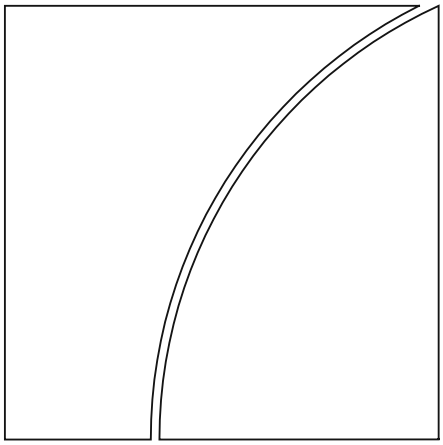
Comité de Bâle sur le contrôle bancaire



Saine gestion des risques de blanchiment de capitaux et de financement du terrorisme

janvier 2014

BANQUE DES RÈGLEMENTS INTERNATIONAUX

Également disponible sur le site de la BRI (www.bis.org).

ISBN 92-9197-211-8 (en ligne)

Sommaire

Saine gestion des risques de blanchiment de capitaux et de financement du terrorisme

I. Introduction

1. Conscient que les banques risquent d'être utilisées, intentionnellement ou non, pour des activités criminelles, le Comité de Bâle sur le contrôle bancaire publie ces lignes directrices expliquant comment intégrer les risques de blanchiment de capitaux (BC) et de financement du terrorisme (FT) à leur gestion globale des risques.

2. Le Comité tient de longue date à promouvoir l'application de saines politiques et procédures de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), indispensables pour préserver la sûreté et la solidité des banques, mais aussi l'intégrité du système financier international. Après une première déclaration en 1988[1], le Comité a publié plusieurs documents dans ce sens. En septembre 2012, il a réaffirmé sa position en publiant la version révisée des *Principes fondamentaux pour un contrôle bancaire efficace*, dont l'un d'eux (Principe fondamental 29) est consacré à l'utilisation abusive des services financiers.

3. Le Comité est favorable à l'adoption des normes émises par le Groupe d'action financière (GAFI)[2]. Celui-ci a publié, en février 2012, une version révisée des *Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération* (normes du GAFI) à laquelle le Comité a contribué[3]. En février 2013, le GAFI a également publié des lignes directrices sur l'inclusion financière dont le Comité a également tenu compte dans la rédaction de ces lignes directrices. L'intention du Comité en publiant ce document est de favoriser l'application nationale des normes du GAFI en examinant des problématiques complémentaires et en mettant l'expertise des deux organisations à profit. Ces lignes directrices reprennent à la fois les normes du GAFI et les Principes fondamentaux de Bâle visant les banques ayant des activités internationales et s'inscrivent dans le cadre général du contrôle bancaire. Elles se veulent donc conformes aux objectifs des normes du GAFI, qu'elles complètent, et ne doivent être en aucun cas considérées comme une modification renforçant ou allégeant ces normes.

4. Sur certains points, ce document comporte des références aux normes du GAFI afin d'aider les banques à respecter les obligations nationales basées sur leur application. Cependant, l'intention du Comité n'est pas de reproduire ici les normes établies par le GAFI et de ce fait, il n'y est pas systématiquement fait référence.

[1] Voir BCBS, *Prévention de l'utilisation du système bancaire pour le blanchiment de fonds d'origine criminelle*, décembre 1988, accessible à l'adresse : http://www.bis.org/publ/bcbsc137fr.pdf.

[2] Le GAFI est un organisme intergouvernemental qui établit des normes internationales et promeut des politiques visant à protéger le système financier mondial contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Il définit le blanchiment de capitaux comme l'opération consistant à retraiter les produits d'origine criminelle pour en masquer l'origine illégale. Il travaille en étroite coopération avec d'autres organismes intervenant dans ce domaine, et, en particulier, avec les membres associés et les observateurs. Le Comité a un statut d'observateur.

[3] L'annexe 3 contient un extrait des principales recommandations du GAFI que les banques et les autorités de contrôle doivent suivre dans la mise en place de leurs mesures de LBC/FT. Cet extrait n'est pas exhaustif et d'autres recommandations du GAFI, notamment les notes interprétatives, peuvent être pertinentes. Le document complet est accessible à l'adresse : http://www.fatf-gafi.org/media/fatf/documents/recommendations/Recommandations_GAFI.pdf.

5. L'engagement du Comité en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme est en parfaite adéquation avec son mandat, qui est de « renforcer la réglementation, le contrôle et les pratiques des banques à travers le monde en vue d'améliorer la stabilité financière[4] ». Une saine gestion des risques de BC/FT est particulièrement importante pour la sûreté et la solidité globale des banques et du système bancaire, premier objectif du contrôle bancaire. En effet :

- elle contribue à protéger la réputation des banques et des systèmes bancaires nationaux en empêchant que les banques soient utilisées pour blanchir des profits illicites ou pour lever ou faire circuler des fonds de soutien au terrorisme ;
- elle préserve l'intégrité du système financier international et protège le travail des États en matière de lutte contre la corruption et le financement du terrorisme.

6. Lorsque les risques de BC/FT ne sont pas gérés ou le sont mal, les banques s'exposent à de graves risques, en particulier à des risques opérationnels, de réputation, de conformité et de concentration. Ces risques ont été mis en relief par les développements récents, notamment les rigoureuses sanctions prises par les autorités de contrôle, et par les coûts directs et indirects encourus par les banques du fait des carences de leurs politiques, procédures et contrôles en matière de gestion des risques. Ces coûts et ces dommages auraient sans doute pu être évités si les banques avaient appliqué des politiques et des procédures de LBC/FT efficaces, fondées sur les risques.

7. Il faut souligner que tous ces risques sont étroitement liés. Cependant, outre les amendes et les sanctions des autorités de contrôle auxquelles ils exposent, tous peuvent individuellement entraîner des coûts financiers importants pour les banques (par exemple à travers la résiliation des facilités de financement de gros, les poursuites contre les banques, les coûts d'investigation, les saisies et gels d'actifs et les pertes sur prêts) et mobiliser des ressources opérationnelles et la direction, dont le temps est précieux, pour résoudre les problèmes.

8. C'est pourquoi ce document doit être lu conjointement avec plusieurs documents apparentés du Comité, notamment :

- *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012[5]
- *The internal audit function in banks*, juin 2012[6]
- *Principles for the sound management of operational risk*, juin 2011[7]
- *Principles for enhancing corporate governance*, octobre 2010[8]
- *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers*, mai 2009[9]
- *Compliance and the compliance function in banks*, avril 2005[10]

4 Voir Comité de Bâle sur le contrôle bancaire, *Charte*, janvier 2013, accessible à l'adresse : http://www.bis.org/bcbs/charter_fr.pdf.

5 Accessible à l'adresse suivante : www.bis.org/publ/bcbs230_fr.pdf.

6 Accessible à l'adresse suivante : www.bis.org/publ/bcbs223.pdf.

7 Accessible à l'adresse suivante : www.bis.org/publ/bcbs195.pdf.

8 Accessible à l'adresse suivante : www.bis.org/publ/bcbs176.pdf.

9 Accessible à l'adresse suivante : www.bis.org/publ/bcbs154.pdf.

10 Accessible à l'adresse suivante : www.bis.org/publ/bcbs113.pdf.

9. Afin de rationaliser les publications du Comité dans le domaine de la LBC/FT, ce document fusionne et remplace deux de ses publications antérieures sur des sujets voisins : *Devoir de diligence des banques au sujet de la clientèle*, octobre 2001, et *Consolidated KYC Risk Management*, octobre 2004. En actualisant ces documents, le Comité s'est, en outre, davantage attaché aux risques associés au recours que font les banques à des tiers apporteurs d'affaires (voir annexe 1) et aux services de correspondance bancaire (voir annexe 2). Malgré leur importance et leur pertinence, d'autres secteurs de risques spécifiques comme les personnes politiquement exposées (PPE), la banque privée et certaines structures juridiques, qui ont été traités dans des documents antérieurs, n'ont pas été développés ici, car le GAFI leur a déjà consacré des publications[11].

10. S'agissant du champ d'application, ces lignes directrices doivent être lues conjointement avec d'autres normes et lignes directrices établies par le Comité qui encouragent le contrôle des groupes bancaires sur une base consolidée[12]. La base consolidée est particulièrement pertinente dans le contexte de la LBC/FT car les clients ont souvent de multiples relations ou plusieurs comptes avec un même groupe bancaire, mais dans des établissements situés dans différents pays.

11. Ces lignes directrices sont applicables à toutes les banques. Des aménagements adaptés au modèle économique ou à la taille des établissements spécialisés ou de taille modeste peuvent être nécessaires pour certaines d'entre elles ; toutefois, ce document n'a pas vocation à traiter ces ajustements.

12. Ces lignes directrices visent expressément les banques, les groupes bancaires (parties II et III respectivement) et les autorités de contrôle bancaire (partie IV). Comme l'indique le Principe fondamental 29, le Comité est conscient de la diversité des dispositifs nationaux visant à garantir le respect des dispositions en matière de LBC/FT, en particulier le partage des fonctions de contrôle entre les autorités bancaires et d'autres autorités comme les cellules de renseignement financier[13]. C'est pourquoi, dans ces lignes directrices, le terme « autorité de contrôle » peut désigner ces autorités. Dans les États où les pouvoirs de contrôle en matière de LBC/FT sont partagés, l'autorité de contrôle bancaire coopère avec les autres autorités pour faire respecter ces lignes directrices.

13. Il faut souligner que ce document ne traite pas des normes du GAFI qui invitent les pays à appliquer d'autres mesures dans leur secteur financier et dans d'autres secteurs non financiers désignés, ou qui établissent les pouvoirs et les missions des autorités compétentes.

II. Composantes essentielles d'une saine gestion des risques de BC/FT

14. La version actualisée des *Principes fondamentaux pour un contrôle bancaire efficace* (2012) prévoit que toutes les banques doivent être tenues de se doter « de politiques et procédures appropriées, notamment de critères stricts de vigilance à l'égard de la clientèle, garantissant un haut degré d'éthique et de professionnalisme dans le secteur financier et empêchant que la banque ne soit utilisée, intentionnellement ou non, dans le cadre d'activités criminelles »[14]. Cette obligation doit être considérée comme un élément particulier de l'obligation générale des banques de mettre en place des

11 Voir, en particulier, GAFI, *Guidance on Politically Exposed Persons* (recommandations 12 et 22), accessible à l'adresse : www.fatf-gafi.org/fr/documents/documents/peps-r12-r22.html.

12 Voir par exemple le Principe fondamental 12, *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012.

13 Les cellules de renseignement financier sont décrites dans la recommandation 26 des normes du GAFI.

14 Voir le Principe fondamental 29, *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012.

programmes de saine gestion des risques pour gérer tous les types de risques, notamment de BC et de FT. Dans ce contexte, des « politiques et procédures appropriées » requièrent l'exécution d'autres mesures complétant des règles efficaces de vigilance à l'égard de la clientèle. Ces mesures doivent, en outre, être adaptées et proportionnées aux risques détectés lors de l'évaluation des risques de BC/FT effectuée par la banque. Ce document présente des recommandations concernant ces mesures. De plus, d'autres lignes directrices (voir plus haut, paragraphe 8) s'appliquent en l'absence de recommandations spécifiques en matière de LBC/FT.

1. Évaluation, compréhension, gestion et atténuation des risques

a) Évaluation et compréhension des risques

15. Une saine gestion des risques[15] suppose de détecter et d'analyser les risques de BC/FT présents au sein de la banque et d'établir et d'appliquer des politiques et procédures proportionnées à ces risques. Lorsqu'elle effectue une évaluation complète des risques de BC/FT, une banque doit considérer tous les facteurs de risques intrinsèques et résiduels pertinents, notamment à l'échelle du pays[16], du secteur, de la banque et des relations d'affaires, afin de déterminer son profil de risques et les mesures d'atténuation qu'il convient d'appliquer. Les politiques et les procédures de vigilance à l'égard de la clientèle, d'acceptation des clients, d'identification des clients et de surveillance de la relation d'affaires et des opérations (produits et services proposés) devront ensuite tenir compte de l'évaluation des risques et du profil de risques de la banque qui en résulte. Une banque doit se doter de mécanismes appropriés pour documenter l'évaluation des risques et donner les informations y afférentes aux autorités compétentes comme ses autorités de contrôle.

16. Une banque doit avoir une parfaite connaissance des risques de BC/FT inhérents à sa clientèle, ses produits, ses canaux de distribution et son offre de services (y compris les produits qui sont en cours de développement ou qu'elle s'apprête à commercialiser), ainsi qu'aux États et territoires dans lesquels elle-même ou ses clients travaillent. Cette connaissance doit reposer sur des données précises relatives à l'activité et aux opérations ainsi que sur d'autres informations recueillies par la banque en interne et auprès de sources externes comme les évaluations nationales de risques et les rapports nationaux émanant des organisations internationales. Les politiques et les procédures d'acceptation des clients, de vigilance et de surveillance continue doivent être conçues et appliquées de façon à maîtriser correctement les risques intrinsèques détectés. Tout risque résiduel doit être géré conformément au profil de risques résultant de l'évaluation des risques. Cette évaluation et cette connaissance des risques doivent pouvoir être démontrées à l'autorité de contrôle bancaire et être jugées acceptables par celle-ci.

b) Cadre de gouvernance approprié

17. Une bonne gestion des risques de BC/FT requiert un cadre de gouvernance approprié, conforme aux descriptions présentées dans les publications antérieures du Comité sur le sujet[17]. L'obligation pour le conseil d'administration d'approuver et de superviser les politiques de risques, de gestion des risques et de conformité est, en particulier, parfaitement pertinente dans le contexte des risques de BC/FT. Le conseil d'administration doit parfaitement mesurer ces risques. Les informations

[15] Voir, en particulier, le Principe fondamental 15, Principes fondamentaux pour un contrôle bancaire efficace, septembre 2012, ainsi que le Principe 6 du document Principles for enhancing corporate governance, octobre 2010.

[16] Le cas échéant, les évaluations des risques de BC/FT réalisées à l'échelon supranational doivent être prises en compte.

[17] Voir, en particulier, *The internal audit function in banks*, juin 2012 ; *Principles for enhancing corporate governance*, octobre 2010 *; Compliance and the compliance function in banks*, avril 2005.

résultant de l'évaluation des risques de BC/FT doivent lui être transmises en temps opportun, être complètes, compréhensibles et exactes afin qu'il dispose de tous les éléments nécessaires pour prendre des décisions éclairées.

18. Le conseil d'administration doit déléguer les responsabilités précises en tenant compte de la structure de gouvernance de la banque afin de garantir une bonne gestion des politiques et des procédures. Le conseil d'administration et la direction générale doivent nommer un responsable de la LBC/FT possédant les qualifications appropriées, qui assumera la responsabilité générale de la fonction LBC/FT et aura le statut et les pouvoirs nécessaires pour que les questions qu'il soulève reçoivent l'attention voulue du conseil d'administration, de la direction générale et des lignes de métier.

c) Les trois lignes de défense

19. En règle générale et dans le contexte de la LBC/FT, les unités opérationnelles (par exemple, front-office, activités en contact avec la clientèle) sont la première ligne de défense. Elles doivent détecter, évaluer et contrôler les risques de leur activité, connaître les politiques et les procédures et disposer de ressources suffisantes pour les appliquer efficacement. La deuxième ligne de défense est formée du responsable de la LBC/FT, de la fonction conformité, mais aussi des ressources humaines ou des services informatiques. Enfin, la troisième ligne de défense est assurée par l'audit interne.

20. Dans le cadre de la **première ligne de défense**, les politiques et procédures doivent être clairement énoncées par écrit et diffusées à l'ensemble du personnel. Elles doivent donner des instructions claires aux salariés, décrire précisément leurs obligations et donner des indications sur les moyens permettant de maintenir la conformité de l'activité de la banque à la réglementation. Des procédures internes doivent être en place pour détecter et déclarer les opérations suspectes.

21. Une banque doit se doter de politiques et procédures appropriées pour la sélection des candidats à un emploi et des salariés en poste afin d'assurer un degré élevé d'éthique et de professionnalisme. Toutes les banques doivent conduire des programmes de formation continue afin que leur personnel soit correctement formé à l'application des politiques et procédures de LBC/FT. Le calendrier et le contenu de la formation des diverses catégories de salariés devront être adaptés aux besoins et au profil de risques de la banque. L'organisation des formations et les supports doivent être adaptés aux responsabilités ou aux fonctions des salariés afin qu'ils disposent de connaissances et d'informations suffisantes pour appliquer efficacement les politiques et procédures de LBC/FT de la banque. Pour les mêmes raisons, les salariés nouvellement recrutés doivent être tenus de suivre une formation dès que possible. Des cours de remise à niveau doivent être assurés afin de rappeler leurs obligations aux salariés et d'actualiser leurs connaissances et leur expertise. Le sujet et la fréquence de ces formations doivent être adaptés aux facteurs de risques auxquels les salariés sont exposés dans leurs fonctions et au niveau et à la nature des risques présents au sein de la banque.

22. Dans le cadre de la **deuxième ligne de défense,** le responsable de la LBC/FT doit être chargé de surveiller en continu l'exécution de toutes les obligations de la banque en matière de LBC/FT. Cette responsabilité implique de procéder à des vérifications de conformité sur échantillons et d'examiner les rapports d'anomalie afin d'alerter la direction générale ou le conseil d'administration s'il apparaît que l'encadrement ne s'acquitte pas des procédures de LBC/FT de manière satisfaisante. Le responsable de la LBC/FT doit être l'interlocuteur des autorités internes et externes pour toutes les questions relatives à la LBC/FT, y compris des autorités de contrôle ou des cellules de renseignement financier.

23. Les intérêts commerciaux d'une banque ne doivent en aucun cas faire obstacle à l'exécution des missions du responsable de la LBC/FT mentionnées ci-dessus. Quelle que soit la taille ou la structure de direction de la banque, les conflits d'intérêts potentiels doivent être évités. Par conséquent, pour pouvoir émettre des jugements objectifs et donner des conseils impartiaux à la direction, le responsable de la LBC/FT ne doit pas, par exemple, avoir de responsabilités relevant des lignes de métier ni de responsabilités relatives à la protection des données ou à la fonction d'audit interne. En cas de conflits d'intérêts entre les lignes de métier et les attributions du responsable LBC/FT, des procédures doivent

être établies afin que les préoccupations en matière de LBC/FT puissent être considérées objectivement au niveau le plus élevé.

24. Le responsable de la LBC/FT peut également être chargé de la supervision des fonctions de contrôle des risques ou de la conformité ou exercer des fonctions équivalentes. Il doit être directement rattaché à la direction générale ou au conseil d'administration. En cas de séparation des missions, les relations entre les responsables précités et leurs fonctions respectives doivent être clairement définies et bien comprises.

25. Le responsable de la LBC/FT doit être également chargé de la déclaration des opérations suspectes. Il doit disposer de ressources suffisantes pour s'acquitter efficacement de toutes ses missions et jouer un rôle central et proactif dans le dispositif de LBC/FT de la banque. À cette fin, il doit parfaitement connaître ce dispositif, les exigences légales et réglementaires et les risques de BC/FT découlant de l'activité.

26. **L'audit interne, troisième ligne de défense,** joue un rôle important en procédant à des évaluations indépendantes de la gestion des risques et des contrôles ; il répond de ses missions devant le comité d'audit du conseil d'administration ou un organe de surveillance similaire et s'acquitte de ses responsabilités en procédant à des évaluations périodiques du respect des politiques et procédures de LBC/FT. Une banque doit établir des politiques applicables à la conduite des audits visant à vérifier i) l'adéquation des politiques et procédures de LBC/FT de la banque aux risques détectés ; ii) l'application, par le personnel, des politiques et procédures de la banque ; iii) l'efficacité de la supervision de la conformité et du contrôle qualité, y compris les paramètres des critères d'alerte automatique et iv) l'efficacité de la formation dispensée par la banque au personnel concerné. La direction générale doit veiller à ce que le personnel chargé des audits possède les connaissances et l'expertise appropriées. Elle doit également s'assurer que le périmètre, la méthodologie et la fréquence des audits sont adaptés au profil de risques de la banque. Les auditeurs internes doivent conduire des audits périodiques du dispositif de LBC/FT à l'échelle de la banque et s'assurer des suites données à leurs constats et recommandations[18]. En règle générale, les procédures d'audit doivent être conformes au mandat plus global de l'audit interne, sous réserve des obligations spécifiques éventuellement applicables aux mesures de LBC/FT.

27. Dans de nombreux pays, les **auditeurs externes** ont également un rôle important à jouer en évaluant les contrôles et procédures internes des banques au cours de leurs audits financiers et en confirmant qu'ils sont conformes à la réglementation en matière de LBC/FT et aux pratiques de contrôle bancaire. Lorsqu'une banque recourt à des auditeurs externes pour évaluer l'efficacité de ses politiques et procédures de LBC/FT, elle doit veiller à ce que le périmètre de l'audit permette de traiter les risques de la banque et que les auditeurs affectés à la mission aient l'expertise et l'expériences nécessaires. Elle doit également exercer une supervision appropriée de ces missions.

d) Système adéquat de surveillance des opérations

28. La taille, les activités et la complexité du système de surveillance doivent être adaptées aux risques présents au sein de la banque. Pour la plupart des banques, surtout celles qui ont des activités internationales, la surveillance devra sans doute être automatisée pour être efficace. Lorsqu'une banque estime que sa situation ne requiert pas de système de surveillance informatique, elle doit documenter sa décision et pouvoir démontrer à son autorité de contrôle ou à ses auditeurs externes qu'une autre solution efficace est en place. Lorsqu'un système informatique est utilisé, il doit couvrir tous les comptes des clients de la banque et l'ensemble des opérations au débit ou au crédit de ces comptes. Il doit

[18] Voir BCBS, *The internal audit function in banks*, juin 2012.

permettre à la banque d'analyser les tendances des opérations bancaires et de déceler les relations d'affaires et les opérations inhabituelles afin de prévenir le BC ou le FT.

29. Ce système doit, en particulier, pouvoir donner des informations exactes à la direction générale sur plusieurs aspects importants, tels qu'une modification du profil des opérations des clients. En établissant le profil du client, la banque doit incorporer les informations actualisées, complètes et exactes que le client lui a communiquées dans le cadre de ses mesures de vigilance à l'égard de la clientèle. Le système informatique doit permettre à la banque, et s'il y a lieu au groupe, de centraliser les informations (organisées par client, par produit, par entité du groupe, opérations effectuées dans un certain laps de temps, etc.). Sans qu'il leur soit demandé d'avoir un fichier clients unique, les banques doivent pouvoir évaluer les risques attachés à leurs clients et gérer les alertes en disposant de toutes les informations pertinentes. Un système de surveillance informatique doit utiliser des paramètres basés sur l'expérience nationale et internationale des méthodes et de la prévention du BC ou du FT. Une banque peut utiliser les paramètres standard prévus par le développeur du système de surveillance informatique mais les paramètres doivent tenir compte des risques propres à la banque.

30. Le système de surveillance informatique doit permettre à une banque d'établir des critères internes additionnels de surveillance, de déposer une déclaration d'opération suspecte (DOS) ou de prendre d'autres mesures pour minimiser le risque. Le responsable de la LBC/FT doit avoir accès au système informatique et pouvoir bénéficier de ses fonctionnalités dans la mesure où il est pertinent pour ses missions (même s'il est géré ou utilisé par d'autres lignes de métier). Les paramètres du système doivent permettre de générer des alertes en cas d'opérations inhabituelles qui feront ensuite l'objet d'une évaluation complémentaire par le responsable de la LBC/FT. Tout critère de risque dans ce contexte doit être adapté à l'évaluation des risques de la banque.

31. L'audit interne doit aussi évaluer le système informatique pour s'assurer qu'il est approprié et que les deux premières lignes de défense l'utilisent efficacement.

2. Politique d'acceptation des clients

32. Une banque doit établir et appliquer des politiques et procédures claires d'acceptation des clients afin de repérer les types de clients susceptibles de poser un risque de BC et de FT compte tenu de son évaluation des risques[19]. Lorsqu'elle évalue le risque, elle doit considérer les facteurs pertinents comme les antécédents du client, sa profession (y compris des fonctions publiques ou médiatisées), la source de ses revenus et de son patrimoine, son pays d'origine et de résidence (s'ils sont différents), les produits utilisés, la nature et l'objet des comptes, les comptes liés, les activités commerciales et d'autres indicateurs de risques axés sur le client afin de déterminer le niveau de risque global et les mesures qu'il convient d'appliquer pour gérer ces risques.

33. Ces politiques et procédures doivent prévoir des mesures de vigilance élémentaires pour tous les clients et des vérifications proportionnées au niveau de risque associé au client. Pour les situations démontrées de risques plus faibles, des mesures simplifiées peuvent être autorisées si la loi le permet. Ainsi, l'application de procédures élémentaires d'ouverture de comptes peut être appropriée pour une personne physique qui pense détenir un faible montant sur son compte bancaire et l'utiliser pour effectuer des opérations courantes de banque de détail. Il est important que la politique d'acceptation des clients ne soit pas restrictive au point de priver le grand public, en particulier les personnes financièrement ou socialement défavorisées, de l'accès aux services bancaires. Les lignes directrices sur

[19] Les normes du GAFI contiennent aussi d'utiles indications sur la manière dont la banque peut appliquer une approche fondée sur les risques (voir, en particulier, la recommandation 1).

l'inclusion financière[20] établies par le GAFI donnent d'utiles pistes pour l'élaboration de procédures de LBC/FT qui ne soient pas trop restrictives pour les personnes financièrement ou socialement défavorisées.

34. Lorsque les risques sont plus élevés, les banques doivent prendre des mesures renforcées pour les atténuer et les gérer. Des vérifications plus étendues peuvent être indispensables pour une personne physique qui prévoit de conserver un montant important sur son compte et d'effectuer régulièrement des virements internationaux ou pour une personne politiquement exposée (PPE). Ces vérifications renforcées sont, en particulier, obligatoires pour les PPE étrangères. Face à des clients dont le risque est plus élevé, la décision d'établir ou de poursuivre une relation d'affaires doit reposer sur des mesures de vigilance renforcées, comme l'autorisation de la direction générale. La politique d'acceptation des clients doit aussi définir les circonstances dans lesquelles la banque refuserait une nouvelle relation d'affaires ou mettrait fin à une relation.

3. Identification, vérification et établissement du profil de risques du client et du bénéficiaire effectif

35. Aux fins de ces lignes directrices et conformément à la recommandation 10 du GAFI, un client désigne toute personne[21] qui établit une relation d'affaires ou effectue une opération financière occasionnelle avec la banque. Les mesures de vigilance à l'égard de la clientèle doivent être appliquées non seulement aux clients mais aussi aux personnes agissant pour leur compte et aux bénéficiaires effectifs[22]. Conformément aux normes du GAFI, les banques doivent identifier les clients et vérifier leur identité[23].

36. Une banque doit établir une procédure systématique pour identifier ses clients, vérifier leur identité et, le cas échéant, celle des personnes agissant pour leur compte et des bénéficiaires effectifs. En règle générale, une banque ne doit pas établir de relation bancaire ni exécuter d'opérations tant que l'identité du client n'a pas été établie et vérifiée conformément à la recommandation 10 du GAFI. Conformément au Principe fondamental 29[24] et aux normes du GAFI, les procédures doivent également prévoir des mesures raisonnables pour vérifier l'identité du bénéficiaire effectif. D'autre part, une banque doit aussi s'assurer que toute personne agissant pour le compte du client est autorisée à le faire et vérifier l'identité de cette personne.

37. L'identité des clients, des bénéficiaires effectifs et des personnes agissant pour leur compte doit être vérifiée à partir de documents sources, de données ou d'informations fiables et indépendants.

20 Voir GAFI, *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion*, février 2013, accessible à l'adresse : http://www.fatf-gafi.org/topics/financialinclusion/.

21 Dans ce contexte, une « personne »désigne une personne physique, une personne morale ou une construction juridique.

22 Le terme « bénéficiaire effectif » dans ces lignes directrices est conforme à la définition et aux précisions fournies par les normes du GAFI. Pour mémoire, le GAFI définit un « bénéficiaire effectif » comme la ou les personnes physiques qui, en dernier lieu, possèdent ou contrôlent un client et/ou la personne physique pour le compte de laquelle une opération est effectuée. Sont également comprises les personnes qui exercent, en dernier lieu, un contrôle effectif sur une personne morale ou une construction juridique.

23 Voir la note interprétative de la recommandation 1 du GAFI. Cette obligation s'applique à moins que le pays ait décidé, sur la base d'une évaluation des risques, d'exonérer, dans des circonstances strictement définies, des catégories particulières d'activités (et de clients associés aux activités), car l'existence d'un risque faible de BC ou de FT a été démontrée conformément à la recommandation 1.

24 Voir le Principe fondamental 29, critère essentiel 5(b), *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012.

Lorsqu'elle se fie à des documents, une banque doit être consciente que les meilleurs documents pour vérifier l'identité sont les plus difficiles à obtenir illégalement ou à contrefaire. Lorsqu'elle s'appuie sur d'autres sources, elle doit s'assurer que les méthodes (qui peuvent comprendre la vérification des références auprès d'autres établissements financiers et l'obtention d'états financiers) et les sources d'informations sont appropriées et conformes à ses politiques et procédures et au profil de risques du client. Une banque peut demander à ses clients de déclarer par écrit l'identité et les coordonnées du bénéficiaire effectif, mais elle ne doit pas se fier à ces seules déclarations. Comme pour tous les éléments du processus de vigilance à l'égard de la clientèle, une banque doit également considérer la nature et le niveau des risques présentés par le client lorsqu'elle détermine les mesures de vigilance applicables[25]. En aucun cas une banque ne doit écarter ses procédures d'identification et de vérification des clients au seul motif que le client n'est pas en mesure d'être présent pour un entretien (clients à distance) ; elle doit également tenir compte des facteurs de risques comme la raison pour laquelle le client a choisi d'ouvrir un compte éloigné de son siège/établissement, en particulier dans un État étranger. Il serait également important de tenir compte des risques associés à des clients venant d'États dont le dispositif de LBC/FT présente des insuffisances stratégiques et d'appliquer des mesures de vigilance renforcées lorsque le GAFI, d'autres organismes internationaux ou les autorités nationales le demandent.

38. Bien que la procédure d'identification du client et de vérification soit applicable au début de la relation ou avant une opération bancaire ponctuelle, une banque doit se servir de ces informations pour comprendre le profil et le comportement du client. L'objet de la relation ou de l'opération bancaire ponctuelle, le niveau des actifs ou le montant des opérations du client et la régularité ou la durée de la relation sont des exemples d'informations habituellement recueillies. Par conséquent, une banque doit aussi instaurer des politiques et des procédures permettant d'exécuter des mesures de vigilance suffisantes pour établir des profils de risques de clients ou de catégories de clients. Les informations recueillies à cette fin doivent être fonction du niveau de risque associé au modèle économique et aux activités du client ainsi qu'aux produits ou services financiers qu'il requiert. Ces profils de risques facilitent la détection de toute activité sur un compte qui s'écarte de l'activité qui serait considérée comme « normale » pour le client ou la catégorie de clients en question et pourrait être considérée comme inhabituelle, voire suspecte. Les profils de risques des clients aideront la banque à déterminer ensuite si le client ou la catégorie de clients présente un risque plus élevé et requiert l'application de mesures de vigilance et de contrôle renforcées. Les profils doivent aussi refléter la connaissance qu'a la banque de l'objet et de la nature intentionnels de la relation d'affaires ou de l'opération bancaire ponctuelle, du niveau d'activité attendu, du type d'opérations et s'il 'y a lieu, de la provenance des fonds, des revenus ou du patrimoine du client ainsi que d'autres considérations similaires. Toute information importante recueillie sur l'activité ou le comportement du client doit être utilisée pour mettre à jour l'évaluation des risques du client effectuée par la banque.

39. Une banque doit obtenir les papiers d'identité du client ainsi que toute information et documentation obtenues dans le cadre des mesures de vigilance à l'égard de la clientèle –copies de documents officiels (passeports, cartes d'identité, permis de conduire…) ou informations figurant dans ces documents, états de comptes (documents relatifs aux opérations) et correspondance commerciale, résultats des analyses réalisées, comme l'évaluation des risques et les demandes d'informations pour établir le contexte et l'objet des relations et des activités.

40. Une banque doit également obtenir tous les éléments nécessaires pour établir de façon certaine l'identité de son client, de toute personne agissant pour celui-ci et des bénéficiaires effectifs. Bien qu'une banque soit tenue d'identifier ses clients et de vérifier leur identité, la nature et l'étendue des informations requises à cette fin dépendent de l'évaluation des risques, notamment de la qualité du

[25] Voir Banque mondiale, *Politically Exposed Persons, Preventive Measures for the Banking Sector,* 2010.

demandeur (personne physique, société, etc.) et de la taille et de l'utilisation attendues du compte. Les mesures exactes à appliquer pour déterminer l'identité des personnes physiques sont habituellement prescrites par la législation nationale. La vérification de l'identité des clients à risque plus élevé nécessitera des mesures de vigilance renforcées. Si la relation est complexe ou si la taille du compte est importante, des mesures d'identification supplémentaires peuvent être opportunes ; elles doivent être décidées en fonction du niveau de risque global.

41. Lorsqu'une banque n'est pas en mesure d'exécuter les mesures de vigilance relatives à la clientèle, elle ne doit pas ouvrir le compte, établir la relation d'affaires ou effectuer l'opération. Néanmoins, dans certaines circonstances, l'exécution des vérifications après l'établissement de la relation d'affaires peut être autorisée parce qu'il serait essentiel de ne pas interrompre la conduite normale de l'activité. Dans ces circonstances, la banque doit adopter des procédures de gestion des risques adéquates quant aux conditions dans lesquelles un client peut utiliser la relation bancaire avant les vérifications. Lorsque, après l'ouverture d'un compte, des problèmes de vérification se posent au cours de l'établissement de la relation bancaire et ne peuvent pas être résolus, la banque doit clore le compte ou bloquer l'accès à celui-ci. En tout état de cause, elle doit envisager d'effectuer une déclaration d'opération suspecte (DOS) lorsqu'elle rencontre des problèmes dans l'exécution des mesures de vigilance à l'égard de la clientèle[26]. En outre, lorsque les vérifications font craindre ou pourraient faire craindre que les actifs ou les fonds du client prospectif puissent être le produit d'infractions sous-jacentes liées au BC/FT, les banques ne doivent pas accepter de plein gré d'ouvrir des comptes pour ces clients. Dans ce cas, elles doivent déposer une DOS auprès des autorités compétentes et veiller à ce que le client n'en soit pas informé, même indirectement.

42. Une banque doit se doter de procédures et de la capacité matérielle nécessaire pour permettre aux activités de front-office en contact avec la clientèle d'identifier toutes personnes physiques ou morales désignées (terroristes, organisations terroristes par exemple) par leur législation nationale et les résolutions du Conseil de sécurité des Nations Unies.

43. Bien que le transfert de fonds d'un compte ouvert au nom du client dans une autre banque soumise aux mêmes règles de vigilance à l'égard de la clientèle que le dépôt initial puisse apporter un certain confort, une banque doit effectuer ses propres vérifications et envisager la possibilité que le précédent chargé de clientèle ait pu demander la fermeture du compte en raison de préoccupations relatives à des activités illicites. Naturellement, les clients ont le droit de changer de banque mais si une banque a la moindre raison de penser qu'un autre établissement a refusé des services bancaires à un demandeur pour ces raisons, elle doit envisager de classer le demandeur dans la catégorie à risque plus élevé et d'appliquer des mesures de vigilance renforcées au client et à la relation bancaire, de déposer une DOS ou de ne pas accepter le client conformément à son évaluation des risques et à ses procédures.

44. Une banque ne doit pas ouvrir un compte ou poursuivre une relation d'affaires avec un client qui exige de garder l'anonymat ou qui donne un nom manifestement fictif. De même, les comptes numérotés confidentiels[27] ne doivent pas fonctionner comme des comptes anonymes mais faire l'objet des mêmes procédures de vigilance que les autres comptes, même si les procédures sont exécutées par du personnel sélectionné. Bien qu'un compte numéroté puisse offrir un supplément de confidentialité à son titulaire, l'identité de celui-ci doit être vérifiée par la banque et connue d'un nombre suffisant d'employés pour faciliter l'application de mesures de vigilance efficaces, surtout si d'autres facteurs de risques indiquent que le client présente un risque élevé plus élevé. Une banque doit veiller à ce que ses

[26] Sous réserve de toute législation nationale concernant la gestion des opérations suspectes.

[27] Dans un compte numéroté, le nom du client et celui du bénéficiaire effectif sont connus de la banque, mais il leur est substitué un numéro de compte ou un nom de code dans les documents ultérieurs.

fonctions de contrôle interne, de conformité, d'audit et ses autres fonctions de supervision, en particulier le responsable de la LBC/FT, ainsi que ses autorités de contrôle aient pleinement accès à ces informations en cas de besoin.

4. Surveillance continue

45. La surveillance continue est un aspect essentiel d'une bonne gestion des risques de BC/FT. Une banque ne peut gérer efficacement ses risques que si elle connaît l'activité bancaire normale et raisonnable de ses clients et peut ainsi identifier les tentatives d'opérations et les opérations inhabituelles qui s'écartent du schéma régulier de l'activité bancaire. Sans ces connaissances, la banque risque de ne pas honorer ses obligations de détection et de déclaration des opérations suspectes aux autorités compétentes. Toutes les relations d'affaires et toutes les opérations doivent faire l'objet d'une surveillance continue, mais le degré de surveillance doit être fonction des risques détectés lors de l'évaluation des risques et des mesures de vigilance à l'égard de la clientèle conduites par la banque. Les clients ou les opérations à risque plus élevé doivent faire l'objet d'une surveillance renforcée. Une banque doit non seulement surveiller ses clients et leurs opérations, mais elle doit aussi effectuer une surveillance transversale aux produits et services afin de repérer et d'atténuer les profils de risques émergents.

46. Toutes les banques doivent disposer de systèmes de détection des opérations ou des profils d'activité inhabituels ou suspects. Lorsqu'elle établit les scénarios destinés à détecter ces activités, une banque doit considérer le profil de risques du client qu'elle a établi à partir de son évaluation des risques, des informations recueillies dans le cadre des mesures de vigilance à l'égard de la clientèle et des autres informations obtenues auprès des autorités chargées de l'application des lois et des autres autorités nationales. Par exemple, une banque peut avoir été informée par les autorités que des dispositifs ou arrangements particuliers de blanchiment des produits d'activités criminelles ont été constatés sur son territoire.. Dans le cadre de sa procédure d'évaluation des risques, la banque aura évalué le risque qu'une activité associée à de tels dispositifs ou arrangements puisse intervenir dans ses services à travers une catégorie de clients, un groupe de comptes, un type d'opération ou l'utilisation de produits. À partir de ces informations, la banque doit concevoir et appliquer des outils de surveillance et des contrôles appropriés pour détecter ces activités – par exemple des scénarios d'alerte pour les systèmes de surveillance informatisée ou des limites fixées pour une classe ou une catégorie d'activité.

47. À partir des informations résultant de ses mesures de vigilance à l'égard de la clientèle, une banque doit pouvoir déterminer les opérations qui ne semblent pas économiquement justifiées, qui impliquent des dépôts d'espèces de montant important ou qui ne sont pas conformes aux opérations normales et attendues du client.

48. Une banque doit avoir établi des politiques et des procédures de vigilance renforcée pour les clients à risque plus élevé qu'elle a identifiés. Outre les politiques et procédures relatives aux autorisations d'ouverture de comptes, elle doit se doter de politiques particulières concernant l'étendue et la nature des mesures de vigilance nécessaires, la fréquence de la surveillance continue et de la mise à jour des informations de vigilance et des autres dossiers. Pour bien suivre et détecter les activités suspectes, une banque a besoin de profils clients et de documents à jour, complets et exacts.

49. Une banque doit veiller à disposer de systèmes d'information de gestion intégrés, proportionnés à sa taille, à la structure ou à la complexité de son organisation, fondés sur l'importance et les risques afin de fournir rapidement aux unités opérationnelles (par exemple les chargés de clientèle) et aux responsables des risques et de la conformité (y compris les personnels effectuant des investigations) les informations nécessaires pour identifier, analyser et surveiller efficacement les comptes clients. Les systèmes utilisés et les informations disponibles doivent permettre une surveillance de ces relations clients transversale aux lignes de métier et comprendre toutes les informations disponibles, y compris l'historique des opérations, les documents manquants à l'ouverture du compte

ainsi que les changements significatifs intervenus dans le comportement du client ou son profil d'activité et les opérations inhabituelles effectuées sur un compte client.

50. La banque doit effectuer des recherches dans ses bases de données de clients à chaque modification des listes de sanctions, mais aussi périodiquement, pour détecter les PPE étrangères et d'autres comptes à risque plus élevé et les soumettre à des mesures de vigilance renforcées.

5. Gestion de l'information

a) Conservation des documents

51. Une banque doit veiller à conserver toutes les informations obtenues dans le cadre de ses mesures de vigilance à l'égard de la clientèle. Cette obligation comprend à la fois i) la conservation des documents qui lui sont remis lorsqu'elle vérifie l'identité du client ou du bénéficiaire effectif et ii) la transcription dans ses systèmes informatiques des informations figurant dans ces documents ou obtenues par d'autres moyens.

52. Une banque doit également instaurer et appliquer des règles claires quant aux documents à consigner pour documenter les mesures de vigilance relatives aux clients et aux opérations. Dans la mesure du possible, ces règles doivent tenir compte des prescriptions en matière de respect de la vie privée. Elles doivent définir les types d'informations et de documents qui doivent figurer dans les dossiers ainsi que leur durée de conservation, laquelle doit être d'au moins cinq ans après la cessation de la relation bancaire ou la conclusion de l'opération ponctuelle[28]. Même si les comptes sont clos, en cas d'enquête ou de litige en cours, tous les documents doivent être conservés jusqu'à la résolution de l'affaire. Les documents conservés doivent être complets et à jour afin que la banque puisse surveiller sa relation avec son client, comprendre l'activité commerciale et les activités de son client et, si nécessaire, fournir une piste d'audit en cas de litige, de procédure judiciaire ou de demande d'informations ou d'enquête susceptible d'aboutir à des sanctions des autorités réglementaires ou à des poursuites pénales.

53. Des documents adéquats retraçant la procédure d'évaluation relative à la surveillance et à l'examen continu ainsi que les conclusions tirées doivent être également conservés et aideront à démontrer que la banque a respecté ses obligations de vigilance à l'égard de la clientèle et qu'elle est capable de gérer le risque de BC/FT.

b) Actualisation des informations

54. Ce n'est que si les banques veillent à ce que leurs documents demeurent exacts, à jour et pertinents en examinant régulièrement leurs dossiers et en mettant à jour les informations obtenues dans le cadre des mesures de vigilance à l'égard de la clientèle que les autorités compétentes, les autorités chargées de l'application des lois ou les cellules de renseignement financier pourront se servir efficacement de ces informations pour s'acquitter de leurs responsabilités dans le contexte de la LBC/FT. En outre, en tenant leurs informations à jour, les banques pourront effectuer un suivi plus efficace des comptes pour détecter les activités inhabituelles ou suspectes.

[28] Voir le Principe fondamental 29, *critère essentiel* 5 f), *Principes fondamentaux pour un contrôle bancaire efficace*, septembre 2012.

c) Communication d'informations aux autorités de contrôle

55. Une banque doit pouvoir démontrer à ses autorités de contrôle lorsque celles-ci le demandent, la pertinence de son évaluation, de sa gestion et de son atténuation des risques de BC/FT, de sa politique d'acceptation des clients, de ses procédures et politiques concernant l'identification des clients et la vérification de leur identité, de sa surveillance continue et de ses procédures de déclaration d'opérations suspectes ainsi que de toutes les mesures prises dans le contexte de la LBC/FT.

6. Déclaration d'opérations suspectes et gel des avoirs

a) Déclaration d'opérations suspectes

56. La surveillance et l'examen continus des comptes et des opérations permettront aux banques de déceler les activités suspectes, d'éliminer les faux positifs et de déclarer rapidement les opérations suspectes. La procédure de détection, d'investigation et de déclaration des opérations suspectes à la cellule de renseignement financier doit être clairement énoncée dans les politiques et procédures de la banque et communiquée à l'ensemble du personnel par des formations régulières. Ces politiques et procédures doivent clairement décrire les obligations des salariés et leur donner des instructions précises pour l'analyse, l'investigation et la déclaration de ces activités au sein de la banque ainsi que des instructions pour compléter ces déclarations.

57. Des procédures doivent être également instaurées pour déterminer si les obligations légales de la banque en vertu des régimes de déclaration des activités suspectes nécessitent que l'opération soit signalée aux autorités chargées de l'application des lois compétentes, à la cellule de renseignement financier ou aux autorités de contrôle. Ces procédures doivent aussi respecter le principe de confidentialité, assurer des investigations rapides et garantir que les rapports contiennent des informations pertinentes et sont produits et soumis en temps opportun. Le responsable de la LBC/FT doit veiller à effectuer des déclarations rapides lorsque des fonds ou d'autres biens suspectés d'être le produit d'activités criminelles sont détenus sur un compte.

58. Dès lors qu'un compte ou une relation bancaire éveille des soupçons, la banque doit déclarer l'activité suspecte mais aussi prendre des mesures appropriées pour atténuer correctement le risque d'être utilisée pour des activités criminelles. Ces mesures peuvent comprendre un réexamen de la classification du risque du client, du compte ou de la relation bancaire tout entière. Elles peuvent nécessiter de remonter les informations au niveau de décision hiérarchique adapté pour déterminer comment gérer la relation, en tenant compte des autres facteurs pertinents comme la coopération avec les autorités chargées de l'application des lois ou la cellule de renseignement financier.

b) Gel des avoirs

59. Le financement du terrorisme offre des similitudes avec le blanchiment de capitaux, mais il présente aussi des spécificités dont les banques doivent tenir compte : les fonds servant à financer des activités terroristes peuvent provenir d'activités criminelles ou de sources légales et la nature des sources de financement peut différer en fonction du type de l'organisation terroriste. Il faut relever, en outre, que les opérations associées au financement de terroristes peuvent porter sur des montants très faibles.

60. Une banque doit pouvoir identifier et appliquer les décisions de gel d'avoirs prises par l'autorité compétente et elle ne doit pas traiter avec des organisations ou personnes physiques désignées (terroristes, organisations terroristes par exemple) par la législation nationale ou les résolutions du Conseil de sécurité des Nations Unies.

61. Les mesures de vigilance à l'égard de la clientèle doivent aider une banque à détecter des opérations potentielles de FT en fournissant des éléments importants pour une meilleure connaissance de ses clients et des opérations qu'ils effectuent. Lorsqu'elle élabore ses politiques et procédures d'acceptation des clients, une banque doit accorder l'importance requise aux risques spécifiques liés à

l'ouverture ou à la poursuite d'une relation d'affaires avec des personnes physiques ou des organisations liées à des groupes terroristes. Avant d'établir une relation d'affaires ou d'exécuter une opération ponctuelle avec de nouveaux clients, une banque doit vérifier que leur nom ne figure pas dans les listes de terroristes avérés ou suspectés émises par les autorités compétentes (nationales et internationales). De même, elle doit effectuer une surveillance continue pour s'assurer que ses clients existants ne figurent pas dans ces listes.

62. Toutes les banques doivent disposer de systèmes de détection des opérations interdites (par exemple des opérations avec des entités désignées par des résolutions du Conseil de sécurité des Nations Unies ou par des autorités nationales). Le contrôle des listes de terroristes n'est pas une mesure de vigilance sensible au risque et elle doit être exécutée indépendamment du profil de risques attribué au client. Pour les besoins de cette mesure, une banque peut adopter des systèmes automatiques, mais elle doit s'assurer qu'ils sont adaptés à l'usage. Les fonds ou les autres biens des personnes et entités désignées doivent être gelés sans délai et sans préavis conformément à la législation et à la réglementation applicable.

III. LBC/FT dans le cadre d'un groupe international

63. Pour une saine gestion des risques de BC/FT, une banque qui a des activités internationales doit tenir compte des obligations légales du pays d'accueil. Compte tenu des risques, des politiques et procédures de LBC/FT doivent être établies à l'échelle du groupe, et appliquées et supervisées de manière homogène dans toutes ses unités. Les politiques et procédures au niveau des succursales ou des filiales, tout en tenant compte des considérations commerciales locales et des exigences du pays d'accueil, doivent demeurer conformes aux politiques et procédures du groupe et les étayer[29]. Lorsque les obligations en vigueur dans le pays d'accueil sont plus strictes que celles du groupe, la politique du groupe doit permettre à la succursale ou à la filiale concernée d'adopter et d'appliquer les exigences locales du pays d'accueil.

1. Procédure globale de gestion des risques clients

64. Une gestion des risques consolidée implique d'appliquer et de coordonner les politiques et les procédures à l'échelle du groupe et d'établir ainsi une référence cohérente et complète pour la gestion des risques de la banque dans toutes ses activités internationales. Les politiques et procédures doivent viser à garantir le strict respect de l'ensemble des lois et règlements applicables, mais aussi plus largement, à détecter, surveiller et atténuer les risques à l'échelle du groupe. Tous les efforts doivent être faits pour que la capacité du groupe à obtenir et examiner les informations conformément à ses politiques et procédures globales de LBC/FT ne soit pas diminuée par des modifications apportées localement aux politiques ou procédures en vue de respecter les obligations légales locales. À cet égard, une banque doit mettre en place un robuste système de partage d'informations entre le siège et toutes les succursales et filiales. En cas de différence entre les obligations légales ou réglementaires minimales des pays d'origine et d'accueil, les établissements situés dans le pays d'accueil doivent appliquer les plus strictes des deux.

[29] Dans ce document, le terme « groupe » désigne une ou plusieurs banques d'une organisation ainsi que leurs succursales et filiales. Le terme « siège » désigne la banque mère ou l'unité qui gère les risques de BC/FT par ligne de métier.

65. En outre, les normes du GAFI[30] prévoient que si le pays d'accueil ne permet pas une bonne application de ces normes, le responsable de la LBC/FT doit en informer les autorités de contrôle du pays d'origine et d'autres mesures doivent être envisagées, y compris s'il y a lieu, la cessation des activités dans le pays d'accueil.

66. Le Comité reconnaît que l'application des procédures de LBC/FT à l'échelle d'un groupe est plus difficile que de nombreuses autres procédures de gestion des risques, car certains États ou territoires maintiennent des restrictions à la transmission à l'étranger de l'identité des clients et des soldes de comptes. Pour une surveillance efficace à l'échelle du groupe et aux fins de la gestion des risques de BC/FT, il est indispensable que les succursales ou filiales soient autorisées à partager des informations sur leurs clients avec leur siège ou leur banque mère, sous réserve d'une protection légale adéquate.

2. Évaluation et gestion des risques

67. La banque doit parfaitement connaître tous les risques associés à ses clients dans l'ensemble du groupe, soit à titre individuel, soit en tant que catégorie, et elle doit aussi les documenter et les actualiser régulièrement en fonction du niveau et de la nature des risques au sein du groupe. Lorsqu'elle évalue le risque client, une banque doit détecter tous les facteurs de risque tels que le lieu des opérations, leurs profils (déclarés ou autodéclarés) et l'utilisation des produits et services bancaires, et établir des critères permettant d'identifier les clients à risque plus élevé. Ces critères doivent être appliqués dans toute la banque, ses succursales et ses filiales ainsi qu'à ses activités sous-traitées (voir annexe 1). Les clients qui posent un risque de BC/FT plus élevé doivent être identifiés dans l'ensemble du groupe sur la base de ces critères. Les évaluations des risques clients doivent être exécutées à l'échelle du groupe ou, au minimum, être cohérentes avec l'évaluation des risques à l'échelle du groupe. Étant donné que les risques diffèrent en fonction de la catégorie de clients, la politique du groupe doit reconnaître que des clients d'une même catégorie peuvent poser différents risques d'un État à l'autre. Les informations recueillies lors de l'évaluation doivent être ensuite utilisées pour déterminer le niveau et la nature du risque global pour le groupe et servir de base à la conception de contrôles de groupe appropriés pour atténuer ces risques. Les mesures d'atténuation peuvent comprendre la communication d'informations complémentaires par le client, une surveillance plus étroite, une actualisation plus fréquente des données personnelles ainsi que des déplacements du personnel de la banque sur le site du client.

68. Le personnel des fonctions conformité et audit interne, en particulier le responsable de la LBC/FT, ou des auditeurs externes doivent évaluer la conformité à tous les aspects des politiques et procédures du groupe, y compris l'efficacité des politiques centralisées de vigilance à l'égard des clients et les obligations de partage d'informations avec les autres membres du groupe et de réponse aux demandes d'informations émanant du siège. Les groupes bancaires qui ont des activités internationales doivent se doter d'une solide fonction d'audit interne et d'une fonction conformité mondiale, car ce sont les principaux mécanismes de surveillance de l'application globale des mesures de vigilance à l'égard de la clientèle et de l'efficacité des politiques et procédures de partage d'informations au sein du groupe. Ces mesures supposent de confier à un responsable de la LBC/FT la surveillance, à l'échelle du groupe, de la conformité aux politiques, procédures et contrôles de LBC/FT sur le territoire national et à l'étranger (voir paragraphes 75 et 76).

[30] Voir la note interprétative de la recommandation 18 (Contrôles internes et succursales et filiales à l'étranger) dans les normes du GAFI.

3. Politiques et procédures de LBC/FT consolidées

69. Une banque doit s'assurer qu'elle comprend parfaitement la mesure dans laquelle la législation en matière de LBC/FT l'autorise à se fier aux procédures engagées par d'autres banques (par exemple au sein du même groupe) lorsqu'un client lui est adressé. Une banque ne doit pas s'appuyer sur des apporteurs d'affaires soumis à des règles moins strictes que celles qui régissent ses propres procédures de LBC/FT, ce qui implique qu'elle doit surveiller et évaluer les règles de LBC/FT en place dans l'État de la banque apporteuse. Une banque peut s'appuyer sur un apporteur d'affaires qui fait partie du même groupe financier et peut envisager d'accorder un niveau de confiance plus élevé aux informations communiquées par celui-ci sous réserve qu'il soit soumis aux mêmes règles qu'elle et que leur application soit supervisée au niveau du groupe. Dans ce cas toutefois, elle doit veiller à obtenir les informations relatives au client auprès de la banque apporteuse (plus amplement décrites à l'annexe 1), car elle pourrait être tenue de déclarer ces informations à la cellule de renseignement financier si une opération impliquant le client qui lui est adressé était jugée suspecte.

70. Le siège du groupe bancaire doit avoir accès aux informations dont il a besoin pour faire respecter les politiques et procédures du groupe en matière de LBC/FT. Chaque établissement du groupe doit respecter les politiques et procédures minimales de LBC/FT et d'accessibilité appliquées par le siège et définies conformément aux lignes directrices du Comité.

71. Les politiques et procédures d'acceptation des clients, de vigilance à l'égard de la clientèle et de conservation des documents doivent être uniformément appliquées dans toute l'organisation, avec les ajustements justifiés par les écarts de risques entre les lignes de métier ou les implantations géographiques des activités. De plus, il est reconnu que différentes approches de la collecte et de la conservation des informations peuvent être nécessaires dans différents États pour respecter les réglementations locales ou les facteurs de risques. Néanmoins, ces approches doivent être conformes aux règles générales du groupe mentionnées plus haut.

72. Indépendamment de sa situation géographique, chaque établissement doit instaurer et appliquer des politiques et procédures de surveillance efficaces et appropriées aux risques présents dans l'État et au sein de la banque. Cette surveillance locale doit être complétée par un solide processus de partage d'informations avec le siège et, le cas échéant, avec d'autres succursales et filiales en ce qui concerne les comptes et les activités susceptibles de présenter un risque plus élevé.

73. Pour bien gérer les risques de BC et de FT découlant de ces comptes, une banque doit intégrer ces informations en se basant non seulement sur le client mais aussi sur la connaissance qu'elle a des bénéficiaires effectifs du client et des fonds en jeu. La surveillance des relations, des soldes et de l'activité des clients importants doit s'effectuer sur une base consolidée, que les comptes soient détenus dans le bilan, hors bilan, sous forme d'actifs sous gestion ou sur une base fiduciaire et indépendamment du lieu de détention. Les normes du GAFI donnent désormais plus de précisions sur la supervision par le siège des fonctions conformité, audit et LBC/FT du groupe[31]. De plus, bien que ces lignes directrices aient été conçues avant tout pour les banques, elles peuvent également intéresser des conglomérats (comprenant des banques).

74. De nombreuses grandes banques qui ont les capacités nécessaires pour le faire centralisent certains systèmes de traitement et bases de données pour une gestion plus efficace. Lorsqu'elle adopte cette approche, une banque doit documenter convenablement et intégrer les fonctions locales et centralisées de surveillance des opérations/des comptes afin de pouvoir surveiller les types d'activités suspects dans l'ensemble du groupe sans se limiter au niveau local ou central.

[31] Voir, en particulier, la recommandation 18 dans les normes du GAFI.

75. Une banque qui exerce ses activités sur le territoire national et à l'étranger doit nommer un responsable de la LBC/FT pour l'ensemble du groupe (responsable de la LBC/FT pour le groupe) dont la mission, dans le cadre de la gestion globale des risques, est de définir et de coordonner une stratégie unique de LBC/FT (comprenant des politiques et procédures obligatoires et l'autorisation de donner des ordres à toutes les succursales, filiales et entités subordonnées sur le territoire national et à l'étranger) et d'évaluer sa mise en œuvre à l'échelle du groupe.

76. Les missions du responsable de la LBC/FT pour le groupe comprennent la surveillance continue du respect du dispositif de LBC/FT à l'échelle du groupe, sur le territoire national et à l'étranger. Il doit donc s'assurer (notamment par des visites sur site régulières) que les règles en matière de LBC/FT sont respectées à l'échelle du groupe. Si nécessaire, il doit être investi des pouvoirs permettant de donner des ordres ou de prendre les mesures requises pour l'ensemble du groupe.

4. Partage d'informations à l'échelle du groupe

77. Les banques doivent superviser la coordination du partage d'informations. Les succursales et les filiales doivent être tenues de fournir spontanément au siège les informations relatives aux clients qui présentent un risque plus élevé et aux activités intéressant les règles globales de LBC/FT, et de répondre rapidement aux demandes d'informations émanant du siège ou d'une banque mère. Les règles à l'échelle du groupe doivent décrire la procédure à suivre sur tous les sites pour identifier, surveiller et investiguer des circonstances inhabituelles et déclarer toute activité suspecte.

78. Les politiques et procédures à l'échelle du groupe doivent tenir compte des aspects et des obligations liés à la législation et à la réglementation locales sur la protection des données et le respect de la vie privée. Elles doivent également tenir compte des différents types d'informations susceptibles d'être partagées au sein d'un groupe et des conditions applicables à la conservation, à l'extraction, au partage ou à la diffusion et à l'utilisation de ces informations.

79. La fonction de gestion des risques de BC/FT du groupe doit évaluer les risques posés par l'activité déclarée par ses succursales et ses filiales et, le cas échéant, évaluer les risques associés à un client ou une catégorie de clients à l'échelle du groupe. Elle doit s'être dotée de politiques et de procédures permettant de déterminer si d'autres succursales ou filiales détiennent des comptes pour le même client (parties liées ou affiliées comprises). La banque doit, en outre, avoir instauré des politiques et des procédures gouvernant les relations globales avec des clients dont le risque est jugé plus élevé ou qui ont été associés à des activités potentiellement suspectes, notamment des procédures de transmission à un niveau hiérarchique supérieur et des lignes directrices relatives à la restriction des activités des comptes, y compris, s'il y a lieu, la clôture des comptes.

80. En outre, une banque, ses succursales et ses filiales doivent, conformément au droit de leur pays d'implantation, répondre aux demandes d'informations sur des clients émanant des autorités chargées de l'application des lois, des autorités de contrôle ou de la cellule de renseignement financier dont ceux-ci ont besoin pour lutter contre le BC et le FT. Le siège d'une banque doit pouvoir demander à toutes les succursales et filiales de rechercher dans leurs dossiers des personnes physiques ou des organisations soupçonnées de complicité de BC et de FT par rapport à des listes ou des demandes et de déclarer les concordances.

81. Une banque doit pouvoir informer ses autorités de contrôle, à leur demande, sur son dispositif global de gestion des risques clients et d'évaluation et de gestion des risques de BC/FT, ses politiques et procédures consolidées de LBC/FT et ses dispositions relatives au partage des informations à l'échelle du groupe.

5. Groupes financiers mixtes

82. De nombreux groupes bancaires ont également des activités dans le secteur des valeurs mobilières et de l'assurance. L'application de contrôles de gestion des risques de BC/FT au sein de groupes financiers mixtes pose des problèmes qui ne sont pas nécessairement présents dans les activités de dépôt et de prêt. Les groupes mixtes doivent pouvoir surveiller et partager les informations sur l'identité des clients, leurs opérations et l'activité de leurs comptes dans l'ensemble du groupe et être attentifs aux clients qui sollicitent leurs services dans différents secteurs, comme l'explique le paragraphe 79 ci-dessus.

83. Les différences que présentent, d'un secteur à l'autre, les activités et les types de relations entre les banques et leurs clients peuvent nécessiter ou justifier d'adapter les obligations en matière de LBC/FT applicables à chaque secteur. Le groupe doit être attentif à ces différences dans le cadre des ventes croisées de produits et de services aux clients de différentes branches d'activité et appliquer des règles de LBC/FT appropriées aux secteurs.

IV. Rôle des autorités de contrôle

84. Les autorités de contrôle bancaire doivent respecter la recommandation 26 du GAFI, qui indique notamment : « Pour les institutions financières soumises aux Principes fondamentaux, les mesures réglementaires et de contrôle applicables à des fins prudentielles et qui sont également pertinentes en matière de blanchiment de capitaux et de financement du terrorisme devraient s'appliquer d'une manière similaire à des fins de LBC/FT. Ceci devrait comprendre la mise en œuvre d'une surveillance consolidée au niveau du groupe à des fins de LBC/FT. ». Le Comité attend des autorités de contrôle que leurs modalités d'application des *Principes fondamentaux pour un contrôle bancaire efficace* à la gestion des banques en matière de risques de BC/FT soient cohérentes avec le contrôle global qu'elles exercent sur les banques et étayent celui-ci. Elles doivent pouvoir appliquer un ensemble de sanctions efficaces, proportionnées et dissuasives aux banques qui ne respectent pas leurs obligations en matière de LBC/FT.

85. Les autorités de contrôle bancaire doivent définir leurs attentes quant aux politiques et procédures de LBC/FT des banques. Les composantes essentielles sont précisées dans ce document et devraient donner aux autorités de contrôle des indications claires sur la façon de procéder pour établir ou améliorer les pratiques de contrôle nationales. Les autorités de contrôle nationales sont encouragées à émettre des lignes directrices afin d'aider les banques à élaborer leurs politiques et procédures internes d'identification des clients. Le Comité a donc établi deux guides spécifiques aux annexes 1 et 2 que les autorités de contrôle peuvent utiliser à cette fin.

86. Les autorités de contrôle doivent adopter une approche fondée sur les risques pour superviser la gestion des risques de BC/FT[32] par les banques. Cette approche requiert i) qu'elles connaissent parfaitement les risques présents sur le territoire national et leur impact potentiel sur les entités contrôlées[33] ; ii) qu'elles évaluent l'adéquation de l'évaluation des risques effectuée par les banques avec

[32] Les autorités de contrôle doivent également tenir compte de l'approche fondée sur les risques en matière de contrôle décrite dans la note interprétative de la recommandation 26 dans les normes du GAFI.

[33] Pour cela, il est anticipé que les autorités de contrôle s'appuieraient sur l'évaluation des pays décrite dans la note interprétative de la recommandation 1 dans les normes du GAFI.

l'évaluation nationale des risques sur le territoire[34] ; iii) qu'elles évaluent les risques présents dans l'entité contrôlée afin de comprendre la nature et l'étendue des risques attachés à la clientèle, aux produits et services de l'entité et aux zones géographiques dans lesquelles la banque et ses clients travaillent ; iv) qu'elles évaluent l'adéquation et l'efficacité des contrôles (dont les mesures de vigilance à l'égard de la clientèle) instaurés par la banque pour exécuter ses obligations en matière de LBC/FT et atténuer les risques et v) qu'elles se servent de ces informations pour allouer les ressources, définir l'étendue de l'examen, déterminer l'expertise et l'expérience nécessaires pour conduire un examen efficace et allouent ces ressources en fonction des risques.

87. Les lignes de métier ou les catégories de clients qui présentent un risque plus élevé peuvent nécessiter une expertise spécialisée et des procédures supplémentaires pour assurer un examen efficace. Le profil de risques de la banque doit être un paramètre de la fréquence et du moment du cycle de contrôle. Là encore, les banques qui ont affaire à des profils de risques plus élevés peuvent nécessiter des examens plus fréquents. Les autorités de contrôle doivent, en outre, vérifier que les banques ont fait bon usage de leur discrétion dans l'application des mesures de LBC/FT fondée sur les risques. Elles doivent aussi évaluer les contrôles internes en place et la manière dont les banques déterminent si elles respectent les lignes directrices prudentielles et réglementaires ainsi que les obligations qui leur sont prescrites. Le contrôle doit non seulement examiner les politiques et les procédures mais aussi, le cas échéant, les documents concernant les clients ainsi qu'un échantillon de comptes et d'opérations, de rapports internes et de déclarations d'opérations suspectes. Les autorités de contrôle doivent toujours avoir un droit d'accès à l'ensemble des documents relatifs aux opérations réalisées ou aux comptes ouverts sur le territoire national, y compris aux analyses effectuées par la banque pour détecter des opérations inhabituelles ou suspectes.

88. Les autorités de contrôle doivent veiller à la qualité de la gestion des risques de BC/FT des banques qu'elles contrôlent non seulement pour leur sécurité et leur solidité, mais aussi pour protéger l'intégrité du système financier[35]. Elles doivent faire savoir clairement qu'en cas de manquement manifeste aux procédures internes et aux obligations réglementaires, elles prononceront les sanctions qui s'imposent, qui peuvent être graves et publiques si les circonstances le justifient, contre les banques et leurs dirigeants. De plus, les autorités de contrôle (ou d'autres autorités nationales compétentes) doivent pouvoir appliquer des contre-mesures appropriées et veiller à ce que les banques connaissent et appliquent les mesures de vigilance à l'égard de la clientèle aux relations d'affaires et aux opérations bancaires qui font l'objet d'une demande du GAFI ou qui impliquent des États ou territoires dont le pays juge les normes de LBC/FT insuffisantes. À cet égard, le GAFI et certaines autorités nationales ont établi une liste d'États et de territoires dont le dispositif de LBC/FT présente des défaillances stratégiques ou

[34] Y compris, le cas échéant, toute évaluation des risques supranationale.

[35] De nombreuses autorités de contrôle ont également le devoir de signaler toute opération suspecte, inhabituelle ou illégale qu'elles détectent, par exemple à l'occasion d'inspections sur site.

qui ne respectent pas les normes internationales en matière de LBC/FT[36] ; ces constats doivent être une composante de la gestion des risques de BC/FT par les banques.

89. Les autorités de contrôle doivent également considérer la surveillance et la supervision globales exercées par une banque en matière de conformité des succursales et des filiales ainsi que la capacité de la politique du groupe à satisfaire aux obligations réglementaires locales, et veiller à ce que les règles les plus strictes soient appliquées en cas d'écart entre les obligations édictées par le groupe et les obligations locales. Elles doivent aussi s'assurer que lorsqu'une succursale ou une filiale ne peut appliquer les règles les plus strictes, les raisons et les différences entre les deux sont documentées et des mesures d'atténuation appropriées mises en place pour gérer les risques qui en résultent.

90. Dans un contexte international, les autorités de contrôle du pays d'origine[37] ne doivent rencontrer aucun obstacle lors des inspections sur site lorsqu'elles vérifient que la banque respecte les politiques et procédures de LBC/FT à l'échelle du groupe. Ces contrôles peuvent nécessiter d'examiner les dossiers clients et un échantillon de comptes ou d'opérations dans le pays d'accueil. Les autorités de contrôle du pays d'origine doivent avoir accès aux informations sur les comptes clients et les opérations sélectionnés et sur les risques nationaux et internationaux spécifiques associés à ces clients dont elles ont besoin pour bien évaluer l'application des normes de vigilance à l'égard de la clientèle et les pratiques de gestion des risques. Cette utilisation des informations à des fins légitimes de contrôle, protégées par les dispositions applicables aux autorités de contrôle en matière de confidentialité, ne doit pas être empêchée par les lois locales sur le secret bancaire ou la protection des données. Bien que les autorités de contrôle du pays d'accueil ou d'autres autorités conservent la responsabilité du contrôle du respect des obligations locales en matière de LBC/FT (qui comprendrait une évaluation de l'adéquation des procédures), les autorités de contrôle du pays d'accueil doivent veiller à pleinement coopérer avec leurs homologues du pays d'origine et à leur apporter toute l'assistance utile, car ces dernières peuvent avoir besoin d'évaluer comment la banque contrôle l'application des politiques et procédures de LBC/FT à l'échelle du groupe.

91. La fonction d'audit (interne et externe) du groupe joue un rôle particulièrement important dans l'évaluation de l'efficacité des politiques et procédures de LBC/FT. Les autorités de contrôle du pays d'origine doivent veiller à ce qu'il existe une politique appropriée, fondée sur les risques, et que des ressources suffisantes soient allouées en ce qui concerne l'étendue et la fréquence des audits de la LBC/FT du groupe. Elles doivent aussi s'assurer que les auditeurs ont accès à l'ensemble des rapports dont ils peuvent avoir besoin au cours de l'audit.

92. Les autorités de contrôle doivent veiller à ce que les informations relatives aux clients et aux opérations des banques soient soumises aux mêmes mesures de confidentialité que celles qui

[36] À titre d'exemple, les États ou territoires peuvent être publiquement désignés par :

- La *Déclaration publique* du GAFI, qui recense :
  - i) les États et territoires dont la LBC/FT présente des défaillances stratégiques et auxquels s'appliquent des contre-mesures ;
  - ii) les États et territoires dont la LBC/FT présente des défaillances stratégiques et qui n'ont pas fait de progrès suffisants pour les corriger ou qui ne se sont pas engagés sur un plan d'action établi avec le GAFI pour les corriger.
- Le document public du GAFI, *Améliorer la conformité aux normes de LBC/FT dans le monde : un processus permanent*, qui recense les États et territoires dont la LBC/FT présente des défaillances stratégiques et qui se sont engagés à un haut niveau politique à corriger ces défaillances en exécutant un plan d'action établi avec le GAFI.

[37] Dans les pays où l'examen est conduit par des auditeurs externes, cette exemption doit aussi s'appliquer aux auditeurs compétents.

s'appliquent au large éventail d'informations partagées entre les autorités de contrôle sur les activités des banques.

93. Il est indispensable que tous les pays qui accueillent des banques étrangères aient un cadre juridique approprié pour faciliter la transmission des informations nécessaires à la gestion des risques clients au siège ou à la banque mère et aux autorités de contrôle du pays d'origine. De même, aucune obstacle ni restriction ne doit s'opposer aux visites des auditeurs, des responsables des risques, des responsables conformité du siège du pays d'origine (y compris le responsable de la LBC/FT ou le responsable de la LBC/FT pour le groupe) ou des autorités de contrôle du pays d'origine sur le site des filiales et des succursales du pays d'accueil, ni à leur accès à l'ensemble des dossiers de la banque du pays d'accueil, y compris au nom et au solde des clients. Cet accès doit être le même pour toutes les succursales et filiales. Si des obstacles au partage d'informations s'avèrent insurmontables et en l'absence de dispositions alternatives satisfaisantes, les autorités de contrôle du pays d'origine doivent indiquer clairement à l'autorité de contrôle du pays d'accueil que la banque peut faire l'objet de mesures de contrôle additionnelles telles que des mesures de contrôle renforcées sur le groupe, et qu'il peut, s'il y a lieu, lui être demandé de cesser ses activités dans le pays d'accueil.

94. Lorsque le personnel du siège d'une banque a accès aux informations sur les clients locaux, rien ne doit s'opposer à ce qu'il transmette ces informations au siège. Ces informations, dont la confidentialité et l'utilisation doivent faire l'objet de protections adéquates, peuvent être soumises aux lois applicables en matière de respect de la vie privée et de secret professionnel dans le pays d'accueil.

95. Le Comité estime que rien ne justifie que la législation locale fasse obstacle au transfert des informations relatives aux clients d'une succursale ou d'une filiale bancaire dans un pays d'accueil au siège ou à la société mère dans le pays d'origine pour les besoins de la gestion des risques, notamment les risques de BC et de FT. Si la loi du pays d'accueil restreint la communication de ces informations à « des tiers », il est essentiel que le siège ou la société mère et les autorités de contrôle bancaire du pays d'origine soient clairement exclus de la définition d'un tiers. Les États ou territoires dont la législation fait obstacle ou peut être considérée comme faisant obstacle à ce partage d'informations aux fins de la gestion des risques de BC/FT sont vivement encouragés à supprimer ces restrictions et à prévoir des passerelles appropriées à cette fin.

Annexe 1

Recours à une autre banque, à un autre établissement financier ou à un tiers pour l'exécution des mesures de vigilance à l'égard de la clientèle

I. Introduction

1. Dans certains pays, les banques sont autorisées à recourir à des banques tierces, des établissements financiers ou d'autres entités pour exécuter les mesures de vigilance à l'égard de la clientèle. Ces dispositions peuvent prendre diverses formes mais elles entrent habituellement dans l'une ou l'autre des catégories suivantes :

Recours à des tiers

2. Dans certains pays, les banques sont autorisées à se fier aux mesures de vigilance à l'égard de la clientèle prises par d'autres établissements financiers ou par des entreprises et des professionnels non financiers désignés, qui sont eux-mêmes supervisés ou surveillés aux fins de la LBC/FT[38]. En règle générale dans ces situations, le tiers est déjà en relation d'affaires avec le client et les banques peuvent être exemptées de leurs mesures de vigilance au début de leur relation. Les normes du GAFI[39] permettent de recourir à un tiers pour les points suivants :

a) Identifier le client et vérifier son identité au moyen de documents, de données et d'informations provenant de sources fiables et indépendantes.

b) Identifier le bénéficiaire effectif et prendre des mesures raisonnables pour vérifier son identité de sorte que l'établissement financier soit certain de connaître l'identité du bénéficiaire effectif. Pour les personnes morales et les constructions juridiques, les établissements financiers doivent connaître la structure du capital et de contrôle du client.

c) Comprendre l'objet et la nature envisagée de la relation d'affaires et, le cas échéant, obtenir des informations sur ces points.

Les normes du GAFI exigent, en outre, qu'un établissement financier qui recourt à un tiers obtienne immédiatement les informations nécessaires concernant ces trois mesures de vigilance.

3. Certains pays limitent les possibilités de recourir à des tiers, par exemple en restreignant le recours à des établissements financiers, en n'autorisant le recours que pour les relations existantes des tiers (et en interdisant les recours en chaîne) ou en interdisant le recours à des entités étrangères.

[38] Voir la recommandation 17 et sa note interprétative dans les normes du GAFI.

[39] Voir la recommandation 17 et la recommandation 10 sur la vigilance à l'égard de la clientèle dans les normes du GAFI.

Sous-traitance/mandat

4. Les banques peuvent également recourir à des tiers pour exécuter certaines de leurs obligations de vigilance à l'égard de la clientèle dans le cadre d'un contrat, souvent de sous-traitance ou de mandat (c'est-à-dire que l'entité sous-traitante applique les mesures de vigilance à l'égard de la clientèle pour le compte de la banque). En général, les restrictions relatives aux personnes susceptibles d'agir en tant que mandataires d'une banque sont moindres, mais cette plus grande liberté est souvent compensée par des obligations relatives aux contrats passés et à la conservation des documents.

5. Tant pour le recours à des tiers que pour la sous-traitance, les banques peuvent choisir de limiter la taille, l'étendue ou la nature des opérations pour lesquelles elles recourent à des tiers. Dans tous les cas, les autorités de contrôle doivent avoir accès en temps opportun aux informations qu'elles demandent sur la clientèle. Bien que ces deux catégories semblent similaires ou voisines, elles présentent d'importantes différences et les banques doivent s'assurer qu'elles les comprennent et en tiennent compte dans leurs politiques et procédures.

II. Recours à des tiers

6. Les banques doivent instaurer des politiques et des procédures claires pour déterminer si et quand il est acceptable et prudent de recourir à une autre banque ou à un autre établissement financier. Ce recours n'exonère en rien la banque de sa responsabilité en dernier ressort, à savoir se doter de politiques et de procédures adéquates de vigilance à l'égard de la clientèle et respecter d'autres exigences de LBC/FT en ce qui concerne les clients – par exemple comprendre l'activité attendue et le niveau de risque des clients et détecter les opérations suspectes.

7. Lorsqu'elles recourent à une autre banque ou à un autre établissement financier pour exécuter certaines mesures de vigilance à l'égard de la clientèle, les banques doivent déterminer si ce recours est raisonnable. Le recours à des tiers doit être légalement autorisé, mais il doit aussi être évalué sur la base des critères suivants :

a) La banque, un établissement financier ou une autre entité (selon ce qu'autorise la législation nationale) sollicité doit être soumis à une réglementation et à un contrôle aussi complets que la banque, être tenu d'obligations comparables en matière d'identification des clients à l'ouverture des comptes et être déjà en relation d'affaires avec le client qui ouvre le compte à la banque. À défaut, la législation nationale peut imposer des mesures ou des contrôles compensatoires.

b) La banque et une autre entité doivent conclure un contrat écrit stipulant que la banque s'appuie sur les procédures de vigilance à l'égard de la clientèle de l'autre établissement financier.

c) Les politiques et procédures de la banque doivent documenter le recours et établir des contrôles et des procédures d'examen adéquats pour cette relation.

d) La banque peut demander au tiers de certifier qu'il a mis en œuvre son programme de lutte contre le blanchiment et que ses mesures de vigilance à l'égard de la clientèle sont pour l'essentiel équivalentes ou conformes aux obligations de la banque.

e) La banque doit dûment tenir compte des informations publiques négatives sur le tiers, comme les sanctions dont il peut faire l'objet pour insuffisances ou violations de ses obligations en matière de lutte contre le blanchiment.

f) La banque doit détecter et atténuer tout risque additionnel posé par le recours à des parties multiples (recours en chaîne) plutôt qu'à une seule entité.

g) L'évaluation des risques conduite par la banque doit identifier le recours à un tiers comme un facteur de risque potentiel.

h) La banque doit périodiquement examiner l'entité tierce pour s'assurer que les mesures de vigilance à l'égard de la clientèle que celle-ci applique demeurent aussi complètes que les siennes. À cette fin, elle doit obtenir l'ensemble des informations et des documents de vigilance à l'égard de la clientèle auprès du tiers auquel elle recourt et évaluer les vérifications effectuées, y compris les vérifications par rapport aux bases de données locales pour garantir le respect de la réglementation locale.

i) Les banques doivent envisager de cesser de recourir à des tiers qui n'appliquent pas de mesures de vigilance adéquates à leurs clients ou qui, d'une autre manière, ne remplissent pas leurs obligations et ne répondent pas aux attentes.

8. Les banques qui ont des filiales ou des succursales à l'étranger recourent fréquemment au groupe financier pour présenter leurs clients à d'autres secteurs du groupe. Dans les pays qui autorisent ce recours international à des sociétés associées, les établissements financiers qui recourent à d'autres secteurs du groupe pour l'identification de clients doivent veiller à ce que les critères d'évaluation ci-dessus soient en place. Les normes du GAFI[40] autorisent les pays à exclure le risque pays de cette évaluation si l'établissement financier est soumis aux règles de LBC/FT à l'échelle du groupe et supervisé à l'échelle du groupe par son autorité de contrôle financier.

III. Sous-traitance/mandat

9. Les banques peuvent choisir d'appliquer directement les procédures d'identification et d'autres procédures de vigilance à l'égard de la clientèle ou de charger un ou plusieurs tiers d'exécuter ces mesures pour leur compte, parfois dans le cadre d'une relation de mandat. Bien que des tiers puissent exercer les fonctions de conformité aux dispositions en matière de LBC/FT, la banque demeure responsable du respect des obligations de vigilance à l'égard de la clientèle et des dispositions en matière de LBC/FT. La mesure dans laquelle la banque recourt à des tiers dépend généralement de son modèle économique ; en principe, les banques qui travaillent par téléphone ou sur Internet ou qui ont peu d'agences « physiques » font davantage appel à des tiers pour développer leur clientèle ou améliorer l'assistance apportée à leurs clients et l'accès global à leurs services.

10. Les banques qui recourent à des tiers doivent veiller à ce qu'un contrat écrit énonce les obligations de la banque en matière de LBC/FT et leurs modalités d'exécution par le tiers. Dans certains pays, la relation entre les banques et leurs tiers est réglementée.

11. Comme il est indiqué plus haut, il est important que les banques comprennent la différence entre le recours à un tiers mandataire et le recours aux procédures d'identification des clients et de vigilance à l'égard de la clientèle d'une autre banque. En général, en vertu du droit du mandat, un mandataire est un prolongement juridique de la banque. Lorsqu'un client ou un client potentiel traite avec un mandataire de la banque, il traite légalement avec celle-ci. Le tiers aura donc l'obligation d'appliquer les politiques et les règles de la banque en matière d'identification, de vérification et de vigilance à l'égard de la clientèle.

12. En pratique, le tiers doit avoir l'expertise technique, les connaissances et la formation nécessaires pour appliquer les mesures d'identification des clients et de vigilance à l'égard de la clientèle

[40] Voir la recommandation 17 des normes du GAFI.

de la banque. Les tiers dont le modèle économique prévoit qu'ils agissent pour plusieurs banques peuvent acquérir une expertise interne considérable. Cependant, les tiers ne sont pas toujours soumis à des obligations de LBC/FT, même si beaucoup le sont. Quel que soit le cas, le tiers doit toujours appliquer les règles de son mandant en matière d'identification et de vigilance à l'égard de la clientèle (lesquelles doivent elles-mêmes être conformes aux obligations légales).

13. Les tiers auxquels les banques ont souvent recours pour exécuter leurs obligations d'identification des clients sont notamment des courtiers en dépôt de détail, des courtiers en prêts immobiliers et des notaires. L'atténuation des risques de BC/FT peut être compromise lorsque les banques ne veillent pas à ce que leurs tiers appliquent les obligations d'identification des clients et de vigilance à l'égard de la clientèle.

14. Comme il est indiqué plus haut, un contrat écrit doit documenter les responsabilités du tiers et prévoir les clauses suivantes :

a) exiger l'application des procédures de la banque en matière d'identification des clients et de vigilance à l'égard de la clientèle (notamment s'informer sur la source des fonds et du patrimoine le cas échéant) ;

b) exiger que, lorsque le client est présent en personne au moment de l'exécution des mesures d'identification ou de vigilance, le tiers applique des procédures d'identification du client qui prévoient la présentation des documents d'identité originaux lorsque la réglementation ou la banque l'impose ;

c) exiger que, lorsque le client n'est pas présent au moment de la vérification d'identité, le tiers applique les règles d'identification à distance prescrites ou stipulées par la banque ;

d) exiger que le tiers préserve la confidentialité des informations relatives au client.

15. Les banques doivent, en outre :

a) s'assurer que, s'il incombe au tiers de déterminer ou d'identifier le bénéficiaire effectif ou une PPE, ces responsabilités sont documentées ;

b) veiller à ce que le tiers fournisse les éléments d'identification du client dans les délais prescrits ;

c) procéder à un examen ou à un audit périodique et systémique de la qualité des informations relatives aux clients recueillies et documentées par le tiers afin de s'assurer qu'il respecte toujours les stipulations de la banque ;

d) définir clairement les hypothèses que la banque considérerait comme un manquement du tiers à ses obligations contractuelles et instaurer une procédure permettant de prendre les mesures appropriées, par exemple mettre fin à la relation en cas de carences.

16. La banque doit obtenir toutes les informations pertinentes auprès du tiers en temps utile et s'assurer que les informations sont complètes et tenues à jour dans le dossier du client.

17. Les contrats conclus avec des tiers doivent être revus et actualisés pour s'assurer qu'ils restent conformes aux missions dont le tiers est chargé et qu'ils tiennent compte de toute évolution de ces missions.

Annexe 2

Correspondance bancaire

I. Considérations générales sur la correspondance bancaire

1. Le glossaire du GAFI définit la correspondance bancaire comme « la prestation de services bancaires par une banque (la « banque correspondante ») à une autre banque (la « banque cliente ») ».

2. Les comptes de correspondants, qui sont utilisés par les banques dans le monde entier, permettent aux banques clientes d'exercer des activités et de fournir des services[41] qu'elles ne peuvent offrir directement (faute de réseau international). Les comptes de correspondants qui méritent une attention particulière concernent la fourniture de services dans des États ou territoires où les banques clientes n'ont pas de présence physique.

3. La banque correspondante traite/exécute des opérations pour les clients de la banque cliente. En général, elle n'a pas de relation d'affaires directe avec les clients de la banque cliente, qui peuvent être de personnes physiques, des sociétés ou des prestataires de services financiers. Le client de la banque correspondante est la banque cliente.

4. En raison de la structure de cette activité et du manque d'informations sur la nature ou l'objet des opérations sous-jacentes, les banques correspondantes peuvent être exposées à des risques particuliers de blanchiment de capitaux et de financement du terrorisme (risques de BC/FT).

II. Évaluation des risques de BC/FT liés à la correspondance bancaire – recueil des informations

5. Les banques qui ont des activités de correspondance bancaire doivent évaluer les risques de BC/FT associés à ces activités et appliquer des mesures appropriées de vigilance à l'égard de la clientèle.

6. Les banques correspondantes doivent recueillir suffisamment d'informations, au début de la relation et de manière continue par la suite, sur leurs banques clientes pour parfaitement comprendre la nature de leurs activités et évaluer correctement les risques de BC/FT en continu.

7. Les banques correspondantes doivent considérer notamment les facteurs suivants :

a) l'État ou le territoire dans lequel la banque cliente est établie ;

b) le groupe auquel appartient la banque cliente et les États ou territoires dans lesquels les filiales et succursales du groupe peuvent être établies ;

[41] Comme « la gestion de trésorerie (par exemple des comptes rémunérés dans plusieurs devises), les virements électroniques internationaux, la compensation de chèques, les comptes de passage et les services de change » comme l'indique le glossaire du GAFI.

c) les informations sur la direction et les propriétaires de la banque cliente (en particulier la présence de bénéficiaires effectifs ou de PPE), sa réputation[42], ses principales activités, ses clients et le lieu où ils sont établis ;

d) l'objet des services fournis à la banque cliente ;

e) l'activité de la banque cliente y compris ses marchés cibles et sa clientèle ;

f) la situation et la qualité de la réglementation et du contrôle bancaires dans le pays de la banque cliente (en particulier les lois et règlements en matière de LBC/FT) ;

g) les politiques et procédures de la banque cliente en matière de prévention et de détection du blanchiment de capitaux, comprenant une description des mesures de vigilance à l'égard de la clientèle qu'elle applique à ses clients ;

h) la possibilité d'obtenir l'identité de toute entité tierce qui pourra faire appel aux services de correspondance bancaire ;

i) l'utilisation potentielle du compte par d'autres banques clientes dans une relation de correspondance bancaire « imbriquée »[43].

8. Les informations relatives aux politiques et aux procédures de LBC/FT peuvent s'appuyer sur des questionnaires remplis par la banque cliente ou sur des informations publiques émanant de celle-ci (comme les informations financières ou toute information réglementée).

III. Exigences en matière de vigilance à l'égard de la clientèle

9. Si les banques correspondantes n'appliquent pas un niveau approprié de vigilance aux relations de correspondance bancaire, elles risquent de détenir ou de transmettre des fonds liés à des activités illicites.

10. Toutes les relations de correspondance bancaire doivent faire l'objet d'un niveau approprié de vigilance à l'égard de la clientèle. Les banques ne doivent pas traiter ces procédures de vigilance comme un exercice purement administratif de constitution de dossier mais comme une véritable évaluation du risque de BC. Le recueil d'informations doit être finalisé, si nécessaire, sur la base d'une réunion avec la direction et le responsable de la conformité de la banque cliente, l'autorité de tutelle/de contrôle, la cellule de renseignement financier et les organismes publics compétents.

11. Les informations recueillies dans le cadre des procédures de vigilance à l'égard de la clientèle doivent être régulièrement revues et actualisées suivant une approche fondée sur les risques. Elles doivent servir à actualiser les procédures d'évaluation des risques de la banque.

[42] La réputation peut comprendre des mesures/sanctions civiles, administratives ou pénales (amende, blâme, etc.) qui ont été prononcées par une juridiction judiciaire ou une autorité de contrôle.

[43] La correspondance bancaire est dite « imbriquée » lorsque plusieurs banques clientes se servent de leurs relations avec une banque directement cliente de la banque correspondante pour effectuer des opérations et accéder à des services financiers.

IV. Acceptation des clients

12. La décision d'accepter (ou de poursuivre) une relation de correspondance bancaire doit être approuvée par la direction générale de la banque correspondante.

13. Les informations peuvent provenir des rapports d'évaluation mutuelle du GAFI et de ses déclarations sur les États ou territoires soumis à des contre-mesures ou dont le dispositif de LBC/FT présente des défaillances stratégiques, ainsi que de rapports d'évaluation mutuelle produits par des organismes régionaux de type GAFI. Les banques peuvent également utiliser toute information publique émanant d'autorités nationales compétentes. Le fait qu'un pays soit soumis à des mesures restrictives doit être pris en compte, en particulier si des interdictions pèsent sur la fourniture de services de correspondance bancaire. Les banques correspondantes doivent être tout particulièrement vigilantes lorsqu'elles engagent ou poursuivent des relations avec des banques clientes sises dans des États ou territoires dont les normes en matière de LBC/FT présentent des insuffisances ou qui ont été qualifiés de « non coopératifs » dans la lutte contre le blanchiment de capitaux et le financement du terrorisme.

14. Les banques correspondantes doivent refuser d'établir ou de poursuivre une relation de correspondance bancaire avec une banque constituée dans un État ou territoire où elle n'a pas de présence physique et qui n'est pas affiliée à un groupe financier réglementé (c'est-à-dire des banques fictives).

V. Surveillance continue

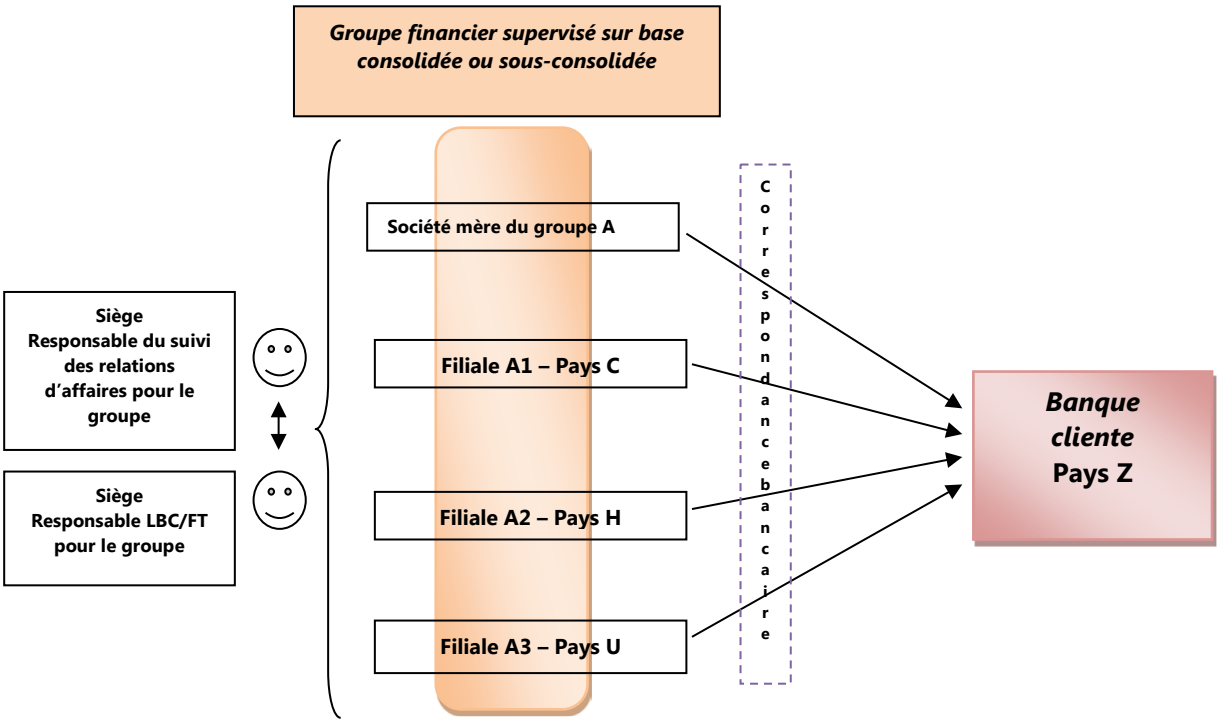
15. Une banque correspondante doit instaurer des politiques et des procédures appropriées afin de pouvoir détecter toute activité non conforme à l'objet des services fournis à la banque cliente ou contraire aux engagements conclus avec celle-ci.

16. Si une banque correspondante décide d'autoriser des tiers à utiliser directement les comptes de correspondants ou à effectuer des opérations pour leur propre compte (comptes de passage), elle doit exercer une surveillance renforcée sur ces activités, adaptée à leurs risques spécifiques. La banque correspondante doit vérifier que la banque cliente a pris des mesures adéquates de vigilance à l'égard des clients qui ont directement accès aux comptes de la banque correspondante et que la banque cliente est en mesure de fournir les informations utiles sur les mesures de vigilance à l'égard de la clientèle à la demande de la banque correspondante.

17. La direction générale doit être régulièrement informée des relations de correspondance bancaire à haut risque et des modalités de surveillance de ces relations.

VI. Considérations relatives aux groupes et aux opérations internationales

18. Lorsqu'une banque cliente a des relations de correspondance bancaire avec plusieurs entités appartenant au même groupe[44] (cas 1), le siège du groupe doit être particulièrement attentif à ce que les évaluations des risques effectuées par les différentes entités du groupe soient conformes à la politique d'évaluation à l'échelle du groupe. Le siège du groupe doit coordonner la surveillance de la relation avec la banque cliente, en particulier s'il s'agit d'une relation à haut risque, et veiller à ce que des mécanismes adéquats de partage d'informations soient en place au sein du groupe.

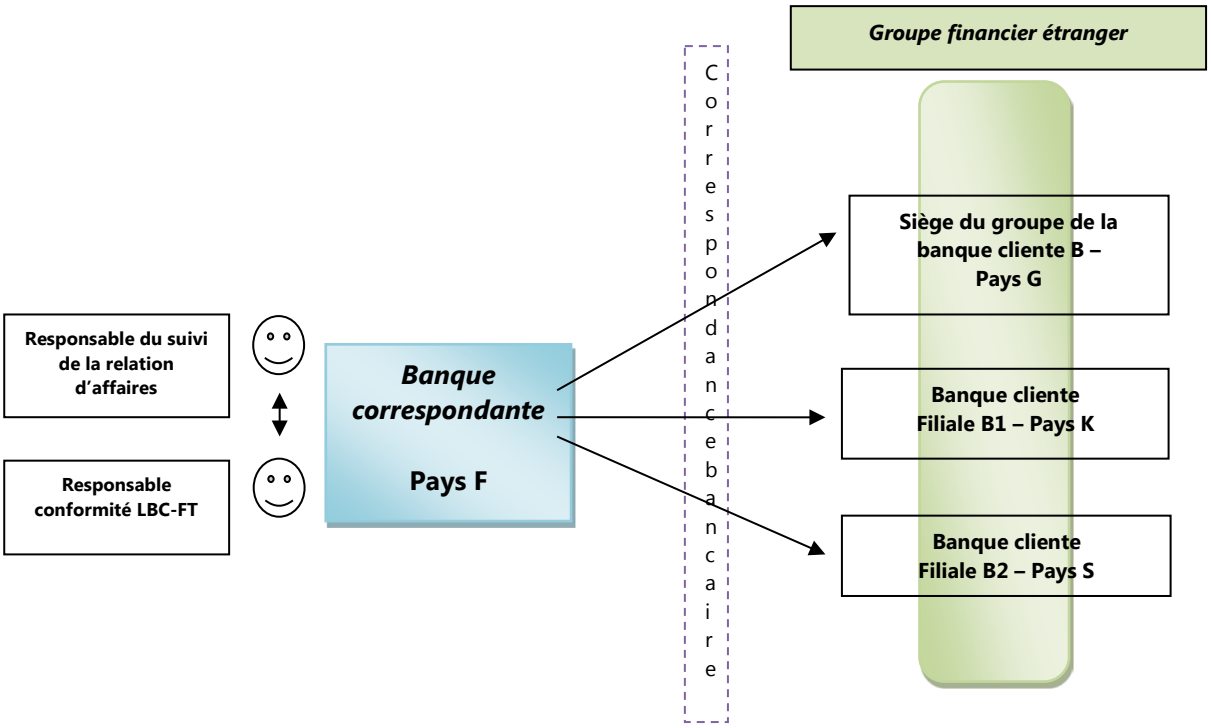


Cas 1

19. Si une banque correspondante a des relations d'affaires avec plusieurs entités appartenant au même groupe mais établies dans différents pays d'accueil (cas 2), elle doit tenir compte du fait que ces entités appartiennent au même groupe. Elle doit néanmoins évaluer les risques de BC/FT présentés par chaque relation d'affaires.

[44] Chaque entité fournit un service de correspondance bancaire dans son pays d'accueil.

Cas 2



VII. Gestion des risques

20. Une banque doit établir des procédures précises pour gérer les relations de correspondance bancaire. Les relations d'affaires doivent être formalisées par des contrats écrits qui définissent clairement les fonctions et responsabilités des banques partenaires.

21. La direction générale doit connaître les responsabilités et les fonctions des différents services (métiers, responsables de la conformité (y compris le responsable de la LBC/FT ou le responsable de la LBC/FT pour le groupe, audit, etc.) au sein de la banque en ce qui concerne les activités bancaires.

22. Les fonctions d'audit interne et de conformité de la banque[45] ont des responsabilités importantes car elles évaluent et assurent le respect des procédures relatives aux activités de correspondance bancaire. Les contrôles internes doivent couvrir les mesures d'identification des banques clientes, la collecte d'informations, la procédure d'évaluation des risques de BC/FT et la surveillance continue des relations de correspondance bancaire.

[45] Voir *The internal audit function in banks*, juin 2012, et le Principe fondamental 26 sur les contrôles internes et l'audit, *Principes fondamentaux pour un contrôle bancaire efficace,* septembre 2012.

Annexe 3

Recommandations correspondantes du GAFI

Nouvelles recommandations du GAFI (notes interprétatives comprises)
• R. 1 : Évaluation des risques et application d'une approche fondée sur les risques
• R. 2 : Coopération et coordination nationales
• R. 9 : Lois sur le secret professionnel des institutions financières
• R. 10 : Devoir de diligence à l'égard de la clientèle
• R. 11 : Conservation des documents
• R. 12 : PPE
• R. 13 : Correspondance bancaire
• R.15 : Nouvelles technologies
• R. 16 : Virements électroniques
• R. 17 : Recours à des tiers
• R. 18 : Contrôles internes et succursales et filiales à l'étranger
• R.20 : Déclaration des opérations suspectes
• R. 26 : Réglementation et contrôle des institutions financières
• R. 40 : Autres formes de coopération internationale