefs délais au SAMIFIN :

- les sommes ou tous autres biens qui sont en leur possession lorsqu'ils pourraient être liés à un crime ou à un délit ou s'inscrire dans un processus de blanchiment de capitaux ou de financement du terrorisme ;
- les opérations qui portent sur des sommes ou biens qui pourraient provenir d'un crime ou d'un délit ou s'inscrire dans un processus de blanchiment de capitaux ou de financement du terrorisme ;
- toute opération dont l'identité du donneur d'ordre ou du bénéficiaire reste douteuse malgré les diligences effectuées conformément aux dispositions en vigueur en matière d'identification de la clientèle ;
- les opérations pour leur propre compte ou pour compte de tiers avec des personnes morales y compris leurs filiales ou établissements, agissant sous forme ou pour le compte de fonds fiduciaires ou de tout autre instrument de gestion d'un patrimoine d'affectation dont l'identité des constituants ou des bénéficiaires n'est pas connue.

La déclaration doit être effectuée avant l'exécution de l'opération.

Lorsque la déclaration porte sur une opération qui n'a pas encore été exécutée, elle est assortie de l'indication de son délai d'exécution.

La déclaration ne peut porter sur des opérations déjà exécutées que lorsqu'il a été impossible de surseoir à leur exécution ou lorsqu'il est apparu, postérieurement à la réalisation de l'opération, que les sommes auraient pu être liées à un crime ou à un délit ou que le report de l'exécution de l'opération serait susceptible d'empêcher la poursuite des bénéficiaires de blanchiment de capitaux ou du financement du terrorisme.

Article 42 – Les établissements assujettis doivent à chaque fin du mois transmettre à la CSBF un récapitulatif des déclarations du mois effectuées auprès du SAMIFIN.

Chapitre.2 - Respect de l'opposition à l'exécution des opérations

Article 43 - Le SAMIFIN peut, avant l'expiration du délai d'exécution mentionné par l'établissement assujetti déclarant, former opposition à l'exécution de l'opération. Cette opposition est notifiée au déclarant par télécopie ou par tout moyen laissant trace écrite par le Directeur Général du SAMIFIN ; l'établissement assujetti s'y soumet pendant une durée de 48 heures. Le délai d'opposition pourrait être prorogé par ordonnance du Président du Tribunal de première instance pour une durée supplémentaire qui ne peut excéder huit jours.

Dans le cas où le SAMIFIN ne forme pas opposition dans le délai imparti, l'établissement assujetti déclarant peut exécuter l'opération.

Dans tous les cas, l'établissement assujetti est tenu de se soumettre aux termes de la décision de blocage provisoire des fonds, des comptes ou des titres concernés par la déclaration.

Chapitre.3 - Obligations de déférer aux réquisitions des autorités judiciaires

Article 44 - Les établissements assujettis sont astreints à l'obligation de coopérer dans le cadre des techniques particulières d'investigation, prévues par l'article 25 de la loi n° 2001-020, mises en œuvre par les autorités judiciaires en vue d'obtenir la preuve de l'infraction d'origine* ainsi que celle des infractions prévues par les textes en vigueur relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Article 45 - Les dirigeants ou les agents des établissements assujettis doivent s'abstenir de porter à la connaissance de leurs clients ou mandataires de l'existence de la DOS faite auprès du SAMIFIN ou de donner des informations sur les suites qui lui ont été réservées.

Chapitre.4 - Conservation des documents

Article 46 - Toutes les pièces se rapportant aux opérations à la fois nationales et internationales, y compris les transactions qui n'ont pas abouti et celles réalisées avec des clients occasionnels doivent être conservées pendant au moins cinq ans ou plus longtemps si une autorité compétente le demande dans des affaires spécifiques et pour l'accomplissement de leur mission.

La valeur probante de l'archivage électronique est admise pour la conservation des documents, sous réserve de la preuve contraire de la part de tout intéressé en cas de contestation.

Article 47 - Toutes les pièces et informations relatives aux clients et aux opérations doivent être mises à disposition des autorités nationales compétentes pour l'accomplissement de leur mission.

Titre III. SANCTIONS

Article 48 - En application de l'article 33 de la loi n° 2001-020, sans préjudice des sanctions que pourra prononcer du même chef l'autorité judiciaire, en cas de grave défaut de vigilance ou d'une carence dans l'organisation des procédures internes de prévention du blanchiment de capitaux et du financement du terrorisme, les établissements assujettis seront passibles des sanctions prévues par la législation bancaire.

Titre IV. DISPOSITIONS FINALES ET TRANSITOIRES

Article 49 - A titre transitoire, la première déclaration en application des articles 13, 38 et 42 doivent être fournis avec les états financiers arrêtés au 30 septembre 2007.

Article 50 - La présente instruction entre en vigueur dès sa notification à l'Association Professionnelle des Etablissements de crédit et aux sections existantes.

Fait à Antananarivo, le 3 août 2007.

Pour la Commission de Supervision
Bancaire et Financière,
LE PRESIDENT,

Frédéric RASAMOELY

DECLARANT

**Déclaration au titre de l'article 13 de l'instruction n° 006/2007-CSBF
relative à la prévention et à la lutte contre le blanchiment de capitaux
et le financement du terrorisme
Identité des correspondants du Service des renseignements financiers
et de la Commission de Supervision Bancaire et Financière**

au : | | | | |

Identité des correspondants						
Qualité ⁽¹⁾	Nom	Prénoms	Fonction	Date de désignation	Numéro de téléphone	Numéro de fax

(1) : Monsieur, Madame ou Mademoiselle

A _____, le.....
SIGNATURE(S) ACCREDITEE(S) ET CACHET

DECLARANT

**Déclaration au titre de l'article 13 de l'instruction n° 006/2007-CSBF
relative à la prévention et à la lutte contre le blanchiment de capitaux
et le financement du terrorisme**
Informations relatives au dispositif de prévention du blanchiment de capitaux
au : |__|__|__|

PROCEDURES INTERNES**I – DÉSIGNATION DES CORRESPONDANTS**

	Oui	Non	Sans objet
1. Les noms des correspondants sont-ils communiqués, dès la désignation de ces derniers, – au SAMIFIN ? – au Secrétariat Général de la Commission de Supervision Bancaire et Financière ?			
2. L'identité des personnes ou du service à contacter pour effectuer une déclaration au SAMIFIN figure-t-elle dans les règles écrites internes de votre établissement ?			
3. Les éventuelles modifications concernant les correspondants intervenues au cours de l'exercice écoulé (désignation de nouveaux correspondants, changement de coordonnées, etc.) ont-elles donné lieu à la mise à jour immédiate des règles écrites internes ?			

II – DISPOSITIF DE DETECTION DES OPERATIONS SUSPECTES ET IMPORTANTES

	Oui	Non	Sans objet
1. Afin de déterminer s'il convient de faire une déclaration d'opérations suspectes DOS (articles 19 et 20 de la loi n° 2001-020) ou de constituer un dossier au titre de l'article 10 de la loi précitée, les procédures mises en place dans votre établissement prévoient-elles de vous renseigner sur : – le montant de l'opération ; – le type de l'opération (dépôt en espèces, virement, etc.) ; – l'existence d'une justification économique de l'opération ; – la devise traitée ; – l'identité du donneur d'ordre réel ; – l'origine de l'opération (origine géographique, organisme financier intervenant en tant qu'intermédiaire, n° du compte utilisé) ; – la personne bénéficiaire de l'opération ; – la destination de l'opération (destination géographique, organisme financier intervenant en tant qu'intermédiaire, n° du compte utilisé).			
2. Les procédures mises en place par votre établissement permettent-elles de détecter toute opération portant sur des sommes qui pourraient provenir du trafic de stupéfiants ou d'activités criminelles organisées ?			

3. Existe-t-il des procédures de gestion des risques comprenant, d'une part, un ensemble de mesures comme une limitation du nombre, du type et/ou du montant des transactions pouvant être exécutées et, d'autre part, la surveillance des transactions importantes ou complexes dépassant les normes imposées pour ce type d'opération ?			
4. Votre établissement accepte-t-il d'ouvrir des comptes anonymes ou des comptes sous des noms fictifs ?			
5. Les procédures mises en place par votre établissement permettent-elles d'appliquer les mesures de vigilance aux clients existants si ces derniers ont ouvert des comptes anonymes ou des comptes sous des noms fictifs ?			
6. Les procédures mises en place par votre établissement vous obligent-elles d'appliquer les mesures de vigilance aux clients existants ?			
7. Les procédures mises en place par votre établissement permettent-elles de déclarer au SAMIFIN toute opération dont l'identité du donneur d'ordre ou du bénéficiaire reste douteuse malgré les diligences d'identification de la clientèle effectuées conformément aux dispositions de la loi n° 2001-020 ?			
8. Les procédures mises en place par votre établissement permettent-elles de déclarer au SAMIFIN les opérations effectuées avec un fonds fiduciaire ou tout autre instrument de gestion d'un patrimoine dont l'identité des constituants ou des bénéficiaires n'est pas connue ?			
9. Les procédures mises en place par votre établissement permettent-elles d'identifier les opérations faites avec les personnes faisant l'objet d'une mesure de gel des avoirs du fait de leurs liens présumés avec une activité criminelle organisée ?			
10. Si une opération porte sur une somme d'un montant unitaire ou total supérieur à 10 millions MGA, ne paraît pas avoir de justification économique ou d'objet licite et se présente dans des conditions inhabituelles de complexité, votre établissement en consigne-t-il les caractéristiques dans un dossier de renseignements ?			
11. Les procédures mises en place par votre établissement permettent-elles d'interdire l'ouverture d'un compte, l'entretien d'une relation d'affaires ou la réalisation d'une transaction en cas d'impossibilité de vérification de l'identité du client et de faire une déclaration d'opérations suspectes (DOS) ?			

III – IDENTIFICATION DE LA CLIENTÈLE

	Oui	Non	Sans objet
1. Avant d'ouvrir un compte à une personne physique, est-il systématiquement demandé à celle-ci de fournir un document officiel d'identité portant sa photographie et en est-il pris copie ?			
2. Avant d'ouvrir un compte à une personne morale, est-il systématiquement demandé une présentation de l'original ou la copie certifiée conforme de tout acte ou extrait de registre officiel constatant sa dénomination, sa forme juridique et son siège social, les noms des dirigeants et administrateurs, les dispositions régissant le pouvoir d'engager la personne morale ainsi que les pouvoirs des personnes agissant en son nom ?			

3. Existe-t-il une procédure de vérification de la délégation de pouvoirs ou de l'autorisation de toute personne qui agit au nom du client et de l'identité de cette personne ?			
4. Existe-t-il une procédure d'identification de la personne au bénéfice de laquelle le compte est ouvert lorsque la personne qui demande l'ouverture du compte ne paraît pas agir pour son compte propre ?			
5. Lors de l'entrée en relation d'affaires avec un client, en dehors d'une ouverture de compte (octroi d'un crédit, caution, transmission d'ordres ...), existe-t-il des procédures équivalentes à celles décrites aux questions 1 et 2 sur l'identification de la clientèle ?			
6. Dans le cas évoqué ci-dessus, existe-t-il une procédure d'identification de la personne au bénéfice de laquelle l'opération est effectuée lorsque la personne qui en demande la réalisation ne paraît pas agir pour son propre compte ?			
<p>7. Si votre établissement offre la possibilité d'ouvrir un compte ou d'effectuer toute autre opération à distance avec des personnes physiques ou morales, quelles sont les démarches systématiquement mises en œuvre pour vous assurer de l'identité du client :</p> <ul style="list-style-type: none"> – votre établissement demande-t-il une copie d'un document officiel d'identité portant la photographie du client ou de tout acte ou extrait de registre officiel constatant la dénomination, la forme juridique, le siège social, les noms des dirigeants et administrateurs, les dispositions régissant le pouvoir d'engager la personne morale ainsi que les pouvoirs des personnes agissant au nom de la personne morale ? – votre établissement demande-t-il la copie d'un justificatif du domicile ou de l'adresse du siège social ou le cas échéant d'une autre adresse de correspondance du client – votre établissement envoie-t-il un courrier avec accusé de réception au domicile ou à l'adresse du siège social ou, le cas échéant, à une autre adresse de correspondance du client ? 			
8. Existe-t-il une procédure pour connaître la propriété et la structure de contrôle du client (pour la clientèle personnes morales), de déterminer les personnes physiques qui possèdent ou contrôlent le client, d'obtenir des informations sur l'objet et la nature envisagée de la relation d'affaires ?			
9. L'ouverture du compte visée à la ligne précédente ne devient-elle effective qu'après la réception du dossier complet et le retour de l'accusé de réception ?			
10. Les documents relatifs à l'identité des clients sont-ils conservés pendant une durée minimale de cinq ans à compter de la clôture de leur compte ou de la cessation de la relation d'affaires ?			
11. Les documents relatifs aux opérations effectuées par les clients –y compris les opérations qui ne se rapportent pas à un compte de dépôts- sont-ils conservés pendant une durée minimale de cinq ans à compter de leur exécution ?			
12. Lors de l'entrée en relation d'affaires, votre établissement procède-t-il à une évaluation du profil de fonctionnement du compte ou des autres opérations attendues relatives au nouveau client au regard de la prévention du blanchiment de capitaux et du financement du terrorisme ?			

IV – IDENTIFICATION DE LA CLIENTÈLE - CLIENT OCCASIONNEL

	Oui	Non	Sans Objet
1. Votre établissement s'assure-t-il de l'identité de toute personne physique, client occasionnel, qui lui demande de faire une opération portant sur une somme supérieure à 3 millions MGA ou de louer un coffre, par la présentation par celle-ci d'un document officiel portant sa photographie ?			
2. Votre établissement s'assure-t-il de l'identité de toute personne morale, client occasionnel, qui lui demande de faire une opération portant sur une somme supérieure à 3 millions MGA ou de louer un coffre, par la présentation de tout acte ou extrait de registre officiel ?			
3. Existe-t-il une procédure d'identification du bénéficiaire de l'opération si la personne qui demande la réalisation de celle-ci ne paraît pas agir pour son propre compte ?			
4. Existe-t-il une procédure d'identification d'un client occasionnel qui demande, dans un court laps de temps, la réalisation de plusieurs opérations entre lesquelles un lien semble exister et dont le montant total excède 3 millions MGA ?			
5. Les documents relatifs à l'identité des clients occasionnels sont-ils conservés pendant une durée minimale de cinq ans à compter de la cessation de leur relation avec votre établissement ?			
6. Les documents relatifs aux opérations effectuées par les clients occasionnels sont-ils conservés pendant une durée minimale de cinq ans à compter de leur exécution ?			

V – AUTRES OBLIGATIONS DE VIGILANCE

	Oui	Non	Sans objet
1. Votre établissement dispose-t-il de procédures internes d'analyse de sa clientèle par profil de clients, permettant de faire ressortir des mouvements financiers atypiques ?			
2. Ces procédures sont-elles informatisées ?			
3. Votre établissement dispose-t-il d'un système informatisé de détection des opérations d'un montant unitaire supérieur à 3 millions MGA réalisées par un client occasionnel ?			
4. Votre établissement dispose-t-il d'un système informatisé de détection des opérations réalisées par un client occasionnel entre lesquelles un lien semble exister et dont le montant total est supérieur à 3 millions MGA ?			
5. Les correspondants du SAMIFIN et de la CSBF de votre établissement sont-ils systématiquement destinataires des informations issues des systèmes visés aux questions 1 à 4 des autres obligations de vigilance ?			
6. Votre établissement conserve-t-il une trace écrite des données d'identification, des livres de comptes et de la correspondance commerciale pendant au moins 5 ans après la réalisation de la transaction, ou plus longtemps si une autorité compétente le demande, dans des affaires spécifiques et pour l'accomplissement de sa mission ?			

V.1. Obligations de vigilance en matière de monnaie électronique :

	Oui	Non	Sans objet
1. Votre établissement dispose-t-il d'un système automatisé de surveillance des transactions inhabituelles ayant comme support la monnaie électronique ?			
2. Si votre établissement distribue de la monnaie électronique, les anomalies constatées ayant un lien avec la circulation de la monnaie électronique sont-elles communiquées à l'établissement émetteur ?			
3. Le ou les correspondants du SAMIFIN et de la CSBF sont-ils destinataires d'un relevé au moins mensuel des anomalies constatées ?			

V.2. Mesures de vigilance envers de personnes politiquement exposées

	Oui	Non	Sans objet
1. Votre établissement dispose-t-il de systèmes de gestion des risques adéquats afin de déterminer si un client potentiel, un client ou le bénéficiaire effectif est une personne politiquement exposée ?			
2. Si votre établissement entre en relation d'affaires avec une personne politiquement exposée, l'autorisation de l'organe exécutif a-t-elle été obtenue ?			
3. Votre établissement dispose-t-il de mesures raisonnables pour identifier l'origine du patrimoine et l'origine des fonds des clients et bénéficiaires effectifs identifiés comme des personnes politiquement exposées ?			
4. Votre établissement assure-t-il une surveillance renforcée et continue d'une relation avec une personne politiquement exposée ?			
5. Votre établissement applique-t-il les mesures de vigilance envers de personnes politiquement exposées détenant des fonctions publiques de premier plan au niveau national ?			

V.3. Obligations de vigilance en matière de relations de correspondant bancaire transfrontalier et relations similaires

	Oui	Non	Sans objet
1. Votre établissement dispose-t-il de mesures permettant de rassembler suffisamment d'information sur le correspondant bancaire, de vérifier si l'institution concernée a fait l'objet d'une enquête ou d'une intervention de l'autorité de surveillance ayant trait au blanchiment de capitaux et au financement du terrorisme ?			
2. Existe-t-il une procédure permettant d'évaluer les contrôles mis en place par le correspondant bancaire en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme et de s'assurer de leur pertinence et de leur efficacité ?			
3. Si votre établissement noue de nouvelles relations de correspondant bancaire, l'autorisation de l'organe exécutif a-t-elle été obtenue ?			

4. Le correspondant bancaire peut-elle fournir des données d'identification pertinentes sur ses clients si votre établissement les demande ?			
--	--	--	--

V.4. Recours à des tiers intermédiaires ou à des tiers pour s'acquitter de certains éléments du devoir de vigilance relatif à la clientèle

	Oui	Non	Sans objet
1. Votre établissement recourt-il à des tiers intermédiaires ou à des tiers pour s'acquitter de certains éléments du devoir de vigilance relatif à la clientèle ?			
2. Votre établissement obtient-il des tiers les informations nécessaires concernant certains éléments de mesures de vigilance relative à la clientèle ?			
3. Votre établissement s'assure-t-il que le tiers peut fournir, sur demande et dans les délais les plus brefs, des copies des données d'identification et autres documents pertinents liés au devoir de vigilance relatif à la clientèle ?			
4. Votre établissement s'assure-t-il que le tiers est soumis à une réglementation et à une surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et qu'il a pris des mesures visant à se conformer aux mesures de vigilance relatives à la clientèle ?			
5. Votre établissement dispose-t-il des informations permettant de savoir si les pays auxquels le tiers s'établit appliquent convenablement les Recommandations du GAFI ?			
6. Quelle est la responsabilité de votre établissement par rapport à la responsabilité du tiers en ce qui concerne l'identification et la vérification de l'identité ?			

V.5. Mesures de vigilance relatives aux virements électroniques

	Oui	Non	Sans objet
1. Votre établissement obtient-il et conserve-t-il des renseignements relatifs au donneur d'ordre du virement et vérifie-t-il l'exactitude et l'utilité des renseignements ?			
2. Concernant les virements transfrontaliers, les renseignements complets sur le donneur d'ordre figurent-ils dans le message ou le formulaire de paiement accompagnant le virement ?			
3. Concernant les virements nationaux, les renseignements complets sur le donneur d'ordre figurent-ils dans le message ou le formulaire de paiement accompagnant le virement ou le relevé d'identité bancaire du donneur d'ordre figure-t-il dans le message ou le formulaire de paiement.			
4. Votre établissement traite-t-il des transactions routinières par lots ?			
5. Si votre établissement est intermédiaire dans la chaîne de paiement, conserve-t-il l'ensemble des renseignements nécessaires sur le donneur d'ordre avec le virement correspondant ?			

6. Pour l'ensemble des virements, les renseignements relatifs au donneur d'ordre du virement et la vérification de l'exactitude et de l'utilité des renseignements sont-ils obtenus et conservés ?			
7. Des procédures efficaces fondées sur une évaluation des risques sont-elles adoptées par votre établissement ?			
8. Votre établissement prévoit-il des mesures efficaces de contrôle du respect des règles et des règlements de mise en œuvre des mesures de vigilance relatives aux virements électroniques ?			

V.6. Mesures de contrôle des transactions

	Oui	Non	Sans objet
1. Votre établissement apporte-t-il une attention particulière à toutes les opérations complexes, d'un montant supérieur à 50 millions MGA, ou à tous les types inhabituels de transactions, lorsqu'elles n'ont pas d'objet économique ou licite apparent ?			
2. Votre établissement étudie-t-il le contexte et l'objet de ces transactions et consigne-t-il les résultats de ces examens par écrit ?			
3. Les résultats de ces examens sont-ils mis à la disposition de SAMIFIN et de la CSBF pour une durée d'au moins cinq ans ?			
4. Votre établissement prête-t-il une attention particulière aux relations d'affaires et transactions avec des personnes morales et des institutions financières résidant dans les pays qui n'appliquent pas ou appliquent insuffisamment les Recommandations du GAFI ?			
5. Dans le cas où un tel pays persiste à ne pas appliquer ou à appliquer insuffisamment les Recommandations du GAFI, votre établissement applique-t-il des contre-mesures adaptées, tels que : <ul style="list-style-type: none"> – L'application de normes strictes d'identification des clients et le renforcement des conseils, notamment sur les questions financières spécifiques à la juridiction, aux institutions financières en vue de l'identification des bénéficiaires effectifs avant que des relations d'affaires ne soient nouées avec des personnes physiques ou morales de ces pays ; – Le renforcement des mécanismes de déclaration correspondants ou la déclaration systématique des transactions financières en considérant que les transactions financières avec ces pays sont probablement suspectes ; – La prise en compte, lors de l'examen des demandes d'approbation de l'établissement dans les pays appliquant la contre-mesure de filiales ou de succursales ou encore de bureaux de représentation d'institutions financières, de fait que l'institution financière concernée est originaire d'un pays qui n'est pas doté d'un dispositif de la lutte contre le blanchiment de capitaux et le financement du terrorisme convenable ; – La mise en garde des entreprises du secteur non financier contre le risque de blanchiment de capitaux et de financement du terrorisme que comportent les transactions avec des personnes physiques ou morales de ce pays ; – La limitation des relations d'affaires ou des transactions financières avec le pays ou des personnes identifiées dans ce pays. 			

V.7. Obligations de déclaration d'opérations suspectes

	Oui	Non	Sans objet
1. Votre établissement fait-il une déclaration d'opérations suspectes (DOS) au SAMIFIN des fonds pour lesquels il existe des motifs raisonnables de suspecter, pour les tentatives d'opérations, quel que soit le montant de l'opération, sur les opérations considérées ou non portant sur des questions fiscales ?			
2. Votre établissement interdit-il ses dirigeants et employés à titre permanent et temporaire de divulguer ou d'avertir le client sur une DOS qui la concerne au SAMIFIN ?			
3. Votre établissement transmet-il à la CSBF un récapitulatif des déclarations du mois effectuées auprès du SAMIFIN ?			

V.8. Mesures de vigilance vis-à-vis des banques fictives

	Oui	Non	Sans objet
1. Votre établissement poursuit-il des relations de correspondant bancaire avec des banques fictives ?			
2. Votre établissement s'assure-t-il que les institutions financières qui font partie de sa clientèle à l'étranger n'autorisent pas des banques fictives à utiliser leurs comptes ?			

VI – INFORMATION ET FORMATION DU PERSONNEL CONCERNÉ

	Oui	Non	Sans objet
1. Tout nouvel agent concerné bénéficie-t-il d'une formation sur le thème de la prévention du blanchiment de capitaux et du financement du terrorisme lors de son recrutement ou au cours des semaines suivantes ?			
2. L'ensemble des agents concernés de votre établissement bénéficie-t-il d'une information régulière sur ce thème ?			

VII – VERIFICATION DE L'APPLICATION DU DISPOSITIF DE PREVENTION CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME

	Oui	Non	Sans objet
1. Existe-t-il des procédures, politiques et mesures de contrôle interne destinées à prévenir le blanchiment de capitaux et le financement du terrorisme ?			
2. Les employés connaissent-ils l'existence de ces procédures, politiques et mesures de contrôle interne ?			
3. Votre établissement a-t-il mis en place un système de surveillance permettant de vérifier le respect des procédures, politiques et mesures de contrôle interne destinées à prévenir le blanchiment de capitaux et le financement du terrorisme ?			
4. Ce système de surveillance comprend-il un dispositif de contrôle interne régulier ?			

5. Ce système de surveillance prévoit-il des inspections périodiques ?			
6. Le responsable du contrôle de la lutte contre le blanchiment de capitaux et le financement du terrorisme et les autres membres du personnel concerné ont-ils accès aux données d'identification des clients et à d'autres renseignements relevant des mesures de vigilance, aux pièces relatives aux transactions et aux autres renseignements pertinents ?			
7. Votre établissement a-t-il un dispositif de contrôle interne indépendant et convenable doté en ressources afin de vérifier le respect (y compris par sondage) des procédures, politiques et mesures de contrôle ?			
8. Votre établissement met-il en place une formation continue des employés concernant les nouvelles évolutions, techniques, méthodes et tendances de blanchiment de capitaux et de financement du terrorisme ?			
9. Vos employés reçoivent-ils des explications claires et suffisantes sur tous les aspects des lois et obligations de la lutte contre le blanchiment de capitaux et le financement du terrorisme et notamment des obligations relatives au devoir de vigilance vis-à-vis de la clientèle et de déclaration des opérations suspectes ?			
10. Votre établissement a-t-il mis en place des procédures appropriées lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants* ?			
11. Le responsable du contrôle de la lutte contre le blanchiment de capitaux et le financement du terrorisme est-il en mesure d'agir de façon indépendante et de rendre compte à l'organe exécutif, sans passer par son supérieur hiérarchique immédiat, ou au Conseil d'administration ?			
12. Vos succursales et filiales à l'étranger observent-elles les mesures de la lutte contre le blanchiment de capitaux et le financement du terrorisme conformément aux obligations prévues dans leur pays d'origine et aux Recommandations du GAFI ?			
13. Dans le cas où le pays d'accueil de vos succursales et filiales à l'étranger n'applique pas ou applique insuffisamment les Recommandations du GAFI, votre établissement veille-t-il au respect des Recommandations du GAFI par ces succursales et filiales à l'étranger ?			
14. Lorsque les normes minimales de la lutte contre le blanchiment de capitaux et le financement du terrorisme des pays d'accueil et d'origine diffèrent, vos succursales et filiales dans les pays d'accueil appliquent-elles la norme la plus rigoureuse ?			
15. Lorsqu'une succursale ou filiale étrangère est dans l'incapacité de respecter les mesures de la lutte contre le blanchiment de capitaux et le financement du terrorisme, votre établissement informe-t-il les autorités de surveillance de leur pays d'origine ?			
16. Votre établissement applique-t-il des mesures de vigilance relatives à la clientèle qui soient cohérentes au niveau du groupe, dans le cas des opérations effectuées par le client dans les différentes succursales et filiales majoritairement contrôlées à l'échelle mondiale ?			
17. L'organe exécutif de votre établissement est-elle informée des déclarations effectuées au SAMIFIN et à la CSBF et des opérations ayant donné lieu à la constitution d'un dossier de renseignements, en application de l'article 10 de la loi n° 2001-020 ?			
18. Le dispositif préventif de lutte contre le blanchiment de capitaux et le financement du terrorisme fait-il partie du champ d'investigation de la personne responsable du contrôle interne de votre établissement ?			

19. La mise en œuvre des procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme est-elle systématiquement vérifiée par le service de contrôle interne lors des missions d'inspection réalisées dans les agences de votre établissement ?			
---	--	--	--

VIII – EXISTENCE DE REGLES ECRITES INTERNES CONFORMES AUX EXIGENCES DE LA REGLEMENTATION

	Oui	Non	Sans objet
<p>1. Les règles écrites internes de votre établissement contiennent-elles :</p> <ul style="list-style-type: none"> – la procédure à suivre au cas où une somme ou une opération paraît susceptible de faire l'objet d'une DOS au Service des renseignements financiers ? – l'interdiction, édictée à l'article 34 de la loi n° 2001-020, de porter à la connaissance du propriétaire des sommes ou de l'auteur d'une opération ayant fait l'objet d'une DOS et l'existence de cette déclaration ? – la procédure à suivre lorsque, dans des cas exceptionnels et en raison notamment de l'urgence, une personne non habilitée est amenée à prendre l'initiative d'effectuer elle-même une DOS au Service des renseignements financiers et à la CSBF ? – les modalités de vérification de l'identité de la clientèle (personnes physiques et personnes morales) ? – la procédure à suivre si le client ne semble pas être le bénéficiaire de l'ouverture de compte ou de la réalisation de l'opération pour laquelle il entre en contact avec votre établissement ? – une précision sur la somme et la nature des opérations devant faire l'objet d'une vigilance particulière (notamment, pour les clients qui ont ouvert un compte, au regard des flux enregistrés habituellement sur leur compte) ? – la définition des diligences spécifiques à accomplir pour le contrôle des chèques aux fins de prévention du blanchiment de capitaux et du financement du terrorisme? – une énumération des diligences à accomplir lorsque des anomalies qui peuvent présenter un intérêt au regard de la prévention du blanchiment de capitaux et du financement du terrorisme sont détectées dans la circulation de la monnaie électronique ? – les indicateurs permettant d'identifier des opérations réalisées par un client occasionnel dans un court laps de temps, et dont le montant total dépasse 3 millions MGA ? – les modalités de constitution des dossiers de renseignements visés à l'article 10 de la loi n° 2001-020 ? – les modalités d'enregistrement et de conservation des documents se rapportant aux opérations ayant donné lieu à la constitution d'un dossier de renseignement au sens de l'article 10 de la loi n° 2001-020 ou à une déclaration de soupçon au Service des renseignements financiers ? 			

2. Dans le cas où votre établissement appartient à un groupe et où les règles écrites internes ont été élaborées à partir d'un canevas réalisé pour l'ensemble du groupe, les procédures en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ont-elles été adaptées à la nature de l'activité de votre établissement ?			
--	--	--	--

IX – COMMUNICATION DES RÈGLES ÉCRITES INTERNES

	Oui	Non	Sans objet
1. Votre établissement possède-t-il un manuel de procédures contenant toutes les consignes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ?			
2. Chaque collaborateur pouvant être concerné par la mise en œuvre des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme reçoit-il à titre individuel un exemplaire du manuel précité ?			
3. Chaque collaborateur pouvant être concerné par la mise en œuvre des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme accuse-t-il réception du manuel précité ?			
4. Dans le cas où votre établissement est affilié à un organe central, les règles écrites internes ont-elles été communiquées à celui-ci ?			

A _____, le.....
SIGNATURE(S) ACCREDITEE(S) ET CACHET

GLOSSAIRE

<i>Termes</i>	<i>Définition</i>
Ayant droit économique (art. 27, 28)	Bénéficiaire économique
Blanchiment	<ul style="list-style-type: none">- La conversion ou le transfert de sommes ou tous autres 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 ;- La dissimulation ou le déguisement de la nature, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété réels de sommes ou tous autres biens ;- L'acquisition, la détention ou l'utilisation de sommes ou tous autres biens, par une personne qui sait que lesdits sommes ou biens constituent un produit du crime.
Court laps de temps (art. 26)	Il appartient aux établissements assujettis de déterminer ce délai en tenant compte de la nature et de l'importance du risque de blanchiment encouru, les antécédents des clients, leur pays d'origine ou de résidence, l'origine de leurs fonds, les liens entre les comptes, les types de transactions qu'ils effectuent sur leurs comptes bancaires ou leurs activités professionnelles.
Critères exigeants (annexe 2, point VII - 10)	Procédures adéquates de sélection lors de l'embauche, lesquelles comprennent, entre autres, une enquête de bonne moralité et s'assurent que la nouvelle recrue n'a pas fait l'objet d'une condamnation pour crime, pour infraction à la législation sur la corruption, pour infraction à la législation sur les stupéfiants, le blanchiment de fonds, le financement du terrorisme et l'usure ou pour tentative ou complicité de toutes ces infractions.
Donneur d'ordre (art. 30, 34, 35, 36, 41)	Le titulaire du compte, ou en l'absence de compte, la personne (physique ou morale) qui donne instruction à l'institution financière de procéder à une opération bancaire (au virement électronique, etc.).
DOS (art. 3, 4, 6, 24, 45)	Déclaration d'Opérations Suspectes.
GAFI (art. 7, 23, 32)	A pour objet la protection du système financier mondial contre le blanchiment de capitaux. Ses publications sont accessibles à l'adresse internet suivante : www.fatf-gafi.org .

<i>Termes</i>	<i>Définition</i>
Infraction d'origine (art. 44)	<p>Toute infraction pénale telle que citée ci-après, même commise à l'étranger, ayant permis à son auteur de se procurer des produits :</p> <ul style="list-style-type: none"> - participation à un groupe criminel organisé et à un racket ; - terrorisme, y compris son financement ; - traite d'êtres humains et trafic illicite de migrants ; - exploitation sexuelle, y compris celle des enfants ; - trafic illicite de stupéfiants et de substances psychotropes ; - trafic d'armes ; - trafic illicite de biens volés et autres biens ; - corruption ; - fraude et l'escroquerie ; - contrefaçon de monnaie ; - contrefaçon et le piratage de produits ; - crimes contre l'environnement ; - meurtres et blessures corporelles graves ; - enlèvement, séquestration et prise d'otages ; - vol ; - contrebande ; - extorsion ; - faux ; - piraterie - délits d'initiés et manipulation de marchés.
Mesures raisonnables (art. 22)	<p>Mesures qui retiendront la sollicitation d'informations pertinentes auprès du client, le recours à des informations disponibles auprès d'autres entités comme le BIANCO sur les personnes politiquement exposées.</p>
Opérations suspectes (art. 2, 3, 27)	<ul style="list-style-type: none"> - Opérations qui portent sur des sommes ou biens qui pourraient provenir d'un crime ou d'un délit ou s'inscrire dans un processus de blanchiment de capitaux ou de financement du terrorisme ; - Sommes ou tous autres biens qui sont en leur possession lorsqu'ils pourraient être liés à un crime ou à un délit ou s'inscrire dans un processus de blanchiment de capitaux ou de financement du terrorisme ; - Opération dont l'identité du donneur d'ordre ou du bénéficiaire reste douteuse malgré les diligences effectuées conformément aux dispositions en vigueur en matière d'identification de la clientèle ; - Opérations effectuées pour propre compte ou pour compte de tiers avec des personnes morales y compris leurs filiales ou établissements, agissant sous forme ou pour le compte de fonds fiduciaires ou de tout autre instrument de gestion d'un patrimoine d'affectation dont l'identité des constituants ou des bénéficiaires n'est pas connue.

<i>Termes</i>	<i>Définition</i>
Organe exécutif (art. 9, 15)	Ensemble des personnes visées par la législation bancaire, appelées à assurer la détermination effective de l'orientation de l'activité de l'établissement. Cet organe est responsable de la gestion quotidienne de l'établissement en tant que chef d'entreprise et la représente vis-à-vis des tiers.
Patrimoine (art. 22, 41)	Ensemble des biens de famille, biens hérités du père et de la mère : – Avoirs : <ul style="list-style-type: none"> • biens immobiliers, • fonds de commerce, • entreprises ou exploitations industrielles, rurales, forestières, ou de pêche, • véhicules, • bateaux, • parts de sociétés, actions, obligations, • biens situés à l'étranger ou échappant à la juridiction malgache, • avoirs détenus par des tiers au nom ou pour le compte du conjoint, – Dettes.
Personne Politiquement Exposée (PPE) (art. 21)	Personne qui exerce ou a exercé d'importantes fonctions publiques telles que : <ul style="list-style-type: none"> – Chef d'Etat, – Chef de Gouvernement, – Politiciens de haut rang, – Hauts responsables au sein des pouvoirs publics : <ul style="list-style-type: none"> • Ministres, • Sénateurs, • Députés, • Chefs d'institution, • Chefs de région, • Maires, • Secrétaires généraux des ministères, • Fonctionnaires occupant des postes de haute responsabilité de niveau égal ou supérieur à celui de directeur de ministère, • Inspecteurs des Domaines, du Trésor, des Douanes, des Impôts et des Finances, • Inspecteurs de l'Inspection Générale de l'Etat, – Magistrats de l'ordre judiciaire, administratif et financier, – Militaires de haut rang : <ul style="list-style-type: none"> • Officiers généraux de l'armée, de la police et de la gendarmerie, • Inspecteurs de l'Inspection Générale de l'Armée et de l'Inspection Générale de la Gendarmerie Nationale, – Dirigeants d'une entreprise publique, – Responsable de parti politique, – Toutes personnes physiques ou morales qui sont clairement liées aux personnes sus-visées. Liaison : conjoint et enfants Ancienneté : 5 ans après cessation de fonction

<i>Termes</i>	<i>Définition</i>
Risque supérieur à la moyenne (art. 20)	Il appartient aux établissements assujettis de déterminer le seuil de risque supérieur à la moyenne en tenant compte de la nature et de l'importance du risque de blanchiment encouru, les antécédents des clients, leur pays d'origine ou de résidence, l'origine de leurs fonds, les liens entre les comptes, les types de transactions qu'ils effectuent sur leurs comptes bancaires ou leurs activités professionnelles.
Sampana Malagasy Iadiana amin'ny Famotsiam-bola ou SAMIFIN (art. 3, 4, 5, 6, 7, 8, 13, 16, 24, 30, 33, 38, 41, 42, 43, 45)	Service de Renseignements Financiers habilité à recevoir les DOS.
Tiers (art 11)	Toutes institutions, soumises à une réglementation et à une surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, pouvant fournir des informations ou renseignements sur la transaction.
Virement électronique (Chapitre 5)	Toute transaction par voie électronique effectuée au nom d'un donneur d'ordre (qu'il s'agisse d'une personne physique ou morale) via une institution financière en vue de mettre à disposition d'un bénéficiaire une certaine somme d'argent dans une autre institution financière. Le donneur d'ordre et le bénéficiaire peuvent être une seule et même personne.
Virement national (art. 36)	Tout virement où l'institution financière du donneur d'ordre et celle du bénéficiaire sont situées dans un même pays. Cela concerne toute chaîne de virements électroniques qui est entièrement exécutée à l'intérieur des frontières d'un même pays, même si le système utilisé pour effectuer un virement électronique est situé dans un autre pays.
Virement transfrontalier (art. 35)	Tout virement où l'institution du donneur d'ordre et celle du bénéficiaire sont situées dans des pays différents. Ce terme se réfère également à toute chaîne de virements électroniques comportant au moins un élément transfrontalier.