

Comité de Bâle sur le contrôle bancaire : Devoir de diligence des banques au sujet de la clientèle Octobre 2001

Groupe de travail sur les activités bancaires transfrontières

Table des matières

| | |
|--|----|
| I. Introduction | 1 |
| II. Importance des normes CC pour les autorités de contrôle et les banques | 2 |
| III. Éléments essentiels des normes CC | 4 |
| 1. Politique d'acceptation des nouveaux clients | 4 |
| 2. Identification de la clientèle | 5 |
| 2.1 Exigences générales d'identification | 6 |
| 2.2 Aspects particuliers de l'identification | 6 |
| 2.2.1 Comptes de fiducie et de mandataire | 6 |
| 2.2.2 Personnes morales | 6 |
| 2.2.3 Clientèle recommandée | 7 |
| 2.2.4 Comptes clients ouverts par des intermédiaires professionnels | 7 |
| 2.2.5 Personnes politiquement exposées (PPE) | 8 |
| 2.2.6. Clients à distance | 9 |
| 2.2.7 Banques correspondantes | 9 |
| 3. Surveillance continue des comptes et transactions | 10 |
| 4. Gestion des risques | 11 |
| IV. Rôle des autorités de contrôle | 12 |
| V. Mise en œuvre des normes CC dans un contexte transfrontière | 12 |
| Annexe 1: Extraits de <i>Méthodologie des Principes fondamentaux</i> | 14 |
| Annexe 2: Extraits des recommandations du GAFI | 16 |

1

Devoir de diligence des banques au sujet de la clientèle

I. Introduction

1. Les autorités de contrôle du monde entier admettent de plus en plus qu'il est essentiel, pour les banques de leur juridiction, de disposer de contrôles et procédures appropriés leur permettant de savoir avec qui elles traitent. Un aspect majeur de ces contrôles réside dans un devoir de diligence adéquat au sujet de la clientèle nouvelle et existante. Si ce devoir de diligence fait défaut, les banques peuvent être amenées à subir un préjudice financier substantiel lié au risque d'atteinte à la réputation, au risque opérationnel, au risque juridique et au risque de concentration.

2. En examinant les résultats d'une étude interne sur les activités bancaires transfrontières en 1999, le Comité de Bâle a décelé des lacunes, dans de nombreux pays, concernant les politiques suivies par les banques en matière de connaissance clientèle (CC). D'un point de vue prudentiel, ces approches présentent, dans certains cas, d'importantes déficiences et sont inexistantes dans d'autres;

même dans les pays dotés de marchés financiers bien développés, elles sont plus ou moins rigoureuses. Le Comité a donc demandé au Groupe de travail sur les activités bancaires transfrontières¹ d'analyser les procédures CC actuellement en vigueur et de définir des

normes dont l'application par les banques serait recommandée pour tous les pays. Le document produit a été publié aux fins de consultation en janvier 2001 puis amendé par le groupe à la suite des commentaires reçus. Le Comité diffuse actuellement dans le monde sa version révisée, dans l'espoir que le dispositif CC présenté serve de référence aux autorités de contrôle pour élaborer des pratiques nationales et aux banques pour concevoir leurs propres programmes. Il convient de préciser que les pratiques prudentielles de certaines juridictions atteignent ou dépassent déjà l'objectif de ce document et n'auront peut-être pas lieu d'être modifiées.

3. La connaissance de la clientèle est très étroitement associée à la lutte contre le blanchiment, qui est essentiellement du ressort du Groupe d'action financière sur le blanchiment de capitaux

(GAFI)². Le Comité, qui n'entend pas reprendre les travaux du GAFI, œuvre dans une perspective prudentielle plus large. De saines politiques et procédures CC jouent un rôle majeur pour préserver la sûreté et la solidité des banques ainsi que l'intégrité des systèmes bancaires. Le Comité et le Groupe offshore des autorités de contrôle bancaire demeurent résolument favorables à l'adoption et la mise en œuvre des recommandations du GAFI, notamment celles qui concernent les banques, et désirent que les normes contenues dans ce document soient compatibles avec les recommandations du GAFI.

Le Comité et le Groupe offshore envisageront également d'adopter des critères plus rigoureux qui seraient introduits par le GAFI, à la suite de la révision qu'il effectue actuellement de ses 40 recommandations. C'est la raison pour laquelle le Groupe de travail maintiendra ses contacts étroits avec le GAFI au fur et à mesure que celui-ci poursuivra sa réflexion.

4. L'approche CC du Comité de Bâle s'inscrit, au-delà de la lutte contre le blanchiment, dans une perspective prudentielle plus vaste. De saines procédures à cet égard doivent être considérées comme un aspect essentiel d'une gestion efficace des risques bancaires. Les mesures de protection dépassent le cadre d'une simple opération d'ouverture et de tenue de compte; elles exigent de la part des banques la mise au point d'une politique d'acceptation de la clientèle et d'un programme d'identification à plusieurs niveaux impliquant un devoir de diligence plus rigoureux à l'égard des comptes à hauts risques et une surveillance vigilante des activités suspectes.

5. L'intérêt du Comité de Bâle pour des normes CC saines est lié à son souci d'intégrité du marché et a été avivé par les pertes, directes et indirectes, encourues par des banques à cause de

1 Groupe de travail conjoint comprenant des membres du Comité de Bâle et du Groupe offshore des autorités de contrôle bancaire.

2 Organisme intergouvernemental qui a pour objectif de concevoir et de promouvoir des stratégies nationales et internationales de lutte contre le blanchiment de capitaux. Le GAFI compte 29 pays membres et deux organisations régionales. Il travaille en étroite coopération avec d'autres instances internationales actives dans ce domaine, telles que le Bureau des Nations Unies du contrôle des drogues et de la prévention des crimes, le Conseil de l'Europe, le Groupe Asie-Pacifique sur le blanchiment d'argent et la Caribbean Financial Action Task Force. Le GAFI définit le blanchiment de capitaux comme le processus consistant à retraiter les produits d'origine criminelle pour en masquer l'origine illégale.

2 leur manque de diligence dans l'application de procédures appropriées. Ces pertes auraient probablement pu être évitées et auraient nettement moins affecté la réputation des établissements si ceux-ci avaient disposé de programmes CC efficaces.

6. Le présent document conforte les principes déjà définis dans des rapports antérieurs du Comité, en fournissant des indications plus précises sur les éléments essentiels des normes CC et sur leur mise en œuvre. À cet effet, le Groupe de travail s'est inspiré des pratiques suivies dans les pays membres et a pris en compte l'évolution dans le domaine prudentiel. Les

éléments essentiels présentés dans ce document constituent des recommandations de normes minimales applicables par les banques à l'échelle mondiale. Ces normes pourront être complétées au besoin et/ou renforcées par des mesures complémentaires adaptées aux risques encourus par des établissements particuliers ou par le système bancaire de tel ou tel pays. Ainsi, un surcroît de diligence est requis à l'égard des comptes à hauts risques ou de la part des banques qui cherchent précisément à attirer une clientèle à patrimoine élevé. Plusieurs parties de ce document comportent des recommandations de normes de diligence plus strictes destinées, le cas échéant, aux domaines à hauts risques des banques.

7. Les banques ne sont pas les seules à avoir besoin de normes de diligence rigoureuses à l'égard de la clientèle. Le Comité est convaincu que des recommandations du même ordre doivent être élaborées pour tous les établissements financiers non bancaires et intermédiaires offrant des services financiers tels que juristes et comptables.

II. Importance des normes CC pour les autorités de contrôle et les banques

8. Le GAFI ainsi que d'autres instances internationales ont œuvré intensément sur les questions CC, et les 40 recommandations du GAFI sur la lutte contre le blanchiment de capitaux sont reconnus et appliqués dans le monde entier³. L'objet du présent document n'est donc pas de reprendre ces travaux.

9. Dans le même temps, de saines procédures CC présentent une importance particulière pour la sécurité et la solidité des banques dans la mesure où:

- elles contribuent à préserver la réputation des banques et l'intégrité des systèmes bancaires, en réduisant la probabilité que les établissements ne deviennent instruments ou victimes de criminalité financière et ne subissent de graves préjudices résultant d'une atteinte à leur réputation;
- elles constituent un élément essentiel d'une saine gestion des risques (par exemple, en permettant l'identification, la limitation et le contrôle des expositions en regard d'actifs et de passifs, y compris les actifs gérés).

10. L'inadéquation ou l'absence de normes CC peut exposer les banques à des risques sérieux liés à sa clientèle et à ses contreparties, notamment **risque d'atteinte à la réputation**, **risque opérationnel**, **risque juridique** et **risque de concentration**. Il est intéressant de noter que tous ces risques, bien qu'interdépendants, peuvent entraîner individuellement des coûts financiers substantiels pour les banques (sous la forme, par exemple, de retraits de fonds par des déposants, de ruptures de facilités interbancaires, d'actions contre l'établissement, de frais d'enquête, de saisies et gels d'actifs ainsi que de pertes sur prêts) et nécessiter, de la part des dirigeants, beaucoup de temps et d'énergie pour résoudre les problèmes qui se posent.

11. Le **risque d'atteinte à la réputation** constitue une lourde menace pour les banques, étant donné que la nature de leurs activités nécessite le maintien de la confiance des déposants, des créanciers et du marché en général. Ce risque se définit comme l'éventualité qu'une publicité défavorable, justifiée ou non, concernant des pratiques et connexions d'une banque n'entraîne une perte de confiance dans l'intégrité de l'établissement. Les banques sont particulièrement vulnérables à ce type de risque, car elles peuvent facilement devenir l'instrument ou la cible d'activités illégales de

³ Recommandations 10 à 19, Annexe 2.

leurs clients. Elles doivent se protéger en exerçant une vigilance constante grâce à un programme CC efficace. Les actifs gérés ou détenus en fiducie peuvent poser des risques spécifiques d'atteinte à la réputation.

12. Le **risque opérationnel** peut se définir comme le risque de pertes directes ou indirectes résultant d'une inadéquation ou d'une défaillance attribuable à des procédures, personnes, systèmes internes ou à des événements extérieurs. Dans le contexte CC, la plupart des cas de risque opérationnel sont liés à des lacunes dans la mise en œuvre des programmes des banques, à l'inefficacité des procédures de contrôle et à des manquements au devoir de

diligence. Si le public a l'impression qu'une banque n'est pas capable de gérer efficacement son risque opérationnel, les affaires de celle-ci peuvent en être perturbées ou compromises.

13. Le *risque juridique* réside dans la possibilité que des procès, des jugements défavorables ou l'impossibilité d'exécution de contrats perturbent ou compromettent les opérations ou la situation d'un établissement. Des banques peuvent faire l'objet de poursuites du fait de la non-observation de normes CC obligatoires ou de manquement au devoir de diligence. Elles peuvent alors encourir des amendes, responsabilités pénales ou sanctions spéciales imposées par les autorités de contrôle.

D'ailleurs, le fait d'être impliqué dans un procès peut avoir pour une banque des répercussions financières bien plus coûteuses que les simples frais de procédure. Les banques ne seront pas en mesure de se protéger efficacement de tels risques juridiques si elles n'assument pas leur devoir de diligence dans l'identification de la clientèle et la connaissance de leurs activités.

14. Les préoccupations prudentielles relatives au *risque de concentration* concernent essentiellement l'actif du bilan. En règle générale, non seulement les autorités de contrôle exigent des banques qu'elles disposent de systèmes d'information permettant de déceler les concentrations de crédits, mais, la plupart du temps, elles fixent aussi des limites prudentielles à leurs expositions envers des emprunteurs individuels ou groupes d'emprunteurs liés. Sans connaissance précise de ses clients et des relations qui existent au sein de sa clientèle, il sera impossible à une banque de mesurer son risque de concentration, surtout en présence de contreparties liées ou de prêts apparentés.

15. Au passif, le risque de concentration est étroitement lié au risque de financement, notamment le risque de retrait anticipé et soudain de fonds de la part de gros déposants, qui peut avoir des conséquences néfastes pour la liquidité de la banque. Le risque de financement est sans doute plus élevé pour les banques de petite taille et les établissements relativement peu actifs sur les marchés de gros. Pour analyser les concentrations de dépôts, les banques doivent connaître les caractéristiques de leurs déposants, c'est-à-dire non seulement leur identité mais aussi les interactions éventuelles avec d'autres déposants. Il est essentiel que les gestionnaires de passif des petites banques connaissent les gros déposants et entretiennent des relations étroites avec eux;

sinon, ils courent le risque de perdre leurs fonds à des moments critiques.

16. Il arrive fréquemment que des clients aient plusieurs comptes auprès du même établissement, mais dans des pays différents. Pour gérer efficacement le risque d'atteinte à la réputation, le risque de non-respect des règles et le risque juridique inhérents à ces comptes, les banques devraient être capables d'agrèger et de surveiller les soldes et transactions importants de ces comptes sur une base consolidée à l'échelle mondiale, que les actifs soient au bilan, gérés au hors-bilan ou détenus en fiducie.

17. Le Comité de Bâle comme le Groupe offshore des autorités de contrôle bancaire sont pleinement convaincus que des pratiques CC efficaces devraient faire partie intégrante des systèmes de gestion des risques et de contrôles internes dans toutes les banques. Il incombe aux responsables prudentiels nationaux de s'assurer que les établissements disposent de normes minimales et de contrôles internes leur procurant une connaissance adéquate de leur clientèle. Les codes de conduite à adhésion volontaire élaborés par les organisations ou associations professionnelles peuvent être très utiles pour étayer les recommandations réglementaires, par les conseils pratiques qu'ils donnent aux banques sur des questions opérationnelles⁴, mais ne sauraient toutefois s'y substituer.

⁴ C'est le cas, par exemple, des *Global anti-money-laundering guidelines for Private Banking* (ou Principes Wolfsberg), publiés en octobre 2000 par douze grandes banques ayant d'importantes activités de banque privée.

III. Éléments essentiels des normes CC

18. Le Comité de Bâle a publié des recommandations CC dans trois documents, qui reflètent l'évolution dans le temps de la pensée prudentielle. Le premier, *Prévention de l'utilisation du système bancaire pour le blanchiment de fonds d'origine criminelle* (1988), expose les principes éthiques de base et encourage les banques à mettre en place des procédures efficaces pour identifier la clientèle, refuser les transactions douteuses et coopérer avec les instances chargées de l'application des lois.

Le deuxième, *Principes fondamentaux pour un contrôle bancaire efficace* (1997), procède à une analyse plus large des contrôles internes; il précise que les banques devraient disposer de politiques, pratiques et procédures appropriées - notamment des règles CC rigoureuses - et que les autorités de contrôle devraient encourager l'adoption des recommandations correspondantes du GAFI. Celles-ci portent sur l'identification des clients et la conservation des documents, une diligence accrue des institutions financières pour détecter et notifier les transactions douteuses ainsi que sur les mesures à appliquer à l'égard des pays où les dispositions contre le blanchiment de capitaux sont inadéquates.

La *Méthodologie des Principes fondamentaux* (1999) complète le document de 1997 en énumérant plusieurs autres critères essentiels additionnels (les passages concernés des *Principes fondamentaux* et de la *Méthodologie* sont reproduits dans l'Annexe 1).

19. Toutes les banques devraient être tenues de «disposer de politiques, pratiques et procédures de nature à promouvoir un haut degré d'éthique et de professionnalisme et à empêcher qu'elles ne soient utilisées, intentionnellement ou non, dans le cadre d'activités criminelles»⁵. Lors de l'élaboration de leurs programmes CC, elles devraient prendre en compte certains éléments essentiels dès le stade de la gestion des risques et des procédures de contrôle: 1) politique d'acceptation des nouveaux clients; 2) identification de la clientèle; 3) surveillance continue des comptes à hauts risques; 4) gestion des risques. Les banques devraient non seulement déterminer l'identité de leurs clients mais surveiller aussi les mouvements de comptes pour déceler les transactions atypiques ou inhabituelles pour un client précis ou une catégorie de compte. La connaissance de la clientèle devrait constituer un élément clé de la gestion des risques et des procédures de contrôle des banques et être régulièrement complétée par des vérifications du respect des règles et un audit interne. Indépendamment de cela, l'intensité des programmes CC devrait être adaptée au degré de risque.

1. Politique d'acceptation des nouveaux clients

20. Les banques devraient définir des politiques et procédures claires d'acceptation des nouveaux clients comprenant notamment la description des types de clientèle susceptibles de représenter pour elles un risque supérieur à la moyenne. Pour cela, elles devraient prendre en compte des facteurs tels que les antécédents de leurs clients, leur pays d'origine, le fait qu'il s'agit de personnages publics ou en vue, les liens entre comptes, leurs activités professionnelles ainsi que d'autres indicateurs de risque. Ces politiques et procédures des banques devraient être graduées, c'est-à-dire qu'elles devraient requérir un renforcement du devoir de diligence vis-à-vis de la clientèle à hauts risques; ainsi, une personne exerçant une activité rémunérée présentant un faible solde pourrait se voir appliquer les exigences les plus élémentaires en matière d'ouverture de compte. Il convient de veiller, cependant, à ce que la politique d'acceptation des nouveaux clients ne soit pas à ce point restrictive qu'elle empêche le grand public, en particulier les personnes en situation financière ou sociale précaire, d'accéder aux services bancaires. En revanche, un devoir de diligence très rigoureux serait indispensable envers une personne ayant une fortune élevée d'origine incertaine. La décision d'ouvrir des relations d'affaires avec des clients à hauts risques, tels que des personnes

politiquement exposées (voir 2.2.3), devrait être prise exclusivement au niveau de la direction générale.

5 Méthodologie des Principes fondamentaux, Critère essentiel n° 1.

2. Identification de la clientèle

21. L'identification de la clientèle est un élément clé des normes CC. Aux fins du présent document, on désigne par le terme «client»:

- toute personne ou entité titulaire d'un compte auprès de la banque ou au nom de laquelle un compte est ouvert (bénéficiaire effectif du compte);
- les bénéficiaires de transactions effectuées par des intermédiaires professionnels;
- toute personne ou entité associée à une transaction financière susceptible d'entraîner, pour la banque, un risque important d'atteinte à la réputation ou d'autre nature.

22. Les banques devraient prévoir une procédure systématique d'identification des nouveaux clients et ne pas ouvrir de relations d'affaires avec un client tant que son identité n'est pas dûment vérifiée.

23. Les banques devraient disposer de «politiques explicitées et appliquées pour identifier les clients et leurs mandataires»⁶. Pour vérifier l'identité des clients, les meilleurs documents sont ceux qui sont le plus difficile à obtenir illicitement et à contrefaire. Une attention particulière devrait être consacrée aux clients non résidents, et une banque ne devrait en aucun cas renoncer aux procédures d'identification pour la simple raison que le nouveau client n'est pas en mesure d'être présent en personne à un entretien. Les banques devraient toujours se demander pourquoi le client a choisi d'ouvrir un compte dans une juridiction étrangère.

24. La procédure d'identification intervient normalement lors de l'établissement de la relation d'affaires. Pour s'assurer que les données qu'elles détiennent sont d'actualité, les banques doivent les revoir régulièrement, par exemple à l'occasion d'une grosse transaction, d'une modification substantielle des normes de documentation sur la clientèle ou d'un changement important dans le mode de gestion du compte⁷. Toutefois, si une banque réalise à un moment donné qu'elle manque d'informations au sujet d'un client existant, elle devra prendre des mesures pour obtenir le plus tôt possible tous les renseignements nécessaires.

25. Les établissements offrant des services de banque privée, particulièrement exposés au risque d'atteinte à la réputation, devraient renforcer leur devoir de diligence sur ces opérations. Des comptes de banque privée, qui impliquent par nature une grande part de confidentialité, peuvent être ouverts au nom d'un individu, d'une entreprise commerciale, d'une société fiduciaire, d'un intermédiaire ou d'une entreprise d'investissement personnalisée. Dans tous les cas, un risque d'atteinte à la réputation peut apparaître si la banque ne suit pas avec diligence les procédures CC établies. Tout nouveau client ou compte devrait être approuvé par au moins une personne, de niveau hiérarchique suffisamment élevé, autre que le chargé de relation pour les activités de banque privée.

Même si des mesures spécifiques sont prises à l'intérieur de la banque pour préserver la confidentialité des clients et de leurs transactions dans ce domaine, les établissements doivent veiller à ce qu'il soit toujours possible de soumettre ces clients et leurs opérations à un examen et une surveillance au moins aussi rigoureux, sous la forme, par exemple, d'une inspection des responsables conformité et des auditeurs.

26. Les banques devraient élaborer «des règles claires [précisant] quelles sont les données à conserver sur l'identification de la clientèle et les transactions individuelles et sur quelle durée»⁸. De telles pratiques sont essentielles pour qu'un établissement puisse surveiller sa relation avec le client, comprendre ses activités courantes et, si nécessaire, fournir des preuves en cas de différend, d'action judiciaire ou d'enquête financière pouvant conduire à des poursuites pénales. Pour entamer la procédure d'identification et en exploiter les résultats, les banques devraient se procurer des pièces d'identité du client et en conserver des copies pendant au moins cinq ans après la clôture du compte.

Elles devraient également garder, sur la même période, tous les enregistrements des transactions financières à compter de leur réalisation.

6 *Méthodologie des Principes fondamentaux*, Critère essentiel n° 2.

7 L'application de nouvelles normes CC aux comptes existants est actuellement soumise à l'appréciation du GAFI.

8 *Méthodologie des Principes fondamentaux*, Critère essentiel n° 2.

2.1 Exigences générales d'identification

27. Les banques doivent obtenir toutes les informations nécessaires pour établir, à leur entière satisfaction, l'identité de chaque nouveau client ainsi que l'objet et la finalité de la relation. L'ampleur et la nature des données dépendent de la qualité du candidat (particulier, entreprise, etc.) et du solde prévu sur le compte. Les autorités de contrôle nationales sont invitées à fournir des recommandations pour aider les banques à mettre au point leurs procédures d'identification. Le Groupe de travail se propose de définir les éléments essentiels des exigences à cet égard.

28. Quand, après l'ouverture d'un compte, apparaissent des problèmes de vérification insolubles, la banque devrait fermer le compte et restituer le solde⁹.

29. Si une banque peut être assez confiante lorsque, pour l'ouverture d'un compte, elle reçoit des fonds d'un autre établissement soumis aux mêmes normes CC, elle devrait cependant envisager la possibilité que le gestionnaire précédent ait demandé la fermeture du compte par crainte d'activités douteuses. Un client a naturellement le droit de transférer un compte d'un établissement à un autre.

Toutefois, si une banque a la moindre raison de penser qu'un candidat s'est vu exclure des services bancaires, elle devrait renforcer les procédures CC à son égard.

30. Une banque ne devrait jamais accepter d'ouvrir un compte ou de maintenir des relations d'affaires avec un client qui exige l'anonymat ou se présente sous un faux nom. Les comptes à numéro confidentiel¹⁰ ne devraient pas, non plus, servir à protéger l'anonymat, mais être soumis aux procédures CC normales, même si les vérifications sont effectuées par un personnel spécial. Si un compte à numéro peut offrir une plus grande confidentialité à son titulaire, l'identité de celui-ci doit cependant être connue d'un nombre d'employés suffisant à l'exercice adéquat du devoir de diligence.

En aucun cas, ces comptes ne sauraient être utilisés pour dissimuler l'identité du client à la fonction conformité de l'établissement ou aux autorités prudentielles.

2.2 Aspects particuliers de l'identification

31. Plusieurs aspects particuliers doivent être précisés. Certains sont actuellement examinés par le GAFI dans le cadre de la révision générale de ses 40 recommandations, et le Groupe de travail reconnaît la nécessité d'une harmonisation avec ses travaux.

2.2.1 Comptes de fiducie et de mandataire

32. Les comptes de fiducie et de mandataire peuvent servir à contourner les procédures d'identification de la clientèle. S'il peut être justifié, dans certaines circonstances, d'offrir un niveau de sécurité supplémentaire pour préserver la confidentialité d'une activité légitime de banque privée, il est essentiel que la banque comprenne la véritable nature de la relation. Elle devrait établir si un client se fait passer pour un autre, s'il sert de «couverture» ou s'il agit au nom d'un tiers en qualité d'intermédiaire, tel que fidéicommiss. En pareil cas, il est nécessaire qu'elle reçoive, préalablement à l'ouverture du compte, des justificatifs de l'identité de tous les intermédiaires et des personnes au nom desquelles ils agissent ainsi que des précisions concernant la nature de la fiducie ou de tout autre arrangement conclu. En présence d'une fiducie, l'identification porte également sur les fidéicommiss, fiduciaires/constituants et bénéficiaires¹¹.

2.2.2 Personnes morales

33. Les banques doivent exercer leur vigilance pour éviter que des particuliers n'aient recours à des personnes morales pour disposer en fait de comptes anonymes. Dans le cas de structures (comme les International Business Companies - IBC) détenant des actifs individuels, l'identification du 9 Sous réserve des réglementations nationales concernant le traitement des opérations suspectes.

10 Le nom du bénéficiaire d'un tel compte est connu de la banque, mais remplacé par un numéro ou code dans la documentation ultérieure.

11 Dans la mesure du possible, les bénéficiaires devraient être identifiés lorsqu'ils sont définis. Cela peut ne pas être possible d'emblée. C'est le cas, par exemple, s'il s'agit d'enfants à naître ou si le bénéfice est subordonné à la réalisation d'événements déterminés. En outre, les bénéficiaires définis comme groupe (par exemple participants à un fonds de pension) peuvent à juste titre être traités à l'instar des comptes collectifs (paragraphe 38-39).

client ou bénéficiaire peut être difficile. Une banque devrait comprendre la structure de la société, déterminer la provenance des fonds et identifier leurs bénéficiaires ainsi que les personnes qui contrôlent ces fonds.

34. Une banque doit être spécialement vigilante lors de l'ouverture de relations avec des sociétés dont le capital est constitué d'actions au porteur ou détenu par des mandataires. Elle doit obtenir des justificatifs établissant de manière satisfaisante l'identité des bénéficiaires. Sa vigilance doit être accrue dans le cas de sociétés dont une part importante du capital se présente sous forme d'actions au porteur, celles-ci pouvant changer de mains à son insu. Il incombe aux banques de mettre en place des procédures satisfaisantes de contrôle de l'identité des principaux bénéficiaires, au besoin en immobilisant les actions, par exemple en les conservant en dépôt.

2.2.3 Clientèle recommandée

35. Les procédures d'identification peuvent prendre beaucoup de temps et les banques désirent naturellement éviter les désagréments pour leurs nouveaux clients. Aussi, dans certains pays, il est courant qu'elles s'en remettent aux procédures menées par d'autres établissements ou des intermédiaires lorsque ceux-ci leur adressent un client. Dans ce cas, elles risquent d'accorder une confiance excessive aux procédures CC que ces tiers sont censés avoir réalisées. Se fonder sur elles, quelle que soit la réputation de l'intermédiaire, ne dispense pas les banques de connaître leur clientèle et ses activités, responsabilité qui leur incombe en dernière instance. Les banques devraient notamment ne pas faire confiance à des intermédiaires soumis à des normes inférieures à leurs propres procédures CC ou qui refusent de communiquer les informations obtenues dans l'exercice de leur devoir de diligence.

36. Le Comité de Bâle recommande à une banque ayant recours à de tels intermédiaires d'évaluer soigneusement leur compétence et leur honorabilité et de vérifier qu'ils exercent le devoir de diligence exigé par les normes exposées dans le présent document. La responsabilité finale en matière de CC incombe toujours à la banque, qui devrait utiliser les critères suivants pour déterminer la fiabilité d'un tiers¹²:

- il doit respecter les pratiques minimales au titre du devoir de diligence exposées dans ce document;
- ses procédures liées au devoir de diligence doivent être aussi rigoureuses que celles que la banque aurait appliquées elle-même à l'égard de sa clientèle;
- la banque doit s'assurer de la fiabilité des systèmes qu'il a mis en place pour vérifier l'identité des clients;
- la banque doit avoir obtenu de lui l'autorisation de vérifier comment il s'acquitte à chaque stade de son devoir de diligence;
- il doit, sans délai, soumettre à la banque les informations de toute nature concernant l'identité des clients et celle-ci doit les examiner soigneusement. Ces informations doivent être tenues à la disposition de l'autorité prudentielle et de l'organisme de renseignement

financier ou autorité exerçant des compétences équivalentes, lorsque la loi leur confère ce pouvoir.

En outre, les banques devraient effectuer des examens périodiques pour s'assurer que l'intermédiaire auquel elles font confiance remplit toujours les critères exposés ci-dessus.

2.2.4 Comptes clients ouverts par des intermédiaires professionnels

37. Lorsqu'une banque sait ou a des raisons de penser qu'un intermédiaire professionnel a ouvert un compte au bénéfice d'un client unique, celui-ci doit être identifié.

38. Les banques disposent souvent de comptes collectifs, soit gérés par des intermédiaires professionnels agissant au nom d'entités telles que fonds communs de placement, fonds de pension et fonds de trésorerie, soit contenant des sommes en dépôt ou sous séquestre gérées par des juristes

12 Le GAFI examine actuellement s'il convient d'agrèer de tels intermédiaires.

ou courtiers en faveur de divers clients. Si les sommes détenues par l'intermédiaire ne sont pas fusionnées mais réparties en sous-comptes correspondant aux différents bénéficiaires, ceux-ci doivent être tous identifiés.

39. Lorsque les sommes sont fusionnées, leur bénéficiaire devrait être transparent pour la banque. Dans certains cas, il n'est peut-être pas nécessaire que la banque aille en amont de l'intermédiaire, par exemple quand celui-ci est soumis aux mêmes réglementations et procédures relatives au contrôle prudentiel et au blanchiment de capitaux, notamment en ce qui concerne le devoir de diligence. Les recommandations des autorités prudentielles nationales devraient clairement

préciser ces cas. Les banques devraient accepter de tels comptes uniquement si elles peuvent établir que l'intermédiaire a effectué un processus CC adéquat et qu'il dispose des systèmes et contrôles nécessaires pour affecter correctement les actifs en compte à leurs propriétaires respectifs. Pour évaluer la façon dont l'intermédiaire s'acquitte de son devoir de diligence, la banque devrait avoir recours aux critères énoncés au paragraphe 36.

40. Lorsque l'intermédiaire n'est pas habilité à fournir à la banque les informations nécessaires sur les bénéficiaires (par exemple, juristes tenus au secret professionnel¹³) ou lorsqu'il n'est pas assujéti à des normes de diligence équivalentes à celles énoncées ici ou à celles d'une législation antiblanchiment rigoureuse), la banque ne devrait pas lui permettre d'ouvrir un compte.

2.2.5 Personnes politiquement exposées (PPE)

41. Entretenir des relations d'affaires avec les détenteurs de postes publics élevés et des personnes ou sociétés qui leur sont clairement liées peut exposer la banque à un risque d'atteinte à la réputation et/ou un risque juridique non négligeables. Les personnes politiquement exposées exercent ou ont exercé d'importantes fonctions publiques: chefs d'État ou de gouvernement, figures politiques, hauts fonctionnaires de l'administration, de la magistrature ou de l'armée, cadres dirigeants de sociétés publiques et responsables de grand parti politique, par exemple. On ne peut exclure, notamment dans les pays où la corruption est répandue, que ces personnes abusent de leur pouvoir officiel pour obtenir un enrichissement personnel par des voies illicites (pots-de-vin, détournement de fonds, etc.).

42. Accepter et gérer les fonds de PPE corrompues entache gravement la réputation de l'établissement et peut ébranler la confiance du public dans les normes éthiques de tout centre financier, étant donné que les affaires de cette nature reçoivent normalement une importante couverture médiatique et suscitent une vive réaction politique, même s'il est souvent difficile de prouver l'origine illicite des actifs. En outre, la banque peut faire l'objet, de la part des autorités policières ou judiciaires, de demandes d'informations et mesures de saisie coûteuses (pouvant aller jusqu'à des procédures internationales d'assistance mutuelle en matière pénale), voire être appelée en dommages-intérêts par l'État lésé ou les victimes d'un régime. Dans certaines circonstances, la banque et/ou ses responsables et employés peuvent être eux-

mêmes exposés à des accusations de blanchiment s'ils savaient, ou auraient dû savoir, que les fonds provenaient d'activités criminelles (corruption, par exemple).

43. Certains pays viennent d'amender, ou modifient, leur législation et leur réglementation de façon à criminaliser la corruption active de fonctionnaires et agents publics étrangers, conformément à la convention internationale sur ce sujet¹⁴. Dans ces juridictions, la corruption d'agents étrangers est qualifiée d'acte de blanchiment et tombe ainsi sous le coup de toutes les lois et réglementations antiblanchiment (par exemple, déclaration des transactions douteuses, interdiction d'informer le client, gel interne des fonds, etc.). Toutefois, même en l'absence d'une telle base légale explicite en droit pénal, il est évidemment peu souhaitable pour une banque, contraire à l'éthique - comme au critère de compétence et d'honorabilité dans la conduite des opérations -, d'accepter ou d'entretenir des relations d'affaires lorsqu'elle sait, ou a toutes les raisons de penser, que les fonds proviennent d'actes de corruption ou d'un détournement de fonds publics. Une banque envisageant d'établir une

13 Le GAFI procède actuellement à un examen des procédures CC régissant les comptes ouverts par des juristes au nom de leurs clients.
14 OCDE: Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales, adoptée par la Conférence de négociations le 21 novembre 1997.⁹

relation d'affaires avec une personne qu'elle soupçonne être politiquement exposée doit l'identifier avec précision, de même que les particuliers et sociétés qui lui sont manifestement liés.

44. Les banques devraient obtenir d'un nouveau client suffisamment de renseignements et vérifier les sources d'information publique afin d'établir s'il s'agit d'une PPE. Dans ce cas, elles devraient se renseigner sur l'origine de ses fonds avant de l'admettre, décision qui relève de la haute direction.

2.2.6. *Clients à distance*

45. De plus en plus, il est demandé aux banques d'ouvrir un compte au nom de clients qui ne se présentent pas en personne pour un entretien. Courante dans le cas de la clientèle non résidente, cette pratique s'est fortement développée avec l'expansion récente de la banque postale, téléphonique et électronique. Les banques devraient appliquer à ces clients des procédures d'identification et des normes de surveillance permanente tout aussi efficaces qu'avec les autres. La possibilité d'une vérification indépendante par un tiers de réputation confirmée a été évoquée à cet égard. L'ensemble de cette question est examiné par le GAFI ainsi que dans le contexte de la modification de la Directive CEE de 1991.

46. L'exemple typique est celui du client qui souhaite effectuer des opérations bancaires par Internet ou une technologie similaire. La banque électronique offre aujourd'hui une large gamme de produits et services accessibles par les réseaux de télécommunications; sa nature impersonnelle et transfrontière, combinée à la vitesse des transactions, rend nécessairement difficile l'identification des clients et la vérification. Les autorités de contrôle attendent des banques, au minimum, qu'elles anticipent les différents risques suscités par les technologies émergentes et mettent au point des procédures d'identification de la clientèle les prenant dûment en compte¹⁵.

47. Bien que la documentation à fournir soit la même pour tous, les banques ont plus de difficulté à vérifier que les informations correspondent au client en l'absence de contact physique. Le problème de la vérification se pose avec encore plus d'acuité dans le cas des relations par voies téléphonique et informatique.

48. Pour accepter de nouveaux clients à distance, les banques devraient:

- leur appliquer des procédures d'identification tout aussi efficaces que pour les clients se présentant à un entretien;
- prendre des mesures spécifiques et adéquates pour limiter ce risque accru, notamment:

- authentification des documents présentés;
- demande de documents supplémentaires;
- contact indépendant avec le client;
- intermédiation d'un tiers, sous réserve des critères énoncés au paragraphe 36; ou
- exigence d'un premier paiement par l'intermédiaire d'un compte ouvert au nom du client auprès d'un établissement soumis à des normes de diligence semblables.

2.2.7 Banques correspondantes

49. Une banque correspondante offre des services bancaires à une autre. Utilisé dans le monde entier, ce système permet aux banques d'exercer des activités et de fournir des services de manière indirecte. Certains comptes, méritant une attention particulière, proposent des services dans des juridictions où la banque n'est pas physiquement présente. Une banque qui n'appliquerait pas à ces comptes un devoir de diligence adéquat s'exposerait aux risques recensés dans le rapport et pourrait détenir et/ou transmettre des fonds liés à une activité illégale telle que corruption ou fraude.

50. Les banques devraient rassembler suffisamment d'informations sur leurs correspondants pour bien comprendre la nature de leurs activités. Elles devraient notamment se renseigner sur les 15 Le Groupe sur la banque électronique du Comité de Bâle a publié, en mai 2001, un document sur les principes de gestion des risques dans la banque électronique.¹⁰

aspects suivants: organes de direction; principales activités et lieu d'implantation; efforts de prévention et de détection du blanchiment; finalité du compte; identité de tous les utilisateurs des services du correspondant; état de la réglementation et du contrôle bancaires dans le pays. Une banque ne devrait établir de relations de correspondant qu'avec des établissements étrangers efficacement contrôlés par les autorités compétentes. De leur côté, ceux-ci devraient disposer de politiques CC efficaces, en particulier pour l'acceptation de nouveaux clients.

51. Les banques devraient notamment refuser d'établir ou de conserver des relations de correspondant avec un établissement soit enregistré dans une juridiction où il n'est pas présent physiquement, soit non apparenté à un groupe financier réglementé (cas des «coquilles vides» ou façades comptables). Elles devraient se montrer particulièrement vigilantes lorsqu'elles maintiennent des relations avec des établissements situés dans des juridictions ayant des normes CC insuffisantes ou ayant été classées «non coopératives» dans la lutte contre le blanchiment. Elles devraient s'assurer que les établissements à qui elles offrent des services de correspondant appliquent leur devoir de diligence conformément aux normes présentées dans ce document et renforcer leurs procédures pour les transactions transitant par les comptes de correspondant.

52. Les banques devraient être particulièrement attentives au risque d'utilisation directe par des tiers de ces comptes de correspondant (sur comptes de passage, par exemple). De tels dispositifs appellent, en général, les mêmes réserves que la clientèle recommandée et devraient être traités conformément aux critères exposés au paragraphe 36.

3. Surveillance continue des comptes et transactions

53. Une surveillance continue est essentielle à l'efficacité des procédures CC. Le contrôle et la réduction des risques ne peuvent être efficaces que si les banques ont une bonne compréhension des activités normales et raisonnables sur les comptes de leur clientèle, de façon à identifier les transactions atypiques. Sans cette connaissance, elles manqueront vraisemblablement à leur devoir de déclaration des transactions suspectes aux autorités appropriées. La nature de la surveillance doit être fonction du degré de risque. Les banques devraient disposer de systèmes permettant, pour tous les comptes, de déceler les activités à caractère inhabituel ou suspect, en recourant, par exemple, à des limites par classe ou catégorie de comptes; une attention particulière devrait être accordée aux dépassements. Certains types d'opérations devraient éveiller les soupçons; c'est notamment le cas de

celles qui ne semblent avoir aucune motivation économique ni commerciale ou qui portent sur des montants en liquide ne cadrant pas avec les transactions habituelles et concevables du client. Des mouvements de fonds démesurés par rapport au solde du compte peuvent être signe de blanchiment.

Les banques trouveront très utile un catalogue d'activités suspectes, qui devrait figurer dans les procédures et/ou recommandations antiblanchiment d'une juridiction prudentielle.

54. Les comptes à hauts risques devraient faire l'objet d'une surveillance accrue. Chaque banque devrait les identifier grâce à une gamme d'indicateurs comportant des informations générales sur le client (pays d'origine et source des fonds, par exemple), le type de transaction et d'autres facteurs de risque. Pour ces comptes:

- les banques devraient s'assurer que les systèmes d'information de la direction sont aptes à fournir rapidement aux dirigeants et aux responsables conformité les renseignements permettant l'identification, l'analyse et la surveillance efficace de ces comptes. Divers rapports peuvent s'avérer nécessaires à cet effet: absence de documentation sur l'ouverture d'un compte, transactions inhabituelles et présentation consolidée des relations d'un client avec la banque;
- les cadres dirigeants chargés des activités de banque privée devraient connaître les détails personnels des clients à hauts risques et être attentifs à toute source d'information émanant de tiers; leurs grosses transactions devraient recevoir l'approbation d'un membre de la direction;
- les banques devraient se doter d'une politique claire ainsi que de lignes directrices, procédures et contrôles internes; elles devraient être extrêmement vigilantes dans leurs relations d'affaires avec les PPE et les personnalités ainsi qu'avec les particuliers et sociétés¹¹ qui leur sont clairement liés ou associés¹⁶. Étant donné que toutes les PPE ne peuvent pas être identifiées d'emblée et que ce statut peut s'acquérir, il importe de réexaminer régulièrement au moins les principaux clients.

4. Gestion des risques

55. L'efficacité des procédures CC repose sur le caractère adéquat de plusieurs éléments: surveillance par la direction, systèmes et contrôles, séparation des tâches, politiques de formation et autres. Le conseil d'administration devrait faire montre d'un engagement sans réserve à travers des procédures CC appropriées et leur application efficace. Les responsabilités devraient être explicitement définies au sein de la banque pour garantir que les politiques et procédures soient bien conduites et répondent, au minimum, aux pratiques prudentielles locales. Les modalités de déclaration des transactions suspectes devraient être clairement précisées par écrit et diffusées à l'ensemble du personnel. Des procédures internes devraient permettre, en outre, de déterminer si, dans le cadre de la législation correspondante, la banque est tenue d'en informer les autorités judiciaires et/ou prudentielles.

56. Une responsabilité majeure des fonctions audit interne et contrôle conformité consiste à vérifier le respect des politiques et procédures CC. En règle générale, le contrôle conformité devrait fournir une évaluation indépendante des politiques et procédures, couvrant également les aspects légaux et réglementaires. Il devrait être chargé, notamment, de la surveillance permanente par sondage de la conformité des prestations des agents et de l'analyse des comptes rendus de manquements, afin d'alerter la direction générale, ou le conseil d'administration s'il estime que celle-ci n'exerce pas pleinement ses responsabilités en matière de procédures CC.

57. L'audit interne a pour importante mission d'évaluer de manière indépendante la gestion et le contrôle des risques; il rend compte au comité d'audit du conseil d'administration ou à un organe de surveillance semblable en lui présentant des rapports périodiques sur le respect de la conformité aux politiques et procédures CC, sans omettre la formation du personnel. La direction devrait s'assurer que cette fonction dispose d'un personnel adéquat maîtrisant ces

politiques et procédures. De plus, les auditeurs devraient faire preuve de diligence en veillant à ce que leurs conclusions et critiques soient suivies d'effet.

58. Chaque banque doit prévoir un programme permanent de formation préparant convenablement son personnel aux procédures CC. Le calendrier et le contenu des séances organisées pour les diverses unités devront être adaptés aux nécessités spécifiques de l'établissement. Les besoins de formation devraient être ajustés en fonction des participants: agents recrutés, employés en contact avec le public, responsables conformité, personnes chargées des nouveaux clients. Au moment de leur recrutement, les agents devraient être sensibilisés à l'importance des politiques CC et aux exigences fondamentales de la banque. Les employés en contact avec le public devraient apprendre à identifier les nouveaux clients, à faire preuve à tout moment de diligence dans le traitement des comptes clientèle et à déceler les activités suspectes.

Des stages devraient rappeler périodiquement au personnel ses responsabilités et le tenir informé des derniers développements. Il est essentiel que chacun comprenne la nécessité des procédures CC et qu'elles soient appliquées de manière uniforme. Leur mise en œuvre efficace passe par une telle approche.

59. Dans de nombreux pays, les auditeurs externes ont également un rôle majeur à jouer en surveillant les contrôles et procédures internes des banques et en confirmant leur conformité aux pratiques prudentielles.

16 Il n'est pas réaliste d'attendre d'une banque qu'elle connaisse ou cherche à connaître toutes les relations familiales (surtout éloignées), politiques ou commerciales d'un client étranger. L'obligation de s'informer à l'apparition de soupçons dépend du volume des actifs ou de l'importance des mouvements de fonds, du contexte économique, de la réputation du pays concerné, de la solidité des explications données par le client, etc. Il convient toutefois de noter que les PPE (ou plus exactement leurs famille et amis) ne se présenteront pas forcément sous ce jour, mais plutôt comme des hommes d'affaires ordinaires (quoique aisés), sans révéler qu'elles doivent uniquement leur position élevée dans une entreprise légitime à leur relation privilégiée avec un haut responsable public.

12

IV. Rôle des autorités de contrôle

60. Il revient aux autorités de contrôle nationales d'élaborer, sur la base des normes internationales CC existantes, une approche prudentielle régissant les programmes des banques dans ce domaine. Les éléments essentiels exposés dans le présent document devraient constituer des recommandations claires permettant aux autorités de contrôle de concevoir ou d'améliorer l'approche prudentielle nationale.

61. Il incombe aux autorités de contrôle non seulement de formuler les éléments fondamentaux à respecter par les établissements bancaires, mais aussi de veiller à ce qu'ils observent constamment de saines procédures CC et des critères éthiques et professionnels. Elles devraient s'assurer qu'ils disposent de contrôles internes adéquats et se conforment aux recommandations prudentielles et réglementaires. Leur processus de surveillance devrait comporter un examen des politiques et procédures mais aussi des fichiers clients ainsi qu'une vérification des comptes par sondage. Elles devraient toujours avoir le droit de consulter l'ensemble de la documentation concernant les comptes ouverts dans leur juridiction, de même que toute étude effectuée par les banques pour déceler les transactions inhabituelles ou douteuses.

62. Les autorités de contrôle sont tenues de s'assurer que les établissements appliquent des normes CC élevées non seulement pour préserver leur sécurité et leur solidité, mais aussi pour protéger l'intégrité du système bancaire national¹⁷. Elles devraient indiquer clairement que, en cas de non-respect avéré des procédures internes et exigences réglementaires, elles prendront des mesures appropriées, sévères et publiques si les circonstances le justifient, à

l'encontre des établissements et de leurs dirigeants. Elles devraient s'assurer, en outre, que les banques sont particulièrement attentives à toute transaction avec les juridictions où les normes ne sont pas considérées adéquates.

Le GAFI et certaines autorités nationales ont établi une liste de pays et juridictions dont le cadre juridique et administratif est jugé non conforme aux normes internationales de lutte contre le blanchiment. Les banques devraient tenir compte de cette information dans leurs politiques et procédures CC.

V. Mise en œuvre des normes CC dans un contexte transfrontière

63. Toutes les autorités de contrôle devraient s'efforcer, dans toute la mesure du possible, d'élaborer et d'appliquer des normes CC nationales pleinement conformes aux normes internationales, de façon à éliminer les éventuels arbitrages réglementaires et à préserver l'intégrité des systèmes bancaires nationaux et internationaux. La mise en œuvre et l'évaluation de telles normes traduisent très concrètement la volonté des autorités de contrôle de coopérer avec leurs homologues et la capacité des banques à gérer les risques à l'échelle du groupe. Il s'agit là d'un enjeu de taille pour les banques comme pour les autorités prudentielles.

64. Les autorités de contrôle attendent des groupes bancaires qu'ils appliquent, pour leurs opérations domestiques et à l'étranger, des politiques et procédures CC obéissant à une norme minimale agréée. Pour être efficace, la surveillance des opérations bancaires internationales doit s'effectuer sur une base consolidée, le risque d'atteinte à la réputation comme les autres risques bancaires ne se confinant pas au territoire national. Les banques mères doivent transmettre leurs politiques et procédures à leurs succursales et filiales à l'étranger, y compris aux unités non bancaires (sociétés fiduciaires, par exemple), et disposer d'un processus régulier de vérification de la conformité à l'égard des normes CC des pays d'origine et d'accueil, pour assurer l'efficacité de leur programme à l'échelle mondiale. Ce processus sera soumis, lui aussi, à l'examen des auditeurs externes et autorités de contrôle. Il importe donc que la documentation CC soit bien archivée et tenue à leur disposition. Dans le cadre des tests de conformité, les autorités prudentielles et les auditeurs externes devraient, dans la plupart des cas, examiner les systèmes et contrôles et analyser par sondage les comptes clients ainsi que le suivi des transactions.

17 De nombreuses autorités de contrôle sont également tenues de déclarer toute transaction suspecte, inhabituelle ou illégale qu'elles ont décelée, par exemple à l'occasion d'examens sur place.¹³

65. Même pour les plus petits établissements à l'étranger, un cadre supérieur devrait être chargé de s'assurer que tous les agents concernés sont formés à respecter des procédures CC conformes aux normes des pays d'origine et d'accueil et s'acquittent de cette tâche. Si cette responsabilité lui incombe directement, il devrait pouvoir s'appuyer, le cas échéant, sur les auditeurs internes et responsables conformité au niveau local et au siège.

66. En cas de différence entre les normes minimales CC des pays d'origine et d'accueil, les succursales et filiales à l'étranger devraient appliquer les plus exigeantes. D'une manière générale, aucun obstacle ne devrait s'opposer à ce qu'un établissement adopte des normes plus rigoureuses que le minimum local. Si, toutefois, le cadre juridique et réglementaire local (notamment en matière de secret bancaire) interdit l'application des normes plus élevées du pays d'origine, les autorités d'accueil devraient s'employer à le faire modifier. En attendant, les établissements locaux seraient tenus de respecter les normes du pays d'accueil, tout en indiquant clairement à leur siège/banque mère et à l'autorité de contrôle d'origine la nature de la différence de régime.

67. Comme les juridictions dressant de tels obstacles sont naturellement propices aux desseins criminels, les groupes bancaires devraient être conscients des gros risques d'atteinte à la réputation qu'elles présentent. Les banques mères devraient disposer d'une procédure pour

examiner la vulnérabilité des diverses unités opérationnelles et adopter, au besoin, des protections supplémentaires. Au pire, les autorités prudentielles devraient envisager des contrôles additionnels sur les banques opérant dans ces juridictions, voire encourager leur départ.

68. Au cours des inspections sur place, les autorités d'origine ou auditeurs devraient pouvoir vérifier en toute liberté la conformité d'un établissement aux politiques et procédures CC, en examinant les fichiers clientèle et en vérifiant les comptes par sondage. Les autorités d'origine devraient avoir accès à l'information obtenue par sondage sur les comptes, dans la mesure où elle leur est nécessaire pour évaluer correctement la mise en œuvre des normes CC et les méthodes de gestion des risques; cet accès ne devrait pas être restreint par la législation locale sur le secret bancaire. Rien ne devrait s'opposer à la déclaration, sur une base consolidée, des concentrations en matière de dépôts et d'emprunts ou à la notification des fonds gérés pour compte de tiers, lorsque l'autorité d'origine l'exige. En outre, celle-ci peut, pour surveiller la concentration de dépôts ou le risque de financement en cas de retrait des dépôts, instituer des critères d'importance relative et des seuils en termes de bilan exigeant la communication de tout dépassement. Des précautions sont cependant indispensables pour que les informations sur un compte particulier soient utilisées exclusivement à des fins prudentielles légitimes et convenablement protégées par leur bénéficiaire.

Une convention de coopération facilitant le partage bilatéral d'informations serait utile à cet égard¹⁸.

69. Dans certains cas, un conflit majeur peut opposer les politiques CC de la banque mère imposées par l'autorité d'origine et les dispositions permises dans l'un de ses établissements à l'étranger. Ainsi, la législation locale peut interdire les inspections sur place des responsables conformité/auditeurs internes de la banque mère ou des autorités d'origine, ou bien permettre à un client d'utiliser un faux nom ou de se dissimuler derrière des agents ou intermédiaires tenus au secret sur l'identité de leur client. Dans de tels cas, l'autorité d'origine devrait entrer en contact avec l'autorité d'accueil pour vérifier la réalité des obstacles juridiques et leur validité extraterritoriale. S'ils s'avèrent insurmontables et qu'aucune autre voie satisfaisante ne s'offre, l'autorité d'origine devrait préciser à son homologue que, à sa requête ou à l'initiative de la banque, l'établissement concerné pourrait être contraint de fermer. De toute façon, les dispositions régissant ces inspections sur place devraient prévoir une solution permettant à l'autorité d'origine d'effectuer une évaluation satisfaisante à son sens; il peut s'avérer utile de recourir à des conventions de coopération ou à des protocoles d'accord en définissant les modalités pratiques. Les autorités d'origine devraient disposer d'un accès à l'information aussi libre que possible et couvrant au minimum les politiques et procédures générales de la banque en matière de connaissance de la clientèle et de traitement des cas suspects.

¹⁸ Comité de Bâle sur le contrôle bancaire, *Essential elements of a statement of cooperation between banking supervisors* (mai 2001).¹⁴

Annexe 1:

Extraits de *Méthodologie des Principes fondamentaux*

Principe 15: Les autorités de contrôle bancaire doivent s'assurer que les banques disposent de politiques, pratiques et procédures appropriées, notamment de critères stricts de connaissance de la clientèle, assurant 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.

Critères essentiels

1. L'autorité de contrôle s'assure que les banques disposent de politiques, pratiques et procédures de nature à promouvoir un haut degré d'éthique et de professionnalisme et à empêcher qu'elles ne soient utilisées, intentionnellement ou non, dans le cadre d'activités

criminelles. Il s'agit notamment de prévenir et de repérer les actes délictueux ou frauduleux et d'informer les autorités compétentes des faits soupçonnés.

2. L'autorité de contrôle s'assure que les banques disposent de politiques explicitées et appliquées pour identifier les clients et leurs mandataires dans le cadre de la lutte contre le blanchiment d'argent. Des règles claires précisent quelles sont les données à conserver sur l'identification de la clientèle et les transactions individuelles et sur quelle durée.

3. L'autorité de contrôle s'assure que les banques disposent de procédures formelles pour identifier les transactions potentiellement suspectes. Il peut s'agir d'autorisations supplémentaires pour les dépôts ou retraits en espèces importants ou de procédures spéciales pour des opérations inhabituelles.

4. L'autorité de contrôle s'assure que les banques chargent explicitement un cadre supérieur de veiller à ce que leurs politiques et procédures soient au moins conformes aux exigences légales et réglementaires locales en matière de lutte contre le blanchiment d'argent.

5. L'autorité de contrôle s'assure que les banques disposent de procédures claires, communiquées à tout le personnel et permettant à chaque agent de signaler toute opération suspecte au responsable de la conformité en matière de lutte contre le blanchiment d'argent.

6. L'autorité de contrôle s'assure que les banques ont établi des circuits de communication avec la direction et avec une fonction de sécurité interne pour rendre compte des problèmes.

7. En plus d'informer les autorités judiciaires compétentes, les banques signalent à l'autorité de contrôle les activités litigieuses et tout cas important de fraude vis-à-vis de la sécurité, de la solidité ou de la réputation de la banque.

8. La législation, les dispositions réglementaires et/ou les politiques des banques garantissent que la responsabilité d'un membre du personnel ne peut être retenue lorsque celui-ci rapporte en toute bonne foi des activités suspectes au cadre supérieur chargé de ces questions, au responsable de la sécurité interne ou, directement, à l'autorité compétente.

9. L'autorité de contrôle vérifie périodiquement le caractère adéquat des contrôles exercés par les banques en matière de blanchiment d'argent ainsi que de leurs systèmes de prévention, de détection et de notification des fraudes. L'autorité de contrôle est habilitée à intenter une action (poursuite administrative et/ou pénale) contre une banque qui ne respecte pas ses obligations de lutte contre le blanchiment d'argent.

10. L'autorité de contrôle peut communiquer, directement ou indirectement, à ses homologues nationales ou étrangères toute information concernant des activités criminelles suspectées ou avérées.

11. L'autorité de contrôle s'assure que les banques ont défini dans un document leurs critères de déontologie et de professionnalisme et que cette déclaration a été explicitement portée à la connaissance de tout le personnel.¹⁵

Critères additionnels

1. Les saines pratiques internationales, telles que la conformité aux quarante recommandations formulées en 1990 (révisées en 1996) par le Groupe d'action financière sur le blanchiment d'argent, figurent dans la législation et/ou les dispositions réglementaires.

2. L'autorité de contrôle s'assure que le personnel bancaire est convenablement formé à détecter et à prévenir le blanchiment d'argent.

3. L'autorité de contrôle est légalement tenue d'informer les autorités judiciaires compétentes de toute transaction suspecte.

4. L'autorité de contrôle peut communiquer, directement ou indirectement, au pouvoir judiciaire compétent toute information concernant des activités criminelles suspectées ou avérées.

5. À moins qu'une autre instance n'en soit chargée, l'autorité de contrôle compte parmi ses effectifs des experts en matière d'obligations liées à la lutte contre la fraude financière et le blanchiment d'argent.

Annexe 2:**Extraits des recommandations du GAFI****C. Rôle du système financier dans la lutte contre le blanchiment de capitaux****Règles d'identification des clients et de conservation des documents**

10. Les institutions financières ne devraient pas tenir de comptes anonymes, ni de comptes sous des noms manifestement fictifs: elles devraient être tenues (par des lois, des règlements, des accords entre autorités de contrôle et institutions financières, ou par des accords d'autodiscipline entre institutions financières) d'identifier, sur la base d'un document officiel ou d'une autre pièce d'identité fiable, leurs clients habituels ou occasionnels, et d'enregistrer cette identité, lorsqu'elles nouent des relations d'affaires ou effectuent des transactions (en particulier lorsqu'elles ouvrent des comptes ou des livrets, lorsqu'elles réalisent des transactions fiduciaires, lorsqu'elles louent des coffres, lorsqu'elles procèdent à des transactions importantes en espèces).

Afin de satisfaire aux exigences d'identification concernant les personnes morales, les institutions financières devraient, si nécessaire, prendre des mesures telles que:

- i) vérifier l'existence et la structure juridiques du client en obtenant de celui-ci ou à partir d'un registre public, ou bien grâce à ces deux sources, une preuve de la constitution en société comprenant des renseignements concernant le nom du client, sa forme juridique, son adresse, les dirigeants et les dispositions régissant le pouvoir d'engager la personne morale;
- ii) vérifier que toute personne prétendant agir au nom du client est autorisée à le faire et identifier cette personne.

11. Les institutions financières devraient prendre des mesures raisonnables pour obtenir des informations sur l'identité véritable des personnes dans l'intérêt desquelles un compte est ouvert ou une transaction est effectuée, s'il y a le moindre doute sur le fait que ces clients pourraient ne pas agir pour leur propre compte, par exemple dans le cas de sociétés de domicile (c'est-à-dire des institutions, des sociétés, des fondations, des fiducies, etc., qui ne se livrent pas à des opérations commerciales ou industrielles, ou à toute autre forme d'activité commerciale, dans le pays où est situé leur siège social).

12. Les institutions financières devraient conserver pendant au moins cinq ans toutes les pièces nécessaires se rapportant aux transactions effectuées, à la fois nationales et internationales, afin de leur permettre de répondre rapidement aux demandes d'information des autorités compétentes. Ces pièces doivent permettre de reconstituer les transactions individuelles (y compris les montants et les types d'espèces en cause, le cas échéant) de façon à fournir, si nécessaire, des preuves en cas de poursuites pour conduite criminelle.

Les institutions financières devraient conserver une trace écrite de la justification d'identité de leurs clients (par exemple, copie ou enregistrement des documents officiels comme les passeports, les cartes d'identité, les permis de conduire, ou des documents similaires), les livres de comptes et la correspondance commerciale pendant cinq ans au moins après la clôture du compte.

Ces documents devraient être à la disposition des autorités nationales compétentes, dans le contexte de leurs poursuites et de leurs enquêtes pénales.

13. Les pays devraient apporter une attention particulière aux menaces de blanchiment de capitaux inhérentes aux technologies nouvelles ou en développement, qui risquent de favoriser l'anonymat, et prendre des mesures supplémentaires, si nécessaire, pour éviter l'utilisation de ces technologies dans les dispositifs de blanchiment de capitaux.¹⁷

Diligence accrue des institutions financières

14. Les institutions financières devraient apporter une attention particulière à toutes les opérations complexes, inhabituelles, importantes, et à tous les types inhabituels de transactions, lorsqu'elles n'ont pas de cause économique ou licite apparente. L'arrière-plan et

l'objet de telles opérations devraient être examinés, dans la mesure du possible; les résultats de cet examen devraient être établis par écrit, et être disponibles pour aider les autorités de contrôle, de détection et de répression, les commissaires aux comptes et les contrôleurs internes ou externes.

15. Si les institutions financières suspectent que des fonds proviennent d'une activité criminelle, elles devraient être obligées de déclarer rapidement leurs soupçons aux autorités compétentes.

16. Les institutions financières, leurs dirigeants et employés devraient être protégés par des dispositions législatives contre toute responsabilité, pénale ou civile, pour violation des règles de confidentialité - qu'elles soient imposées par contrat ou par toute disposition législative, réglementaire ou administrative - si elles déclarent de bonne foi leurs soupçons aux autorités compétentes, même si elles ne savaient pas précisément quelle était l'activité criminelle en question, et même si l'activité illégale soupçonnée n'est pas réellement intervenue.

17. Les institutions financières, leurs dirigeants et employés ne devraient pas avertir leurs clients, ou, le cas échéant, ne devraient pas être autorisés à les avertir, lorsqu'ils portent à la connaissance des autorités compétentes des informations qui sont relatives à ces clients.

18. Les institutions financières déclarant leurs soupçons devraient se conformer aux instructions en provenance des autorités compétentes.

19. Les institutions financières devraient mettre au point des programmes de lutte contre le blanchiment de capitaux, qui devraient comprendre au minimum:

- i) des politiques, des procédures et des contrôles internes, y compris la désignation de personnes responsables au niveau de la direction générale, et des procédures adéquates lors de l'embauche des employés, de façon à s'assurer qu'elle s'effectue selon des critères exigeants;
- ii) un programme continu de formation des employés;
- iii) un dispositif de contrôle interne pour vérifier l'efficacité du système.