REPUBLIQUE DU SENEGAL

Un Peuple – Un But – Une Foi

MINISTERE DES FINANCES ET DU BUDGET

DIRECTION GÉNÉRALE DU SECTEUR FINANCIER ET DE LA COMPÉTITIVITÉ

DIRECTION DES ASSURANCES

LIGNES DIRECTRICES SUR LA LBC/FTP

Document de nature explicative

1 GLOSSAIRE

ABR : approche basée sur les risques

Dans le contexte de la LBC/FTP, une approche basée sur les risques englobe les éléments suivants :

- l'évaluation des risques que présentent les activités et les clients de votre entreprise à l'aide de certains éléments prévus par la réglementation, y compris les produits, les services, les modes de prestation et de distribution, les aspects géographiques, les clients, les relations d'affaires et d'autres facteurs pertinents ;
- l'atténuation des risques grâce à la mise en œuvre de contrôles et de mesures;
- la tenue à jour de l'information sur l'identité des clients et les relations d'affaires;
- le contrôle continu des opérations et des relations d'affaires.

ANIF : Agence Nationale d'Investigation Financière. Elle est chargée de centraliser et de traiter les déclarations de soupçon et toutes les autres informations communiquées par les assujettis, les autorités judiciaires et les autorités de contrôle dans les Etats membres de la Communauté Economique et Monétaire de l'Afrique centrale (CEMAC).

Blanchiment de capitaux : L'infraction constituée par un ou plusieurs des agissements ci-après, commis intentionnellement, à savoir :

a) La conversion, le transfert ou la manipulation de biens, dont l'auteur sait qu'ils proviennent d'un crime ou d'un délit ou d'une participation à ce crime ou délit, dans le but de dissimuler ou de déguiser l'origine illicite desdits biens ou d'aider toute personne

impliquée dans la commission de ce crime ou délit à échapper aux conséquences judiciaires de ses actes ;

b) La dissimulation, le déguisement de la nature, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété réelle de biens ou de droits y relatifs dont l'auteur sait qu'ils proviennent d'un crime ou d'un délit, tels que définis par les législations nationales des Etats membres ou d'une participation à ce crime ou délit;

c) L'acquisition, la détention ou l'utilisation de biens dont l'auteur sait au moment de la réception desdits biens, qu'ils proviennent d'un crime ou d'un délit ou d'une participation à ce crime ou délit ;

d) La participation à l'un des actes visés aux points a), b) et c), le fait de s'associer pour le commettre, de tenter de le commettre, d'aider ou d'inciter quelqu'un à le commettre ou de le conseiller à cet effet, ou de faciliter l'exécution d'un tel acte.

CENTIF : Cellule Nationale de Traitement des Informations Financières instituée dans chaque Etat membre de l'Union Economique et Monétaire Ouest Africaine (UEMOA) dont la mission est de recueillir et de traiter les renseignements financiers sur les circuits de blanchiment de capitaux et de financement du terrorisme et de la prolifération des armes de destruction massive.

CIMA ou la Conférence : Conférence Interafricaine des Marchés d'Assurances.

CRCA ou la Commission : Commission Régionale de Contrôle des Assurances.

CRF : Cellule de Renseignement Financier (CENTIF, ANIF).

Déclaration de soupçon : déclaration portant sur des activités jugées suspectes, faite auprès de l'ANIF ou de la CENTIF par le correspondant de la société ou dans des cas exceptionnels, et notamment en raison de l'urgence, par tout dirigeant ou préposé de l'Entreprise (article 21 alinéa 9 Règlement N°001/CIMA/PCMA/PCE/SG/2021 du 02 mars 2021).

Financement du terrorisme : Le financement du terrorisme est défini comme l'infraction constituée par le fait, par quelque moyen que ce soit, directement ou indirectement, délibérément, de fournir, réunir ou gérer ou de tenter de fournir, réunir ou gérer des fonds, biens, services financiers ou autres, dans l'intention de les voir utilisés, ou en sachant qu'ils seront utilisés, en tout ou partie, en vue de la commission :

a) d'un ou de plusieurs actes terroristes ;

b) d'un ou de plusieurs actes terroristes par une organisation terroriste ;

c) d'un ou de plusieurs actes, par un terroriste ou un groupe de terroristes ;

d) de tout autre acte destiné à tuer ou à blesser grièvement un civil, ou toute autre personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, lorsque, par sa nature ou son contexte, cet acte vise à intimider une population ou à contraindre un Gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque.

La tentative de commettre une infraction de financement du terrorisme ou le fait d'aider, d'inciter ou d'assister quelqu'un en vue

de la commettre, ou le fait d'en faciliter l'exécution, constitue également une infraction de financement du terrorisme.

Financement de la prolifération des armes de destruction massive: acte destiné à fournir des fonds ou des services financiers qui sont utilisés en tout ou partie pour fabriquer, se procurer, mettre au point, posséder, développer, transporter, transférer, exporter, transborder, pour le courtage, le stockage et l'utilisation des armes nucléaires, chimiques ou biologiques ou leurs vecteurs et éléments connexes, en particulier à des fins terroristes.

GABAC : Groupe d'Action contre le Blanchiment d'Argent en Afrique Centrale.

GAFI : Le Groupe d'Action Financière est un organisme intergouvernemental en charge de l'élaboration des normes et de la promotion de l'efficace application de mesures législatives, réglementaires et opérationnelles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et les autres menaces liées pour l'intégrité du système financier international.

GIABA : Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest.

Groupe Egmont : Regroupement des CRF du monde.

LBC/FTP : Lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive.

Opération atypique : opération sans relation avec l'activité, les habitudes financières ou le patrimoine de leur auteur. La loi nationale a fixé un montant en espèces supérieur à 10 millions de francs CFA. (Article 15 du Règlement N°001/CIMA/PCMA/PCE/SG/2021 du 02 mars 2021).

Opérations suspectes : les sommes inscrites dans les livres de l'assureur, du réassureur ou du courtier en assurances ou en réassurances dont ces derniers savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une activité criminelle ou ont un rapport avec une infraction de blanchiment de capitaux, de financement du terrorisme, ou de financement de la prolifération. Les tentatives d'accomplir des opérations douteuses sont également visées.

ORTG : Organe Régional de Type ou style GAFI (démembrement régional du GAFI : GIABA et GABAC).

Organisme d'assurance : société d'assurance, de réassurance et courtier d'assurance ou de réassurance.

PPE : Personnes Politiquement Exposées.

PPE étrangères : les personnes physiques qui exercent ou qui ont exercé d'importantes fonctions publiques dans un autre Etat membre ou un Etat tiers, à savoir :

a) les Chefs d'État ou de gouvernement, les Ministres, les Ministres délégués et les secrétaires d'État ;

b) Les membres de familles royales ;

c) Les Directeurs généraux des ministères ;

d) Les parlementaires ;

e) Les membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles ;

f) Les membres des cours des comptes ou des conseils ou directoires des banques centrales ;

g) Les ambassadeurs, les chargés d'affaires et les officiers supérieurs des forces armées ;

h) Les membres des organes d'administration, de direction ou de surveillance des entreprises publiques ;

i) Les hauts responsables des partis politiques ;

j) les membres de la famille d'une PPE, en l'occurrence :

- Le conjoint ;
- Tout partenaire considéré comme l'équivalent d'un conjoint ;
- Les enfants et leurs conjoints ou partenaires ;
- Les autres parents.

k) les personnes connues pour être étroitement associées à une PPE ;

l) Toute autre personne désignée par les lois et règlements pris au plan national dans les Etats membres.

- **PPE nationales** : les personnes physiques qui exercent ou qui ont exercé d'importantes fonctions publiques dans l'un des Etats membres de la CIMA notamment les personnes physiques visées au a) à j) ci-dessus.

- **PPE des organisations internationales** : les personnes qui exercent ou qui ont exercé d'importantes fonctions au sein de ou pour le compte d'une organisation internationale, notamment les membres de la haute direction, en particulier, les directeurs, les directeurs adjoints et les membres du Conseil d'Administration et toutes les personnes exerçant des fonctions équivalentes, ainsi que les membres de leur famille, en l'occurrence ceux énumérés au point j) ci-dessus.

Table des matières

Les présentes lignes directrices sont élaborées par la direction des assurances du Sénégal à la suite de l'adoption par le Conseil des ministres du règlement n°001/CIMA/PCMA/PCE/SG/2021 définissant les procédures applicables par les organismes d'assurances dans les Etats membres de la CIMA dans le cadre de la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive.

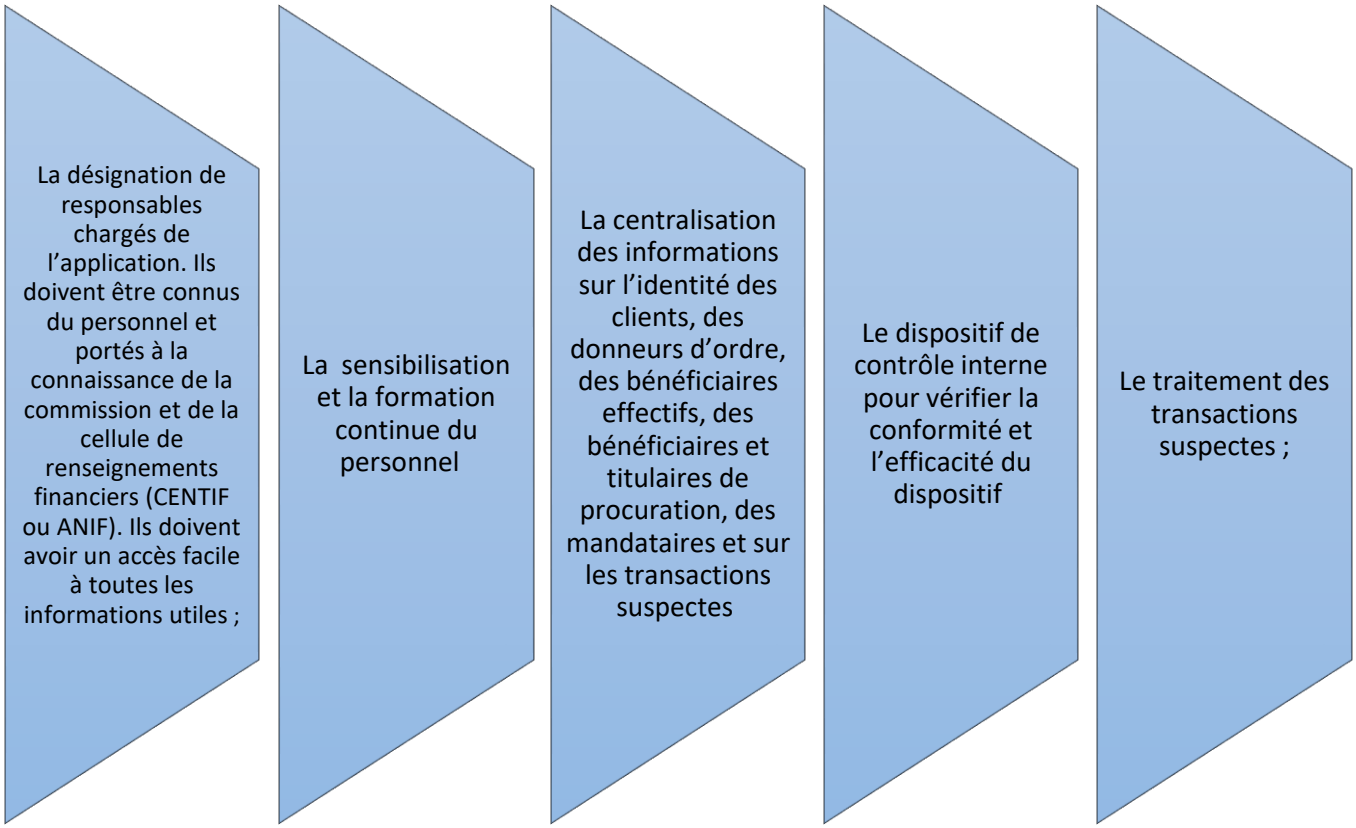
Elles présentent une analyse de la réglementation en vigueur concernant les obligations de déclaration et d'information aux CRF (CENTIF et ANIF) ainsi que leurs conséquences sur les différentes étapes du processus conduisant, le cas échéant, à une déclaration de soupçon. Il s'agit d'un document de nature explicative qui n'a pas de caractère contraignant en lui-même.

Ces lignes directrices feront l'objet de mise à jour continue afin de répondre à toute évolution notamment de la réglementation et du niveau de risques de blanchiment dans le secteur des assurances.

A. Organisation du dispositif LBC/FTP au sein de l'organisme d'assurance

L'organisme d'assurance doit mettre en place un dispositif qui doit être documenté et validé par le Conseil d'administration ou l'organe délibérant de la société.

Ce dispositif doit comprendre notamment les éléments suivants :



B. Structure interne en charge de l'application des programmes LBC/FTP

En fonction de la taille, l'organisme d'assurance peut soit :

- mettre en place une structure interne de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ;
- confier les responsabilités en matière de LBC/FTP à l'audit interne, au contrôle de gestion, à la gestion des risques ou à la fonction conformité. Cependant, il serait préférable de ne pas confier cette fonction à l'audit interne qui doit trôner sur la troisième ligne de défense de l'organisme financier.

Cette structure doit avoir une indépendance opérationnelle et ne doit pas être impliquée dans l'exécution des tâches opérationnelles notamment la gestion de la production et des prestations.

Elle doit être dotée de moyens humains et matériels pour exécuter ses missions :

- assurer la diffusion des procédures aux personnes concernées ;
- centraliser les faisceaux d'indices de soupçons identifiés par le personnel ;
- instruire en interne les dossiers de déclaration de soupçon ;
- rédiger les déclarations de soupçon et les transmettre à la CRF (CENTIF ou ANIF) ;
- répondre aux requêtes régulières ou ponctuelles de la CRCA, de la Cellule de renseignement financier ou des institutions partenaires ;
- se joindre au responsable des ressources humaines au moment du recrutement, sensibiliser et surveiller les personnels sensibles;
- participer à l'organisation des actions de formation et de sensibilisation du personnel en matière de lutte conte la LBC/FTP ;
- préparer et proposer aux organes délibérants, le rapport LBC/FTP annuel pour examen et approbation ;
- préparer et communiquer à la DA et à la CIMA, le rapport annuel LBC/FTP, le rapport d'audit du dispositif, le questionnaire LBC/FTP et le rapport de contrôle interne avant le 01 juin de l'exercice N+1 ;

- communiquer régulièrement au personnel placé au-devant de la lutte (front office : commerciaux, producteurs, régleurs de sinistres) la liste des personnes black listées et des personnes visées par des mesures de gel des avoirs ;
- procéder à une veille réglementaire ;
- pendre en charge toutes autres diligences dans le cadre du dispositif interne de prévention et de détection du blanchiment de capitaux, du financement du terrorisme et de la prolifération des armes de destruction massive.

C. Identification et connaissance de la clientèle

1. Mise en œuvre d'une approche fondée sur les risques

L'objectif est d'adapter les mesures de vigilance au profil de risque de son client aussi bien à l'entrée qu'en cours de contrat.

Dès qu'il y'a relation d'affaires c'est-à-dire contrat d'assurance, l'assureur ou le courtier doit être en mesure d'apprécier le niveau de risque de LBC/FTP en utilisant une approche par les risques conformément à l'article 4 du règlement.

L'évaluation des risques pourra prendre en compte les éléments suivants :

Client	Contrat	Nature des opérations	Profil de risque (faible, moyen et élevé)	Niveau de vigilance (allégé, standard et renforcé)

12 Par rapport à chaque critère : client, contrat et opérations, l'évaluation pourra être menée comme suit :

- Client

Critère de classification	Facteurs de risque	Coefficient de pondération	Risque faible Score 20%	Risque moyen Score 50%	Risque élevé Score 80%	Profil de risque (faible, moyen et élevé)
CLIENT	Type					
	Souscripteur					
	Activité					
	Régime juridique pour les personnes morales					
	PPE					
	Personne en relation avec une PPE					
	Résidence y compris fiscal					
	Nationalité (vérifier si ressortissant d'un pays représentant un risque élevé (Pays inscrits sur la liste noire ou grise du GAFI, pays mal réputé)					
	Assuré (Age, nature relation avec le souscripteur, le bénéficiaire)					

13

➢ Contrat

Critère de classification	Facteurs de risque	Coefficient de pondération	Risque faible Score 20%	Risque moyen Score 50%	Risque élevé Score 80%	Profil de risque (faible, moyen et élevé)
CONTRAT	Objet					
	Montant de la prime					
	Périodicité des cotisations					
	Caractéristiques du contrat					
	Contrat collectif ou non					
	Anonymat du souscripteur ou des bénéficiaires					
	Processus de souscription					
	Mode de distribution					

➢ Nature des opérations

Critère de classification	Facteurs de risque	Coefficient de pondération	Risque faible Score 20%	Risque moyen Score 50%	Risque élevé Score 80%	Profil de risque (faible, moyen et élevé)
CONTRAT NATURE DES OPERATIONS	Renonciation					
	Rachat/avance					
	Nantissement					
	Versement exceptionnel					
	Origine géographique des fonds					
	Destination géographique des fonds					
	Moyens de paiement					
	Motif de l'opération					

Chaque relation d'affaires est analysée et évaluée par rapport à son exposition au risque de LBC/FTP en tenant compte des facteurs ci-dessus qui sont donnés à titre indicatif. Ainsi, chaque organisme d'assurance pourra approfondir son évaluation en considérant d'autres facteurs de risques qu'il estime pertinent.

Dans la pratique, il sera difficile voire impossible de faire une évaluation contrat par contrat. C'est pourquoi, les organismes

d'assurances doivent disposer d'un système d'information qui permet de faire :

- le profilage des clients en fonction des produits d'assurances souscrits ;
- le filtrage en temps réel des clients et des opérations réalisées auprès de l'entreprise ou de l'organisme d'assurance depuis le début de la relation d'affaires ;
- le suivi des opérations des clients par dates, montants, origine, cumul des opérations réalisées par un même client. Ce suivi doit permettre la génération des alertes ;
- la détermination du montant global de l'ensemble des capitaux en risque pour un même client ;
- le recensement des opérations par un même client, qu'il soit occasionnel ou habituel ;
- l'identification des opérations à caractère suspect ou inhabituel ;
- le recensement des clients ayant réalisé dans l'année des paiements, des rachats ou remboursements pour un montant supérieur au minimum fixé par la réglementation en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ou à défaut par les dispositions nationales (10 millions de FCFA pour les paiements en espèces) ;
- le suivi particulier des comptes bancaires ou postaux de la société qui centralise les arrivées de fonds.

Le système d'information doit faire l'objet d'un examen périodique de son efficacité, au moins une fois par an, en vue de l'adapter en fonction de la nature et de l'évolution de l'activité de l'entreprise ou

de l'organisme d'assurance assujetti ainsi que l'environnement légal et réglementaire.

Il convient de signaler que cette évaluation devra être mise à jour régulièrement.

2. Niveau de vigilance

La vigilance correspond à l'ensemble des diligences que l'organisme d'assurance entreprend pour connaitre sa relation d'affaires. A chaque niveau de vigilance correspond un niveau de risque propre à la relation d'affaires :

Vigilance simplifiée	Vigilance standard	Vigilance renforcée
Continue sur les opérations	Connaissance de la relation d'affaires	Approbation des dirigeants

3. Vérification de l'identité

Des informations doivent être recueillies par l'organisme d'assurance selon que la relation d'affaires est une personne physique ou morale :

❖ Cas de la personne physique

Personnes physiques	Diligences à effectuer
Personnes physiques	Relever l'identité de tous les cocontractants (nom, prénoms, date et lieu de naissance, nationalité) quels que soient les montants versés. Doivent être considérés comme cocontractants les personnes suivantes : le souscripteur, le donneur d'ordre, le ou les mandants, toute personne payant une prime. Lorsque le souscripteur est différent de l'assuré, la compagnie d'assurance peut aussi relever l'identité de ce dernier si elle le juge nécessaire. Pour chacun des cocontractants, demander une pièce d'identité probante, en prendre une photocopie et faire

	les vérifications nécessaires : examiner le document (recto verso pour la carte d'identité) afin de juger de son authenticité (attention aux éventuels gommages, grattages, surcharges, anomalies dans la jonction entre la photocopie et la pièce d'identité…) ; comparer la personne avec sa photographie (attention aux permis de conduire, souvent anciens) ; comparer la personne avec sa description : sexe, âge, etc. ; avoir un soupçon si le document paraît douteux, ou la photo non ressemblante (si nécessaire, procéder à une vérification à partir d'un annuaire, de quittances, etc.) ; comparer la signature avec celle relevée sur le chèque ou sur tout autre document contractuel ou précontractuel signé par la personne.

❖ Cas de la personne morale

Personnes morales	Diligences à effectuer
Personnes morales ayant leur siège dans l'espace CIMA	1) Sauf en matière d'assurance collective, les souscriptions faites par des personnes morales sont a priori suspectes. 2) D'une manière générale, relever : a) le nom ou la raison sociale ; b) la forme sociale ; c) l'objet social ; d) les noms des dirigeants (Président, administrateurs, principaux directeurs) ; e) des renseignements sur les personnes qui détiennent ou qui contrôlent l'entreprise. 3) Demander, examiner et prendre copie des documents suivants :

	a) une pièce d'identité des dirigeants ; b) une pièce d'identité des représentants des personnes morales, avec leur pouvoir ; c) les décisions ayant désigné les mandataires légaux et défini les pouvoirs des autres mandataires ; d) les statuts certifiés conformes notamment pour les associations; e) l'original, l'expédition ou la copie certifiée conforme de moins de trois mois de tout acte ou extrait d'un registre officiel (registre du commerce et des sociétés, ou répertoire des métiers pour les artisans) constatant la dénomination, la forme juridique et le siège social); f) un extrait du registre du commerce et du crédit mobilier de moins de trois mois.
Personnes morales étrangères	Sauf en matière d'assurances collectives, les souscriptions faites par des personnes morales provenant de certains pays étrangers sont a priori suspectes. 1) D'une manière générale, relever : a) le nom ou la raison sociale ; b) la forme sociale ; c) l'objet social ; d) les noms des dirigeants (Président,

	administrateurs, principaux directeurs) ; e) des renseignements sur les personnes qui détiennent ou qui contrôlent l'entreprise. 2) Demander, examiner et prendre copie des documents relatifs à l'entreprise ou à ses dirigeants dans la mesure où ils présentent un niveau d'équivalence avec les documents exigés des entreprises ayant leur activité en zone OHADA, et par exemple : a) un certificat de validité juridique avec une traduction authentique ; b) certificate of incorporation ; c) the name(s) and adress(es) of the beneficial owner(s) ; d) memorandum and articles of Association ; e) a signed director's statement as to the nature of the company's business. 3) Lorsqu'il s'agit d'un trustee agissant pour le compte d'un trust, demander, examiner et prendre copie des documents suivants : a) l'identité du settlor ; b) le trust deed ou la letter of wishes pour vérifier si le trustee a bien les pouvoirs de souscrire un contrat d'assurance). 4) Lorsqu'il s'agit d'une fondation, demander, examiner et prendre copie des documents suivants :

a) l'identité du fondateur ;

b) le règlement de fondation ;

c) tout autre document nécessaire pour identifier le trust, le trustee et les bénéficiaires du trust.

5) Lorsqu'il s'agit d'un des cas particuliers listés ci-après, obtenir l'identité du bénéficiaire économique. En cas de refus, faire obligatoirement une déclaration de soupçon à la Cellule de Renseignements Financiers. Liste non exhaustive de ces cas particuliers :

a) International Business Company (Jersey, Guernesey, Ile de man, Bahamas, Barbade, Iles Vierges britanniques) ;

b) Exempt company (Jersey, Guernesey, Ile de Man, Gibraltar) ;

c) Qualifying company (Bermudes, Iles Cayman) ;

d) Aruba vrijgestelde vennootschap (ou AVV) ;

e) ou d'une quelconque forme de holding anonyme (Anstalt du Liechtenstein, holding luxembourgeoise ou suisse, Soparfi luxembourgeoise, société civile monégasque, etc.).

6) Lorsqu'il s'agit d'entreprises d'assurance situées à l'étranger

Concernant les affaires reçues en acceptation provenant d'entreprises situées hors de la zone

	CIMA, les entreprises et organismes d'assurance doivent, en plus des mesures de vigilance normale : a) identifier et vérifier l'identification de l'entreprise d'assurance étrangère ; b) recueillir des informations sur la nature des activités de l'entreprise d'assurance étrangère ; c) évaluer la réputation de l'entreprise d'assurance étrangère et le degré de surveillance à laquelle elle est soumise, sur la base d'informations publiquement disponibles ; d) évaluer les contrôles mis en place par l'entreprise d'assurance étrangère pour lutter contre le blanchiment de capitaux, le financement du terrorisme et la prolifération ; e) les responsables habilités des entreprises assujetties doivent avoir préalablement autorisé la conclusion d'une relation avec l'entreprise d'assurance étrangère.

❖ Cas d'une personne physique ou morale pour le compte d'un tiers

Opérations réalisées par une personne physique ou morale pour le compte d'un tiers	Diligences à effectuer
Opérations réalisées par une personne physique ou morale pour le compte d'un tiers	Lorsqu'une opération paraît être réalisée pour le compte d'un tiers, l'entreprise d'assurance doit se renseigner sur l'identité véritable de ce tiers. Si les renseignements obtenus ne lui permettent pas d'avoir une certitude sur l'identité des personnes au bénéfice desquelles l'opération est réalisée, l'entreprise d'assurance devra obligatoirement faire une déclaration de soupçon à la Cellule de Renseignements Financiers, indépendamment de sa faculté propre de refuser l'opération.

❖ Cas de la personne politiquement exposée

Personnes Politiquement Exposées	Diligences à effectuer
Personnes Politiquement Exposées (PPE)	Les entreprises et organismes d'assurance doivent, en plus des mesures de vigilance normales, prendre les mesures spécifiques ci-après, lorsqu'elles nouent des relations d'affaires ou lorsqu'elles effectuent des transactions avec ou pour le

compte de PPE nationales, étrangères ou des organisations internationales au sens de l'article 2 du présent règlement :

1° mettre en œuvre des procédures adéquates et adaptées, en fonction du risque, de manière à pouvoir déterminer si le client ou un bénéficiaire effectif du client est une PPE ;

2° obtenir l'autorisation de la Direction générale ou d'un organe hiérarchique équivalent avant de nouer une relation d'affaires avec de tels clients ;

3° prendre toute mesure appropriée, en fonction du risque, pour établir l'origine du patrimoine et l'origine des fonds impliqués dans la relation d'affaires ou la transaction ;

4° assurer une surveillance continue renforcée de la relation d'affaires. Les mesures visées ci-dessus, aux points 2, 3 et 4 ne sont appliquées pour les PPE nationales ou les PPE des organisations internationales qu'en cas de relations d'affaires à risque plus élevé. Sous réserve de l'application de mesures de vigilance renforcées, en fonction d'une appréciation du risque lié à la clientèle, les entreprises et organismes d'assurance ne sont pas tenues de considérer comme politiquement exposée, une

	personne qui n'a pas occupé de fonction publique importante, au sens des alinéas premier et 2 ci-dessus, pendant une période d'au moins six mois.

❖ **Cas de la vente à distance**

Vente à distance	Diligences à effectuer
Vente à distance (par correspondance, téléphone, Internet).	1° Demander copie d'une pièce d'identité et d'une quittance de moins de trois mois attestant d'un domicile. 2° Demander un R.I.B. et vérifier la correspondance entre le chèque et le R.I.B. 3° Envoyer le contrat par lettre recommandée avec accusé de réception en vérifiant la cohérence de l'adresse. 4° Avoir un soupçon en cas d'incohérence, ou en cas de virement d'argent en provenance de l'étranger. Ce soupçon doit être aggravé s'il y a plusieurs anomalies. 5° Si le paiement arrive avant les pièces, ne pas ristourner tant que ces pièces n'ont pas été reçues.

❖ **Résidences**

Résidences (y compris fiscale)	En cas de doute, réclamer une facture d'eau d'électricité ou une autre quittance de moins de trois mois, ou procéder à une vérification à partir d'un annuaire, ou par tout autre moyen. Le soupçon doit être aggravé dans les cas suivants : a) il n'y a pas d'explication convaincante pour une domiciliation anormale (boîte postale, chez un tiers, société de domiciliation) ; b) la résidence physique est dans un pays différent de la résidence fiscale ; c) les contrats sont souscrits auprès d'intermédiaires dans le ressort desquels la personne n'a ni son siège, ni une activité significative ; d) pour certaines personnes morales présentant un profil particulier (sociétés de domiciliation, trusts, fiducies, fondations, Anstalt du Liechtenstein, sociétés domiciliées dans des paradis fiscaux ou sans objet social défini, etc.).

❖ **Profession**

Profession du client.	Diligences à effectuer
Profession du client.	1) Ne pas se contenter de mentions vagues telles que commerçant, dirigeant d'entreprise ou homme d'affaires. Se renseigner sur les affaires du client, dans quel secteur il opère, pour ou avec quelles entreprises, etc. 2) Evaluer le patrimoine et le train de vie du client. 3) Déterminer quels sont les objectifs de l'opération. 4) D'une manière générale, le client n'est pas forcé de répondre, mais l'entreprise ou l'organisme assujetti (ou ses mandants) ne devrait pas garder les soupçons pour elle. Il doit y avoir obligatoirement soupçon dans les cas suivants (liste non exhaustive) : a) le client refuse de répondre aux questions les plus générales ; b) les montants sont sans rapport avec l'activité ou les ressources du client ; c) le client insiste sur le fait qu'il s'agit

	d'une opération de « maximisation fiscale » ou « d'optimisation fiscale » (de tels objectifs avoués peuvent en cacher d'autres moins avouables) ; d) le client est très préoccupé par son droit à résilier rapidement le contrat et par le montant qu'il pourra récupérer ; e) le client ne se préoccupe pas de la rentabilité de son placement (notamment pour les bons de capitalisation anonymes). Un modèle de fiche d'identification est proposé en annexe à titre indicatif. Les informations recueillies ci-dessus sont mises à jour à la date d'anniversaire du contrat et analysées pour s'assurer qu'elles restent pertinentes pour favoriser une connaissance appropriée de la clientèle.

4. Personnes ayant fait l'objet de sanctions (conseil de sécurité des Nations Unies, Union Européenne par exemple)

Les organismes d'assurance sont tenus de mettre en place des mesures adéquates leur permettant au moins de :

– disposer des listes de personnes faisant l'objet de sanctions financières ciblées et de leurs mises à jour régulières ;

- disposer d'un outil informatique spécifique pour pouvoir accéder et exploiter ces listes de sanction de façon continue ;
- établir un filtrage ponctuel du client et de ses bénéficiaires effectifs au niveau des listes de sanctions. Si le résultat de l'opération de filtrage est positif alors l'organisme d'assurance doit mettre fin à cette relation d'affaires et informer la CENTIF ;
- établir et maintenir un filtrage massif régulier de tout le portefeuille afin d'identifier des clients qui ont été sanctionnés après l'entrée en relation ;
- vérifier au moment du paiement des sinistres que les clients et bénéficiaires effectifs des opérations d'assurance ne figurent pas parmi ces listes ;
- être en mesure de bloquer toute opération dont le souscripteur, l'assuré, le bénéficiaire ou le bénéficiaire effectif a figuré sur ces listes ou entretient des liens avec lesdites personnes.

5. Conservation des documents

Les documents sont archivés sur une période de 10 ans.

6. Mesures de vigilance propres aux sociétés de réassurance

Les organismes de réassurance doivent adopter une approche par les risques propres aux sociétés d'assurances partenaires :

- Filtrage des bénéficiaires effectifs des sociétés d'assurances partenaires ;
- Pays de résidence des sociétés d'assurances partenaires ;
- Nature de la convention adoptée (traité ou facultative) ;

- Niveau de conformité de la société d'assurance partenaire (existence ou non d'un dispositif LBC/FTP informatisé) ;
- Volume transactionnel annuel, etc.

D. Procédures internes de prévention

Les organismes d'assurances doivent se doter de procédures écrites de maitrise du risque de LBC/FTP. Ces procédures doivent prendre en compte les diligences à accomplir et les règles à respecter en matière :

- d'identification et de connaissance de la clientèle et le cas échéant du bénéficiaire effectif ;
- de constitution, de suivi et d'actualisation des dossiers de la clientèle ;
- de fixation de délais pour la vérification ;
- de l'identité des clients et la mise à jour des informations y afférentes afin de conserver une connaissance adéquate de ceux-ci et le cas échéant des bénéficiaires effectifs ;
- d'enregistrement, d'archivage et de conservation des pièces et documents relatifs à l'identité des clients selon les modalités propres à en assurer la confidentialité et la disponibilité ;
- de constitution et de conservation de bases de données relatives aux opérations des clients, recueillies dans le cadre des obligations de vigilance ;
- de surveillance et d'examen des opérations et des transactions inhabituelles ;
- d'identification et de suivi des opérations concernant des personnes politiquement exposées aux risques de blanchiment

de capitaux et de financement du terrorisme et de la prolifération ;

- d'analyse informatisée et de détection des opérations susceptibles de faire l'objet d'une déclaration de soupçon à la CENTIF ;
- de suivi des opérations exécutées par internet et autres supports électroniques ;
- d'élaboration d'une cartographie et d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme et de la prolifération ;
- de traitement de demandes de la CENTIF ainsi que des autorités d'enquêtes et de poursuites ;
- d'identification, d'évaluation et d'approbation préalable de tous nouveaux produits, politiques commerciales, services, ou application informatiques par rapport aux risques de blanchiment de capitaux et de financement du terrorisme et de la prolifération, etc. (Cf. article 6 du nouveau règlement).

E. Recrutement et surveillance des personnels sensibles

Les entreprises d'assurance doivent mettre en œuvre des procédures appropriées lors de l'embauche des employés, notamment le personnel jugé sensible pour s'assurer qu'elle s'effectue selon des critères exigeants.

Elles doivent en outre maintenir une surveillance ultérieure des personnels sensibles notamment des procédures d'échanges entre le responsable des ressources humaines et le correspondant.

F. Formation et information du personnel

Les entreprises et organismes d'assurance doivent :

- mettre en place, au profit de leur personnel un programme de formation et de sensibilisation en matière de LBC/FTP. Cette formation peut être interne ou externe et doit concerner les anciens comme les nouveaux ;
- tenir des réunions d'information pour les employés afin de les tenir au courant des évolutions quant aux techniques, et tendances de blanchiment et de financement du terrorisme ainsi qu'aux règles préventives à respecter en la matière ;
- diffuser une documentation relative à la LBC/FTP.

G. Recours à des tiers

Les entreprises et organismes d'assurance doivent s'assurer, avant de recourir à des tiers dans le cadre de la souscription d'affaires (courtier d'assurance ou de réassurance, coassureur, réassureur, institution de micro finance, banque, ou des relations similaires), que ces derniers sont soumis au contrôle d'une autorité.

Ils doivent réclamer un document par lequel le tiers déclare :

- avoir pris connaissance des lois et règlements relatifs à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération et s'engage à s'y conformer ;
- respecter toutes les procédures exigées par l'entreprise ou l'organisme d'assurance ;
- accepter toute inspection sur place diligentée par l'organisme d'assurance.

Les entreprises et organismes d'assurance tiennent un dossier de suivi concernant les tiers mentionnés ci-dessus, où seront notées toutes les anomalies constatées.

H. Déclarations de soupçon

Le Responsable interne chargé de l'application des programmes de lutte contre le blanchiment doit procéder aux déclarations de soupçon nécessaires à destination de la CENTIF. Il est tenu de transmettre à la CENTIF les dossiers et les informations ayant fait l'objet d'une véritable analyse et d'un travail de réflexion effectif en faisant apparaître cette analyse et ce travail dans la déclaration.

Les opérations déclarées ne doivent en aucun cas être divulguées (confidentialité absolue)

Un registre des signalements (déclarés ou non) doit être ouvert. Ce registre doit être présenté à l'occasion des missions de contrôle.

L'absence de poursuites civiles ou pénales à l'encontre des personnes physiques ou morales ayant réalisé des opérations donnant lieu à soupçon ne s'applique que si la déclaration de soupçon a été effectuée de bonne foi.

Cette déclaration de soupçon est dématérialisée. Chaque correspondant aura accès à la plateforme mise en place par la CENTIF pour faire ses déclarations de soupçon. Il pourra également créer des sous comptes pour certains de ses collaborateurs mais sera seul autorisé à déclarer à la CENTIF.

I. Statistiques et indicateurs

Les organismes d'assurances doivent tenir des statistiques se rapportant à la mise en œuvre du dispositif : nombre de formation interne et externe, de réunions d'informations, de diffusion périodique d'une documentation relative à la LBC/FTP, de déclarations de soupçon adressées au responsable, de déclarations de soupçon adressées par le responsable à la CENTIF, état des alertes, état des déclarations de soupçon, etc.

J. Audit du dispositif

Les sociétés d'assurance doivent assurer un contrôle de la bonne application des programmes et procédures internes relatifs à la LBC/FTP.

Il est procédé au moins **une fois par an à un audit central et des audits décentralisés** sur chacun des sites (directions régionales, agences, succursales, filiales, etc.).

Le rapport d'audit doit être soumis au conseil d'administration (organe délibérant équivalent) qui prend les mesures nécessaires pour le suivi.

Par ailleurs, elles élaborent un rapport annuel (canevas bien défini) sur la mise en œuvre de l'ensemble de leur dispositif interne de lutte contre la LBC/FTP. Ce rapport approuvé par le conseil d'administration est transmis au Ministre en charge des assurances et à la CRCA.

ANNEXES

- Exemple de canevas de procédures internes (Fiche 1)
- Exemple de canevas de rapport d'audit (Fiche 2)
- Exemple de canevas de rapport annuel (Fiche 3)
- Exemple de cycle de l'approche basé sur les risques (Fiche 4)
- Résultats de l'évaluation des risques du secteur des assurances mis à jour en 2022 (Fiche 5)
- Liens utiles (Fiche 6)

<u>Fiche 1</u> : Exemple de canevas pour l'élaboration d'un manuel de procédures LBC/FTP :

I. Définitions et lexique
II. Rappel du cadre législatif et réglementaire
   A. Le règlement CIMA
   B. La loi nationale de 2018
III. Information et formation du personnel
IV. Identification et connaissance de la clientèle
V. Analyse informatisée des opérations
VI. Enregistrement et l'archivage des documents
VII. Contrôles et audit du dispositif
VIII. Sanctions prévues

Fiche 2 : Exemple de canevas de rapport d'audit

1. Le correspondant : Rattachement, formation et expérience
2. La cartographie des risques BC/FTP
3. Les procédures écrites LBC/FTP
4. La formation du personnel interne et externe (formation initiale et d'actualisation)
5. Les relations avec les tiers (intermédiaires d'assurances, coassureurs, réassureurs)
6. La surveillance du personnel
7. Les mesures préventives de contrôle des personnes et des opérations
    a) Les mesures préventives de contrôle des personnes
    b) Les mesures préventives de contrôle des opérations
8. Le Système d'alerte et de détection des opérations suspectes
9. La déclaration de soupçon
10. L'archivage des documents
11. Le contrôle de l'efficacité du dispositif
    a) Le contrôle interne
    b) L'audit interne et le suivi des recommandations

Fiche 3 : **Exemple de canevas de rapport annuel**

Les entreprises et organismes d'assurance assujettis élaborent un rapport annuel sur la mise en œuvre de l'ensemble de leur dispositif interne de lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération.

Ce rapport doit notamment :

1) décrire l'organisation et les moyens de l'entité en matière de prévention et de lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération ;
2) relater les actions de formation et de sensibilisation menées ;
3) inventorier les contrôles effectués pour s'assurer de la bonne mise en œuvre et du respect des procédures d'identification de la clientèle, de conservation des données, de détection et de déclaration de transaction suspectes ;
4) faire ressortir les résultats des investigations, notamment en ce qui concerne les faiblesses relevées dans les procédures et dans leur respect, ainsi que les statistiques se rapportant à la mise en œuvre du dispositif de déclaration de soupçon ;
5) relater le nombre de déclarations de soupçons adressées par le personnel au responsable interne chargé de l'application des programmes de LBC/FTP et le nombre de déclarations transmises par ce dernier à la Cellule de Renseignements Financiers ;
6) signaler, le cas échéant, la nature des informations transmises à des institutions tierces, y compris celles établies à l'extérieur du pays d'implantation ;

7) dresser une cartographie des opérations suspectes les plus courantes, en indiquant les évolutions observées ;
8) rendre compte des difficultés de mise en œuvre du dispositif LBC/FTP ;
9) présenter les perspectives et le programme d'actions pour l'année à venir.

Fiche 4 : Cycle approche basée sur les risques

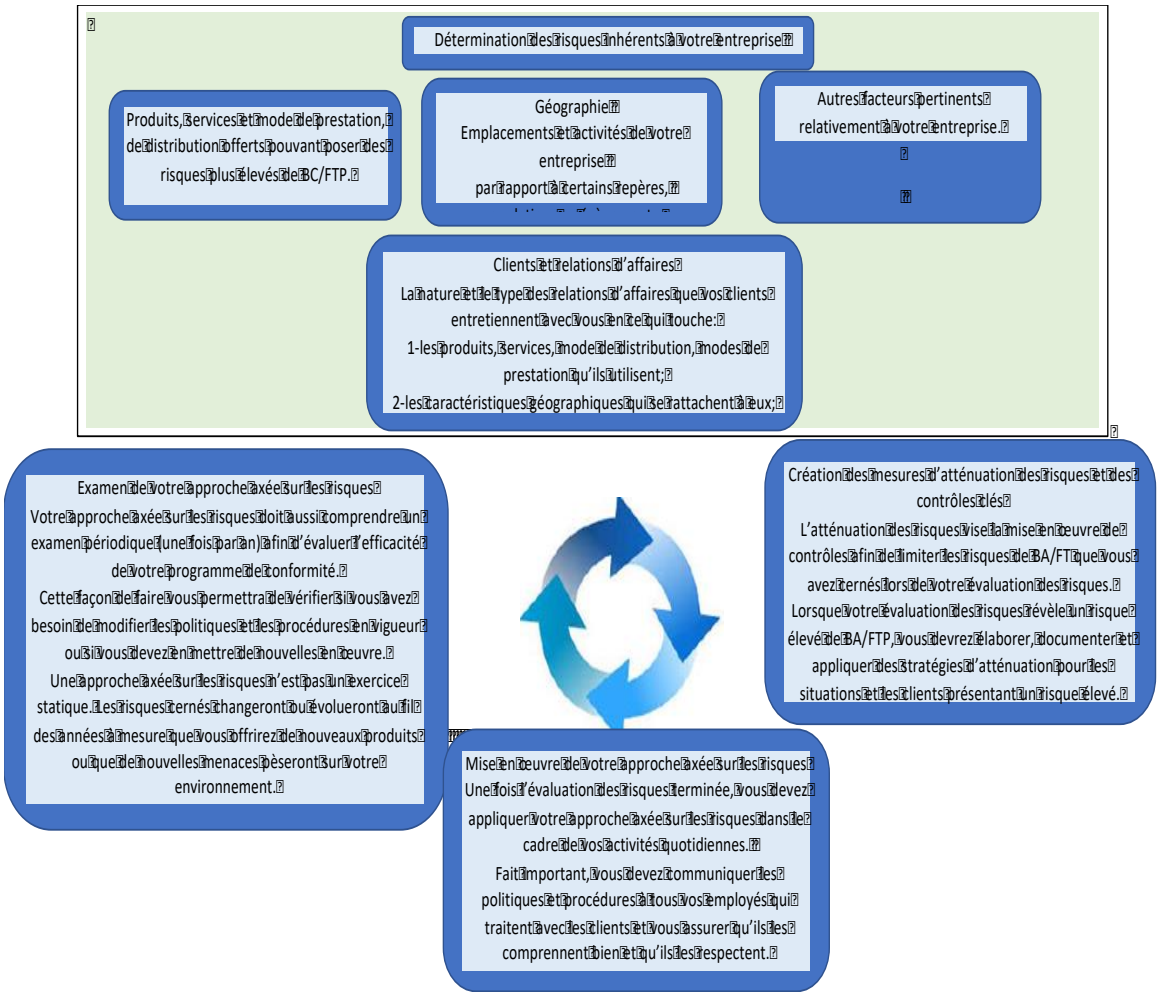
Le cycle suivant représente les principales étapes de votre approche axée sur les risques :

1. détermination des risques inhérents à votre entreprise;

2. création de mesures d'atténuation des risques et de contrôles clés;

3. mise en œuvre de votre approche axée sur les risques;

4. examen de votre approche axée sur les risques.



<u>Fiche 5</u> : Résultats de l'évaluation des risques de LBC/FTP du secteur des assurances en 2022

C'est le point de départ de toute cartographie des risques d'une compagnie d'assurance. Les résultats de l'évaluation des risques de BC/FTP se présentent comme suit :

1. Le sous-secteur de l'assurance vie :

Le croisement des menaces et vulnérabilités résiduelles après mesures d'atténuation, conduit à un niveau de risque modéré pour le secteur de l'assurance-vie.

A l'issue d'une évaluation du secteur conduite en avril 2022, les risques sur les produits d'assurance-vie se présentent ainsi :

Produits	Evaluation
Bons de capitalisation	moyennement bas
Produits de protection pure	moyennement bas
Assurances en cas de vie : épargne	moyennement bas
Assurances mixtes	moyennement bas
Autres produits	moyennement bas
Pays à risque	

Affaires situées hors Sénégal	moyennement bas
Coassurance Sénégal	moyennement bas
Coassurance communautaire	moyennement bas
Réassurance : acceptation	bas

Echelle d'évaluation 1 : pas analysé ; 2 : bas ; 3 : moyennement bas ; 4 : moyen ; 5 : moyennement élevé ; 6 : élevé.

Cotation du risque pour le secteur de l'assurance-vie

2. Le sous-secteur de l'assurance non vie :

L'assurance non-vie présente en matière de BC-FTP peu de menaces. L'objet du contrat d'assurance est de se prémunir contre un risque, le paiement des primes d'assurance correspondant au prix de ce risque.

Néanmoins, le marché des véhicules, notamment des véhicules d'occasion, peut présenter des risques de blanchiment ou de financement du terrorisme (opérations répétées d'achat/revente afin d'écouler des espèces, fraude aux assurances, cavalerie, trafic de véhicules et exportation vers des pays à risque). Les contrats

d'assurance automobile obligatoires constituent un moyen de surveiller ce secteur d'activité. Au global, la menace est considérée comme faible.

Les contrats d'assurance non-vie sont majoritairement des produits grand-public qui présentent de faibles vulnérabilités, notamment parce qu'ils ne véhiculent pas d'épargne. Toutefois, les personnes dont les avoirs sont gelés sont plus susceptibles de détenir des produits non-vie que de détenir des produits vie.

Au global, la vulnérabilité intrinsèque est donc faible.

Lors de l'évaluation d'avril 2022 du secteur, les risques associés aux produits non-vie ont été mesurés comme suit :

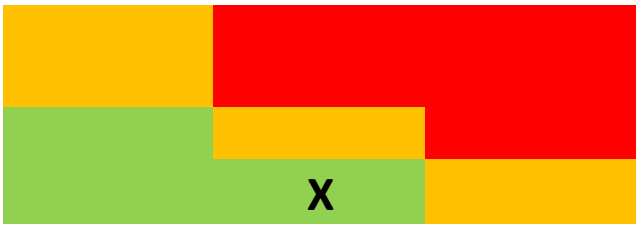
Produits	Evaluation des risques
Risque produits	
Incendie	Moyennement bas
Vol	Moyennement bas
Dégâts des eaux	Moyennement bas
Bris de glaces	Moyennement bas
Automobile	Moyennement bas
Responsabilité civile générale	Moyennement bas
Bris de machines	Moyennement bas
Tous risques informatiques	Moyennement bas

Assurance construction	Moyennement bas
Assurance maladie	Moyennement bas
Individuel accident	Moyennement bas
Assurance-crédit	Moyennement bas
Assurance caution	Moyennement bas
Assurance agricole	Moyennement bas
Marchandises Transportées quel que soit le moyen de transport	Moyennement bas
Corps de véhicules maritimes, lacustres et fluviaux	Moyennement bas
Corps de véhicules aériens	bas
Assistance	bas
Autres produits	bas
Risque géographique	
Pays à risque	
Affaires situées hors Sénégal	Moyennement bas
Coassurance Sénégal	bas
Coassurance communautaire	bas
Réassurance : acceptation	Pas analysé

Echelle d'évaluation 1 : pas analysé ; 2 : bas ; 3 : moyennement bas ; 4 : moyen ; 5 : moyennement élevé ; 6 : élevé.

En conséquence, le croisement des menaces et vulnérabilités résiduelles, après mesures d'atténuation, conduit en matière de blanchiment de capitaux et de financement du terrorisme à un risque modéré pour l'assurance-vie et faible pour l'assurance non-vie.

MENACE



VULNERABILITES

Légende

Niveau de risque

élevé
modéré
faible

Cotation du risque pour l'assurance non-vie

Fiche 6 : Liens utiles

1. CENTIF

www.centif.sn

2. GAFI

www.fatf-gafi.org

3. GIABA

www.giaba.org

4. CIMA

www.cima-afrique.org

5. DIRECTION DES ASSURANCES DU SENEGAL

www.dna.finances.gouv.sn