



Banque de la République d'Haïti
CIRCULAIRE
No 100-4

AUX BANQUES

La présente circulaire détermine les mesures que les banques doivent prendre dans le cadre de la mise en œuvre de leur programme de prévention du blanchiment de capitaux, du financement du terrorisme et de la prolifération des armes de destruction massive, ce conformément aux articles 31, 32 et 34 du décret du 30 avril 2023.

Du programme de prévention du blanchiment de capitaux, du financement du terrorisme et de la prolifération

Le programme de prévention doit refléter la nature, l'ampleur et la complexité des activités de l'institution concernée et doit comprendre les éléments suivants :

1. des politiques, des procédures et des contrôles internes, y compris des dispositifs de contrôle de la conformité, et des procédures appropriées lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants ;
2. la centralisation des informations sur l'identité des clients, des donneurs d'ordre, des bénéficiaires effectifs, des bénéficiaires et titulaires de procuration, les mandataires et sur les transactions suspectes ;
3. la désignation d'un officier de conformité et la désignation de responsables de conformité au niveau de l'administration centrale, de chaque succursale et de chaque agence ;
4. l'évaluation des risques de l'institution ;
5. l'élaboration d'un programme de formation continue à l'intention des employés ;
6. un dispositif de contrôle interne pour vérifier la conformité, l'observance et l'efficacité des mesures adoptées ;
7. la mise en place d'un dispositif de tests indépendants du contrôle de la conformité à la lutte anti-blanchiment ;
8. le traitement des opérations suspectes

Le programme de prévention doit être approuvé par le conseil d'administration de la banque.

1. Politiques, procédures et méthodes

Les banques sont tenues d'élaborer un programme de prévention comprenant des politiques, procédures et méthodes consignées par écrit et permettant d'identifier les facteurs de risques et d'évaluer les risques de blanchiment de capitaux et de financement des activités terroristes que présentent leurs activités.

Les politiques, procédures et méthodes doivent être approuvées par le conseil d'administration et tenues à jour. Elles doivent être clairement communiquées à tous les cadres appelés à traiter avec des clients.

Les politiques et procédures doivent couvrir toutes les obligations de déclaration, de tenue de documents, de conservation de documents, d'identification des clients, de contrôle, d'évaluation et d'atténuation des risques qui s'appliquent à la banque. Elles doivent être intégrées à la stratégie globale de gestion des risques de la banque et comporter des étapes appropriées pour prévenir, détecter, évaluer, surveiller, gérer, atténuer en permanence les risques de blanchiment de capitaux et de financement du terrorisme liés aux clients, pays ou zones géographiques, ou encore aux produits, services, nouvelles technologies, opérations et canaux de distribution.

Les politiques et procédures doivent également couvrir le traitement des sanctions internationales (liste de l'Organisation des Nations Unies ou autres), les modalités de gel des avoirs dans le cadre de lutte contre le financement du terrorisme et de la prolifération.

Les politiques, procédures et méthodes doivent s'appliquer à toutes les succursales et les filiales, s'il s'agit d'un groupe tel que défini à l'article 13 de la loi du 14 mai 2012 sur les banques et autres institutions financières. Dans ce cas, les banques doivent inclure des politiques et des procédures de partage des informations au sein du groupe aux fins du devoir de vigilance relatif à la clientèle et de gestion du risque de blanchiment de capitaux, de financement du terrorisme et de la prolifération. Des garanties adéquates en matière de confidentialité et d'utilisation des informations échangées doivent être mises en place. Elles doivent s'assurer de la mise à disposition des informations relatives aux clients, aux comptes et aux opérations provenant de leurs succursales et de leurs filiales aux fonctions de conformité, d'audit et/ou de la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération au niveau du groupe. En outre, les banques doivent veiller à ce que leurs filiales à l'étranger, le cas échéant, et qui exercent les mêmes activités qu'elles-mêmes, mettent en application le programme de prévention du blanchiment de capitaux, du financement du terrorisme et de la prolifération du groupe y compris les politiques et procédures de partage des informations au sein du groupe.

Les politiques et procédures doivent prendre en compte les relations avec les banques correspondantes et couvrir les questions relatives à la collecte d'information sur leurs banques correspondantes (nature de leurs activités, leur clientèle, le contrôle exercé par les autorités compétentes, etc.) ainsi que la suspension et le non-établissement de relations de correspondance avec :

- a) des banques étrangères qui ne disposent pas de procédures suffisantes de contrôle à l'égard des activités criminelles, ou
- b) des banques étrangères qui ne sont pas assujetties à une surveillance efficace de la part des autorités compétentes, ou
- c) des banques fictives.

Les banques sont également tenues d'élaborer des procédures appropriées de sélection garantissant le recrutement des employés selon des critères exigeants.



2. Centralisation des informations

Les banques doivent se doter d'un système informatique permettant la centralisation des données. Les succursales et agences doivent être reliées au siège principal, de manière à ce que toutes les opérations effectuées dans l'une de ces succursales ou agences puissent être constatées en temps réel par toutes les entités de l'institution.

3. Nomination d'un officier de conformité

Toute banque doit procéder à la nomination d'un officier de conformité. Cet officier doit être un cadre supérieur de l'institution, sélectionné en fonction de sa compétence, de son expérience, de sa probité et de son éthique professionnelle. Il doit connaître les fonctions et la structure de l'institution, et être au fait des risques et des vulnérabilités liés au blanchiment de capitaux et au financement du terrorisme dans le secteur bancaire ainsi que des tendances et des typologies qui caractérisent ces menaces. Il devra dépendre directement du conseil d'administration pour tout ce qui a trait aux questions liées à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération.

L'officier de conformité a notamment pour attributions de :

- a) assurer l'application de la législation et de la réglementation ;
- b) faire respecter les procédures et méthodes internes de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ;
- c) identifier les carences et faire les recommandations qui s'imposent ;
- d) proposer des programmes de formation sur une base périodique ;
- e) assurer la liaison avec l'Unité Centrale de Renseignements Financiers (UCREF) ;
- f) préparer et acheminer les déclarations de soupçons à l'UCREF ;
- g) s'assurer que les déclarations de transactions sont complétées et acheminées à l'UCREF dans les délais requis ;
- h) recevoir et donner suite aux demandes d'informations de l'UCREF et de toute autre autorité agissant dans le cadre de la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération.

Les banques doivent désigner, dans chaque succursale ou agence, un cadre chargé de faire respecter les lois et réglementations anti-blanchiment et d'assurer la coordination avec l'officier de conformité. En aucun cas, la désignation de ce cadre ne dispense l'officier de conformité de ses responsabilités par rapport à la loi.

4. Evaluation des risques

Le programme de prévention et de conformité doit comprendre un volet relatif à l'évaluation des risques de blanchiment de capitaux et de financement du terrorisme.

L'évaluation des risques est une analyse des menaces et faiblesses en matière de blanchiment de capitaux ou du financement du terrorisme que présentent les activités de la banque. Cette

évaluation varie notamment selon la taille de la banque, son emplacement géographique et selon les activités exercées.

L'évaluation des risques implique que les employés soient bien imbus des activités de l'institution et qu'ils fassent preuve de jugement afin d'évaluer les risques. Cette évaluation ne doit pas être statique et devra être modifiée au moins tous les douze (12) mois.

5. Formation continue

Le programme de prévention doit inclure une composante de formation. Tous les employés qui sont en contact avec les clients, qui ont connaissance d'opérations effectuées par des clients ou qui manipulent des espèces ou des fonds de quelque façon que ce soit ou qui sont responsables de la mise en œuvre ou de la surveillance du régime de conformité doivent comprendre notamment les obligations de déclaration, d'identification des clients et de tenue de documents.

Le programme de formation doit être consigné par écrit et tenu à jour. Les modalités entourant la fréquence et la méthode de formation doivent être établies. On doit y indiquer notamment les catégories de participants, les sujets qui seront couverts et la fréquence des séances de formation. Chaque nouvel employé doit être formé avant de commencer à travailler avec des clients.

Des mises à jour du programme devraient avoir lieu périodiquement afin de tenir toutes les parties intéressées au courant des modifications législatives et réglementaires. La méthode de formation dépendra de la taille de la banque et de la complexité de ses activités.

6. Dispositif de contrôle interne

Les banques doivent faire preuve d'une vigilance constante et se doter d'une organisation et de procédures internes propres à assurer le respect des dispositions prévues par la loi et permettant aux responsables des opérations de prévenir et d'identifier toute tentative de blanchiment de capitaux ou de financement du terrorisme. L'un des rôles de ce contrôle est d'éviter l'utilisation du système financier à des fins de blanchiment ou de financement du terrorisme ou de la prolifération et de minimiser les risques auxquels font face les institutions.

Ce système de contrôle interne doit contenir, entre autres :

- a) un mécanisme de contrôle des politiques, procédures et méthodes internes de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération ;
- b) une structure garantissant la confidentialité du traitement des informations ;
- c) des mesures d'identification des éléments à risques liés au blanchiment de capitaux, au financement du terrorisme et de la prolifération, et des systèmes d'évaluation de ces risques;
- d) un système de surveillance pouvant garantir la maîtrise des risques relatifs au blanchiment de capitaux, au financement du terrorisme et de la prolifération ;
- e) un système centralisé de documentation et d'information ;
- f) un système d'informations sur les initiatives prises en matière de conformité, de déficiences dans ce domaine et des mesures correctives prises.

Le système de contrôle en place doit s'étendre à toutes les composantes de l'institution. Les banques sont donc tenues de prendre les mesures nécessaires pour garantir la stricte application des politiques, procédures et méthodes en vigueur spécialement celles relatives au blanchiment de capitaux, au financement du terrorisme et de la prolifération.

7. Dispositif de tests indépendants

Lors des tests indépendants périodiques portant sur le respect des procédures internes, ou la bonne surveillance des risques, une vérification spécifique sur le volet blanchiment de capitaux, financement du terrorisme et de la prolifération doit être effectuée par l'audit interne de l'institution.

Les vérifications peuvent notamment s'appliquer aux points suivants :

- a) l'évaluation de la qualité de la gestion et du contrôle des risques pour toutes les opérations et dans toutes les succursales ;
- b) des entrevues auprès des employés chargés des opérations et de leurs superviseurs pour évaluer leur degré de connaissance et de respect des procédures de lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération adoptées par l'institution ;
- c) le respect des procédures d'ouverture et de fermeture de comptes ;
- d) l'examen d'un échantillon de formulaires d'archivage des documents et de formulaires de renseignements sur les transactions financières douteuses ;
- e) une vérification du système de tenue des documents ;
- f) l'existence des justificatifs joints ou référencés aux pièces comptables ;
- g) la connaissance de la clientèle par les succursales et les responsables des opérations, en tenant compte des éléments suivants : activité professionnelle, fonctionnement du compte, situation financière et documentation comptable et financière concordante avec les crédits consentis et les volumes d'affaires traitées. Une attention particulière doit être portée à la justification économique des opérations et leur adéquation avec la situation connue de la clientèle ;
- h) des examens périodiques de toutes les relations de correspondants bancaires établies avec des banques étrangères afin de détecter les partenaires à haut risque ;
- i) la connaissance par les collaborateurs des règles internes anti-blanchiment.

Les résultats de toute vérification doivent être soumis au conseil d'administration. Suivant la structure hiérarchique de l'institution, les questions relatives aux mesures prises ou à prendre et aux échéanciers prévus à cet égard doivent être connues et divulguées au personnel exécutant.

8. Traitement des opérations suspectes

Les banques doivent élaborer et mettre en application des politiques quant à l'identification et au suivi des transactions inhabituelles ou suspectes. Ces politiques devront définir ce qui est considéré comme suspect ou inhabituel, et fournir des exemples à cet égard.

L'identification des transactions inhabituelles ou suspectes peut être fait par la surveillance des transactions, les contacts avec le client (rencontres, visites, discussions, etc.), des informations en

provenance de tiers (journaux, internet, etc.), la connaissance qu'à la banque de l'environnement du client.

9. Sanctions

Par suite d'une carence constatée dans l'organisation de procédures internes de prévention du blanchiment de capitaux, de financement du terrorisme et de la prolifération, conformément à l'article 116 du décret du 30 avril 2023 et à l'article 109 de la loi du 14 mai 2012, la BRH se réserve le droit de prendre toutes sanctions administratives allant de l'avertissement jusqu'au retrait d'agrément dans les cas les plus graves, sans préjudice de celles prévues par la loi.

10. Abrogation et entrée en vigueur

La présente circulaire abroge la circulaire 100-3 et entre en vigueur le 14 août 2023.

Port-au-Prince, le 27 juillet 2023.


Jean Baden Dubois
Gouverneur